RISE
Research Industrial Systems Engineering

RISE Konnektor

Bedienungsanleitung

Research Industrial Systems Engineering (RISE)
Stand: 26.07.2021
Version: 1.5.5

Diese Bedienungsanleitung gilt für den RISE Konnektor 3.5.9

Inhaltsverzeichnis

1 Einleitung

1.1 Allgemeines

Diese Bedienungsanleitung beschreibt den RISE Konnektor und enthält wichtige Informationen zur sicheren Produktübernahme, Inbetriebnahme, operativen Betrieb und Außerbetriebnahme. Lesen Sie die Bedienungsanleitung sorgfältig, bevor Sie den RISE Konnektor in den produktiven Einsatz bringen.

Diese Bedienungsanleitung wird den Service-Partnern (Händler[1] beziehungsweise Infrastrukturdienstleister bezeichnet) über einen abgesicherten Weg in der jeweils aktuellsten Version zur Verfügung gestellt. Die Service-Partner sind verpflichtet, diese den Leistungserbringerinstituten auf Anforderung bereit zu stellen.

Die RISE Konnektor Bedienungsanleitung richtet sich an das Leistungserbringerinstitut generell und im Speziellen an die Administratoren des RISE Konnektors, um den hohen Sicherheitsansprüchen zu genügen. Dies gilt für sämtliche Sicherheitshinweise in diesem Dokument. Im Besonderen sind unsichere Zustände durch Fehlkonfiguration des RISE Konnektors zu vermeiden.

Bei den in diesem Dokument eingebetteten Bildern handelt es sich um Symbolbilder. Diese dienen zur Verständlichkeit. Die Darstellungen können sich, abhängig vom verwendeten Browser und der Firmware-Version, unterscheiden. Alle Screenshots zeigen die Sicht eines Benutzers der Rolle “Super-Administrator”.

Der RISE Konnektor ist ausschließlich für den Gebrauch im Innenbereich bestimmt. Verwenden Sie den RISE Konnektor nur wie in dieser Bedienungsanleitung beschrieben. Jede andere Verwendung gilt als nicht bestimmungsgemäß und kann zu Schäden führen. Der Hersteller oder Händler übernimmt keine Haftung für Schäden, welche durch nicht bestimmungsgemäßen oder falschen Gebrauch entstanden sind.

Sicherheitshinweis: Bei der aktuell vorliegenden Konnektor-Version handelt es sich um ein sicheres und zugelassenes Produkt der gematik, jedoch ist dieser Firmware-Stand ein Minor-Release und erhält aufgrund dessen kein explizites Zertifikat nach Common Criteria. Daher ist der folgende Abschnitt auf diesen Softwarestand nicht anwendbar. Alle Inhalte dieses Handbuchs gelten jedoch vollumfänglich auch für die vorliegende Software-Version. Der Konnektor kann und muss ungeachtet der Software-Version so betrieben und verwaltet werden, als würde ein Zertifikat nach Common Critera vorliegen.

[1] Auch als Zwischenhändler bezeichnet

1.2 Herunterladen des Zertifizierungsreports

- Öffnen Sie die Seite mit den vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierten Produkten: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/Zertifizierte-Produkte-nach-CC/zertifizierte-produkte-nach-cc_node.html (letzter Zugriff 26.07.2021)
- Klicken Sie auf die Zertifizierungsnummer des Produkts "RISE Konnektor V4.0". Alternativ können Sie auch im Suchfeld "rise konnektor V4.0" eingeben.
- Klicken Sie auf "Zertifizierungsreport / Certification Report" und laden Sie diesen herunter.

1.3 Prüfen der Authentizität und Integrität des Dokuments

Bevor Sie den Anweisungen der vorliegenden Bedienungsanleitung folgen, überprüfen Sie bitte die Authentizität und Integrität des Dokuments. Gehen Sie dabei wie folgt vor:

- Laden Sie zunächst den Zertifizierungsreports für den RISE Konnektor herunter (siehe Abschnitt 1.2).
- Im Zertifizierungsreport finden Sie die Prüfsumme (SHA-256) der Bedienungsanleitung.
- Berechnen Sie nun für sich selbst die Prüfsumme (SHA-256) der vorliegenden Bedienungsanleitung.
- Vergleichen Sie die Prüfsummen. Stimmen die Werte überein, haben Sie die Authentizität Ihrer Bedienungsanleitung erfolgreich verifiziert.

1.4 Sicherstellung der Nutzung einer zugelassenen Version

Bevor Sie den Konnektor initial oder nach einem Firmware-Update nutzen, überprüfen Sie bitte die Authentizität und Integrität der Firmware-Version. Gehen Sie dabei wie folgt vor:

- Laden Sie zunächst den Zertifizierungsreports für den RISE Konnektor herunter (siehe Abschnitt 1.2).
- Im Zertifizierungsreport finden Sie in Tabelle 2 - "Auslieferungsumfang des EVG" die zugelassene Firmware-Version.

Zum Vergleich können Sie die aktuell installierte Firmware-Version Ihres Konnektors folgendermaßen über einen Browser auslesen:

- Greifen Sie über die Addresse http://<IP-Adresse des RISE Konnektors>/connector.sds[2] auf den Dienstverzeichnisdienst Ihres Konnektors zu.
- Diese Anfrage liefert eine XML-Datei zurück. Ein Beispiel dafür ist in Abbildung 1 gegeben, wobei die Firmware-Version farblich hervorgehoben ist.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:ConnectorServices xmlns="http://ws.gematik.de/int/version/ProductInformation/v1.1" xmlns:ns2="http://ws.
    <ProductInformation>
        <InformationDate>2020-02-03T15:55:11.238+02:00</InformationDate>
        <ProductTypeInformation>
            <ProductType>Konnektor</ProductType>
            <ProductTypeVersion>3.6.0</ProductTypeVersion>
        </ProductTypeInformation>
        <ProductIdentification>
            <ProductVendorID>RISEG</ProductVendorID>
            <ProductCode>RKONN</ProductCode>
            <ProductVersion>
                <Local>
                    <HWVersion>1.0.0</HWVersion>
                    <FWVersion>3.5.9</FWVersion>
                </Local>
            </ProductVersion>
        </ProductIdentification>
        <ProductMiscellaneous>
                <ProductVendorName>Research Industrial Systems Engineering (RISE) GmbH</ProductVendorName>
                <ProductName>RISE Konnektor</ProductName>
        </ProductMiscellaneous>
    </ProductInformation>
```

Abbildung 1: Beispiel für die XML-Datei, welche nach Aufruf des Dienstverzeichnisdienstes zurückgeliefert wird

Nur wenn die Firmware-Version Ihres Konnektors mit der des Zertifizierungsreports übereinstimmt, ist die Nutzung einer zugelassenen Version des RISE Konnektors erfolgreich verifiziert.

[2] Nur möglich, wenn ANCL_DVD_OPEN=Enabled. Wenn ANCL_DVD_OPEN=Disabled, dann ist der Zugriff nur für die entsprechend der Konfiguration aus Abschnitt 6.3.1 authentisierten Clientsystemen mittels http (bei ANCL_TLS_MANDATORY=Disabled) bzw. https (bei ANCL_TLS_MANDATORY=Enabled) möglich.

1.5 Frontseite des RISE Konnektors

Abbildung 2: RISE Konnektor Frontseite

Die Frontseite des RISE Konnektors ist mit 4 LEDs ausgestattet. Über diese Anzeige-LEDs werden die unterschiedlichen Betriebszustände (siehe Tabelle 1) angezeigt:

Anzeige-LED	Zustand	Bedeutung
TI	Grün	VPN-Verbindung in die Telematikinfrastruktur (TI) ist erfolgreich aufgebaut.
SIS	Grün	VPN-Verbindung zum Sicheren-Internet-Service (SIS) ist erfolgreich aufgebaut.
Error	Rot	Genereller Fehlerzustand des RISE Konnektors. Detailbeschreibungen sind über das Management-Interface verfügbar.
Error	Orange	Der RISE Konnektor fährt hoch. Während dieser Zeit ist die Management-Oberfläche nicht erreichbar.
Power	Grün	Der RISE Konnektor ist mit Strom versorgt.

Tabelle 1: Anzeige-LEDs und Betriebszustände des RISE Konnektors

Abbildung 3 zeigt die Rückseite und die Abmessungen des RISE Konnektors.

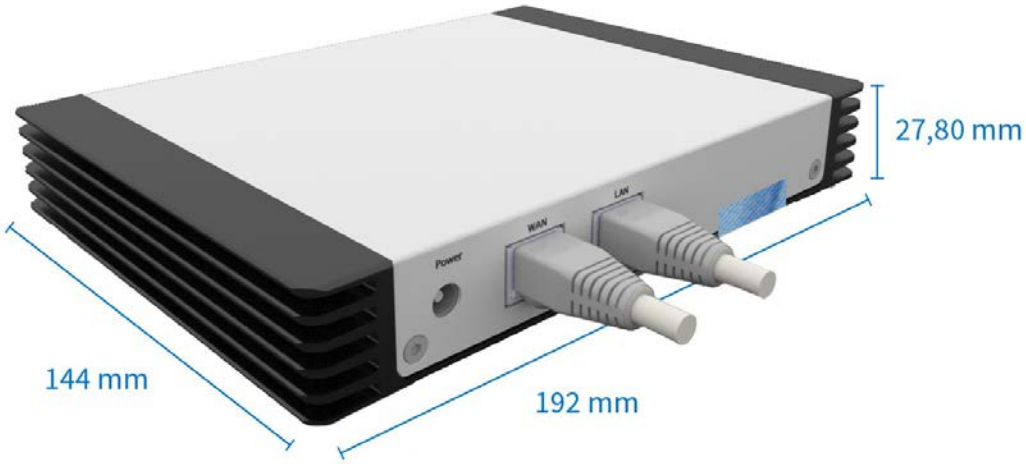


Abbildung 3: RISE Konnektor Rückseite und Abmessungen

Interface	Bedeutung
Power	Netzstecker für die Stromversorgung
WAN	Anschluss des Netzwerkkabels (RJ-45) für die Anbindung an das Internet (IAG)
LAN	Anschluss des Netzwerkkabels (RJ-45) für das lokale Netzwerk

Tabelle 2: Rückseitige Anschlüsse des RISE Konnektors

1.6 Technische Daten des RISE Konnektors

Interface	Bedeutung
CPU (x86)	Intel Braswell N3160, Taktfrequenz: 1,6 GHz (Burst: 2,24 GHz)
RAM	Standard Arbeitsspeicher: 8 GB
Netzwerk	Zwei getrennte Netzwerkcontroller für für LAN und WAN, je 1000Base-T, IEEE802.3 Clause 40
Kühlung	Passives Kühlkonzept
Betrieb	Wärmehaushalt des Systems (vollständig geschlossenes Gehäuse) und Stromversorgung für 24x7-Dauerbetrieb ausgelegt
Netzteil	Externes Netzteil mit 36W Nennleistung
Energieverbrauch	Es ist mit 10W Energieaufnahme zu rechnen
Sicherheit	Gehäusesiegel zur optischen Kontrolle zum Öffnungsschutz
Umgebungsbedingungen Betrieb	0° bis +50°C
Umgebungsbedingungen Lagerung	+20° bis +60°C
Herstellungsland, Fertiger	Bundesrepublik Deutschland
Umweltrichtlinien	Europäische Union RoHS, WEEE

Tabelle 3: Technische Daten des RISE Konnektors

2 Kontaktdaten des RISE Konnektor Herstellers

Wenden Sie sich bei Fragen zum RISE Konnektor, welche nicht von Ihrem Händler beziehungsweise Infrastrukturdienstleister beantwortet werden können, per E-Mail bzw. telefonisch an den Hersteller.

Es wird empfohlen in erster Instanz immer Unterstützung von Ihrem direkten Vertragshändler und Infrastrukturdienstleister einzuholen. Falls auf diesem Weg keine zufriedenstellende Lösung gefunden werden kann, ist es möglich Kontakt zum RISE Konnektor Hersteller aufzunehmen. Auf der RISE Konnektor-Webseite befinden sich sämtliche Kontaktdetails des Herstellers. Die RISE Konnektor-Seriennummer und der Händlername sind bei zielgerichteten Fragen zum Produkt anzugeben.

Des Weiteren finden Sie auf der Website auch eine Liste, sowie den direkten Download-Link zu allen verifizierten Web-Browser-Versionen, mit denen die RISE Konnektor Management-Oberfläche getestet wurde.

https://www.rise-konnektor.de/

Research Industrial Systems Engineering (RISE)
Forschungs-, Entwicklungs- und Großprojektberatung GmbH
Concorde Business Park
2320 Schwechat
Österreich

3 Sichere Produktübernahme

Die sichere Produktübernahme beim Leistungserbringer ist zentraler Bestandteil der Inbetriebnahme des Konnektors und muss jedenfalls bei Erhalt des Konnektors durchgeführt werden.

Diese sichere Übernahme hat den Anspruch, jegliche unerkannte Veränderung oder das Austauschen des Produktes während der Zustellung auszuschließen. Um mögliche Manipulationen feststellen zu können und somit die Echtheit eines RISE Konnektors für einen Endkunden überprüfbar zu machen, werden innerhalb der folgenden Abschnitte eine Reihe an Überprüfungsmaßnahmen vorgestellt, welche nach Erhalt des RISE Konnektors durch das Leistungserbringerinstitut durchzuführen sind.

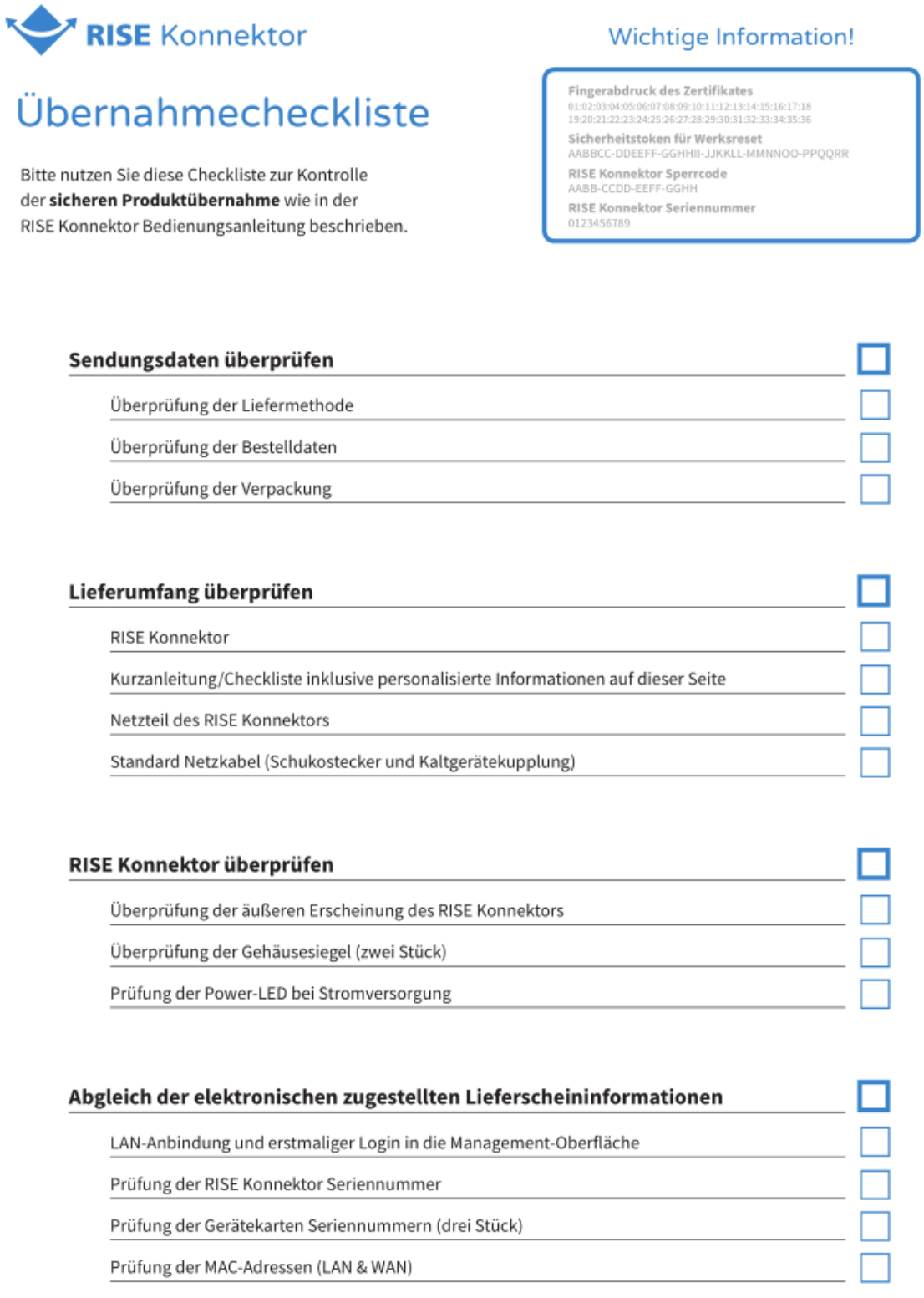
Um den Überprüfungsvorgang zu vereinfachen, werden die Maßnahmen zur Überprüfung der Zusendung chronologisch ab Erhalt des Paketes angeführt und erläutert.

Unterstützend beschreibt die Übernahmecheckliste (siehe Abschnitt 3.1) alle durchzuführenden Schritte ab Erhalt des Paketes und dient dem Leistungserbringer als Hilfestellung bei der Sicherstellung der sicheren Produktübernahme des RISE Konnektors. Thematisch gliedert sich die sichere Übernahme in Übernahmebestimmungen des Produktes und Maßnahmen vor Inbetriebnahme des RISE Konnektors.

Wenn eine oder mehrere Maßnahmen Diskrepanzen aufzeigen, sollten jedenfalls der Händler und in zweiter Instanz der Hersteller kontaktiert werden (siehe Abschnitt 2).

Sicherheitshinweis: Erst sobald sämtliche Checkboxen der Liste durch den Leistungserbringer angekreuzt werden können, gilt der RISE Konnektor als sicher übernommen.

3.1 RISE Konnektor Übernahmecheckliste



RISE Konnektor

Übernahmecheckliste

Bitte nutzen Sie diese Checkliste zur Kontrolle der **sicheren Produktübernahme** wie in der RISE Konnektor Bedienungsanleitung beschrieben.

Wichtige Information!

Fingerabdruck des Zertifikates
01:02:03:04:05:06:07:08:09:10:11:12:13:14:15:16:17:18
19:20:21:22:23:24:25:26:27:28:29:30:31:32:33:34:35:36

Sicherheitstoken für Werksreset
AABBCC-DDEEFF-GGHHII-JJKKLL-MMNNOO-PPQQRR

RISE Konnektor Sperrcode
AABB-CCDD-EEFF-GGHH

RISE Konnektor Seriennummer
0123456789

Sendungsdaten überprüfen

- Überprüfung der Liefermethode
- Überprüfung der Bestelldaten
- Überprüfung der Verpackung

Lieferumfang überprüfen

- RISE Konnektor
- Kurzanleitung/Checkliste inklusive personalisierte Informationen auf dieser Seite
- Netzteil des RISE Konnektors
- Standard Netzkabel (Schukostecker und Kaltgerätekupplung)

RISE Konnektor überprüfen

- Überprüfung der äußeren Erscheinung des RISE Konnektors
- Überprüfung der Gehäusesiegel (zwei Stück)
- Prüfung der Power-LED bei Stromversorgung

Abgleich der elektronischen zugestellten Lieferscheininformationen

- LAN-Anbindung und erstmaliger Login in die Management-Oberfläche
- Prüfung der RISE Konnektor Seriennummer
- Prüfung der Gerätekarten Seriennummern (drei Stück)
- Prüfung der MAC-Adressen (LAN & WAN)

Abbildung 4: RISE Konnektor Übernahmecheckliste

3.2 Übernahmebestimmungen

Die Überschriften in diesem Kapitel beziehen sich auf die einzelnen Schritte der Übernahmecheckliste des RISE Konnektors.

3.2.1 Schritt 1: Überprüfung der Liefermethode

Bei Übernahme des RISE Konnektors ist neben Maßnahmen zur Identifikation und Sicherung der Integrität besonders auf die fachgerechte Liefermethode des Produktes zu achten.

Folgende Liefermethoden zum Leistungserbringer sind zulässig:

- Zustellung des RISE Konnektors geschützt durch eine sichere Versandtasche des Zustellers.
- Eigentransport direkt durch den RISE Konnektor-Händler. Die Übernahmebestimmungen müssen vom Leistungserbringer auch in diesem Fall eigenverantwortlich durchgeführt werden.

Hinweis: Eine Liste der legitimen Zusteller für den RISE Konnektor finden Sie auf der Webseite des Herstellers (siehe Abschnitt 2).

Ein RISE Konnektor darf daher nur von einem Händler bezogen werden, welcher auch auf der Internetseite des Herstellers (siehe Abschnitt 2) gelistet ist. Dort befinden sich Informationen zu allen an der sicheren Lieferkette beteiligten Organisationen und ihrer Rolle im Rahmen der sicheren Lieferkette des RISE Konnektors.

Zusätzlich zur physischen Paketlieferung des Konnektors wird bei Bestellung eine elektronische Datenübertragung auf eine verpflichtend anzugebende E-Mail-Adresse des Leistungserbringers durchgeführt. Die übertragenen Daten umfassen die Sendungsnummer und weitere Details, welche für die folgenden Überprüfungsschritte relevant sind. Die Überprüfung der korrekten Lieferung muss wie folgt durchgeführt werden:

- Überprüfen Sie die Lieferpapiere. Der Firmenname muss mit jenem aus der Bestellung des RISE Konnektors übereinstimmen.
- Lassen Sie sich den Ausweis des Lieferanten zeigen. Dabei müssen die Daten des Firmenausweises des Transporteurs mit denen, die vor Lieferung an Sie signiert übermittelt wurden, übereinstimmen.

3.2.2 Schritt 2: Überprüfung der Bestelldaten

Bei Zustellung des Paketes muss im ersten Schritt die an der Verpackung erkenntliche Sendungsnummer des Paketes mit den elektronisch zugestellten Lieferdaten verglichen werden. Lediglich bei Übereinstimmung darf mit dem hier definierten Maßnahmenkatalog fortgefahren werden.

Sicherheitshinweis: Sollte die Sendungsnummer des Paketes nicht mit den elektronisch zugestellten Lieferdaten übereinstimmen, muss der Händlersupport kontaktiert werden. Der RISE Konnektor darf in diesem Fall nicht ohne Abklärung des Sachverhalts mit dem Händlersupport in Betrieb genommen werden.

3.2.3 Schritt 3: Überprüfung der Verpackung

Je nach Methode kann die äußere Erscheinungsform des Zustellpaketes variieren, allerdings muss sich innerhalb der händlerspezifischen Verpackung die Originalverpackung befinden, wie in Abbildung 7 dargestellt. Es handelt es sich um einen Faltkarton, welcher durch eine Verpackungsversiegelung mit Öffnungsschutz vor unerkennbarer Öffnung geschützt ist. In Abbildung 5 ist ein unversehrtes Verpackungssiegel abgebildet, so wie es auch auf dem Faltkarton zwei Mal vorhanden sein muss (siehe Abbildung 7).

Abbildung 5: RISE Konnektor – unversehrte Verpackungsversiegelung

Abbildung 6: RISE Konnektor – manipulierte Verpackungsversiegelung

Zwischenhändler dürfen keine Änderungen am Produkt oder der Herstellerverpackung des Produktes vornehmen. Somit muss sich der Konnektor bei Lieferung in der originalen Hersteller-Einzelverpackung befinden. Andernfalls ist davon auszugehen, dass die sichere Lieferkette unterbrochen wurde. Sollte dies der Fall sein, oder andere Manipulationen der Herstellerverpackung oder des Verpackungssiegels vorliegen (siehe Abbildung 6), muss unverzüglich der Händlersupport kontaktiert werden. Des Weiteren darf der RISE Konnektor nicht

ohne Aufklärung durch den Händler hinsichtlich möglicher Manipulationen in den Produktivbetrieb übernommen werden.

Sicherheitshinweis: Sollten die beiden Seriennummern der Verpackungsversiegelung nicht mit den elektronisch zugestellten Lieferdaten übereinstimmen, muss der Händlersupport kontaktiert werden.

Abbildung 7: RISE Konnektor Herstellerverpackung

3.2.4 Schritt 4: Überprüfung des Lieferumfangs

Nach erfolgter Überprüfung der Herstellerverpackung ist diese, mit der dafür vorgesehenen Öffnungslasche, aufzureißen und der Inhalt des Paketes zu prüfen.

Die Herstellerverpackung beinhaltet folgenden Lieferumfang:

- RISE Konnektor als Tischgerät
- Kurzanleitung/Checkliste zum RISE Konnektor inkl. aufgeklebtem, personalisiertem Label bestehend aus:
  - Fingerprint des Sicherheitszertifikates für den Zugriff auf die Management-Oberfläche
  - Sicherheitstoken für die Durchführung eines Werksresets
  - RISE Konnektor Sperrcode
  - RISE Konnektor Seriennummer
- Kabelnetzteil
- Standard Netzkabel (Schukostecker und Kaltgerätekupplung)

3.2.5 Schritt 5: Überprüfung der äußeren Erscheinung des Konnektors

Nach Prüfung des Lieferumfangs ist das äußere Erscheinungsbild des Konnektors auf Schäden, Manipulationen und andere offensichtliche Mängel zu untersuchen.

Hierzu illustrieren Abbildung 8 und Abbildung 9 das Aussehen eines intakten RISE Konnektors, frei von jeglichen Manipulationen.

Abbildung 8: RISE Konnektor Frontansicht mit Siegel

Abbildung 9: RISE Konnektor Rückansicht mit Siegel

Hinweis: Die seitlich angebrachten Kühlkörper sorgen für die Kühlung des RISE Konnektors und dürfen weder verbaut noch abgedeckt werden. Wenn die seitlich angebrachten Kühlkörper abgedeckt sind, kann es zur Überhitzung und zu Funktionsstörungen des RISE Konnektors kommen. RISE Konnektoren dürfen nicht übereinander aufgestellt werden. Jeder RISE Konnektor muss auf einem gut belüfteten Platz stehen.

Sollte sich der gelieferte RISE Konnektor offensichtlich vom illustrierten Konnektor unterscheiden oder sonstige Mängel an der Konnektor-Verpackung erkennbar sein, ist der Händlersupport zu kontaktieren.

3.2.6 Schritt 6: Überprüfung der Gehäusesiegel

Um eine Manipulation des RISE Konnektors erkennbar zu machen, umfasst das Gehäuse zwei getrennte Gehäusesiegel, welche sowohl an der Front-, als auch an der Rückseite des RISE Konnektors platziert sind. Durch diesen Aufbau kann der RISE Konnektor nicht geöffnet werden, ohne mindestens eines der Gehäusesiegel zu beschädigen.

Abbildung 8 und Abbildung 9 zeigen die Lage dieser Siegel auf dem Gehäuse des RISE Konnektors. In Abbildung 5 ist die Detailansicht eines intakten Gehäusesiegels zu sehen.

Sollte eines dieser Gehäusesiegel offensichtlich beschädigt bzw. geöffnet (siehe Abbildung 6) oder gar durchtrennt sein, ist eine Inbetriebnahme des Konnektors keinesfalls erlaubt und es muss der Händlersupport kontaktiert werden. Lediglich bei Unversehrtheit der Gehäusesiegel darf mit dem nächsten Schritt fortgefahren werden.

Hinweis: Auch nach Inbetriebnahme des Konnektors dürften die Gehäusesiegel nicht beschädigt, manipuliert oder entfernt werden. Im Falle einer Beschädigung oder eines Aufbrechens eines oder beider Gehäusesiegel gehen die Gewährleistungsansprüche und gegebenenfalls auch die Garantieansprüche verloren; dies gilt ebenso für eine Manipulation der Gehäusesiegel.

3.3 Maßnahmen vor Inbetriebnahme des RISE Konnektors

Vor Inbetriebnahme des RISE Konnektors muss eine sichere Betriebsumgebung im Leistungserbringerinstitut sichergestellt sein. Die funktionalen und sicherheitstechnischen Mindestanforderungen sind in Abschnitt 4.4 beschrieben.

Hinweis: Die Anforderungen für eine sichere Betriebsumgebung müssen bei Inbetriebnahme erfüllt sein.

Hinweis: Verwenden Sie den RISE Konnektor ausschließlich mit dem mitgelieferten Netzteil.

Warnung: Trennen Sie während des gesamten Boot-Vorganges auf keinen Fall das Gerät von der Stromversorgung! Es kann dadurch zu irreparablen Schäden kommen.

Sicherheitshinweis: Der RISE Konnektor ist für einen 24-Stunden-Dauerbetrieb ausgelegt. Es wird empfohlen, dass der RISE Konnektor nur in Ausnahmefällen ausgeschaltet wird.

3.3.1 Schritt 7: LAN-Anbindung und erstmaliger Login auf der Management-Oberfläche

Hinweis: Falls Sie in Ihrem lokalen Netzwerk eine Firewall einsetzen, ist die Firewall entsprechend Abschnitt 4.4.2 zu konfigurieren.

3.3.1.1 Schritt 7a: LAN-Anbindung

Nach der physischen Überprüfung des gelieferten RISE Konnektors muss dieser innerhalb der zukünftigen Betriebsumgebung mithilfe des Netzkabels an das Stromnetz, sowie mittels eines handelsüblichen LAN-Netzwerkkabels an das lokale Netzwerk des Leistungserbringers angeschlossen werden (siehe Abschnitt 4.4.3). Bitte beachten Sie, dass für die Durchführung des Bootprozesses am LAN-Anschluß eine aktive Netzwerkverbindung erforderlich ist (siehe Abschnitt 4.7.3).

Hinweis: Stellen Sie sicher, dass in Ihrem LAN ein DHCP-Server zur Verfügung steht. Andernfalls erhält der RISE Konnektor eine IP-Adresse aus dem Bereich 169.254/16 und ist möglicherweise von Ihrem Rechner aus nicht erreichbar.

Hierfür sind die in Abbildung 10 illustrierten Steckplätze für die LAN-Anbindung, sowie die Stromversorgung zu verwenden.

Hinweis: Das (optionale) Anschließen der WAN-Anbindung ist in Abschnitt 3.3.4.6 beschrieben.

Hinweis: Sollte der RISE Konnektor nach Anschluss an die Stromversorgung keine Betriebszeichen zeigen, insbesondere kein Leuchten der "Power"-LED an der Vorderseite (siehe Abbildung 8), ist der Händlersupport zu kontaktieren.

Hinweis: Der komplette Startvorgang nach Anschluss an die Stromversorgung dauert ca. 6 Minuten. Nach ca. 2 Minuten, beginnt die "Error"-LED orange zu leuchten. Solange die "Error"-LED orange leuchtet, ist die Management-Oberfläche des RISE Konnektors nicht erreichbar.

Hinweis: Wird der RISE Konnektor zum ersten Mal in Betrieb genommen, fällt dieser in den so genannten "kritischen Betriebszustand" (siehe Abschnitt 4.7.1), weil erforderliche Installationsschritte ausständig sind. Nach erfolgreicher Fertigstellung der verbleibenden Installationsschritte ist der "kritische Betriebszustand" aufgehoben.

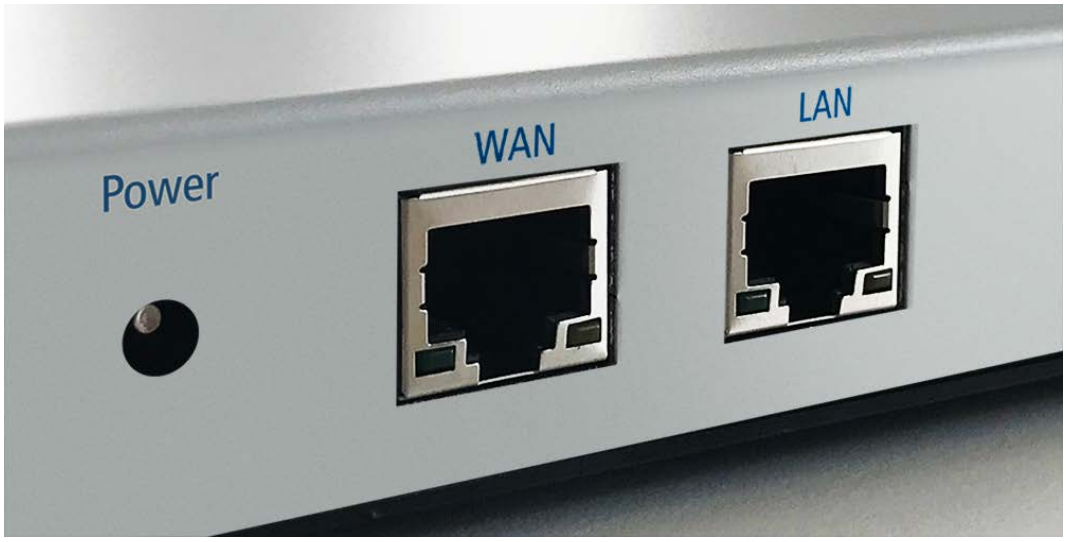


Abbildung 10: RISE Konnektor LAN- und WAN-Anbindung

3.3.1.2 Schritt 7b: Setzen der Logindaten bei erstmaligem Login auf der Management-Oberfläche

Nun müssen für den erstmaligen Login in die Management-Oberfläche des RISE Konnektors folgende Punkte durchgeführt werden:

- Ermitteln Sie die IP-Adresse <IP-Adresse> des RISE Konnektors in Ihrem lokalen Netzwerk

Hinweis: Informationen zum Ermitteln der von Ihrem DHCP-Server vergebenen IP-Adresse finden Sie z.B. im Handbuch Ihres Routers.

- Durch einen Web-Browser kann die Management-Oberfläche erstmalig aufgerufen werden. Geben Sie dazu in der Adressleiste folgenden Link ein:

https://<IP-Adresse>:8443

- Ihr Browser wird Sie möglicherweise darauf aufmerksam machen, dass die Verbindung nicht vertrauenswürdig ist. Fügen Sie daher eine entsprechende Ausnahme zu Ihrem Browser hinzu. Beachten Sie dazu auch die Informationen im Abschnitt 4.2.

Sicherheitshinweis: Aus Sicherheitsgründen muss nach dem Hinzufügen einer Ausnahme, der unsicheren Verbindung zu vertrauen, der SHA-256-Fingerabdruck des Zertifikates des RISE Konnektors mit dem gedruckten Fingerabdruck (siehe Label auf der RISE Konnektor Kurzanleitung) verglichen werden. Stimmen diese nicht überein, muss der Händlersupport kontaktiert werden (siehe Abschnitt 2).

- Als nächsten Schritt werden Sie unmittelbar nach dem Aufruf der RISE Konnektor Management-Oberfläche zur Wahl eines Benutzernamens und eines Passworts für einen Benutzer der Benutzerrolle “Super-Administrator” aufgefordert.
- Nach Einrichtung dieses Accounts kann auf sämtliche Konfigurationsmöglichkeiten des RISE Konnektors zugegriffen werden.

Sicherheitshinweis: Vor dem Setzen von Passwörtern sind die Sicherheitsrichtlinien in Abschnitt 4.1 zu berücksichtigen.

Sicherheitshinweis: Erfolgt beim erstmaligen Login keine Aufforderung, einen initialen Benutzernamen und Passwort zu setzen, befindet sich der RISE Konnektor nicht im Auslieferungszustand! Dies könnte darauf hinweisen, dass dieses Gerät bereits im Einsatz war. Bitte wenden Sie sich in diesem Fall an den Händlersupport (siehe Abschnitt 2).

Sicherheitshinweis: Vor jedem Login in die Management-Oberfläche des RISE Konnektors ist die Anzeige einer TLS-Verbindung (Sichere Verbindung) zu prüfen (siehe Abschnitt 4.2). Sollte dies nicht der Fall sein, prüfen Sie, ob sie einen unterstützten Browser verwenden und wenden Sie sich in weiterer Folge an den Händlersupport (siehe Abschnitt 2).

Sicherheitshinweis: Es wird aus Sicherheitsgründen empfohlen, Passwörter nicht vom Browser speichern zu lassen.

Sicherheitshinweis: Es wird empfohlen, Browser zu verwenden, die die Extended Master Secret Extension unterstützen oder sich durch andere Mechanismen vor Triple Handshake Angriffen schützen. Beispielsweise wie bei Safari, indem eine Renegotiation standardmäßig dasselbe Zertifikat bereitstellen muss wie in der Originalverbindung.

Hinweis: Die Management-Oberfläche des RISE Konnektors wurde mit den gängigsten Web-Browsern getestet. Auf der Internet-Seite des Herstellers (siehe Abschnitt 2) finden Sie eine Liste sowie Download-Links zu den verifizierten Browser-Versionen und die Möglichkeit, bei Interoperabilitätsproblemen, Support zu erhalten.

Hinweis: Die Management-Oberfläche des RISE Konnektors verwendet Cookies. Achten Sie deshalb darauf, dass Ihr Browser so konfiguriert ist, dass er Cookies akzeptiert.

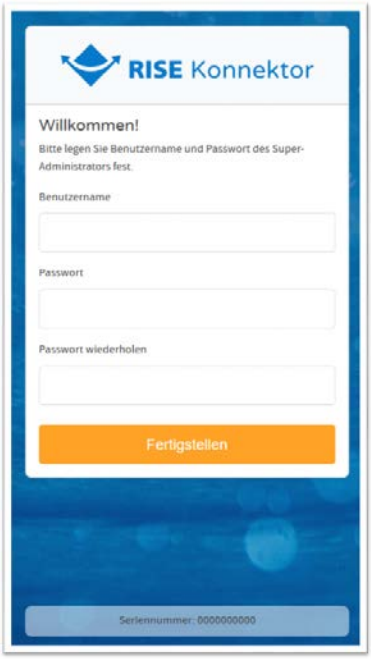


Abbildung 11: Startbildschirm der Management-Oberfläche

3.3.2 Schritt 8: Überprüfung der RISE Konnektor Seriennummer

Vergleichen Sie die über die Management-Oberfläche des RISE Konnektors bereitgestellte Seriennummer (siehe auch Abschnitt 6.1.1) einerseits mit der Seriennummer, die in den elektronisch zugestellten Bestelldetails zu finden ist, und andererseits mit der Seriennummer, welche auf der Übernahmecheckliste rechts oben angegeben ist.

Stimmen die bereitgestellten Daten nicht mit den Bestelldetails überein, muss der Händlersupport kontaktiert werden (siehe Abschnitt 2). Der Konnektor darf in so einem Fall nicht in den Produktivbetrieb gesetzt werden.

3.3.3 Schritt 9: Überprüfung der Gerätekarten Seriennummer/MAC-Adressen (LAN & WAN)

Vergleichen Sie die über die Management-Oberfläche des RISE Konnektors bereitgestellten Seriennummern der drei gSMC-K Gerätekarten (siehe Abbildung 31) mit den Seriennummern der gSMC-K Gerätekarten, die in den elektronisch zugestellten Bestelldetails zu finden sind.

Vergleichen Sie des Weiteren die über die Management-Oberfläche des RISE Konnektors bereitgestellten MAC-Adressen des LAN- & WAN-Interfaces (siehe Abschnitt 6.1.1) mit den MAC-Adressen, die in den elektronisch zugestellten Bestelldetails zu finden sind.

Stimmen die bereitgestellten Daten nicht mit den Bestelldetails überein, muss der Händlersupport kontaktiert werden (siehe Abschnitt 2). Der Konnektor darf in so einem Fall nicht in den Produktivbetrieb gesetzt werden.

3.3.4 Schritt 10: Abschluss der Überprüfung & Installation des Konnektors

Die folgenden Schritte (Schritt 10a bis Schritt 10i) müssen durchgeführt werden, um die Überprüfung und die Installation des Konnektors abzuschließen.

Hinweis: Bevor in den nächsten Schritten die Clientsysteme mit dem Konnektor verbunden werden und das WAN-Netzwerkkabel angeschlossen wird, ist es empfehlenswert, die Mindestschwere-Parameter der Protokollierung initial festzulegen, siehe dazu Abschnitt 6.1.2.8.

3.3.4.1 Schritt 10a: Arbeitsplatz, Mandant, Clientsystem

Der RISE Konnektor kann für eine Vielzahl an Konfigurationen von Arbeitsumgebungen verwendet werden. Im Regelfall müssen für den RISE Konnektor zumindest ein Arbeitsplatz, ein Mandant und ein Clientsystem eingerichtet werden.

In einer einfachen Beschreibung entspricht ein Mandant einem Arzt bzw. einer Einrichtung. Ein Clientsystem ist gleichzusetzen mit einem System, welches etwa über eine Ärztesoftware auf Funktionalitäten des Konnektors zugreifen möchte. Ein Arbeitsplatz ist sinngemäß als ein physischer Ort, an dem über Kartenterminals auf den RISE Konnektor zugegriffen werden kann, zu verstehen.

Eine einfache Beschreibung der Vorgehensweise für die Konfiguration ist im Abschnitt 6.1.4.2.1 an Hand eines Beispiels erklärt.

3.3.4.2 Schritt 10b: Herunterladen und Importieren der TSL

Bevor Kartenterminals hinzugefügt werden können, muss diesen vertraut werden. Daher ist das Herunterladen und Importieren einer TSL (Trust-service Status List) erforderlich. Gehen Sie dabei wie folgt vor:

- Herunterladen der Datei https://download.tsl.ti-dienste.de/TSL.xml
- "Leistungsumfang online" deaktivieren (siehe Abschnitt 6.1.8)
- Importieren der heruntergeladenen TSL (siehe Abschnitt 6.3.5.2)

3.3.4.3 Schritt 10c: Pairen des ersten Kartenterminals

Damit der RISE Konnektor mit Kartenterminals kommunizieren kann, müssen diese Komponenten im Netzwerk des Leistungserbringers verfügbar sein. Sämtliche im

Netzwerk verfügbare Kartenterminals werden hierfür im RISE Konnektor als Liste angezeigt (siehe Abschnitt 6.3.4.1). Für das Pairen eines Kartenterminals muss ein Administrator beim jeweiligen Kartenterminal in der Management-Oberfläche Statusänderungen durchführen (siehe Abschnitt 6.3.4.1.1) sodass sich das Kartenterminal im Status "gepaired" befindet.

Hinweis: Es kann bis zu 30 Sekunden dauern, bis das Pairing tatsächlich abgeschlossen wurde und erste Abfragen getätigt werden können.

3.3.4.4 Schritt 10d: Institutionsidentität durch die SMC-B definieren

In einem gepairten Kartenterminal muss die ausgestellte SMC-B Karte eingesteckt sein, um in der Management-Oberfläche des RISE Konnektors angezeigt zu werden. Wählen Sie dazu die gewünschte SMC-B aus, um diese Institutsidentität festzulegen (siehe Abschnitt 6.2.6.4).

Hinweis: Die Institutionsidentität ist eine durch eine SMC-B repräsentierte Identität der Institution des Leistungserbringers bzw. einer Organisationseinheit in einer solchen Institution.

3.3.4.5 Schritt 10e: Arbeitsumgebung vervollständigen

Die gepairten Kartenterminals können jetzt Arbeitsplätzen zugewiesen werden. Auch die SMC-B kann einem Mandanten zugeordnet werden.

Eine einfache Beschreibung der Vorgehensweise für die Konfiguration ist in Abschnitt 6.1.4.2.2 und Abschnitt 6.1.4.2.3 an Hand eines Beispiels erklärt.

3.3.4.6 Schritt 10f: Grundeinstellungen des RISE Konnektors vornehmen

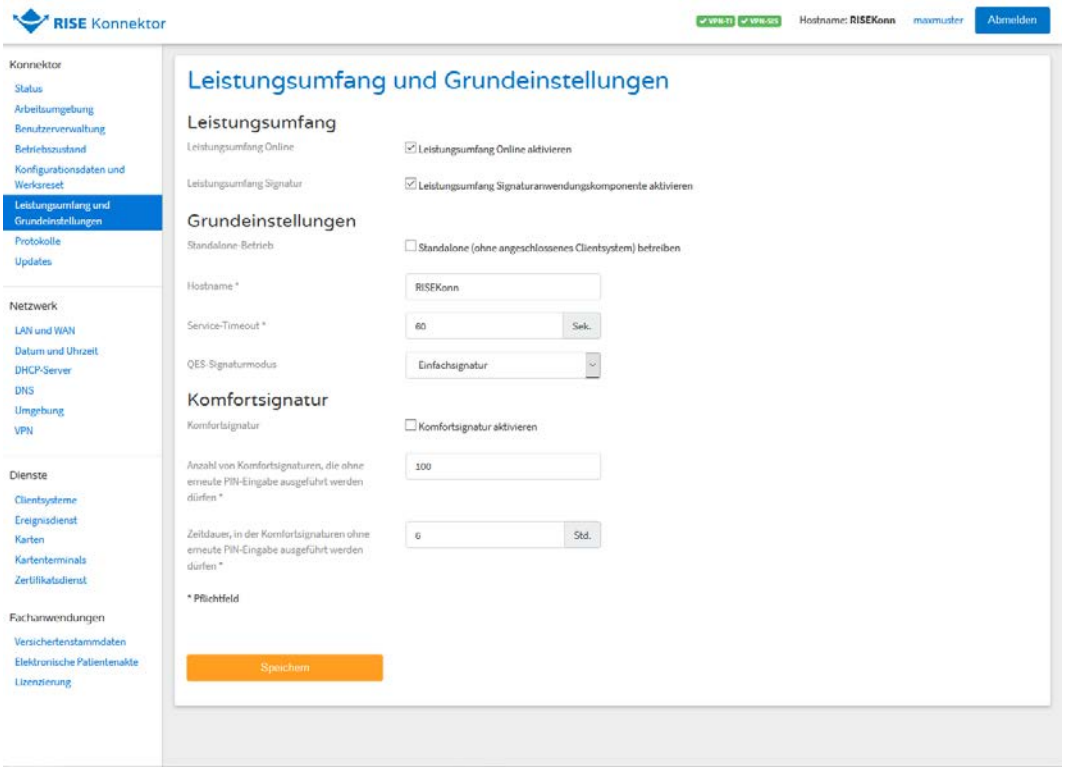


Abbildung 12: Grundeinstellungen des RISE Konnektors

Hinweis: Der Hostname des RISE Konnektors muss einen eindeutigen Namen im Netzwerk des Leistungserbringers aufweisen.

Eine detaillierte Beschreibung der einzelnen Einstellungsmöglichkeiten des Menüs "Leistungsumfang und Grundeinstellungen" ist in Abschnitt 6.1.8 zu finden.

Nachdem die Grundeinstellungen vorgenommen wurden, kann der "Leistungsumfang online" wieder aktiviert werden (siehe Abschnitt 6.1.8).

Hinweis: Das Aktivieren der Option "Leistungsumfang Online" kann mehrere Minuten in Anspruch nehmen.

3.3.4.7 Schritt 10g: Registrierung des RISE Konnektors

Mit der Registrierung des RISE Konnektors wird eine eindeutige Beziehung zwischen RISE Konnektor, Organisation des Gesundheitswesens und Leistungserbringer hergestellt. Die Anbindung dafür basiert auf dem sogenannten VPN Zugangsdienst.

Hinweis: Die Registrierung funktioniert nur, wenn eine Verbindung mit dem Internet besteht und der DNS-Domänenname (Zugangsdienste) richtig konfiguriert wurde (siehe Abschnitt 6.2.1.3). Für das Konfigurieren der Internetverbindungen siehe auch Abschnitt 4.5, Abschnitt 4.6 bzw. Abschnitt 6.2.

Hinweis: Die Registrierung des RISE Konnektors und der nachfolgende VPN-Aufbau funktioniert nur, wenn der konfigurierte DNS-Server DNSSEC unterstützt (siehe Abschnitt 6.2.1.3, "DNS-Server für das WAN Transportnetz").

Der Anbieter des VPN-Zugangsdienstes stellt dem Leistungserbringerinstitut die erforderliche Vertragsnummer (Contract-ID) für die Registrierung zur Verfügung. Über die Management-Oberfläche des RISE Konnektors (Registrierungsdienst) kann die Registrierung abgeschlossen werden (siehe auch Abschnitt 6.2.6.4):

- Eingabe der Contract-ID des VPN-Zugangsdienstes.
- Auswahl der SMC-B, welche für die Registrierung verwendet werden soll.
- Bestätigung der Registrierung durch die Eingabe der SMC-B PIN.

3.3.4.8 Schritt 10h: Abschluss der Überprüfung & Installation

Nach erfolgreichem Durchlaufen der zuvor genannten Schritte kann die Konfiguration des RISE Konnektors durch den Administrator über eine Reihe von Konfigurationsparametern an die Aufgaben und die Betriebsumgebung angepasst werden. Die hierfür erforderlichen Informationen sind in Abschnitt 4, Abschnitt 5 und Abschnitt 6 beschrieben.

Warnung: Wird ein eigenständiger Router vom Leistungserbringer zur Anbindung des LANs des Leistungserbringers an das Internet eingesetzt, kann der RISE Konnektor keine Firewall-Funktionalität zwischen Internet und LAN des Leistungserbringers umsetzen. Der Leistungserbringer hat dann mit eigenen Mitteln dafür zu sorgen, dass das Leistungserbringernetzwerk vor Angriffen aus dem Internet geschützt ist, insbesondere dass die LAN-Schnittstelle nie aus dem öffentlichen Netz (Transportnetz) erreichbar ist. Wird der RISE Konnektor zur Internet-Anbindung verwendet, können die Firewall-Funktionalitäten zum Schutz vor Zugriffen aus dem Internet in das Leistungserbringer-LAN genutzt werden. Siehe dazu auch Abschnitt 4.6.

3.3.4.9 Schritt 10i: Clientsysteme einrichten (optional)

Eine Anbindung der Clientsysteme ist nötig, damit diese Verbindungen zum RISE Konnektor aufbauen und Anfragen an den RISE Konnektor senden können. Eine Beschreibung, wie die Anbindung zu erfolgen hat, ist in Abschnitt 6.3.1 zu finden.

3.4 Außerbetriebnahme des RISE Konnektors

Eine sichere Außerbetriebnahme des RISE Konnektors durch den Endkunden muss immer dann erfolgen, wenn der RISE Konnektor die sichere Betriebsumgebung des Endkunden verlässt. Dies wäre beispielweise der Fall bei:

- Strukturierte RMA-Rückführung oder Garantiefall vor einer Rücksendung des RISE Konnektors.
- Außerbetriebnahme aufgrund einer Altgerätentsorgung.
- Weiterverkauf oder Verschenkung des RISE Konnektors durch das Leistungserbringerinstitut an einen weiteren berechtigten Leistungserbringer.

Dazu müssen aus Sicherheitsgründen durch den zuständigen Administrator folgende Maßnahmen in der beschriebenen Reihenfolge durchgeführt werden:

1. De-Registrierung des betroffenen Konnektors beim Zugangsdienstprovider.
2. Durchführung eines Werksresets.

Vor der Durchführung einer De-Registrierung sollte Kontakt mit dem Zugangsdienstprovider aufgenommen werden. Die Durchführung eines Werksresets wird im Abschnitt 3.4.1 beschrieben.

Warnung: Sollte die De-Registrierung bzw. der Werksreset nicht mehr möglich sein, müssen die Gerätekarten des RISE Konnektors vernichtet werden (siehe Abschnitt 3.4.2).

Warnung: Bei Weiterverkauf/Verschenkung des RISE Konnektors ist die Einhaltung der sicheren Lieferkette nicht mehr gewährleistet. Der RISE Konnektor verliert seine Zertifizierung und kann somit nicht mehr zertifikatskonform betrieben werden!

Anmerkung: Entsorgen Sie das RISE Konnektor Altgerät niemals über den Hausmüll, sondern beachten Sie die Entsorgungsvorschriften (siehe Abschnitt 7).

3.4.1 Durchführung eines Werksresets

Durch einen Werksreset werden sämtliche Konfigurationen am RISE Konnektor in den Ursprungszustand zurückgesetzt und sensitive Informationen im Datenspeicher gelöscht.

Soll der RISE Konnektor auf den Werkszustand zurückgesetzt werden, geschieht dies über die Management-Oberfläche des RISE Konnektors. Ein Werksreset kann auf zwei unterschiedliche Arten durchgeführt werden:

- Durchführung eines Werksreset durch einen berechtigten, in der Management-Oberfläche angemeldeten Administrator.
- Durchführung eines Werksreset mittels Sicherheitstoken ohne Anmeldung auf der Management-Oberfläche.

Warnung: Die Durchführung eines Werksresets kann nicht mehr rückgängig gemacht werden! Bitte beachten Sie, dass unmittelbar nach einem Werksreset sämtliche Einstellungen des RISE Konnektors verloren gehen und das Gerät vollumfänglich neu eingerichtet werden muss.

Sicherheitshinweis: Nach einem erfolgreichen Werksreset muss die Aufforderung zum Setzen des Benutzernamens und des Passworts für den Super-Administrator erscheinen (gem. Abbildung 11). Ist dies nach mehreren Versuchen nicht der Fall, kontaktieren Sie bitte umgehend den Händlersupport (siehe Abschnitt 2).

3.4.1.1 Durchführung eines Werksresets durch einen berechtigten, in der Management-Oberfläche angemeldeten Administrator

Ausschließlich Super-Administratoren bzw. durch den Super-Administrator dafür berechtigte Administratoren sind autorisiert, einen Werksreset über die Management-Oberfläche des RISE Konnektors auszulösen. Die Funktion für den Werksreset erreichen Sie im Menü unter “Konfigurationsdaten und Werksreset”.

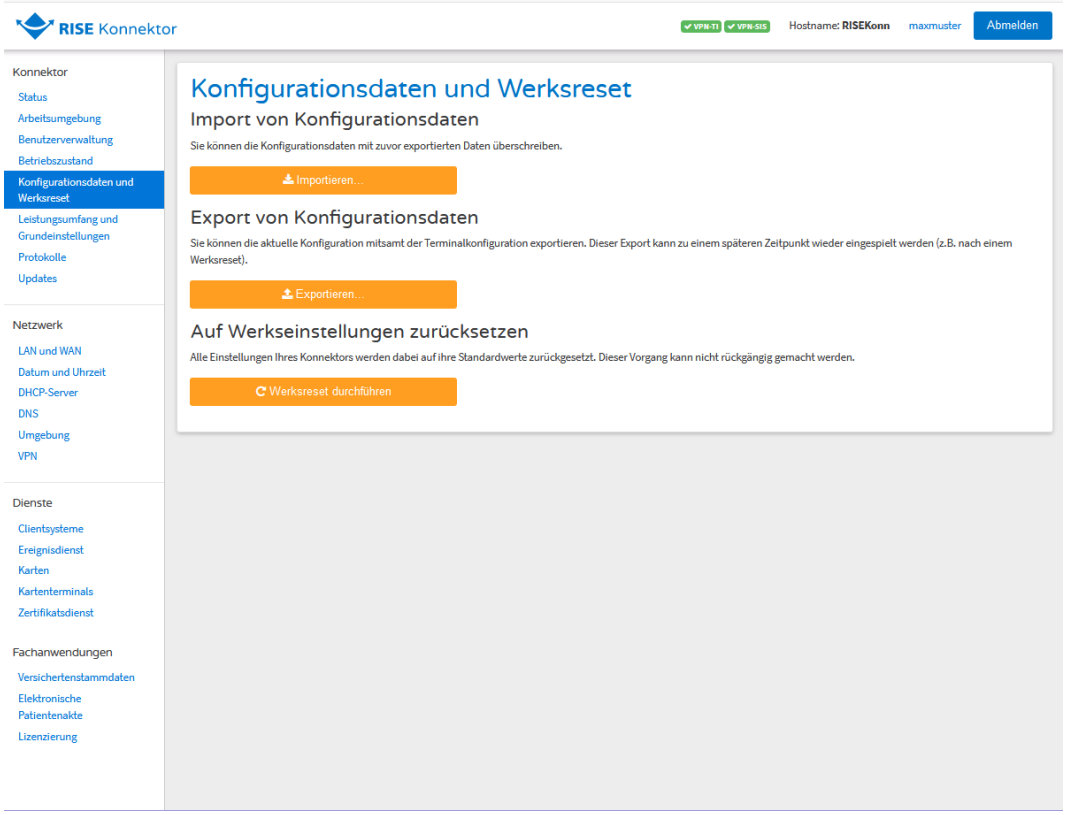


Abbildung 13: Import und Export von Konfigurationsdaten und Werksreset durch einen berechtigten Administrator

Hinweis: Es wird empfohlen, die Konfiguration des RISE Konnektors auf einem lokalen Computer zu sichern, um diese bei Bedarf wieder importieren zu können (siehe Abschnitt 6.1.7). Der abgespeicherte Konfigurationszustand des RISE Konnektors kann somit zu jeder Zeit wiederhergestellt werden.

Warnung: Sollten Sie keine Sicherheitskopie angelegt haben, müssen Sie den RISE Konnektor neu einrichten. Das betrifft alle in Abschnitt 3.3.4 beschriebenen Schritte mit Ausnahme von Abschnitt 3.3.4.2.

Hinweis: Nach dem Werksreset bezieht der RISE Konnektor wieder eine IP-Adresse vom DHCP-Server (siehe Abschnitt 3.3.1.1).

3.4.1.2 Durchführung eines Werksresets mittels Sicherheitstoken

In der Herstellerverpackung des RISE Konnektors befindet sich eine Kurzanleitung, auf der sich auf der Rückseite ein aufgedruckter Sicherheitstoken für die Durchführung eines Werksresets befindet.

Um einen Werksreset ohne eine erfolgreiche Anmeldung eines Administrators auf der Management-Oberfläche des RISE Konnektors durchzuführen, wählen Sie das Menü “Werksreset durchführen” am Startbildschirm (siehe Abbildung 14), ohne dass Sie eingeloggt sind. Geben Sie anschließend die Zeichenkette des Tokens in die Eingabemaske ein und starten Sie die Durchführung mit “Werksreset durchführen” (siehe Abbildung 15).

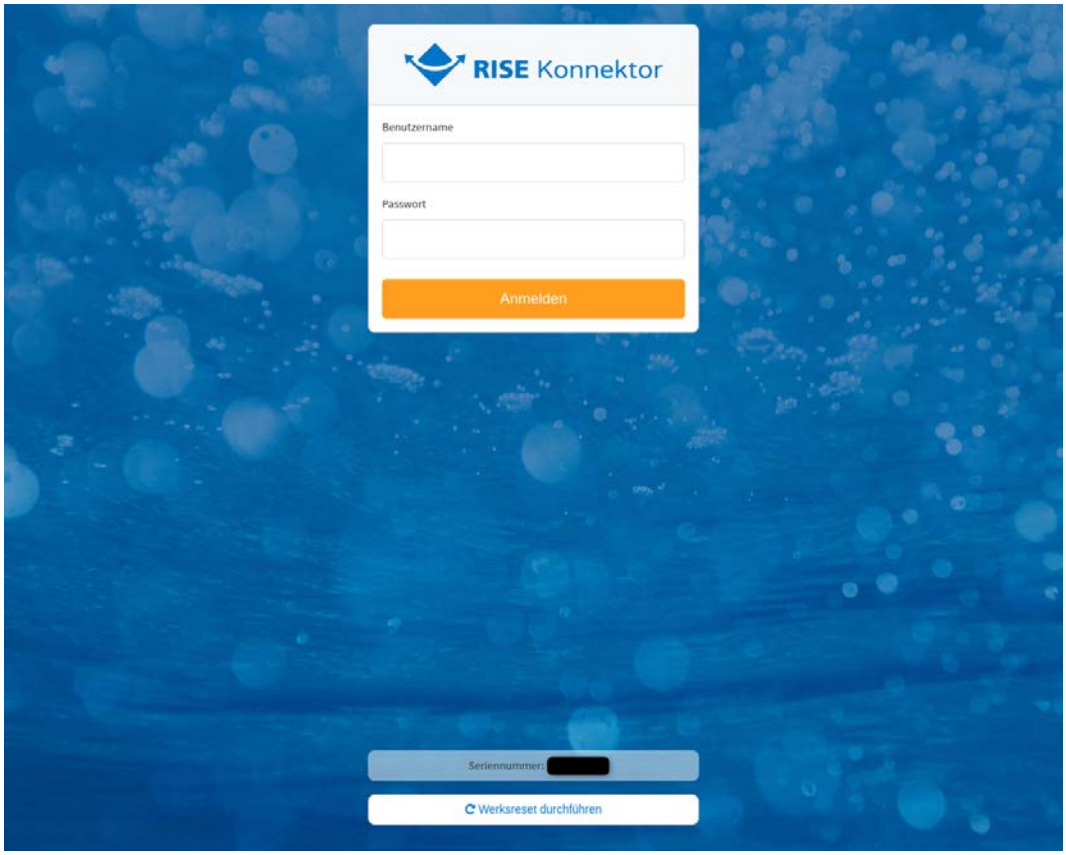


Abbildung 14: Loginmaske mit "Werksreset durchführen

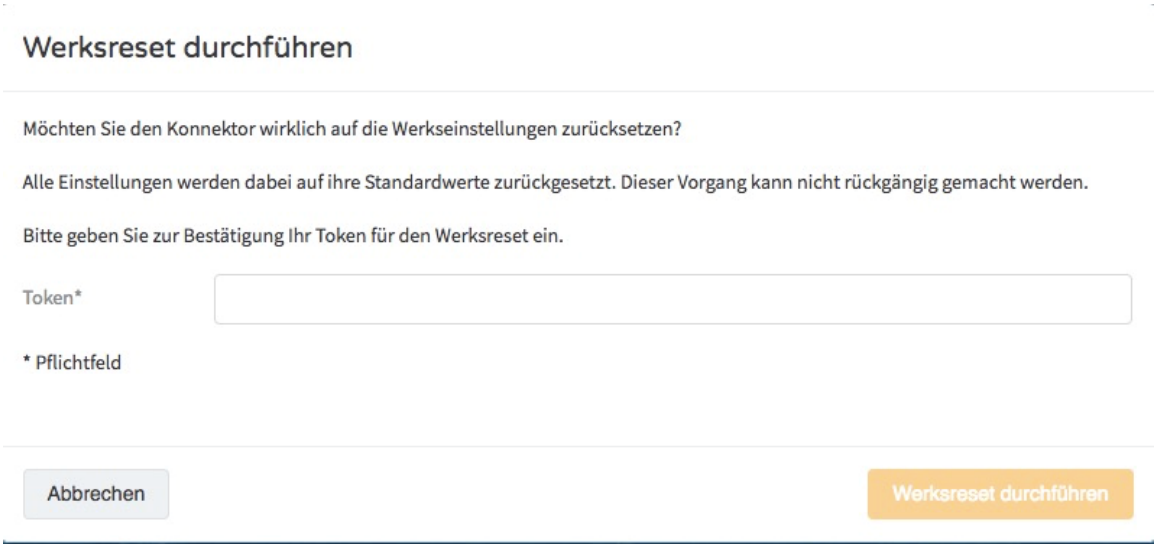


Abbildung 15: Werksreset mittels Sicherheitstoken

Anschließend wird der RISE Konnektor neu gestartet und Sie können mit Abschnitt 3.3.1.2 fortfahren.

Hinweis: Dieser Sicherheitstoken wird NICHT für die Installation des RISE Konnektors benötigt.

Der Sicherheitstoken dient der Herstellung der Werkskonfiguration des RISE Konnektors im Zuge einer gesicherten Außerbetriebnahme falls das Benutzerkonto des Super-Administrators nicht mehr zugänglich ist, beispielsweise auf Grund eines vergessenen Passworts.

Sicherheitshinweis: Der Sicherheitstoken dient der Authentisierung für den Werksreset und muss vom Leistungserbringer auf sichere Art und Weise (z.B. verschlossen in einem Tresor) verwahrt werden.

3.4.2 Außerbetriebnahme des RISE Konnektors ohne Werksreset

Sollten alle bereits angeführten Optionen für einen Werksreset nicht mehr möglich sein, müssen die gSMC-K Gerätekarten des RISE Konnektors vernichtet werden. Damit wird sichergestellt, dass die sensitiven Daten am Gerät nicht missbräuchlich verwendet werden können.

Hinweis: Beachten Sie bitte, dass dadurch der RISE Konnektor unwiderruflich nicht wieder in Betrieb genommen werden kann.

Hierfür ist das Gehäuse des RISE Konnektors zu öffnen:

- Abbildung 16 zeigt die drei sichtbaren Positionen der Gehäuseschrauben der Abdeckung, welche zu lösen sind. Eine vierte Schraube befindet sich an der verbleibenden, nicht sichtbaren Ecke.
- Das front- und rückseitige Gehäusesiegel sind zu durchtrennen.

- Die Abdeckung kann anschließend nach oben abgehoben werden.
- Die drei RISE Konnektor Gerätekarten (ähnlich einer SIM-Karte eines Mobilfunktelefons) befinden sich auf der Oberseite der RISE Konnektor-Platine.
- Diese drei Gerätekarten sind zu entnehmen und zu zerstören (beispielsweise durch Lochung).

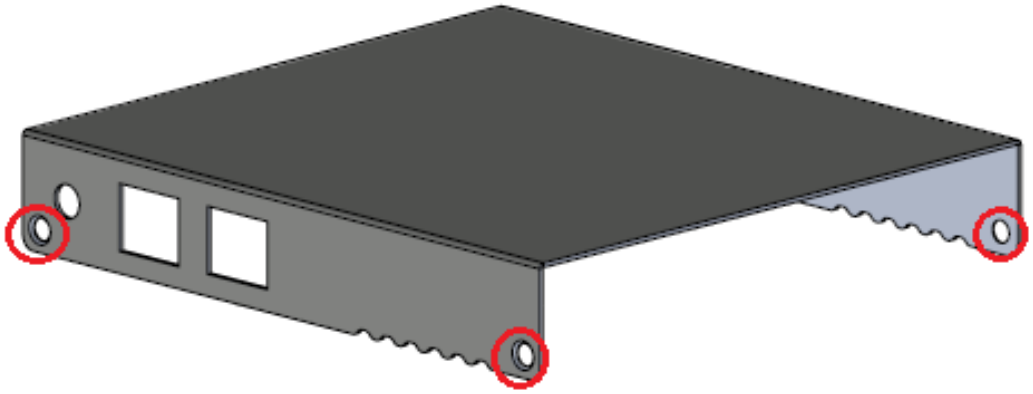


Abbildung 16: Verschraubung der RISE Konnektor-Abdeckung

Hinweis: Durch die Vernichtung der drei Gerätekarten wird das nicht-autorisierte Auslesen von sensitiven Daten am RISE Konnektor verhindert.

3.4.3 Diebstahl eines RISE Konnektors

Wird ein RISE Konnektor gestohlen, muss dies dem Händler bzw. dem Hersteller unmittelbar gemeldet werden. Dieser wird aus Sicherheitsgründen im Zuge dieser Meldung eine De-Registrierung und Sperrung des RISE Konnektors in der Telematikinfrastruktur veranlassen.

Hinweis: Für die Sperrung durch den Hersteller ist eine eindeutige Identifikation des Leistungserbringers erforderlich, wofür ein Sperrcode bekannt gegeben werden muss. Dieser ist auf der Übernahmecheckliste (siehe Abbildung 4) aufgedruckt.

4 Der RISE Konnektor

Der RISE Konnektor ist für den Betrieb in Arztpraxen, Krankenhäusern und Apotheken ausgelegt. Der Konnektor kann entweder an der Wand befestigt oder auf dem Tisch stehend betrieben werden. Um eine sichere Installation des RISE Konnektors durchführen zu können, ist die Errichtung einer sicheren Betriebsumgebung, in welcher der Konnektor installiert und betrieben wird, unerlässlich. Diese Anforderungen sind bereits vor der Installation des RISE Konnektors zu erfüllen.

Sicherheitshinweis: Der Leistungserbringer muss bereits bei der Inbetriebnahme dafür Sorge tragen, dass ein Diebstahl bzw. eine Manipulation innerhalb kurzer Zeit erkannt und nachverfolgt werden kann.

Sicherheitshinweis: Um den RISE Konnektor sicher zu betreiben, informieren Sie sich regelmäßig über mögliche Schwachstellen der Telematikinfrastruktur unter https://www.gematik.de/aktuelles/ .

4.1 Sicherheitsrichtlinie für Passwörter

Die folgenden Richtlinien sind bei der Wahl von Passwörtern zu befolgen. Diese Vorgaben werden aus Sicherheitsgründen bei der Passwortvergabe durch den RISE Konnektor überprüft, um die Vergabe von starken Passwörtern zu forcieren:

- Sämtliche Benutzer müssen die Zeichen eines Passworts aus den Zeichenklassen Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Ziffern wählen. Ein valides Passwort muss Zeichen aus mindestens drei dieser Zeichenklassen enthalten.
- Ein Passwort muss mindestens 8 Zeichen lang sein.
- Ein Passwort darf nicht die zugehörige Benutzerkennung enthalten (weder vorwärts noch rückwärts, bei Vergleich unter Ignorierung der Groß- und Kleinschreibung).
- Die Wiederholung alter Passwörter beim Passwortwechsel durch den Benutzer selbst ist nicht zulässig (Passworthistorie). Dabei werden jeweils pro Benutzer die letzten 3 Passwörter gespeichert und beim Versuch, sie erneut zu setzen, abgelehnt.

Des Weiteren gelten folgende Bestimmungen für valide gesetzte Passwörter:

- Für die Erstanmeldung neuer Benutzer werden Einmalpasswörter durch den Super-Administrator vergeben. Hierbei handelt es sich um Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen. Gleiches gilt, wenn ein Passwort eines Benutzers vom Super-Administrator zurückgesetzt wird.
- Jeder Benutzer kann nach erfolgreicher Authentifizierung sein eigenes Passwort jederzeit ändern.
- Der Super-Administrator ist dafür verantwortlich, dass jeder Benutzer einen eigenen Benutzer-Account mit dazugehörigem Passwort verwendet und es keine gemeinsamen Benutzer gibt.

- Bei der Eingabe wird das Passwort nicht im Klartext auf dem Bildschirm angezeigt.
- Der RISE Konnektor initiiert nach einem durch den Super-Administrator konfigurierbaren Zeitraum einen Passwortwechsel beim nächsten Login (siehe Abschnitt 6.1.5).
- Erfolglose Anmeldeversuche werden mit einer kurzen Fehlermeldung ohne Angabe von näheren Einzelheiten abgelehnt. Des Weiteren wird nicht angegeben, welcher Teil der Login-Daten (Benutzername oder Passwort) falsch war.
- Nach einer Fehleingabe des Passworts erfolgt eine 3 Sekunden lange Verzögerung bis zur nächsten Eingabemöglichkeit des Passworts für dieselbe Benutzerkennung.

Es wird aus Sicherheitsgründen empfohlen möglichst lange Passwörter (Passphrasen) zu verwenden.

Warnung: Der Administrator ist verantwortlich, dass sämtliche Passwörter auf einem sicheren Weg zu den Benutzern gelangen und zu jedem Zeitpunkt vor dem Missbrauch Dritter geschützt sind.

Sicherheitshinweis: Die sichere Verwahrung von Passwörtern der Administratoren und Super-Administratoren muss durch die Benutzer selbst sichergestellt werden (z.B. elektronisch verschlüsselt bzw. verschlossen in einem Tresor).

Sicherheitshinweis: Jeder Benutzer ist selbst für die Qualität der verwendeten Passwörter verantwortlich. Es sollen stets möglichst lange und sichere Passwörter verwendet werden. Die Qualitätsanzeige dient lediglich zur Indikation unsicherer Standardpasswörter und soll allein eine zusätzliche Hilfestellung sein. Schulen Sie das Personal beim Leistungserbringer dahingehend ein!

Sicherheitshinweis: Achten Sie beim Eingeben von Passwörtern stets darauf, dass Sie dabei unbeobachtet sind.

Hinweis: Die maximale Länge der Benutzernamen ist auf 256 Zeichen festgelegt. Das Passwort darf eine maximale Länge von 512 Zeichen aufweisen.

4.2 Sichere Verbindung zum RISE Konnektor

Bei jedem Login ist darauf zu achten, dass der Web-Browser eine sichere Verbindung anzeigt. Die Form der Anzeige ist Browser-abhängig und kann beispielsweise durch ein Schloss-Symbol links neben der Adressleiste des Browsers symbolisiert werden. Dies stellt sicher, dass eine TLS (HTTPS)-Verbindung existiert, bevor sich der Benutzer am System anmeldet.

Abbildung 17: Beispiel für die Indikation für eine sichere Verbindung

Sicherheitshinweis: Sollte das Zertifikat von Ihrem Browser nicht als sicher erkannt werden, überprüfen Sie den Fingerprint des Zertifikates mit jenem aus der Kurzanleitung. Sind die Fingerprints ident oder wird das Zertifikat des Browsers als sicher erkannt, wurde eine HTTPS-Verbindung erfolgreich aufgebaut.

Hinweis: Um einen reibungslosen Ablauf in Ihrem Institut zu gewährleisten, sind Sie berechtigt, den Finderabdruck zu extrahieren und zu vervielfältigen, um jedem Benutzer der Management-Oberfläche die Möglichkeit zu geben, den Fingerabdruck jederzeit prüfen zu können. Der Fingerabdruck ist nicht vertraulich.

4.3 Übernahme von Einstellungen

Werden Änderungen an den Einstellungen durchgeführt, müssen diese gespeichert werden. Ein grünes Statusfenster (siehe Abbildung 18), welches nach dem Ändern von Einstellungen erscheint, symbolisiert das. Dieses bestätigt, dass die neu gesetzten Parameter und Einstellungen auch korrekt übernommen und gespeichert wurden.

Abbildung 18: Bestätigung für eine erfolgreiche Übernahme von Einstellungen

Hinweis: Aus Sicherheitsgründen kann es beim Übernehmen einiger Einstellungen oder beim Auslösen bestimmter Aktionen vorkommen, dass während der Verarbeitung keine anderen Vorgänge gestartet werden können. Dies gilt z.B. beim Aufbau von VPN-Verbindungen oder Aktionen, die automatisch einen VPN-Auf-/Abbau auslösen. Wird vor Abschluss solcher Vorgänge eine andere Aktion ausgelöst, wird ein entsprechender Hinweis angezeigt. Die maximale Verarbeitungszeit derartiger Vorgänge beträgt 300 Sekunden.

4.4 Erstellung einer sicheren Betriebsumgebung

Der RISE Konnektor ist Teil einer Einbox-Lösung, welche aus einem selbständigen Gerät besteht und in der Einsatzumgebung der sogenannten "Leistungserbringer" verwendet wird. Hierbei verbindet das Gerät die lokale Einsatzumgebung, beispielweise in Arztpraxen, mit der zentralen Telematikinfrastruktur und ermöglicht so einen sicheren Datenaustausch zwischen den beiden Netzwerken. Hierbei muss der Leistungserbringer sowohl in physischer, als auch logischer Hinsicht, eine sichere Betriebsumgebung bereitstellen.

Im Rahmen dieser sicheren Betriebsumgebung sind einige Komponenten vom Leistungserbringer bereitzustellen, um einen sicheren Betrieb zu ermöglichen.

4.4.1 Funktionelle Anforderungen an die Betriebsumgebung

Der RISE Konnektor besitzt einige funktionelle Anforderungen, welche der Leistungserbringer durch Komponenten oder das lokale Netzwerk bereitstellen muss, um einen vollständigen und ordnungsgemäßen Betrieb ermöglichen zu können:

- Bereitstellung eines Clientsystems
- Bereitstellung von eHealth-Kartenterminals
- Bereitstellung von Chipkarten

4.4.1.1 Bereitstellung eines Clientsystems

Eine funktionelle Anforderung zur ordnungsgemäßen Verwendung des RISE Konnektors ist die Bereitstellung eines Clientsystems, etwa eine Praxisverwaltungssoftware (PVS), ein Krankenhausinformationssystem (KIS) oder ein Apotheken-Verwaltungssystem (AVS). Diese Clientsysteme nutzen die Dienstleistungen des RISE Konnektors und der Fachmodule für die Kommunikation mit den Fachdiensten der Telematikinfrastruktur.

Sicherheitshinweise:

- Die Clientsysteme, die mit dem RISE Konnektor kommunizieren, werden als vertrauenswürdig angesehen, d.h. es erfolgen keine Angriffe aus den Clientsystemen und es ist sichergestellt, dass sie die ihre anvertrauten Daten und Informationen nicht missbrauchen. Sofern ein Clientsystem eine gesicherte Kommunikation mit dem RISE Konnektor unterstützt, muss das Schlüsselmaterial zum Aufbau und Betrieb des sicheren Kommunikationskanals adäquat geschützt werden. Dies gilt auch bei Verwendung von Terminal-Servern: Hier werden die Terminal-Server und die genutzten Thin-Clients in der angegebenen Weise als vertrauenswürdig angesehen.**
- Das Clientsystem kontrolliert den Zugriff auf die Entschlüsselungsfunktion des RISE Konnektors, so dass keine unkontrollierten Entschlüsselungen (ohne Zustimmung des HBA-Inhabers, z.B. durch nicht autorisiertes medizinisches Personal) möglich sind. Das Clientsystem kontrolliert den Zugriff auf die Verschlüsselungsfunktion des RISE Konnektors, sodass keine nicht intendierten Verschlüsselungen oder nicht intendierte Empfänger an den Konnektor übergeben werden.
- Das Clientsystem stellt Rückmeldungen, Warnungen und Fehlermeldungen des Konnektors sowie über den Systeminformationsdienst gemeldete kritische Betriebszustände korrekt, sofort und verständlich dar.

4.4.1.2 Bereitstellung von eHealth-Kartenterminals

Um den Leistungsumfang der Funktionen des RISE Konnektors voll ausnützen zu können, muss der Leistungserbringer innerhalb seines lokalen Netzwerkes von der gematik zugelassene Kartenterminals zur Verfügung stellen.

Der RISE Konnektor unterstützt prinzipiell sowohl die lokale Eingabe von PINs am Kartenterminal, als auch eine entfernte (Remote-)Eingabe von PINs.

Sicherheitshinweis: Als Kartenterminal dürfen nur Geräte eingesetzt werden, die nach dem Schutzprofil für das eHealth-Kartenterminals der elektronischen Gesundheitskarte[3] evaluiert und zertifiziert sind.

4.4.1.3 Bereitstellung von Chipkarten

Für den Betrieb des RISE Konnektors sind folgenden Chipkarten relevant:

- **eGK (Elektronische Gesundheitskarte):** die Elektronische Gesundheitskarte dient als sicherer Informationsspeicher der Versichertenstammdaten und Daten der Gesundheitsanwendungen, kryptographischer Schlüssel und Zertifikate für die Verschlüsselung und Authentisierung sowie als PIN-Empfänger für die Kartenhalter-PIN. Die eGK wird von den Patienten des Leistungserbringers bereitgestellt.
- **HBA (Heilberufsausweis):** der Heilberufsausweis dient als sicherer Informationsspeicher für kryptographische Schlüssel und Zertifikate sowie als PIN-Empfänger für die Kartenhalter-PIN. Der HBA wird vom Leistungserbringer bereitgestellt und identifiziert diesen eindeutig.
- **SMC-B (Security Module Card – B):** die SMC-B dient als sicherer Informationsspeicher für kryptographische Schlüssel und Zertifikate. Die Verwendung der SMC-B wird durch eine PIN geschützt, um die Leistungserbringer-Institution bei Verwendung eindeutig zu identifizieren.
- **gSMC-KT (gerätespezifische Security Module Card Typ KT):** die gSMC-KT ist das Sicherheitsmodul für Kartenterminals.

4.4.2 Firewall-Konfiguration beim Leistungserbringer

Beim Leistungserbringer sind in der bestehenden Netzwerkinfrastruktur mit Firewall bei der Integration des RISE Konnektor Freischaltungen entsprechend Tabelle 4 und ggf. Tabelle 5 vorzusehen. Verbindungen, die der RISE Konnektor in das Internet aufbauen muss, sind in Tabelle 5 separat zusammengefasst.

Hinweis: Dieser Abschnitt ist für Sie nur relevant, wenn Sie in Ihrem lokalen Netzwerk oder zwischen WAN-Interface am RISE Konnektor und dem IAG eine Firewall einsetzen.

Tabelle 4 listet alle Ports/Verbindungen auf, die Sie im Falle einer Firewall zwischen dem LAN-Interface und dem Clientsytem (Ärzte-PCs, Kartenterminals, …) freischalten müssen.

[3] Protection Profile Electronic Health Card Terminal, BSI-PP-0032, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 3.7, 21.09.2016

Tabelle 5 listet alle Ports/Verbindungen auf, die Sie im Falle einer Firewall zwischen dem LAN- (bei Anbindungsmodus[4] "Parallel") bzw. dem WAN-Interface (bei Anbindungsmodus "InReihe") und dem Internet (IAG) freischalten müssen.

"Eingehend" bedeutet Zugriffe in Richtung RISE Konnektor, "Ausgehend" bedeutet, dass der RISE Konnektor Pakete versendet. "Ja" bedeutet, dass der angegebene Port für einen Verbindungsaufbau in der angegebenen Richtung freigeschaltet sein muss. "N/A" bedeutet, dass die Firewall-Einstellung nicht relevant ist, d.h. sie kann von einer Firewall auch verboten werden.

Hinweis: Bei Fragen zur Konfiguration Ihres bestehenden Netzwerks bzw. wie die entsprechende Konfiguration an Ihrer bestehenden Firewall angepasst werden muss, ziehen Sie bitte deren Dokumentation/Bedienungsanleitung in Betracht. Es kann zudem auch sein, dass Sie einen Router mit Firewall-Funktionalität haben. Die Anforderungen zur Konfiguration dessen Firewall gelten dann analog.

Die in Tabelle 4 und Tabelle 5 angeführten Ports müssen an der/den von Ihnen (optional bereits bisher) eingesetzten Firewall(s) erlaubt sein, damit der RISE Konnektor ordnungsgemäß funktioniert. Wenn Sie einzelne nachfolgend aufgelistete Ports nicht erlauben, stehen einzelne Funktionen des RISE Konnektors nicht zur Verfügung bzw. kann der RISE Konnektor nicht in der vorgesehenen Konfiguration betrieben werden.

Service	Port	Protokoll	Kommentar	ein-gehend	aus-gehend
DHCP Client	67, 68	UDP/DHCP	Für Zuweisung der Netzwerkadresse des RISE Konnektors durch den DHCP Server in der lokalen Infrastruktur.	N/A	Ja
RISE Konnektor Management Oberfläche	8443	TCP / HTTPS	Sichere Verbindung zur Management Oberfläche des RISE Konnektors.	Ja	N/A
Dienstverzeichnis-dienst	80, 443	TCP/ HTTP(S)	Clientsysteme rufen beim Initialisieren den Dienstverzeichnis-dienst des RISE Konnektors für Konfigurations-zwecke auf.	Ja	N/A

[4] Siehe Tabelle 16, Anbindungsmodus (ANLW_ANBINDUNGS_MODUS)

Service	Port	Protokoll	Kommentar	ein-gehend	aus-gehend
SOAP Services	80, 443	TCP/ HTTP(S)	SOAP-Endpunkte über welche das Clientsystem die einzelnen Dienstoperationen des RISE Konnektors erreicht.	Ja	N/A
Event Service	dynamisch[5]	TCP/CETP	Das Port XX entspricht dem konfigurierten Port beim Abonnieren von Events	N/A	Ja
Kartenterminaldienst	4742	TCP, UDP	Protokoll (Secure Interoperable ChipCard Terminal) für die Kommunikation zw. dem RISE Konnektor und den Chipkarten-terminals.	Ja	Ja
DHCP Server	67, 68	UDP/DHCP	Für Zuweisung der Netzwerkkonfiguration an die Clients durch den DHCP-Server des RISE Konnektors.	Ja	Ja
Zeitdienst	123	UDP/NTP	Für NTP-Anfragen von Clients zum RISE Konnektor.	Ja	N/A
Namensdienst	53	TCP, UDP/DNS	Domain Name System (DNS) für die Beantwortung der Anfragen zur Namensauflösung im Clientnetzwerk.	Ja	Ja
Ping	-	ICMP	Diagnose-	Ja	Ja

[5] https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/schemata-wsdl-und-andere-dateien/, Download Schnittstellendefinitionen im XSD- und WSDL-Format für den PTV3-Konnektor, Schnittstellendefinition conn/EventService.*, Befehl Subscribe, letzter Zugriff 30.04.2020

Service	Port	Protokoll	Kommentar	ein-gehend	aus-gehend
			Werkzeug für die Erreichbarkeits-prüfung von Komponenten im Clientsystem bzw. des RISE Konnektors.		

Tabelle 4: Übersicht über verwendete Ports des RISE Konnektors im Netzwerk des Leistungserbringers

Service	Port	Proto-koll	Kommentar	ein-gehend	aus-gehend	Ziel- bzw. Quelladresse(n)
Namens-dienst	53, 80, 443	TCP, UDP	Domain Name System (DNS) für die Beantwortung von RISE Konnektor Anfragen zur Namensauflös-ung im Internet; Aktualisierung des DNS-Vertrauens-ankers.	N/A	Ja	DNS_SERVERS_I NT (vgl. Tabelle 21), data.iana.org
Zertifikats-dienst	80, 443, 8090 (dynami sch)	TCP	Ermittlung des Zugangspunktes und Download von Zertifikats-Sperrlisten.	N/A	Ja	CERT_CRL_DOW NLOAD_ADDRES S (vgl. Tabelle 49), www.d-trust.net
Hash&URL	80, 443	TCP	Ermittlung der Hash&URL Server.	N/A	Ja	Hash&URL-Server[6]
Registrie-rungsdienst	80, 443, 8443 (dynami sch)	TCP	Ermittlung der Registrierungs-Server und Registrierung des Konnektors	N/A	Ja	Registrierungs-Server[7]
VPN-	500,	UDP	TI bzw. SiS RISE	Ja	Ja	VPN-

[6] Die Adresse des Hash&URL-Servers kann beim Anbieter des VPN-Zugangsdienstes erfragt werden.
[7] Die Adresse und das verwendete Port des Registrierungs-Servers kann beim Anbieter des VPN-Zugangsdienstes erfragt werden.

Service	Port	Proto-koll	Kommentar	ein-gehend	aus-gehend	Ziel- bzw. Quelladresse(n)
Verbindung TI und SIS	4500		Konnektor Verbindung zu den VPN-Zugangsdienst-providern im Internet.			Konzentratoren TI, SIS und RA
VPN-Verbindung TI und SIS	-	ESP	TI bzw. SiS RISE Konnektor Verbindung zu den VPN-Zugangsdienst-providern im Internet.	Ja	Ja	VPN-Konzentratoren TI, SIS und RA
Ping	-	ICMP	Diagnose-Werkzeug für die Erreichbarkeits-prüfung von Konzentratoren im Internet.	Ja	Ja	Alle

Tabelle 5: Übersicht über verwendete Ports des RISE Konnektors Richtung Internet

Hinweis: Stellen Sie sicher, dass die eingesetzte Firewall Richtung Internet Connection Tracking unterstützt.

4.4.3 Sicherheitsziele der Betriebsumgebung

Zusätzlich zu den beschriebenen funktionalen Anforderungen muss auch die Sicherheit der Betriebsumgebung des RISE Konnektors eingehalten werden. Dies umfasst insbesondere:

- **Korrekte Nutzung des RISE Konnektors durch Clientsysteme und andere aktive Komponenten in der Netzwerkumgebung des Leistungserbringers.** Im Rahmen der lokalen Netzwerkumgebung des Leistungserbringers haben einige Clientsysteme Zugriff auf die Funktionalitäten des RISE Konnektors. Um den RISE-Konnektor sicher zu betreiben, müssen verbundenen Clientsysteme und andere verbundene aktive Komponenten im LAN der jeweiligen Arztpraxis oder eines Krankenhauses die Funktionalitäten des Konnektors korrekt aufrufen. Des Weiteren muss der Zugriff auf Bestandsnetze und offene Fachanwendungen lediglich durch aktive Komponenten im LAN, in den dafür vorhergesehenen IP-Bereichen, erfolgen.
- **Sicherer Betrieb der Clientsysteme:** Der Leistungserbringer setzt nur Clientsysteme ein, welche nach aktuellem Stand der Technik entwickelt wurden und das spezifizierte Verhalten zeigen. Des Weiteren administriert der Leistungserbringer Clientsysteme auf sichere Art und Weise. Hierbei trägt der Betreiber die Verantwortung dafür, dass die

Clientsysteme den Konnektor in spezifizierter Art und Weise, also insbesondere die spezifizierten Schnittstellen, nutzen.

- **Physischer Schutz des RISE Konnektors:** Es müssen während des Betriebs des Konnektors geeignete Maßnahmen durch den Betreiber getroffen werden, sodass ein Schutz vor physischem Zugriff unbefugter Personen gegeben ist. Als befugt gelten in diesem Kontext nur durch den Betreiber namentlich autorisierte Personen (Leistungserbringer, medizinisches Personal, etc.). Durch Sicherheitsmechanismen in der Betriebsumgebung muss sichergestellt werden, dass ein Diebstahl und/oder eine Manipulation des Konnektors rechtzeitig erkannt wird, sodass organisatorische und/oder personelle Maßnahmen Schaden vermeiden.
- **Schutz des Netzwerks vor Angriffen:** Der Leistungserbringer hat dafür Sorge zu tragen, dass das lokale Netzwerk gegen unbefugten Zugriff bzw. Nutzung geschützt ist. Des Weiteren müssen die verbundenen Systeme im Netzwerk immer auf dem aktuellsten Stand sein (regelmäßige Updates) um sie gegen Schadsoftware zu schützen und somit auch das lokale Netzwerk.
- **Sichere Administration des RISE Konnektors:** Der Betreiber des RISE Konnektors muss dafür sorgen, dass administrative Tätigkeiten der lokalen und zentralen Administration in Übereinstimmung mit der Administrator-Dokumentation des Produkts durchgeführt werden. Insbesondere muss für diese Tätigkeiten vertrauenswürdiges, mit der Benutzerdokumentation vertrautes, sachkundiges Personal eingesetzt werden. Die Administratoren müssen Authentisierungsinformationen und –token (z.B. Token für Werksreset) geheim halten bzw. dürfen diese nicht an Unberechtigte weitergeben.

4.5 Betriebsmodi

Der RISE Konnektor kann in zwei verschiedenen Betriebsmodi betrieben werden:

- Online-Modus
- Offline-Modus

4.5.1 Online-Modus

Im Online-Modus kann der Konnektor aktiv Verbindungen zu unterschiedlichen Diensten der Zentralen Telematikinfrastruktur, sowie optional deren Sicheren Internet Services (SIS) und Bestandsnetze aufbauen. Um die Sicherheit dieser Verbindungen umsetzen zu können, werden grundlegende Daten unterschiedlicher Dienste, etwa des Zeit-, des Zertifikats- oder des Namensdiensts in regelmäßigen Abständen aktiv über diese Verbindungen aktualisiert. Schlagen Aktualisierungsvorgänge ein- oder mehrmals fehl, beziehungsweise können diese nicht in einem vorgegebenen Zeitintervall durchgeführt werden, wechselt der Konnektor in den sogenannten “kritischen Betriebszustand”.

Als Beispiel für solch ein Verhalten dient die Aktualisierung der Systemzeit durch den Zeitdienst des Konnektors. Dieser synchronisiert sich automatisch mit der Standardzeit der Telematikinfrastruktur. Schlägt diese Synchronisation fehl oder

weicht die Konnektor-Systemzeit um einen konfigurierbaren Wert von der Systemzeit der Telematikinfrastruktur ab, wird der kritische Betriebszustand ausgelöst. Des Weiteren ist die Aktualisierung des RISE Konnektors durch den Download eines Update-Pakets von einem Update-Server lediglich im Online-Betriebsmodus möglich.

Der Online-Modus kann mittels des Konfigurationsparameters "Leistungsumfang online" (siehe auch Abschnitt 6.1.8) durch einen Administrator aktiviert und deaktiviert werden.

Hinweis: Wenn die Telematikinfrastruktur nicht erreichbar ist, wird die Verbindung zum SIS ebenfalls getrennt. Bis diese Trennung abgeschlossen ist, werden Pakete weiterhin über das SIS geroutet.

4.5.2 Offline-Modus

Sollte sich der RISE Konnektor im Offline-Modus ("Leistungsumfang online" deaktiviert, siehe auch Abschnitt 6.1.8) befinden, sind sämtliche Verbindungen zur Telematikinfrastruktur, dem SIS und den Bestandsnetzen unterbunden. Der Konnektor kann in diesem Betriebsmodus keinesfalls Abfragen von Daten der zentralen Dienste der TI durchführen. Dadurch können auch keine Aktualisierungen der Zertifikatsdaten des Konnektors durchgeführt werden. Erreichen diese Daten das Ende ihrer Gültigkeitsdauer, wechselt der Konnektor automatisch in den kritischen Betriebszustand. Erst wenn entweder der Administrator eine Aktualisierung durch manuelles Hochladen aktueller Zertifikatsdaten auf den RISE Konnektor (siehe Abschnitt 6.3.5) vorgenommen oder den Online-Modus aktiviert hat ("Leistungsumfang online" aktiviert, siehe auch Abschnitt 6.1.8), damit der RISE Konnektor eine automatische Aktualisierung vornehmen kann, wird dieser kritische Betriebszustand wieder verlassen und der RISE Konnektor kann wieder bestimmungsgemäß verwendet werden.

Neben der Deaktivierung der automatischen Aktualisierung von Zertifikatssperrlisten und anderer Zertifikatsdaten deaktiviert der Offline-Modus den Kommunikationskanal zur Telematikinfrastruktur vollständig. Naturgemäß können in diesem Fall die Basisdienste und Fachmodule des Konnektors keine Daten von der zentralen Telematikinfrastruktur abfragen. Somit ist im Offlinemodus der Funktionsumfang des Konnektors eingeschränkt.

4.6 RISE Konnektor Anbindungs-Szenarien im dezentralen Umfeld

Im Folgenden werden zwei Szenarien für die Anbindung des RISE Konnektors an die Zentrale Telematikinfrastruktur bei den Leistungserbringerinstituten beschrieben:

1. Integration in eine beim Leistungserbringer bestehende Infrastruktur

2. Einfache Installation ohne bestehende Infrastruktur beim Leistungserbringer

Die vorliegenden Abbildungen in diesem Kapitel fokussieren auf das dezentrale Umfeld und verzichten daher auf die Darstellung der zentralen Anteile, wie das zentrale Netzwerk der Telematikinfrastruktur, welches über den "VPN-Konzentrator TI" erreichbar ist.

Sicherheitshinweis: Der RISE Konnektor, sowie die Netzwerkkomponenten Switch und IAG (Internet Access Gateway) sind in den folgenden Szenarien zum Schutz vor unerlaubtem Zugriff gemäß den Annahmen des Sicherheitskonzeptes (siehe Abschnitt 4.4) vor unbefugten physischen Zugriffen geschützt installiert.

Hinweis: Beschreibungen zu weiteren Einsatzszenarien des RISE Konnektors stehen auf dem gematik-Fachportal zum Download zur Verfügung. Ein aktueller Downloadlink ist auf der Website des RISE Konnektors zu finden (siehe Abschnitt 2).

Abschnitt 4.6.1 und Abschnitt 4.6.2 beschreiben die zwei angeführten Einsatzszenarien.

4.6.1 Integration des RISE Konnektors in eine bestehende Infrastruktur

Im Falle einer bereits vorhandenen Infrastruktur[8] im dezentralen Bereich können die Produkte der Telematikinfrastruktur, insbesondere der RISE Konnektor, so integriert werden, dass Bestandsanwendungen bereits erprobte Kommunikationswege weiter nutzen können.

Wie in Abbildung 19 beispielhaft dargestellt, existiert bereits eine Infrastruktur, die sowohl einen Internetzugang für die Arbeitsplätze ermöglicht (gestrichelte Linie in türkis), als auch eine Nebenstelle über VPN anbindet (gestrichelte Linie in blau). In diesem Fall wird der Konnektor als zusätzliches Gerät an das bestehende Netzwerk angeschlossen und nutzt den bereits vorhandenen Internetanschluss zur Kommunikation in die Telematikinfrastruktur.

Für die Clientsysteme muss in diesem Szenario, je nach individuellem Anforderungsprofil, entschieden werden, ob das jeweilige Clientsystem über die Telematikinfrastruktur kommunizieren können soll und den gesicherten Internetzugang (SIS) nutzen soll oder nicht.

Soll ein Clientsystem nicht über die Telematikinfrastruktur kommunizieren, bleibt der IAG als Standard-Gateway dieses Clientsystems konfiguriert. In diesem Fall routet der IAG die eingehenden IP-Pakete mit öffentlichen Zieladressen weiter in das Internet. Die gestrichelte Linie in türkis zeigt beispielhaft einen Zugriff in das Internet.

[8] https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/konzepte-und-spezifikationen/, letzter Zugriff 30.04.2020

Soll ein Clientsystem über die Telematikinfrastruktur kommunizieren oder den gesicherten Internetzugang (SIS, Sicherer Internet Service) nutzen, muss der Konnektor als Standard-Gateway konfiguriert werden. In diesem Fall leitet der RISE Konnektor Anfragen, die nicht für ihn bestimmt sind, entweder durch den VPN-Tunnel der TI über die Telematikinfrastruktur in ein angeschlossenes Bestandsnetz (gestrichelte Linie in rot), oder durch den VPN-Tunnel zum SIS in das Internet (gestrichelte Linie in grün). Sollte kein sicherer Internetzugang konfiguriert sein, würde der Konnektor die Anfragen verwerfen und ggf. dem Client ein anderes Gateway (IAG) vorschlagen. Alternativ können die für die Clients erforderlichen Routing-Informationen manuell oder mittels DHCP konfiguriert werden.

Eine Firewall im lokalen Netz, die beispielsweise vor dem LAN-Interface des RISE Konnektors in dem vor physischen Zugriffen geschützten Bereich eingesetzt wird, müssen Ports anhand Abschnitt 4.4.2 freigegeben werden.

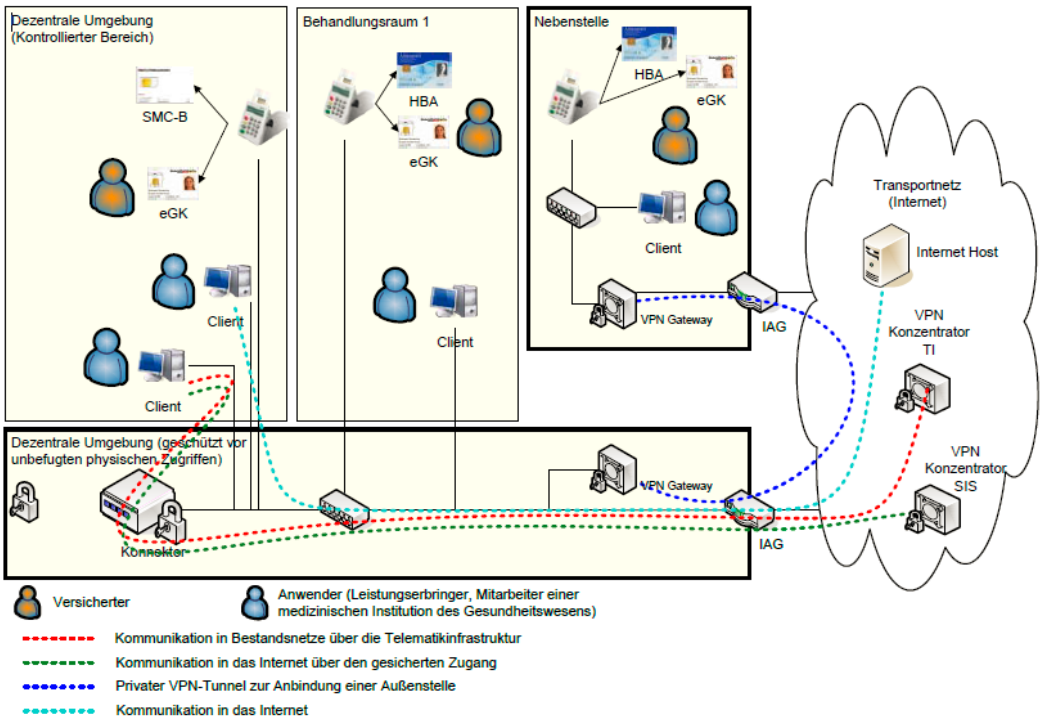


Abbildung 19: Szenario einer Integration der TI-Produkte in eine bestehende Infrastruktur

Voraussetzungen:

- Die bestehende Infrastruktur verfügt über einen Internetzugang
- Verfügbarkeit einer SMC-B und mindestens eines Kartenterminals
- Die Clientsysteme und Kartenterminals und deren Relationen sind dem RISE Konnektor über Konfiguration bekannt gemacht worden.
- Im physikalisch geschützten Bereich befindet sich zwischen Konnektor und IAG die Firewall, über welche sämtliche Verbindungen der Netzwerkinfrastruktur verwaltet werden.

Auswirkungen:

- Der RISE Konnektor kann "minimal-invasiv" in die bestehende Infrastruktur integriert werden. Bestehende Kommunikationswege können weiter genutzt werden.
- Für Clients kann je nach individuellen Anforderungsprofil der sichere Internetzugang über den Konnektor genutzt werden, oder der direkte Internetzugang über den bestehenden IAG

Hinweis: In diesem Szenario kommt die WAN-Schnittstelle des RISE Konnektors nicht zum Einsatz, weil der bestehende Kommunikationsweg über das IAG weiterhin genutzt wird.

4.6.2 Einfache Installation des RISE Konnektors ohne bestehende Infrastruktur beim Leistungserbringer

Abbildung 20 zeigt ein einfaches Szenario[9] für das dezentrale Umfeld. Es wird der RISE Konnektor als Standard-Gateway für jegliche Kommunikation aus dem LAN (Lokales Netzwerk des Leistungserbringers) in das WAN (Internet) eingesetzt. Dabei übernimmt der RISE Konnektor die Weiterleitung der Kommunikation über das Internet in die zu verwendenden Netzwerke (z.B. Zentrale Telematikinfrastruktur). Die Bezeichnung IAG (Internet Access Gateway) steht für die Geräte, die den Internetzugang ermöglichen und typischerweise vom Internet Service Provider (ISP) zur Verfügung gestellt werden (z.B. DSL Router und DSL Modem).

Ein oder mehrere Clientsysteme können über den RISE Konnektor Anwendungsfälle der Telematikinfrastruktur initiieren und über den Konnektor und die Zentrale Telematikinfrastruktur-Plattform in Bestandsnetze kommunizieren (rote gestrichelte Linie). Dabei ist die Nutzung der Anwendungsfälle der Telematikinfrastruktur, je nach Konfiguration des Konnektors, entweder nur authentifizierten Clients oder beliebigen Clients möglich.

In diesem einfachen Szenario werden über ein einziges Kartenterminal die SMC-B, der HBA und auch die eGK des Versicherten gelesen. Es können dazu alternativ jedoch auch mehrere Kartenterminals genutzt werden.

Darüber hinaus können die Clientsysteme über den SIS auf Dienste des Internets zugreifen.

[9] https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/konzepte-und-spezifikationen/, letzter Zugriff 30.04.2020

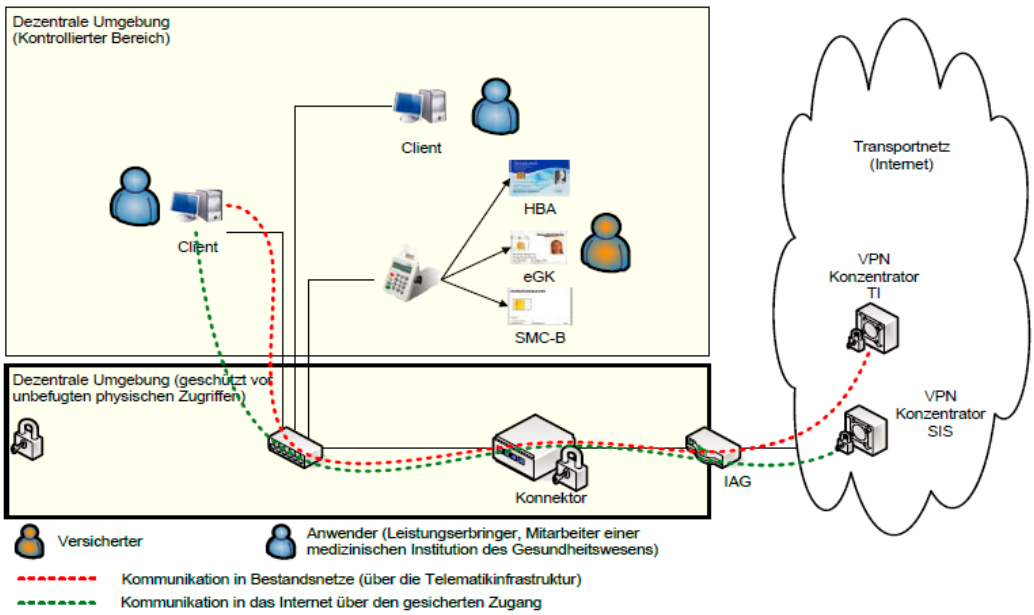


Abbildung 20: Szenario einer einfachen Installation

Voraussetzungen:

- Eine Anbindung der bestehenden Clientsysteme an ein, zum RISE Konnektor kompatibles LAN muss möglich sein.
- Konfiguration des RISE Konnektors als Standard-Gateway in den Clientsystemen und Konfiguration der erforderlichen VPN-Tunnel im RISE Konnektor, um in die verschiedenen Netze weiterzuleiten.
- Verfügbarkeit einer SMC-B

Auswirkungen:

- Die Clientsysteme können über den RISE Konnektor Anwendungsfälle der Telematikinfrastruktur initiieren.
- Die Clientsysteme können über den RISE Konnektor auf das Internet und Bestandsnetze zugreifen.

Hinweis: In diesem Szenario kommt die WAN-Schnittstelle des RISE Konnektors zum Einsatz und wird direkt mit dem IAG verbunden.

4.7 Betriebs- und Fehlerzustände

Fehlerzustände innerhalb des RISE Konnektors treten auf, wenn im Rahmen des operativen Einsatzes bei Komponenten des Konnektors Fehler oder unerwartete Ereignisse eingetreten sind. Diese Fehlerzustände können einen unterschiedlichen Schweregrad aufweisen, welcher von rein informativer Natur (Schweregrad = Info) bis zu schwerwiegend sicherheitskritischer Natur (Schweregrad = Fatal) reicht.

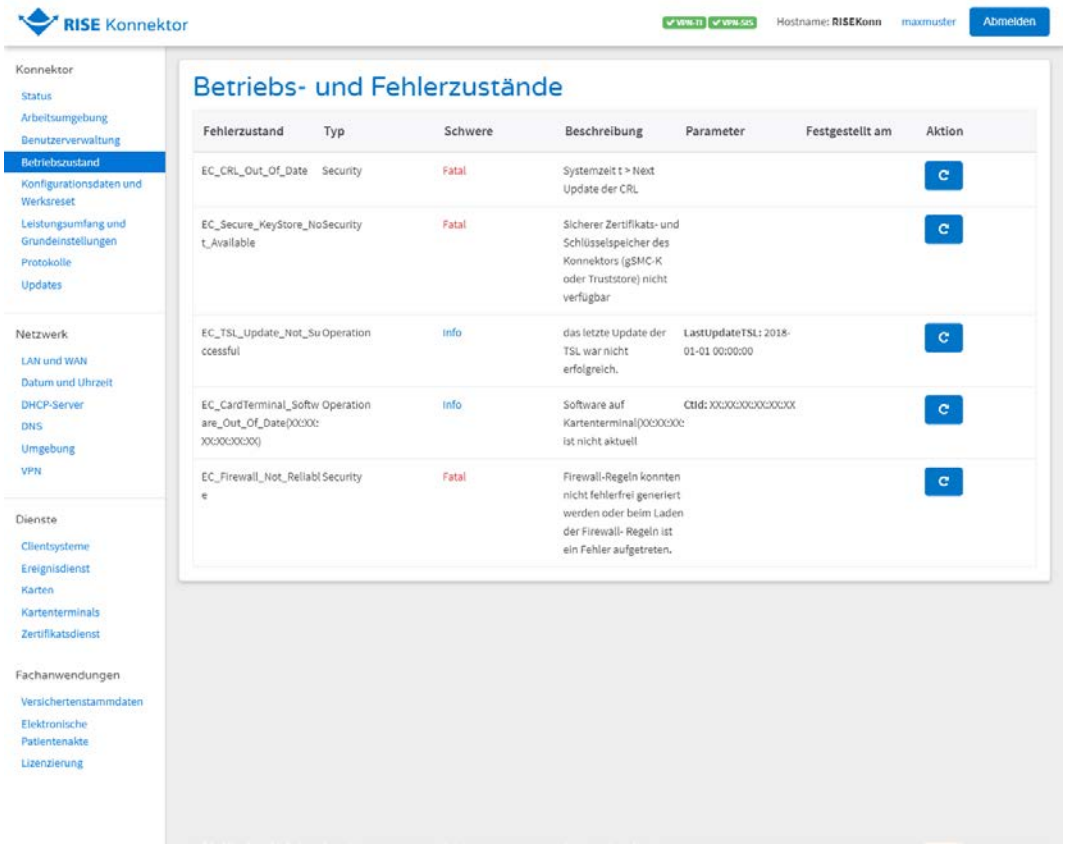


Abbildung 21: Betriebs- und Fehlerzustände

Wenn sich der RISE Konnektor in einem sicherheitskritischen Fehlerzustand (Fatal) befindet, wird dies durch die rote Error-Statusleuchte auf der Frontseite des RISE Konnektors angezeigt (siehe Abbildung 2). Des Weiteren können über die Management-Oberfläche zusätzliche Informationen zum Fehlerzustand entnommen werden.

Nachfolgend werden Fehlerzustände des RISE Konnektors in tabellarischer Form angegeben, wobei die folgenden Eigenschaften der Fehlerzustände berücksichtigt werden:

- **Fehlerzustand** gibt den Namen des Fehlerzustandes an
- **Beschreibung** liefert eine grundlegende Beschreibung des Fehlers
- **Typ** gibt den Protokollierungstyp des Fehlerzustandes an:
  - **Security (Sec)** bedeutet ein Sicherheitsproblem
  - **Operation (Op)** entspricht einer Funktionsstörung
  - **Infrastructure** weist auf ein Problem mit der Infrastruktur hin
- **Schweregrad** gibt den Schweregrad des Fehlerzustandes an:
  - **Info** hat rein informativen Charakter.
  - **Warning** beschreibt eine Warnung, die von einem Administrator behandelt werden sollte.

- **Error** beschreibt einen Fehler, der von einem Administrator behandelt werden muss.
- **Fatal** erfordert die Unterstützung eines Super-Administrators und könnte in weiterer Folge eine Kontaktaufnahme mit dem Händlersupport bedingen (siehe Abschnitt 2).

Hinweis: Unabhängig von den Betriebs- und Fehlerzuständen sind zusätzlich noch Fehlercodes für verschiedene Fehlermeldungen vorhanden (wie z.B. bei der Protokollierungsfunktion in Abschnitt 6.1.2.6).

Herstellerspezifische Fehlercodes werden in der Klasse "RiseErrorMessages" gesammelt und entsprechend aufbereitet.

4.7.1 Kritischer Betriebszustand

Der kritische Betriebszustand des RISE Konnektors bezeichnet jenen Betriebsmodus, welchen der Konnektor annimmt, nachdem ein sicherheitskritischer Fehler im operativen Betrieb zu einem Fehlerzustand des Konnektors geführt hat.

Hierbei können einige unterschiedliche Fehler zu einem sicherheitskritischen Fehlerzustand führen. Eine Liste dieser Zustände ist durch Abschnitt 4.7.1.1. Der kritische Betriebszustand deaktiviert einen Großteil der Funktionen des RISE Konnektors. Unabhängig vom verursachten Fehler, zeichnet sich dieser Betriebszustand durch einen stark eingeschränkten Funktionsumfang aus. Tabelle 6 stellt dar, welche Funktionen unter den angeführten Fehlern nicht mehr zur Verfügung stehen. Diese werden mit einem "-" dargestellt, ein "X" bedeutet, dass die Funktionen weiterhin verwendet werden können.

Ein kritischer Betriebszustand wird durch die entsprechende Statusleuchte auf der Frontseite des Konnektors angezeigt.

Die Ursache für den kritischen Betriebszustand kann anhand der Protokolle des Konnektors diagnostiziert werden. Um den kritischen Betriebszustand aufzuheben, muss ein (Super-) Administrator den auslösenden Fehler durch die Management-Oberfläche beheben. Anschließend geht der Konnektor wiederum in den, durch den Parameter "Leistungsumfang online" (siehe auch Abschnitt 6.1.8) angegebenen, On- beziehungsweise Offlinemodus über.

Abschnitt 4.7.2 listet nicht-kritische und sonstige Fehlerzustände auf, in denen sich der Konnektor befinden kann.

Sämtliche vorgegebenen Betriebs- und Fehlerzustände[10] sind abschließend in der Abschnitt 4.7.1.1 und Abschnitt 4.7.2 aufgelistet.

[10] https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/konzepte-und-spezifikationen/, letzter Zugriff 30.04.2020

4.7.1.1 Aufhebung des kritischen Betriebszustandes

Folgende Lösungsansätze sind bei den jeweilen Zuständen durchzuführen. Die Auflistung folgt dabei dem Format "**Bezeichnung Betriebszustand** (Typ, Schweregrad): Beschreibung. Lösung."

- **EC_CRL_Out_Of_Date** (Security, Fatal): Die Systemzeit liegt über der geplanten Zeit für das nächste Update der CRL – CRL gilt als veraltet. **LÖSUNG:** Import einer CRL auf der Management-Oberfläche (siehe Abschnitt 6.3.5.2). Sollte der Fehlerzustand immer noch bestehen, nehmen Sie bitte Kontakt mit dem Händlersupport auf (siehe Abschnitt 2).
- **EC_Firewall_Not_Reliable** (Security, Fatal): Die Firewall-Regeln konnten nicht fehlerfrei generiert werden oder beim Laden der Firewall-Regeln ist ein Fehler aufgetreten **LÖSUNG:** siehe Abschnitt 4.7.4.
- **EC_Secure_KeyStore_Not_Available** (Security, Fatal): Sicherer Zertifikats- und Schlüsselspeicher des Konnektors (gSMC-K oder Truststore) ist nicht verfügbar. **LÖSUNG:** Neustart des Konnektors. Sollte der Fehlerzustand immer noch bestehen, nehmen Sie bitte Kontakt mit dem Händlersupport auf (siehe Abschnitt 2).
- **EC_Time_Difference_Intolerable** (Security, Fatal): Abweichung zwischen der lokalen Zeit und der per NTP empfangenen Zeit bei der Zeitsynchronisation ist größer als NTP_MAX_TIMEDIFFERENCE. **LÖSUNG:** Der Administrator kann auf der Management-Oberfläche die Zeit manuell setzen (siehe Abschnitt 6.2.2). Danach kann erneut versucht werden, die Zeit des Konnektors zu synchronisieren.
- **EC_Time_Sync_Pending_Critical** (Security, Fatal): MGM_LU_ONLINE=Enabled (siehe auch Abschnitt 6.1.8) und keine erfolgreiche Synchronisation der Systemzeit seit mehr als durch den NTP_GRACE_PERIOD Parameter angegebenen Tagen. **LÖSUNG:** Der Administrator kann auf der Management-Oberfläche die Zeit manuell setzen (siehe Abschnitt 6.2.2). Danach kann erneut versucht werden, die Zeit des Konnektors zu synchronisieren.
- **EC_TSL_Trust_Anchor_Out_Of_Date** (Security, Fatal): Gültigkeit des Vertrauensankers ist abgelaufen. **LÖSUNG:** Import einer TSL auf der Management-Oberfläche (siehe Abschnitt 6.3.5.2). Sollte der Fehlerzustand immer noch bestehen, nehmen Sie bitte Kontakt mit dem Händlersupport auf (siehe Abschnitt 2).
- **EC_TSL_Out_Of_Date_Beyond_Grace_Period** (Security, Fatal): Die Systemzeit liegt über der geplanten Zeit für das nächste Update der TSL, es wurde des Weiteren die durch den CERT_TSL_DEFAULT_GRACE_PERIOD_DAYS Parameter angegebene Grace Period überschritten und eine neue TSL ist nicht verfügbar. **LÖSUNG:** Import einer TSL auf der Management-Oberfläche (siehe Abschnitt 6.3.5.2). Sollte der Fehlerzustand immer noch bestehen, nehmen Sie bitte Kontakt zum Hersteller auf.
- **EC_Security_Log_Not_Writable** (Operational, Fatal): Das Sicherheitslog kann nicht geschrieben werden. **LÖSUNG:** Bitte versuchen Sie, das Problem zu beheben, indem Sie einen niedrigeren Wert als Speicherdauer des Sicherheitsprotokolls auf der Management-Oberfläche konfigurieren (siehe Abschnitt 6.1.2.8). Sollte der Fehlerzustand immer noch bestehen, nehmen Sie Kontakt mit dem Händlersupport auf (siehe Abschnitt 2).

- **EC_Software_Integrity_Check_Failed** (Security, Fatal): Die Integritätsprüfung ist fehlgeschlagen. **LÖSUNG:** siehe Abschnitt 4.7.4.

4.7.1.2 Auswirkungen von sicherheitskritischen Fehlerzuständen

Legende zu Tabelle 6:

1. EC_CRL_Out_Of_Date
2. EC_Firewall_Not_Reliable
3. EC_Secure_KeyStore_Not_Available
4. EC_Time_Difference_Intolerable
5. EC_Time_Sync_Pending_Critical
6. EC_TSL_Trust_Anchor_Out_Of_Date
7. EC_TSL_Out_Of_Date_Beyond_Grace_Period
8. EC_Security_Log_Not_Writable

Funktion	1	2	3	4	5	6	7	8
Kartentransaktionen	-	-	-	X	X	X	-	-
Kartendienst	-	X	X	X	X	X	X	X
Kartenterminaldienst	-	X	X	X	X	X	X	X
Ereignisdienst	-	X	X	X	X	X	X	X
Zertifikatsdienst	-	-	-	X	X	X	X	X
Zeitdienst	-	-	-	X	X	X	-	X
Resource-Information	-	X	X	X	X	X	X	X
Softwareaktualisierung	X	X	X	X	X	X	X	X
Protokolleinsicht	X	X	X	X	X	X	X	X
Werksreset	X	X	X	X	X	X	X	X

Tabelle 6: Auswirkungen von sicherheitskritischen Fehlerzuständen auf den RISE Konnektor

4.7.2 Sonstige Fehlerzustände

Die in in Folge angegebenen Fehlerzustände werden allgemein als "nicht-kritische Fehlerzustände" betrachtet und haben keinen Einfluss auf den aktuell konfigurierten Konnektor Betriebsmodus. Die Auflistung folgt dabei dem Format "**Bezeichnung Betriebszustand** (Typ, Schweregrad): Beschreibung. Lösung."

- **EC_CardTerminal_Software_Out_Of_Date(<ctId>)** (Op, Info): Software auf Kartenterminal (<ctId>) ist nicht aktuell. (<ctId>) identifiziert hierbei das Kartenterminal anhand der im Konnektor eingetragenen Kartenterminal-ID. **LÖSUNG:** Ein Update der Kartenterminalsoftware (Karten Firmwareupdate) kann vom Administrator auf der Management-Oberfläche initiiert werden (siehe Abschnitt 6.1.3).
- **EC_Connector_Software_Out_Of_Date** (Op, Info): Es ist ein Software-Update des RISE Konnektors vorhanden, deren Priorität als "kritisch" eingestuft wurde. **LÖSUNG:** Ein Update der RISE Konnektor Software kann vom Administrator auf der Management-Oberfläche durchgeführt werden (siehe Abschnitt 6.1.3).
- **EC_Time_Sync_Not_Successful** (Op, Info): Der letzte Synchronisationsversuch der Systemzeit war nicht erfolgreich. **LÖSUNG:** Der Administrator kann auf der Management-Oberfläche die Zeit des Konnektors synchronisieren oder alternativ auch manuell setzen (siehe Abschnitt 6.2.2). Nach dem Setzen der neuen Uhrzeit ist ein Neustart des Konnektors erforderlich (siehe Abschnitt 6.1.1).
- **EC_TSL_Update_Not_Successful** (Op, Info): Das letzte Update der TSL war nicht erfolgreich und die vorhandene TSL wird weiterverwendet. **LÖSUNG:** Import einer TSL auf der Management-Oberfläche (siehe Abschnitt 6.3.5.2). Alternativ: Stellen Sie sicher, dass der Konnektor über VPN mit der Telematikinfrastruktur verbunden ist und starten Sie den Konnektor neu.
- **EC_TSL_Expiring** (Sec, Info): Wenn das tägliche Update der TSL wiederholt fehlschlägt, wird der Nutzer 7 Tage vor Ablauf der TSL darüber informiert. **LÖSUNG:** Import einer TSL auf der Management-Oberfläche (siehe Abschnitt 6.3.5.2). Alternativ: Stellen Sie sicher, dass der Konnektor über VPN mit der Telematikinfrastruktur verbunden ist und starten Sie den Konnektor neu.
- **EC_TSL_Trust_Anchor_Expiring** (Sec, Info): Die Gültigkeit des Vertrauensankers der TSL ist noch nicht abgelaufen, läuft aber innerhalb von 30 Tagen ab. **LÖSUNG:** Import einer TSL auf der Management-Oberfläche (siehe Abschnitt 6.3.5.2). Alternativ: Stellen Sie sicher, dass der Konnektor über VPN mit der Telematikinfrastruktur verbunden ist und starten Sie den Konnektor neu.
- **EC_LOG_OVERFLOW** (Op, Warning): Tritt auf, wenn Logging-Einträge überschrieben werden, die nicht älter sind als die konfigurierte Speicherdauer. (siehe auch Abschnitt 6.1.2.8) **LÖSUNG:** Der Fehlerzustand kann nur durch einen Administrator manuell auf der Management-Oberfläche wieder zurückgesetzt werden (Button "Zurücksetzen" bei der Fehlermeldung).
- **EC_CRL_Expiring** (Sec, Warning): Das nächste geplante Update der CRL wird in weniger als 3 Tagen zum Zeitpunkt der Meldung fällig. **LÖSUNG:** Import einer CRL auf der Management-Oberfläche (siehe Abschnitt 6.3.5.2). Alternativ: Stellen Sie sicher, dass der Konnektor über VPN mit der Telematikinfrastruktur verbunden ist und starten Sie den Konnektor neu.
- **EC_Time_Sync_Pending_Warning** (Sec, Warning): Der Online-Betriebsmodus des Konnektors ist aktiviert (MGM_LU_ONLINE=Enabled) (siehe auch Abschnitt 6.1.8) und es konnte seit mehr als durch den NTP_WARN_PERIOD Parameter angegebenen Tagen keine erfolgreiche Synchronisation der Systemzeit stattfinden. Hierbei wurde allerdings die durch den NTP_GRACE_PERIOD Parameter angegebene Grace Period noch nicht

überschritten. **LÖSUNG:** Der Administrator kann auf der Management-Oberfläche die Zeit des Konnektors synchronisieren (siehe Abschnitt 6.2.2).

- **EC_TSL_Out_Of_Date_Within_Grace_Period** (Sec, Warning): Die Systemzeit liegt nach der geplanten Zeit für das nächste Update der TSL und die durch den CERT_TSL_DEFAULT_GRACE_-PERIOD_DAYS Parameter angegebene Grace Period wurde überschritten. Eine neue TSL ist nicht verfügbar. **LÖSUNG:** Import einer TSL auf der Management-Oberfläche (siehe Abschnitt 6.3.5.2). Alternativ: Stellen Sie sicher, dass der Konnektor über VPN mit der Telematikinfrastruktur verbunden ist und starten Sie den Konnektor neu.
- **EC_CardTerminal_Not_Available (<ctId>)** (Op, Error): Kartenterminal (<ctId>) ist nicht verfügbar. Dieser Betriebszustand bezieht sich auf die als "aktiv" gekennzeichneten Kartenterminals. (<ctId>) identifiziert hierbei das Kartenterminal anhand der im Konnektor eingetragenen Kartenterminal-ID. **LÖSUNG:** Der Administrator kann die Kartenterminals in der Management-Oberfläche suchen und hinzufügen (siehe Abschnitt 6.3.4).
- **EC_No_VPN_TI_Connection** (Op, Error): Kein sicherer Kanal (VPN) in die Telematikinfrastruktur aufgebaut. **LÖSUNG:** Der Administrator kann über die Management-Oberfläche erneut versuchen, den Konnektor über VPN mit der Telematikinfrastruktur zu verbinden (siehe Abschnitt 6.2.6.1).
- **EC_No_VPN_SIS_Connection** (Op, Error): Kein sicherer Kanal (VPN) zu den Sicheren Internet Services aufgebaut. **LÖSUNG:** Der Administrator kann über die Management-Oberfläche erneut versuchen, den Konnektor über VPN mit der Sicheren Internet Service (SIS) zu verbinden (siehe Abschnitt 6.2.6.1).
- **EC_No_Online_Connection** (Op, Error): Der RISE Konnektor kann Dienste im Transportnetz nicht erreichen. **LÖSUNG:** Der Administrator kann in der Management-Oberfläche Konfigurationen die Netzwerk-Konfiguration prüfen und verändern (siehe Abschnitt 6.2.1).
- **EC_IP_Adresses_Not_Available** (Sec, Error): Die IP-Adressen des Konnektors sind nicht oder falsch gesetzt. **LÖSUNG:** Der Administrator kann in der Management-Oberfläche die IP-Adressen des Konnektors überprüfen und korrigieren (siehe Abschnitt 6.2.1).
- **EC_CRYPTOPERATION_ALARM** (Sec, Warning): Es wurde ein potentieller Missbrauch einer kryptographischen Operation erkannt. **LÖSUNG:** Der Administrator muss die sichere Umgebung mit Hinblick auf potentiellen Missbrauch kontrollieren. Nach abgeschlossener Analyse kann ausschließlich ein Administrator auf der Management-Oberfläche den Fehlerzustand beenden, in dem er den Zähler der Crypto-Operationen zurücksetzt (Button "Zurücksetzen" bei der Fehlermeldung).

4.7.3 Keine aktive Verbindung ins LAN

Der RISE Konnektor benötigt für den regulären Betrieb eine aktive Verbindung in das LAN der Leistungserbringer-Institution. Zeigt die Signalisierung das in Tabelle 7 beschriebene Muster, prüfen Sie, ob es über das LAN-Kabel eine aktive Verbindung zum lokalen Netz des Leistungserbringers gibt.

TI	SIS	Error	Bedeutung
Orange	Aus	Orange	Keine aktive Verbindung in das LAN des Leistungserbringers

Tabelle 7: LED-Signalisierung des RISE Konnektors, wenn keine aktive Verbindung ins LAN besteht

4.7.4 Abgesicherter Modus

Der RISE Konnektor führt beim Starten und auf Anfrage Integritätsprüfungen (siehe Abschnitt 6.1.1.3) und während des Betriebs Prüfungen der Firewall-Regeln durch. Wird bei der Prüfung einer Firewall-Regel oder der Integrität ein Problem festgestellt, fällt der RISE Konnektor in einen abgesicherten Modus zurück. Es ist dann keine Kommunikation über die Netzwerkschnittstellen mehr möglich.

Ein weiterer Fall, in dem der Konnektor während des Betriebs in den abgesicherten Modus versetzt wird, liegt vor, wenn es während einem ECC-Vertrauensraumwechsel zu einem inkonsistenten Systemzustand kommt (siehe Abschnitt 6.3.5.2).

Sie erkennen den abgesicherten Modus an der in Tabelle 8 beschriebenen Signalisierung.

TI	SIS	Error	Bedeutung
Orange	Orange	Rot	Prüfung der Firewall-Regeln fehlgeschlagen (EC_FIREWALL_NOT_RELIABLE)
Rot	Rot	Rot	Fehler beim Prüfen der Integrität

Tabelle 8: LED-Signalisierung des RISE Konnektors im abgesicherten Modus

Hinweis: Signalisiert der RISE Konnektor den abgesicherten Modus, kontaktieren Sie umgehend den Händlersupport (siehe Abschnitt 2).

4.8 Erstellung und Verifikation von Signaturen

Sicherheitshinweis: Der Benutzer des Clientsystems muss vor der Übermittlung von Dokumenten an den RISE Konnektor sicherstellen, dass er nur solche Daten zur Signaturerzeugung und zur Signaturprüfung über sein Clientsystem an den RISE Konnektor übergibt, welche er auch tatsächlich signieren bzw. verifizieren will.

Sicherheitshinweis: Das Clientsystem stellt im Rahmen der Erzeugung und Prüfung einer QES die Dokumente, Zertifikate, Jobnummer und Fortschrittsanzeige der Stapelsignatur korrekt und vertrauenswürdig dar und ermöglicht die Nutzung der vom RISE Konnektor angebotenen Abbruch-Funktion der Stapelsignatur.

4.8.1 Gebrauch der Jobnummer

Beim Signieren von Dokumenten ist die Eingabe einer PIN erforderlich.

Warnung: Die PIN darf über die Tastatur des eHealth-Kartenterminals nur dann eingeben werden, wenn am Signaturproxy bzw. am Primärsystem und am Display des Kartenterminals die gleiche Jobnummer angezeigt wird. Stimmen die beiden Nummern nicht überein, so darf die PIN nicht eingegeben werden und es müssen weitergehende Schritte zur Klärung des aufgetretenen Fehlverhaltens eingeleitet werden.

4.8.2 Komfortsignatur

Ist die Komfortsignatur aktiviert (siehe Abschnitt 6.1.8), so muss für die in den Einstellungen angegebene Anzahl an Signaturen beziehungsweise den ebenfalls dort angegebenen Zeitraum die PIN des verwendeten HBA nicht erneut verifiziert werden.

4.8.2.1 Aktivierung

Um die Komfortsignatur zu aktivieren, muss der in Abschnitt 6.1.8 beschriebene Parameter SAK_COMFORT_SIGNATURE aktiviert werden, was nur möglich ist, wenn auch ANCL_TLS_MANDATORY und ANCL_CAUT_MANDATORY aktiviert sind. Ist dies nicht der Fall, so erscheint ein entsprechender Hinweis (siehe Abbildung 22). Nach der Aktivierung von SAK_COMFORT_SIGNATURE und der Festlegung der gewünschten Parameter für die maximale Anzahl der Signaturen beziehungsweise dem maximalen Zeitraum der Komfortsignatur werden diese Änderungen durch einen Klick auf “Speichern” bestätigt. Anschließend erscheint auf dem entsprechenden Kartenterminal die folgende Aufforderung, die PIN.QES des gesteckten Heilberufsausweises einzugeben:

Eingabe Signatur-PIN HBA
PIN.QES:

Wurde diese erfolgreich verifiziert, so ist die Komfortsignatur aktiviert.

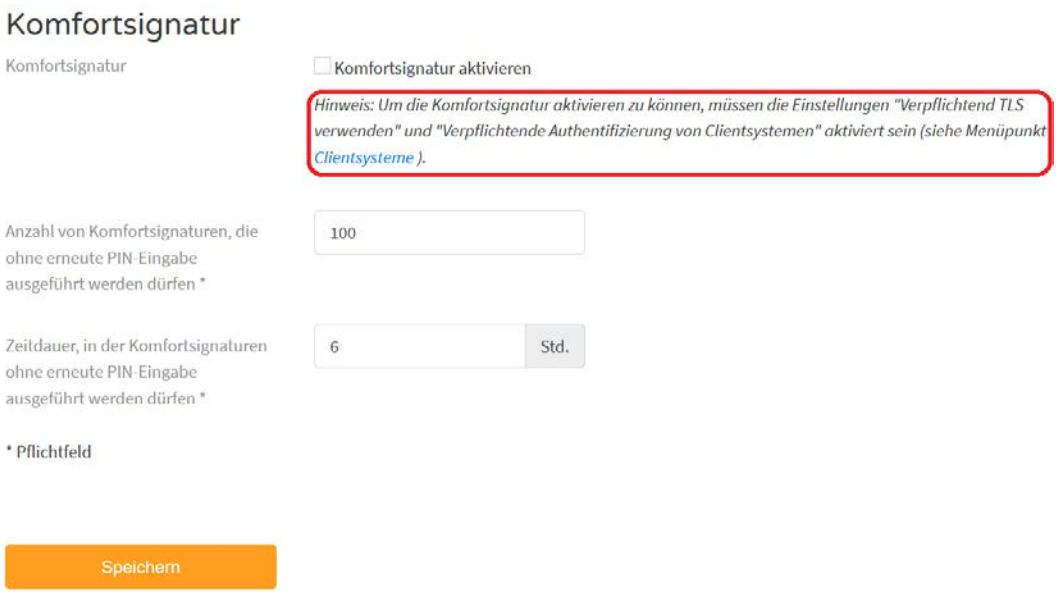


Abbildung 22: Hinweis beim Aktivieren der Komfortsignatur

4.8.2.2 Deaktivierung

Um die Komfortsignatur zu deaktivieren gibt es mehrere Möglichkeiten:

- Der Parameter SAK_COMFORT_SIGNATURE kann direkt deaktiviert und diese Änderung gespeichert werden, was eine Deaktivierung der Komfortsignaturfunktion für alle HBA bewirkt, für die diese Funktion aktiviert wurde.
- Einer der beiden Parameter ANCL_TLS_MANDATORY und ANCL_CAUT_MANDATORY kann deaktiviert werden, was gemeinsam mit einem entsprechenden Hinweis (siehe Abbildung 23) eine automatische Deaktivierung der Komfortsignaturfunktion für alle HBA bewirkt, für die diese Funktion aktiviert wurde.
- Läuft entweder der interne Timer (festgelegt durch SAK_COMFORT_SIGNATURE_TIMER) oder der interne Counter (festgelegt durch SAK_COMFORT_SIGNATURE_MAX) der Komfortsignatur eines bestimmten HBAs ab, so wird die Komfortsignaturfunktion nur konkret für diesen HBA automatisch deaktiviert.

Hinweis: Ist ein Signaturprozess im Gange, wenn der Timer abläuft, so wird dieser Signaturvorgang noch vollständig abgeschlossen und die Komfortsignatur erst im Anschluss daran deaktiviert.

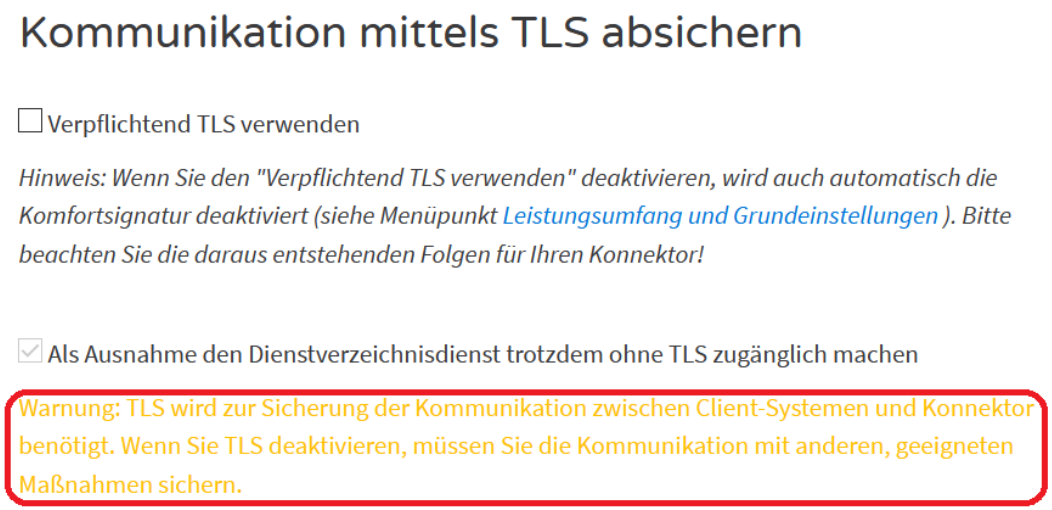


Abbildung 23: Hinweis beim Deaktivieren der Komfortsignatur

4.8.2.3 Signaturerstellung

Die Erstellung einer Signatur folgt im Falle einer aktiven Komfortsignatur dem Ablauf der anderen möglichen Signaturmodi mit dem Unterschied, dass keine erneute PIN-Eingabe und -Verifikation pro Signatur benötigt wird.

4.8.3 Externe Authentisierung

Es ist möglich, zum Zweck der externen Authentisierung, Binärstrings zu signieren.

Warnung: Das Signaturformat PKCS#1 darf nur zu Authentisierungszwecken mit dem Authentisierungsschlüssel des HBAx und des SM-B verwendet werden.

4.8.4 Signaturrichtlinien

Der RISE Konnektor setzt zur Erstellung und Verifikation von Signaturen Signaturrichtlinien um. Diese sind in Abschnitt 8 detailliert ausgeführt.

Sicherheitshinweis: Der Administrator muss Anwender umgehend informieren und sich um das Aufspielen einer neuen Firmware kümmern, sobald bekannt wird, dass mindestens ein Algorithmus des RISE Konnektors nicht mehr für QES-Signatur-Erzeugung und/oder für QES-Signatur-Verifikation geeignet ist.

Sicherheitshinweis: Externe Komponenten, die in der Betriebsumgebung des Konnektors XML-Daten und PDF-Dokumente verarbeiten und anzeigen, müssen sich selbst vor möglichen XML- bzw. PDF-Angriffen (bspw. auf die Anzeigekomponente) schützen.

4.8.5 Signaturprüfungsergebnis

Bei einem verminderten Beweiswert liefert eine Signaturprüfung als Rückgabewert "INCONCLUSIVE". Dies ist der Fall, wenn der OCSP-Server (aufgrund fehlender TI-Verbindung) nicht erreicht werden kann.

Im Ergebnis der Korrektheitsprüdung einer digitalen Signatur, dem "VerificationReport", wird die Suitability der verwendeten Algorithmen im Feld "/VerificationReport/IndividualReport/Details/DetailedSignatureReport/SignatureOK/SignatureAlgorithm" angegeben.

Wurde eine Signatur nicht mit einem Algorithmus aus der folgenden Liste unterstützter Algorithmen erstellt, so wird diese als "INVALID" ausgewiesen.

- SHA-256, SHA-384, SHA-512
- RSASSA-PSS nach PKCS#1
- RSASSA-PKCS1-v1_5 nach PKCS#1
- bei RSA muss ein Modulus zwischen 1976 bis 4096 Bit verwendbar sein
- ECDSA basierend auf E(F_p) auf der Kurve P256r1

Sicherheitshinweis: Das Clientsystem ist selbst dafür verantwortlich, vom Konnektor gelieferte Signaturverifikationsergebnisse korrekt und integer darzustellen.

4.9 Ver- und Entschlüsselung von Dokumenten

Bei der Ver- und Entschlüsselung von Dokumenten führt der RISE Konnektor keine Dokumentvalidierung durch. Der Aufrufer ist daher selbst dafür verantwortlich, erforderliche Validierungen vor oder nach der Operation durchzuführen.

Sicherheitshinweis: Die verwendeten CA-Zertifikate sollen eine Schlüssellänge von mind. 2048 bit aufweisen und die Extension "X509v3 Subject Key Identifier" und "X509v3 Authority Key Identifier" enthalten.

5 Benutzerrollen

5.1 Benutzerrollenübersicht

Der RISE Konnektor umfasst die folgenden drei Benutzerrollen. Im Rahmen dieses Dokumentes werden die lokalen Benutzerrollen "Leistungserbringer", "Administrator" und "Super-Administrator" betrachtet.

- **Leistungserbringer:** Unter dieser Benutzerrolle werden sämtliche Clientsysteme innerhalb des lokalen Netzwerkes des Leistungserbringers verstanden, welche auf die Funktionen des Konnektors zugreifen. Diese Systeme nutzen die Funktionalität zum Verbindungsaufbau zur Telematikinfrastruktur, deren Sicheren Internet Service (SIS), oder unterschiedliche Funktionen der Fachmodule und Basisdienste des Konnektors.
- **Administrator:** Unter der Rolle des Administrators versteht man jene Benutzerrolle, welche dazu ermächtigt ist, die Konfiguration des RISE Konnektors vorzunehmen. Diese Benutzerrolle besitzt vielfältige Berechtigungen, um die jeweiligen Einstellungen der einzelnen Komponenten oder Dienste des Konnektors zu konfigurieren und so an ihre Betriebsumgebung und -aufgaben anzupassen. Bei "Administrator" handelt es sich um die Standard Administratorenrolle, welche hauptsächlich lokal im Netzwerk des Leistungserbringers die Konfiguration des RISE Konnektors durchführt und im Weiteren als "Administrator" bezeichnet wird. Die Benutzerdatenverwaltung ist den lokalen Administratoren jedoch nicht zugänglich, sondern kann nur von einem Super-Administrator durchgeführt werden.
- **Super-Administrator:** Die Super-Administratorrolle stellt prinzipiell einen Spezialfall des lokalen Administrators dar, welcher zusätzlich zu den bereits dargelegten Administratorrechten die Benutzerkontenverwaltung verantwortet.

Tabelle 9 erläutert die Berechtigungsstufen der unterschiedlichen Administratorrollen des RISE Konnektors.

Administrator	Zugriff zu Management-Oberfläche	Verwaltet	Ausgenommen
Lokaler Administrator	Lokaler Endpunkt	Konfigurationsdaten, Werksreset	Benutzerverwaltung, Import von Konfigurationen
Super-Administrator	Lokaler Endpunkt	Konfigurationsdaten, Benutzerverwaltung und Werksreset	

Tabelle 9: Benutzerrollen des RISE Konnektors

Sicherheitshinweis: Beim Verlassen des Arbeitsplatzes muss jeder Administrator seinen Computer sperren oder sich ausloggen, um einen nicht-autorisierten Zugriff auf den RISE Konnektor zu unterbinden.

Sicherheitshinweis: Nach 20 Minuten Inaktivität oder spätestens nach 4 Stunden müssen Sie sich aus Sicherheitsgründen neu am RISE Konnektor anmelden.

5.2 Benutzerrolle “Leistungserbringer”

5.2.1 Beschreibung

Der Leistungserbringer ist der Hauptnutzer des Konnektors in all seinen Funktionalitäten.

Der Leistungserbringer ist auch für die Sicherheit der Betriebsumgebung sowie zur Wahrung eines fachgerechten Betriebs verantwortlich. Zur Bereitstellung und Wahrung der sicheren Einsatzumgebung des RISE Konnektors müssen die genannten Richtlinien und Kernpunkte aus Abschnitt 4.4.3 eingehalten werden.

Die Nutzung der Funktionalitäten des Konnektors basiert auf der Verwendung eines oder mehrerer geeigneter Clientsysteme, wie etwa einer Praxisverwaltungssoftware (PVS), eines Krankenhausinformationssystems (KIS) oder einer Apothekenverwaltungssoftware (AVS). Diese Clientsysteme müssen über entsprechende Schnittstellen verfügen, welche die Funktionalitäten des Konnektors ansprechen.

5.2.2 Benutzerrechte

Leistungserbringer führen über den RISE Konnektor fachliche Funktionen durch. Keinesfalls können Leistungserbringer Konfigurationen des Konnektors ändern. Dies ist aus Sicherheitsgründen auf die Rollen der (Super-) Administratoren eingeschränkt.

5.3 Benutzerrolle “Administrator”

5.3.1 Beschreibung

Der Administrator ist gemäß Abschnitt 5.1 eine der drei im Rahmen dieses Dokumentes vorgestellten Benutzerrollen und ist dazu befähigt, unterschiedliche Konfigurationen im Rahmen des RISE Konnektors zu verändern.

Im Gegensatz zu der in Abschnitt 5.2 besprochenen Benutzerrolle des Leistungserbringers, greift der Administrator nicht primär über Clientsysteme auf die Funktionen des RISE Konnektors zu, sondern nutzt die RISE Konnektor Management-Oberfläche, um die unterschiedlichen Konfigurationsparameter einzustellen. Um Zugriff auf die Konfigurationsoptionen zu erhalten, muss sich der Administrator an der Management-Oberfläche des Managementdienstes authentifizieren. Nach erfolgreich durchgeführter Authentifizierung wird ihm über

die Management-Oberfläche die entsprechende Funktionalität zur Administrierung des RISE Konnektors zur Verfügung gestellt.

5.3.2 Benutzerrechte

Die Benutzerrolle des Administrators umfasst sicherheitskritische Konfigurationen, welche zum Erhalt eines sicheren Betriebes des Konnektors administriert und kontrolliert werden müssen. So lassen sich im Rahmen der Konfigurierbarkeit des RISE Konnektors die folgenden Komponenten identifizieren (sofern vom Super-Administrator die entsprechenden Berechtigungen gewährt bzw. nicht entfernt wurden):

- Der Administrator kann sämtliche in Abschnitt 6 beschriebenen Funktionalitäten konfigurieren, mit Ausnahme der Benutzerverwaltung (siehe Abschnitt 6.1.5) und dem Importieren von Konfigurationsdaten (siehe Abschnitt 6.1.7.2), dies ist lediglich einem Super-Administrator vorbehalten.
- In den Standard-Berechtigungen des Administrators ist der Werksreset deaktiviert. Der Super-Administrator kann den Administrator dazu berechtigen.

Eine Übersicht über alle Berechtigungen, die der Administrator standardmäßig hat, ist in Abbildung 63 zu sehen. Die in der Grafik nicht ausgewählten/ausgegrauten Rechte, sind jene, die einem Administrator auch nicht zugewiesen werden können und zu jeder Zeit nur einem Super-Administrator vorbehalten sind.

Warnung: Eine Fehlkonfiguration der angeführten Parameter kann zu einem Ausfall der Funktionalität im Netzwerk des Leistungserbringerinstitutes führen.

In Abschnitt 6 werden die einzelnen Komponenten und deren Parametrisierung erklärt.

5.4 Benutzerrolle “Super-Administrator”

5.4.1 Beschreibung

Der Super-Administrator ist gemäß Abschnitt 5.1 eine Benutzerrolle, welche über dieselben Rechte wie der Administrator verfügt und führt, genau wie dieser, die Konfiguration über die Management-Oberfläche des RISE Konnektors durch. Zusätzlich zu den Administrator-Rechten kann der Super-Administrator die Benutzerkonten verwalten (siehe Abschnitt 6.1.5.1). Dazu gehört auch die Vergabe von Zugriffsrechten bezüglich der Konfigurationsbereiche. Des Weiteren kann der Super-Administrator ein Werksreset (siehe Abschnitt 3.4.1) durchführen, Konfigurationsdaten importieren bzw. in der Benutzerverwaltung einen Administrator dazu berechtigen, dies zu tun.

Die Berechtigungen eines Super-Administrators sind in Abbildung 62 zu sehen.

Hinweis: Ein Werksreset ohne Kenntnis des Werksreset-Tokens kann entweder von einem Super-Administrator selbst durchgeführt werden oder von einem lokalen Administrator, der in der Benutzerverwaltung vom Super-Administrator dazu berechtigt wurde.

5.4.2 Benutzerrechte

Der Super-Administrator verfügt, zusätzlich zu den Rechten eines Administrators, noch über die in Tabelle 10 gelisteten Rechte.

ReferenzID	Belegung	Bedeutung
MGM_USER_LIST	Liste von Benutzernamen und deren Kontaktdaten	Liste von Benutzern und deren Kontaktdaten. Benutzerkonten müssen angelegt, geändert und gelöscht werden können. Das Passwort eines Benutzerkontos muss neu gesetzt werden können (siehe Abschnitt 6.1.5).
MGM_ADMIN_RIGHTS	Liste von Zugriffsrechten eines Benutzers	Eindeutige Zuordnung eines Benutzerkontos zu einer Rolle.

Tabelle 10: Zusätzliche Rechte des Super-Administrators

Gewähren/Entziehen von Rechten für Benutzerkonten (Ergänzung zu Tabelle 10, ReferenzID "MGM_ADMIN_RIGHTS"):

- Zugriffsrechte auf die unterschiedlichen Konfigurationsbereiche
- Recht für ein Werksreset (USER_RESET_PERMISSION)

Darüber hinaus hat ein Super-Administrator noch folgende Berechtigungen:

- Zeitraum für Passwortwechsel setzen: Der Super-Administrator hat die Möglichkeit, einen Zeitraum zu setzen (Voreinstellung: 120 Tage), nach dem der RISE Konnektor einen Passwortwechsel beim Login des Benutzers initiiert. (Menüpunkt "Benutzerverwaltung" – Reiter "Konfiguration" – siehe Abschnitt 6.1.5.1)
- Import von Konfigurationsdaten: Der Super-Administrator hat die Berechtigung, Konfigurationsdaten zu importieren (siehe Abschnitt 6.1.7.2).

Sicherheitswarnung: Die Rechteverwaltung der Benutzer und der Administratoren hat hohe sicherheitskritische Auswirkungen auf das Gesamtsystem des Leistungserbringerinstitutes.

6 Konfiguration der Komponenten des RISE Konnektors

Der RISE Konnektor wird über die Management-Oberfläche administriert.

Die unterschiedlichen RISE Konnektor-Benutzermasken, Konfigurationsparameter und Statusanzeigen werden durch das dieses Kapitel beschrieben. Es dient den Administratoren des Leistungserbringerinstitutes als Hilfestellung bei der Konfiguration des RISE Konnektors.

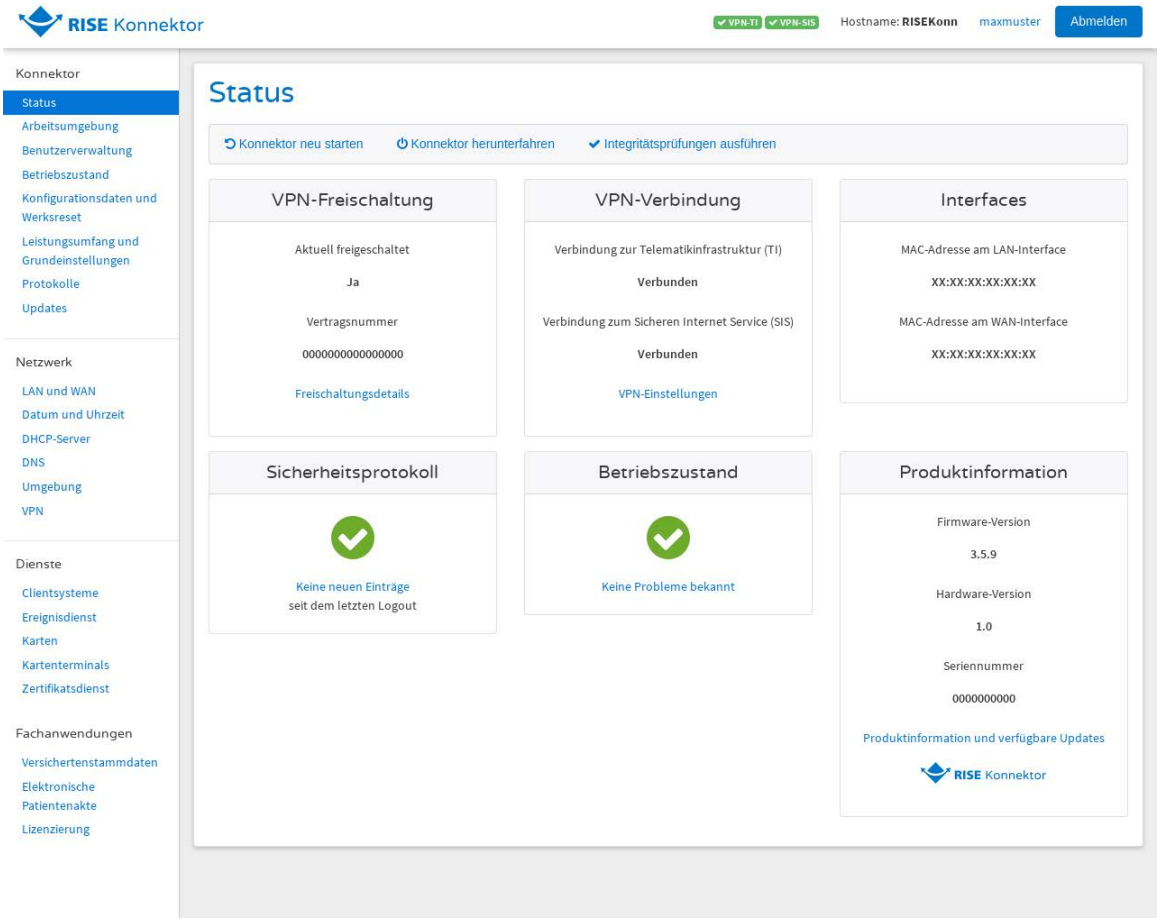


Abbildung 24: RISE Konnektor Management-Oberfläche

Die linke Seite der Management-Oberfläche (siehe Abbildung 24) zeigt das Menü des Konnektors. Unterhalb der vier Hauptmenüeinträge ("Konnektor", "Netzwerk", "Dienste" und "Fachanwendungen") befinden sich jeweils Untermenüs, in denen diverse Konfigurationen und Einstellungen des Konnektors eingesehen bzw. geändert werden können.

In der rechten oberen Ecke der Management-Oberfläche (siehe Abbildung 24) findet sich wiederum der Hostname des Konnektors, der Benutzername des aktuell eingeloggten Users, sowie ein Button für das Logout. Beim Klick auf den

Benutzernamen können Einstellungen zum jeweiligen Benutzer vorgenommen werden.

Eine genaue Beschreibung der eigentlichen Status-Seite ist in Abschnitt 6.1.1 zu finden.

In den folgenden Abschnitten werden jetzt die einzelnen Menüpunkte des Konnektors inkl. Screenshots beschrieben. Die in den Screenshots ersichtlichen Konfigurationsparameter werden in Tabellenform beschrieben. In der Spalte "ReferenzID" ist hier jeweils die Bezeichnung im Screenshot zu finden inkl. der in Klammer geschriebenen technischen Bezeichnung des Parameters.

Sicherheitshinweis: Die Administrator-Rollen können die folgenden Einstellungen am RISE Konnektor mandantenübergreifend vornehmen. Jeder Administrator hat sicherzustellen, dass sämtliche Sicherheitsvorgaben aller beteiligten Mandanten umgesetzt werden. Bei Änderungen von Einstellungen hat der Administrator vorab die Zustimmung aller Mandanten einzuholen. Ohne diese Zustimmung aller Mandaten darf eine Änderung nicht vorgenommen werden. Sind Vorgaben der Mandanten widersprüchlich, wird daher empfohlen, mehrere RISE Konnektoren mit entsprechend unterschiedlichen Einstellungen zu verwenden.

6.1 Konfigurationsmenü des RISE Konnektors

Das Konfigurationsmenü des RISE Konnektors setzt sich aus mehreren Unterpunkten zusammen, die in Abschnitt 6.1.1 bis Abschnitt 6.1.8 im Detail erläutert werden:

- RISE Konnektor Status (Abschnitt 6.1.1)
- RISE Konnektor Protokolle (Abschnitt 6.1.2)
- RISE Konnektor Updates (Abschnitt 6.1.3)
- RISE Konnektor Arbeitsumgebung (Abschnitt 6.1.4)
- RISE Konnektor Betriebszustand (Abschnitt 6.1.6)
- RISE Konnektor Konfigurationsdaten und Werksreset (Abschnitt 6.1.7)
- RISE Konnektor Leistungsumfang und Grundeinstellungen (Abschnitt 6.1.8)
- RISE Konnektor Benutzereinstellungen (Abschnitt 6.1.9)

6.1.1 RISE Konnektor Status

6.1.1.1 Übersicht

Der Konnektor Status (siehe Abbildung 24) ist zugleich die Startseite, die beim Öffnen der Management-Oberfläche nach einem erfolgreichen Login angezeigt wird.

Der Benutzer erhält dabei eine Übersicht über die wichtigsten Parameter des aktuellen Zustands des RISE Konnektors. Dies sind Informationen zu:

- **VPN-Freischaltung:** Direktlink zur Freischaltung und Anzeige, ob VPN aktuell freigeschaltet ist und die Vertragsnummer.
- **VPN-Verbindung:** Verbindungsstatus des VPN zur Telematikinfrastruktur (TI) bzw. Sicheren Internet Service (SIS)
- **Interfaces:** MAC-Adressen am LAN- und WAN-Interface
- **Sicherheitsprotokoll:** Direktlink auf neue Protokolleinträge
- **Betriebszustand:** Fehler und Warnungen werden mit einem Symbol dargestellt mit Direktlink zum Betriebszustand-Menüpunkt.
- **Produktinformation:** Aktuelle Firmware-Version, Hardware-Version und die Seriennummer des RISE Konnektors.
- **Status des Vertrauensraumes:** siehe Abschnitt 6.3.5.1

Des Weiteren besteht auf dieser Seite im oberen Bereich auch die Möglichkeit, den Konnektor neu zu starten, herunterzufahren oder Integritätsprüfungen (Selbsttests) durchzuführen.

6.1.1.2 RISE Konnektor neu starten oder herunterfahren

Um den RISE Konnektor neu zu starten oder herunterzufahren, wählen Sie die entsprechende Funktion. Bevor der Neustart bzw. das Herunterfahren tatsächlich durchgeführt werden, muss die in Abbildung 25 bzw. Abbildung 26 abgebildete Sicherheitsabfrage bestätigt werden.

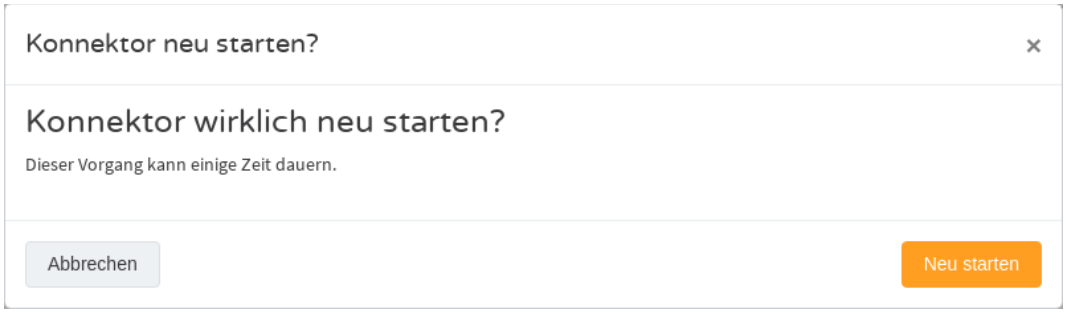


Abbildung 25: RISE Konnektor neu starten

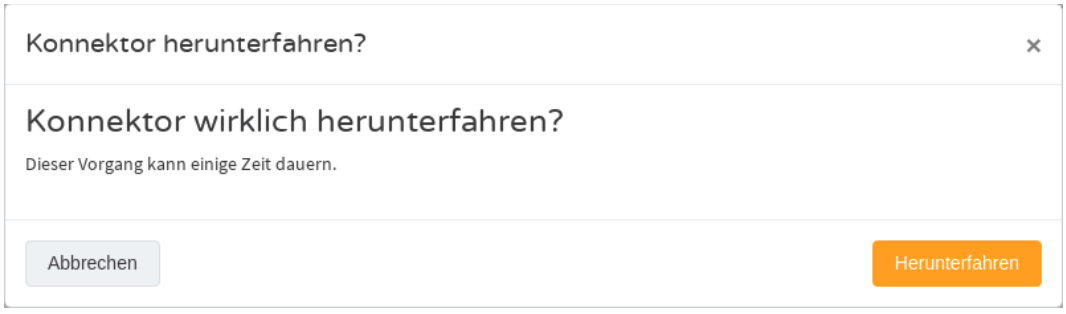


Abbildung 26: RISE Konnektor herunterfahren

Warnung: Während der RISE Konnektor neu startet bzw. heruntergefahren wird/ist, stehen dem Leistungserbringer sämtliche Funktionen nicht mehr zur Verfügung. Informieren Sie daher das Personal des Leistungserbringers rechtzeitig, wenn Sie planen, den RISE Konnektor neu zu starten bzw. herunterzufahren.

Sicherheitshinweis: Bevor Sie den RISE Konnektor von der Stromversorgung trennen, wird generell empfohlen, diesen vorher immer herunterzufahren.

6.1.1.3 Integritätsprüfungen ausführen

Der RISE Konnektor bietet die Möglichkeit, Integritätsprüfungen durchzuführen. Wählen Sie dazu die entsprechende Funktion. Dabei werden die Integrität des ausgeführten Programmcodes und die Sicherheitsfunktionalitäten geprüft. Die Prüfung kann jederzeit erfolgen und stört den laufenden Betrieb nicht.

Sicherheitshinweis: Lösen Sie die Integritätsprüfung regelmäßig aus.

Hinweis: Sollte eine der Integritätsprüfungen fehlschlagen, fällt der Konnektor in den abgesicherten Modus (siehe Abschnitt 4.7.4).

6.1.2 RISE Konnektor Protokolle

Der RISE Konnektor protokolliert system- und sicherheitsrelevante Ereignisse, sowie Ereignisse im Kontext der Performancemessung innerhalb des Konnektors. Auch Ereignisse von Fachmodulen können protokolliert werden. Dabei unterscheidet der RISE Konnektor zwischen System- und Sicherheitsprotokoll, sowie Fachmodulprotokollen. Je Fachmodul ist ein getrenntes Protokoll vorhanden.

Im Sicherheitsprotokoll werden alle Ereignisse eingetragen, die Auswirkungen auf Sicherheitsmerkmale des Konnektors haben können (Änderungen an der Firewall-Konfiguration, Authentisierungsfehler etc.). Ereignisse im Kontext der Performancemessung innerhalb des Konnektors werden in das Konnektor-Performanceprotokoll geschrieben.

Die Protokolle werden gespeichert.

Im Konnektor-Menü “Protokolle” können die jeweiligen Protokolle eingesehen werden – siehe Abschnitt 6.1.2.2. Die Konfiguration des Protokollierungsdienstes wird in Abschnitt 6.1.2.8 beschrieben.

6.1.2.1 Protokollarten

Alle zu protokollierenden Ereignisse werden nach Typ und Fachmodulname in den Protokollspeicher geschrieben. Um den Speicherbedarf der unterschiedlichen Protokolle möglichst gering zu halten, werden sämtlichen Protokolle in einem

komprimierten Zustand abgespeichert. Tabelle 11 beschreibt die unterschiedlichen Typen von Protokoll-Kategorien.

Protokollart	Bedeutung
Sicherheitsprotokoll	In diesem Protokoll werden all jene Ereignisse eingetragen, welche Auswirkungen auf die Sicherheitsmerkmale des RISE Konnektors haben könnten, beispielsweise Änderungen der Firewall-Konfiguration. Im Sicherheitsprotokoll werden alle Fehlercodes vom Typ ‚Security' (Sec) gespeichert.
Performanceprotokoll	In diesem Protokoll werden Ereignisse im Kontext der Performancemessung innerhalb des RISE Konnektors festgehalten. Hierbei werden Ereignisse, welche die Performance des Gesamtsystems des RISE Konnektors betreffen, in das Konnektor-Performanceprotokoll eingetragen. Performancemessungen einzelner Fachmodule werden hingegen im jeweiligen Fachmodulperformanceprotokoll festgehalten.
Systemprotokoll	Sämtliche Ereignisse, welche keine Auswirkungen auf die Sicherheitsmerkmale des RISE Konnektors haben können, beziehungsweise nicht zu Performancemessungen gehören und trotzdem das Gesamtsystem betreffen werden im Systemprotokoll vermerkt. Im Systemprotokoll werden alle Fehlercodes vom Typ ‚Technical', ‚Business', ‚Operation' (Op) und ‚Infrastructure' (Infra) gespeichert.
Fachmodulprotokolle	Sämtliche Ereignisse, welche keine Auswirkungen auf die Sicherheitsmerkmale des RISE Konnektors haben können und lediglich einzelne oder mehrere Fachmodule betreffen, werden im jeweiligen Fachmodulprotokoll festgehalten. Hierbei existiert zu jedem Fachmodul eine eigene Protokolldatei.
Fachmodul-Performanceprotokoll	In diesem Protokoll werden Ereignisse im Kontext der Performancemessung innerhalb einzelner Fachmodule festgehalten. Hierbei existiert zu jedem Fachmodul ein eigenes Fachmodul-Performanceprotokoll, welches durch ‚fmName' definiert wird.

Tabelle 11: RISE Konnektor Protokollarten

Abbildung 27 stellt die verfügbaren Protokolle und Protokollarten dar und zeigt, in welchem Protokoll sich die einzelnen Typen befinden.

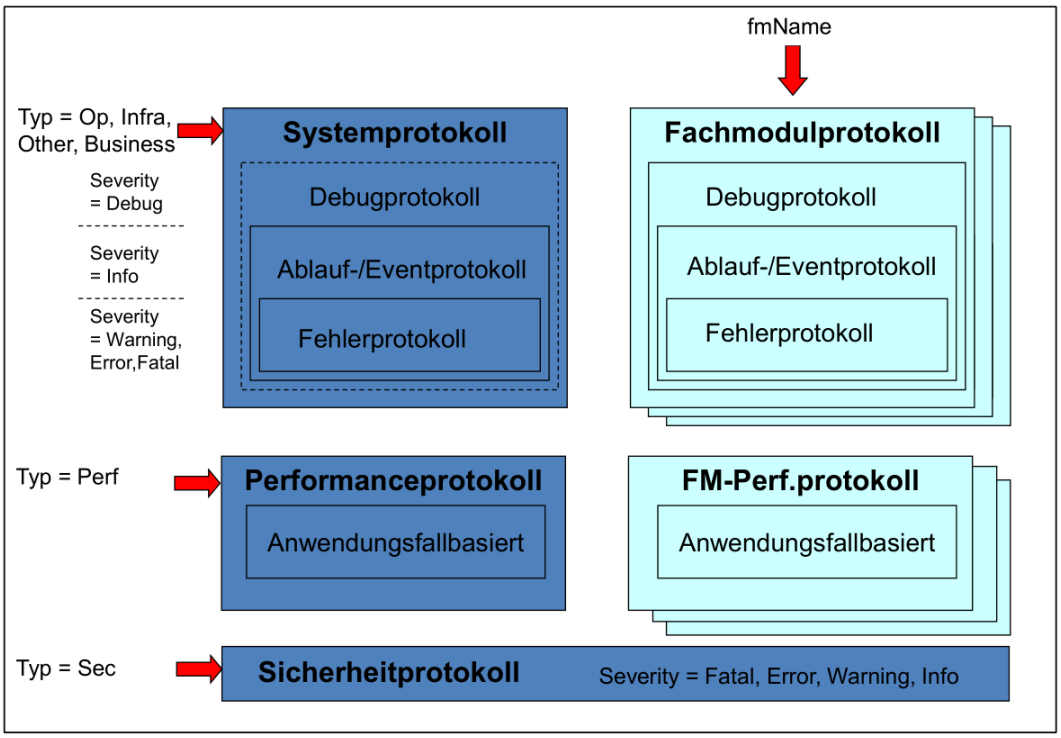


Abbildung 27: Aufbau und Struktur der Protokolldateien für Plattform und Fachmodule

6.1.2.2 Anzeigen der Protokolle

Der Administrator kann die protokollierten Ereignisse über die Management-Oberfläche einsehen. Hierbei kann mit Hilfe der Reiter "Sicherheit", "Performance" und "System" zwischen den einzelnen Protokollarten gewechselt werden. Außerdem kann bei "Performance" und "System" durch eine weitere Leiste von Reitern zwischen "Konnektor", "VSDM", "AMTS", "NFDM" und "ePA" unterschieden werden. Abbildung 28 zeigt beispielhaft das Systemprotokoll für den Konnektor. Bei allen Protokollen besteht im oberen Bereich die Möglichkeit, nach Zeitpunkt, Nachrichtentext und Schweregrad zu filtern. Darunter werden in einer Liste die einzelnen Protokolleinträge angezeigt:

- **Zeitpunkt:** Eintritt des protokollierten Ereignisses
- **Schwere:** Schweregrad des Ereignisses. Mögliche Werte: "Info", "Warning", "Error" und "Fatal". Weitere Informationen zu den Schweregraden sind in Abschnitt 4.7 zu finden.
- **Nachricht:** die Fehlermeldung
- **Details** ("Auge"-Symbol): Hier können Details zum Protokolleintrag eingesehen werden

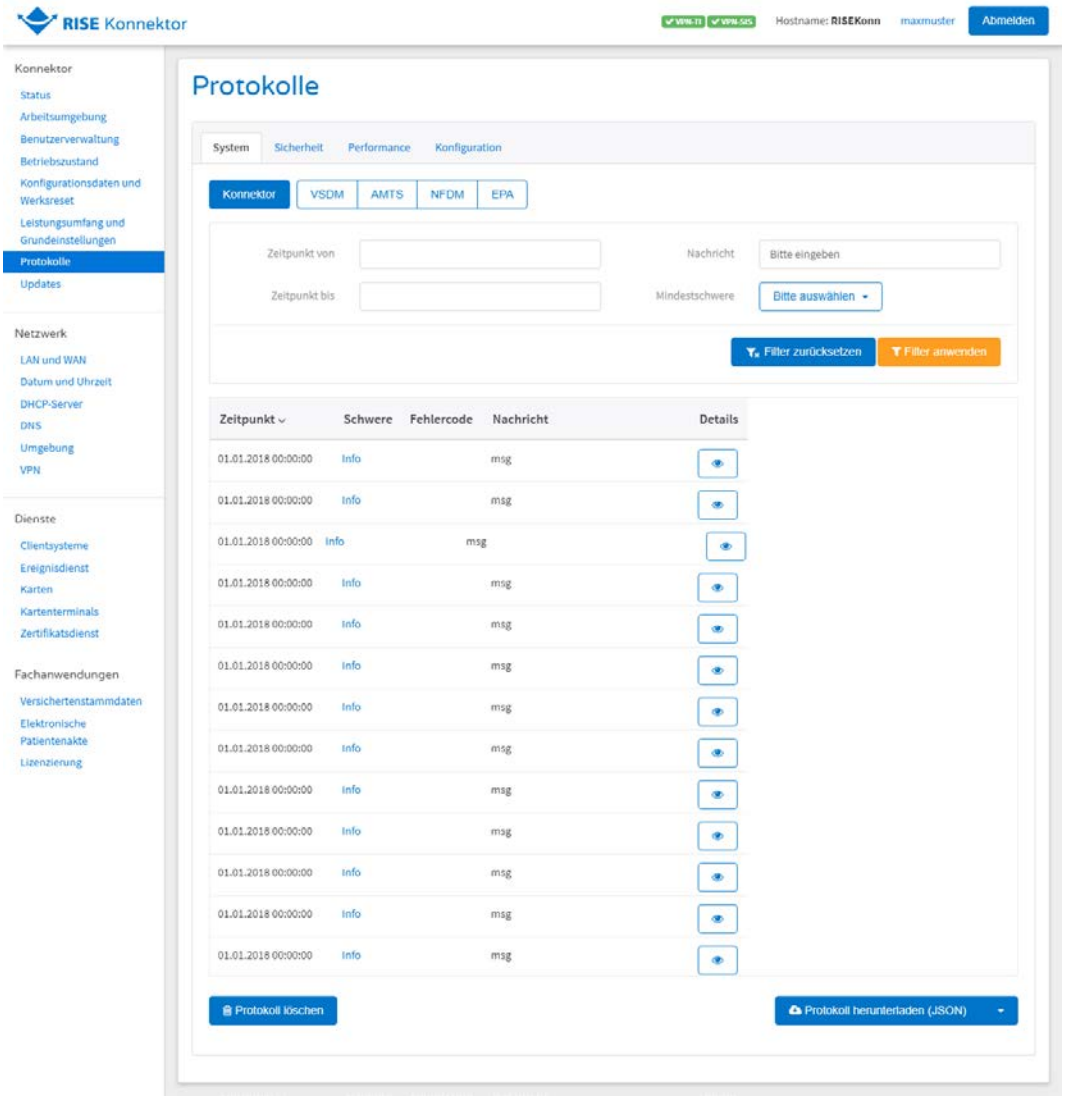


Abbildung 28: RISE Konnektor Protokoll "System"

Hinweis: Damit die Änderung der Anzahl der Protokoll-Einträge pro Seite, des Filters, des Zeitpunktes oder der Schwere wirksam wird, muss dies mit Klick auf den Button "Filter anwenden" bestätigt werden.

Darüber hinaus gibt es jeweils noch die Möglichkeit der Filterung nach Zeitpunkt, Fehler-Nachricht und Schwere des Fehlers.

- Wenn aufgrund der Limitierung nicht alle zu einer Filtereinstellung passenden Protokolleinträge zurückgegeben wurden, wird der Hinweistext "Bitte schränken Sie Ihre Suche ein" angezeigt.
- Um Logeinträge außerhalb der angezeigten Einträge zu suchen, kann über die Filter-Funktion genauer festgelegt werden, welche Protokolleinträge zurückgegeben werden sollen. Beispielsweise kann mit Hilfe der Filterung nach Datum/Uhrzeit ein anderes Zeitfenster gewählt werden.
- Die Seitennavigation bewegt sich nur innerhalb der limitierten Anzahl von Protokolleinträgen.

Die Sortierung der Protokolleinträge erfolgt durch einen Klick auf die Überschrift der jeweiligen Spalte. So kann z.B. durch Auswahl der Überschrift "Zeitpunkt" eine zeitlich aufsteigende / absteigende Sortierung gewählt werden.

6.1.2.3 Analyse der Einträge

Der RISE Konnektor legt Protokolleinträge so an, dass eine Analyse der Einträge in der Management-Oberfläche unterstützt wird:

- Die Protokolleinträge unterstützten eine patternbasierte Filterung. Protokollwert/-texte sowie Attribute sind in ihren Namensstrukturen hierauf abgestimmt.
- Zwischen Key/Value-Paaren wird als Trennzeichen ";" (Semikolon) verwendet.
- Als Zeitstempelformat wird dd.MM.yyyy HH:mm:ss.SSS verwendet. Dabei steht dd für den Tag, MM für den Monat, yyyy für das Jahr, HH für die Stunde, mm für die Minute, ss für die Sekunde und SSS für die Millisekunde. Die Zeit ist entsprechend §4 EinhZeitG (Einheiten- und Zeitgesetz) angegeben.

6.1.2.4 Löschen von Protokolleinträgen

Das Löschen folgender Protokolleinträge kann von einem Administrator durchgeführt werden:

- Systemprotokoll.
- Das jeweils durch den Fachmodulnamen spezifizierte Fachmodulprotokoll.
- Performanceprotokoll.
- Das jeweils durch Fachmodulnamen spezifizierte Fachmodul-Performanceprotokoll.

Das Löschen des Sicherheitsprotokolls ist für den Administrator nicht möglich.

Vor dem Löschen sämtlicher Protokolleinträge muss eine Sicherheitsabfrage bestätigt werden.

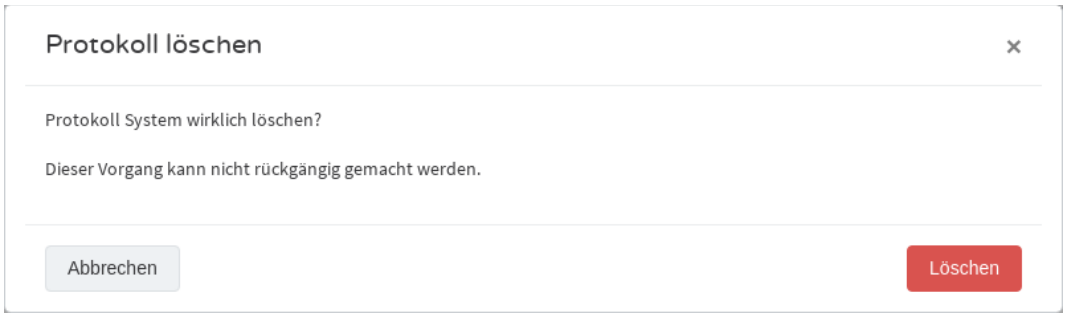


Abbildung 29: Sicherheitsabfrage vor dem Löschen von Protokolleinträgen

Warnung: Gelöschte Protokolleinträge können nicht wiederhergestellt werden!

6.1.2.5 Hinweis auf neue Sicherheitsprotokolleinträge

Nachdem sich der Administrator an der Management-Oberfläche eingeloggt hat, weist der RISE Konnektor automatisch auf Sicherheitsprotokolleinträge hin, die seit dem letzten Ausloggen dieses Administrators hinzugekommen sind.

6.1.2.6 Fehlercodes der Protokollierungsfunktion

Im Rahmen der Protokollierungsfunktion können Fehlercodes, wie in Tabelle 12 beschrieben, auftreten. Um die Fehler zu beheben, können Administratoren Protokolle löschen oder Protokollierungseinstellungen ändern (siehe Abschnitt 6.1.2.8).

Fehlercode	Fehlertyp	Schweregrad	Fehlertext
4150	Technical	Fatal	Fehler beim Schreiben des Systemprotokolls
4151	Technical	Fatal	Fehler beim Schreiben eines Fachmodulprotokolls
4152	Security	Error	Fehler beim Schreiben des Sicherheitsprotokolls
4216	Technical	Fatal	Fehler beim Schreiben des Konnektor-Performanceprotokolls
4217	Technical	Fatal	Fehler beim Schreiben eines Fachmodul-Performanceprotokolls
4153	Technical	Fatal	Zugriff auf Sicherheitsprotokoll nicht möglich
4154	Technical	Fatal	Zugriff auf Systemprotokoll nicht möglich
4155	Technical	Fatal	Zugriff auf Fachmodulprotokolle nicht möglich
4218	Technical	Fatal	Zugriff auf Konnektor-Performance-protokoll nicht möglich
4219	Technical	Fatal	Zugriff auf Fachmodul-Performanceprotokoll nicht möglich

Tabelle 12: Fehlercodes der Protokollierungsfunktion

6.1.2.7 Export von Protokolleinträgen

Durch das Auswählen der Option “Protokoll herunterladen” können die angezeigten Protokolleinträge exportiert werden. Dabei wird auch der gerade aktive Filter berücksichtigt.

Folgende Formate werden unterstützt:

- JSON[11]
- text/plain

Für manuelle Analyse der Protokolle ist das Format text/plain empfohlen; für maschinelle Auswertungen das JSON Format.

- Die aktuell gesetzten Filtereinstellungen wirken sich auf den Export aus.

Bei den Fachmodul-Performanceprotokollen ist als zusätzliches Exportformat "Report" der jeweilige Fachmodul-Performancebericht verfügbar. Detaillierte Beschreibungen zum Aufbau der exportierten JSON-Datensätze der Fachmodule befinden sich in Abschnitt 6.4.1.1.

6.1.2.8 Konfiguration

Im Reiter "Konfiguration" können generelle Einstellungen zum Protokolldienst getroffen werden. Darunter fallen die Speicherdauer der Protokolle, die Mindestschwere, die ein Fehler aufweisen muss, um im Protokoll ausgegeben zu werden, sowie die Aktivierung von Performanceprotokollen. Die Konfiguration wird dabei stets auf drei Ebenen individuell getroffen:

- Sicherheitsprotokoll
- Performance- & Systemprotokoll
- Für das jeweilige Fachmodulprotokoll
  - Versichertenstammdatenmanagement-Protokoll (VSDM-Protokoll)
  - Arzneimitteltherapiesicherheit-Protokoll (AMTS-Protokoll)
  - Notfalldatenmanagement-Protokoll (NFDM-Protokoll)
  - Elektronische Patientenakte-Protokoll (ePA-Protokoll)

Abbildung 30 zeigt den Reiter "Konfiguration", mit dem unterschiedliche Konfigurationen für die Protokollierung durchgeführt werden können. Details zu den Konfigurationsparametern hierzu sind in Tabelle 13 zu finden.

[11] https://de.wikipedia.org/wiki/JavaScript_Object_Notation, letzter Zugriff 30.04.2020

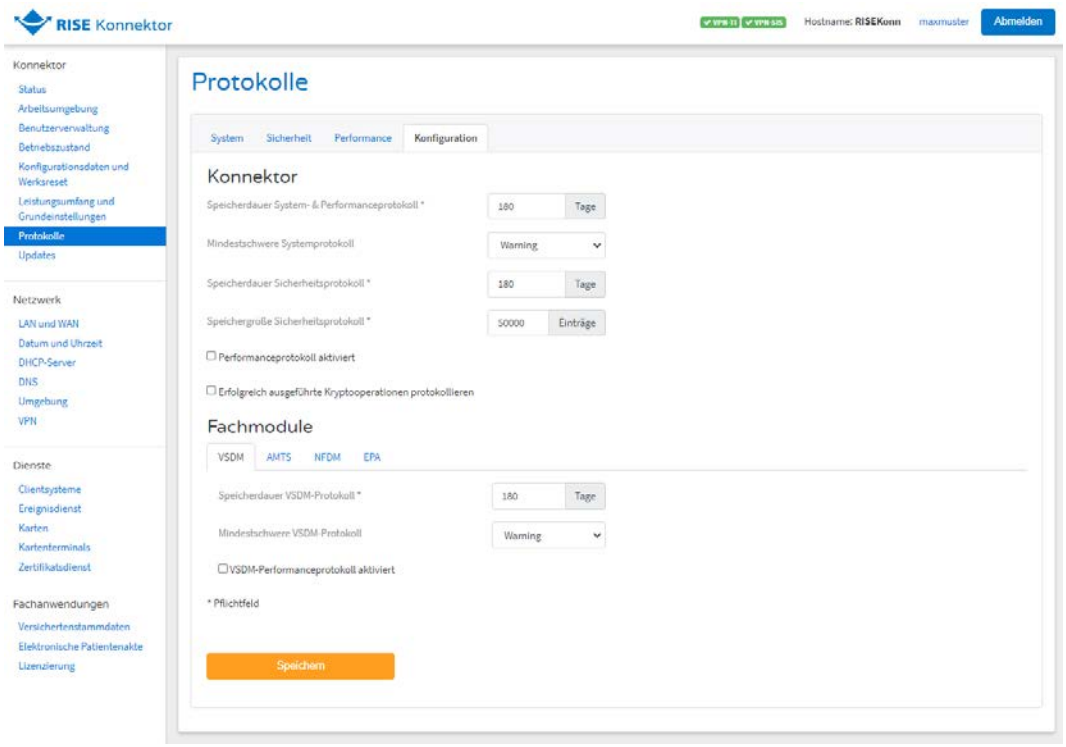


Abbildung 30: RISE Konnektor Protokoll-Einstellungen

ReferenzID	Belegung	Bedeutung
Speicherdauer Sicherheitsprotokoll (SECURITY_LOG_DAYS)	X Tage; Standard-Wert: 180	Der Administrator kann festlegen, für wie viele Tage das Sicherheitsprotokoll gespeichert werden soll. Dabei darf der eingestellte Wert nicht unter der Mindestgröße von 10 Tagen oder über der Maximalgröße von einem Jahr (365 Tage) liegen.
Speichergröße Sicherheitsprotokoll (SECURITY_LOG_SIZE)	X Einträge; Standard-Wert: 50000	Der Administrator kann festlegen, wie viele Einträge das Sicherheitsprotokoll enthalten soll. Wird diese Zahl überschritten, so werden die ältesten Einträge überschrieben. Dabei darf der eingestellte Wert nicht unter der Mindestgröße von 10000 oder über der herstellerspezifischen Maximalgröße liegen.
Speicherdauer Performance- und	X Tage; Standard-	Der Administrator kann

ReferenzID	Belegung	Bedeutung
Systemprotokoll (LOG_DAYS)	Wert: 180	festlegen, für wie viele Tage das Systemprotokoll und das Konnektor-Performanceprotokoll gespeichert werden soll. Dabei darf der eingestellte Wert nicht unter der Mindestgröße von 10 Tagen oder über der Maximalgröße von einem Jahr (365 Tage) liegen.
Speicherdauer VSDM-Protokoll / Speicherdauer AMTS-Protokoll / Speicherdauer NFDM-Protokoll / Speicherdauer ePA-Protokoll (FM_<fmName>_LOG_DAYS)	X Tage; Standard-Wert: 180	Der Administrator kann die Anzahl der gespeicherten Tage für die fachmodul-spezifischen Protokolle festlegen. Es gibt je Fachmodul einen Konfigurationsparameter für LOG_DAYS, der gemeinsam für das Fachmodulprotokoll und das Fachmodul-Performanceprotokoll gilt. Dabei darf der eingestellte Wert nicht unter der Mindestgröße von 10 Tagen oder über der Maximalgröße von einem Jahr (365 Tage) liegen.
Mindestschwere Systemprotokoll (LOG_LEVEL_SYSLOG)	Info, Warning, Error, Fatal; Standard-Wert: Warning	Der Administrator kann den Detaillierungsgrad des Systemprotokolls durch Festlegung der Mindest-Schwere der zu protokollierenden Einträge festlegen.
Mindestschwere VSDM-Protokoll / Mindestschwere AMTS-Protokoll / Mindestschwere NFDM-Protokoll / Mindestschwere ePA-Protokoll (FM_<fmName>_LOG_LEVEL)	Debug, Info, Warning, Error, Fatal; Standardwert: Warning	Der Administrator kann den Detaillierungsgrad der Fachmodulprotokolle durch Festlegung der Mindest-Schwere der zu protokollierenden Einträge festlegen.
Performanceprotokoll aktiviert (LOG_PERF)	Enabled / Disabled; Standard-Wert: Disabled	Der Administrator kann festlegen, ob auch Performanceprotokolle

ReferenzID	Belegung	Bedeutung
		geschrieben werden.
VSDM-Performanceprotokoll aktiviert / AMTS-Performanceprotokoll aktiviert / NFDM-Performanceprotokoll aktiviert / ePA-Performanceprotokoll aktiviert	Enabled / Disabled; Standard-Wert: Disabled	Der Administrator kann festlegen, ob auch Fachmodul-Performanceprotokolle geschrieben werden.
Erfolgreich ausgeführte Kryptooperationen protokollieren (LOG_SUCCESSFUL_CRYPTO_OPS)	Enabled / Disabled; Standard-Wert: Disabled	Der Administrator kann festlegen, ob auch erfolgreich ausgeführte Kryptooperationen im Sicherheitslog protokolliert werden sollen.

Tabelle 13: Parameter zur Protokollierung

Sicherheitshinweis: Um die Kontinuität der Protokolleinträge sicherzustellen, muss der Konnektor vor Änderung eines Mindestschwere-Parameters (LOG_LEVEL_SYSLOG oder FM_<fmName>_LOG_LEVEL) von den verbundenen Clientsystemen und von der TI getrennt (bspw. durch Abstecken beider Netzwerk-Interfaces WAN und LAN, vlg. Abbildung 3) und anschließend direkt mit dem vertrauenswürdigen Administrations-Rechner über die LAN-Schnittstelle für die Administration verbunden werden. Alternativ können diese Parameter im Zuge der Inbetriebnahme gesetzt werden, siehe dazu Abschnitt 3.3.4.

6.1.2.9 Tägliche Rotation

Die tägliche Rotation, also das Löschen von Protokolleinträgen (jeweils zum Tageswechsel), die älter als die konfigurierte maximale Speicherdauer von Sicherheits-, Performance-, System- bzw. Fachmodul-Protokoll sind, wird durch eine entsprechende Konfiguration durchgeführt (siehe auch Abschnitt 6.1.2.8).

6.1.2.10 Überlastschutz bei Protokolleinträgen

Neue Protokolleinträge überschreiben alte Protokolleinträge mit gleichem oder niedrigerem Schweregrad, wenn das Überlastkriterium eintritt.

6.1.3 RISE Konnektor Updates

Dieser Abschnitt behandelt die Aktualisierung der RISE Konnektor Software und der eHealth-Kartenterminal-Software. Die Aktualisierung der Bestandsnetze ist in Abschnitt 6.2.1.2 beschrieben.

6.1.3.1 Information zur aktuell installierten Softwareversion erhalten

Der Reiter “Info” gibt eine Übersicht über die aktuell installierte Firmware-Version (Software-Version) auf dem RISE Konnektor bzw. über die verwendete Hardware. Folgende Daten werden unter “Info” dargestellt:

- Konnektor
  - **Produkttyp:** Typenbezeichnung des Produkts.
  - **Produkttypversion:** Aktuelle Version des Produkttyps.
  - **Produktkürzel:** Herstellerspezifisches Kürzel.
  - **Hersteller-ID:** Eindeutige Herstellerkennung.
  - **Name des Herstellers:** Vollständiger Name des Herstellers.
  - **Firmwareversion:** Aktuelle Version der Firmware.
  - **Gruppenversion:** Aktuelle Gruppenversion.
- Hardware-Information
  - **Hardwareversion:** Aktuelle Version der Hardware.
  - **Seriennummer:** Die offizielle Seriennummer des Gerätes.
  - **Seriennummer gSMC-K 1, 2, 3:** Seriennummern der eingesetzten gSMC-Ks.
  - MAC-Adresse am LAN Interface
  - MAC-Adresse am WAN Interface
- Aktuell aktive Fachmodule
  - **AMTS:** Aktuelle Version des Fachmoduls AMTS
  - **NFDM:** Aktuelle Version des Fachmoduls NFDM
  - **EPA:** Aktuelle Version des Fachmoduls ePA

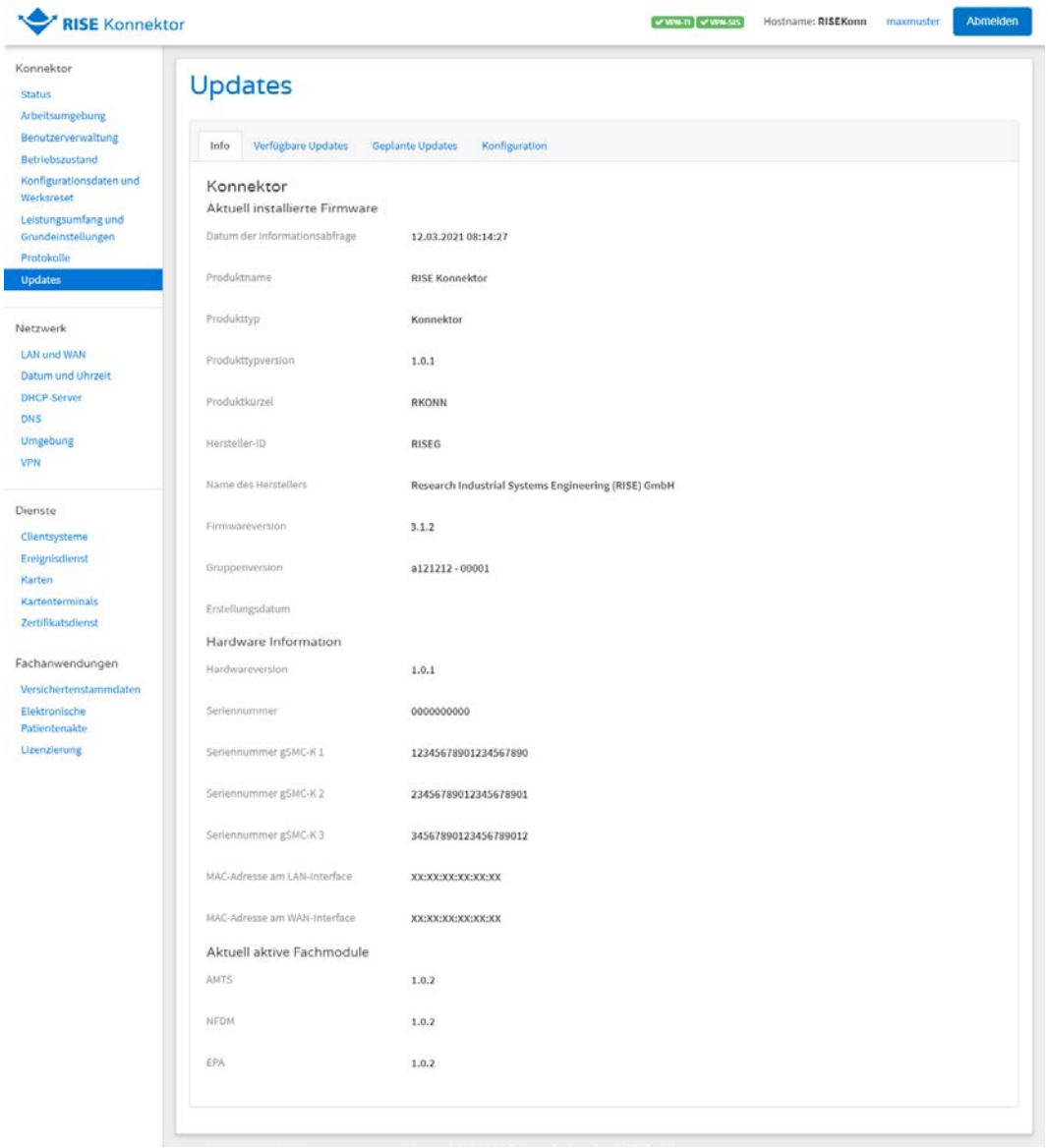


Abbildung 31: RISE Konnektor Updates "Info"

6.1.3.2 Verfügbare Updates

Der Administrator hat auf der Management-Oberfläche eine Übersichtsliste, die einen Geräteeintrag für den RISE Konnektor selbst, sowie eine Liste von Geräteeinträgen für jedes physische und gepairte/aktualisierende/aktive Kartenterminal enthält.

Alle zur Verfügung stehenden Updates, deren Software-Version neuer ist, als die installierte, werden angezeigt. Sicherheitskritische Updates sind rot hervorgehoben.

Falls nicht, wie in Abschnitt 6.1.3.4.2 beschrieben, der automatische Download aktiviert wurde, hat der Administrator die Möglichkeit, die Aktualisierung der Liste aller zur Verfügung stehenden Updates manuell anzustoßen.

Abbildung 32 listet beispielhaft Updatepakete, die für den RISE Konnektor und für Kartenterminals verfügbar sind.

Sicherheitshinweis: Der Hersteller empfiehlt, den RISE Konnektor inkl. Kartenterminal-Software stets aktuell zu halten. Sollten neue Versionen für Ihre Geräte gelistet sein, installieren Sie diese umgehend.

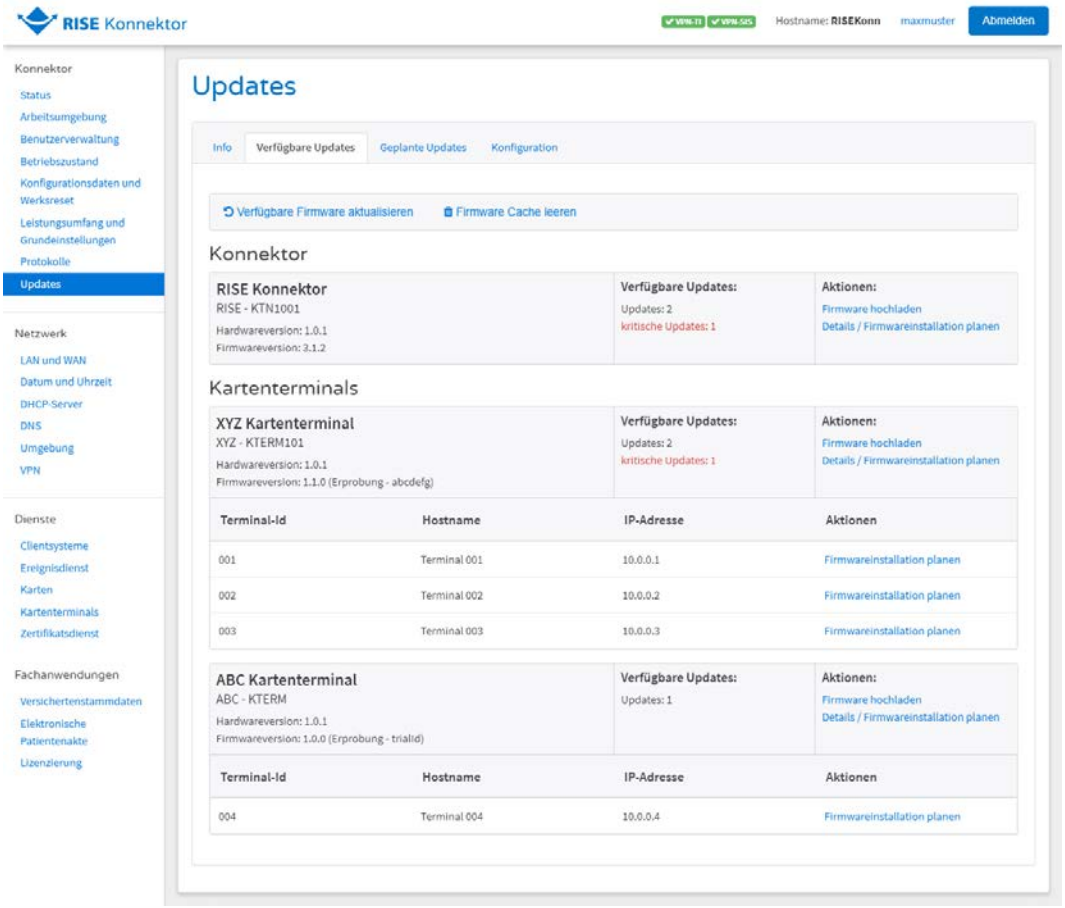


Abbildung 32: RISE Konnektor Updates "Verfügbare Updates"

Sind Updates verfügbar, gibt es jeweils in der Spalte "Aktionen" einen Link "Details/Firmwareinstallation planen". Hier können weitere Details und Informationen zu diesem verfügbaren Update angezeigt werden bzw. auch die Installation geplant bzw. durchgeführt werden (siehe Abschnitt 6.1.3.3).

6.1.3.2.1 Verfügbare Firmware aktualisieren

Wenn der RISE Konnektor online ist und die Option "Aktualisierungen automatisch suchen" (siehe Abbildung 36) eingeschaltet ist, wird in regelmäßigen Abständen automatisch nach Updates gesucht. Sie können jedoch jederzeit manuell eine Abfrage auf neue Versionen durchführen, indem Sie das Menü "Verfügbare Firmware aktualisieren" auswählen (siehe Abbildung 32).

6.1.3.2.2 Firmware Cache leeren

Sind die Daten für ein Update bereits heruntergeladen oder manuell importiert, wird Speicherplatz belegt. Sie können die Daten von Updates jederzeit löschen und

danach ggf. neu herunter- oder hochladen. Um Speicherplatz freizugeben, wählen Sie das Menü “Firmware Cache leeren”.

6.1.3.2.3 Firmware hochladen

Durch Auswahl des Menüs “Firmware hochladen” können Sie ein lokal verfügbares RISE Konnektor Updatepaket oder ein Update für Kartenterminals auf den RISE Konnektor laden.

- Für ein lokal verfügbares RISE Konnektor Firmware-Update sind immer eine .zip und eine .sig-Datei auf einem lokal verfügbaren Laufwerk anzugeben. Nach Überprüfung der Authentizität des Update-Pakets steht es zur Freischaltung bereit.
- Liegt lokal eine Kartenterminal-Software vom Kartenterminal Hersteller vor, ist lediglich eine Datei anzugeben, wobei der Dateityp beliebig sein kann. Hier findet zunächst keine Überprüfung der Authentizität statt, dies übernimmt in weiterer Folge das Kartenterminal. Des Weiteren muss beim Hochladen eines Kartenterminal-Updates ein eindeutiger Name (Bezeichnung) für die ausgewählte Datei vergeben werden (siehe Abbildung 33). Der Updatevorgang kann danach mit Hilfe dieser Bezeichnung identifiziert werden.

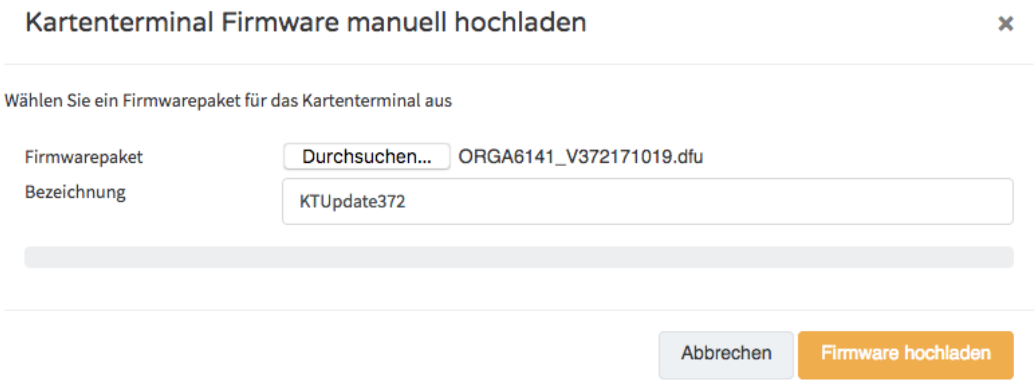


Abbildung 33: RISE Konnektor Updates – Kartenterminal-Firmware manuell hochladen

6.1.3.2.4 Details – Firmwareinstallation planen

Durch Auswahl des Menüs “Details / Firmwareinstallation planen” können Sie die Details des Firmwarepakets einsehen und die Installation planen.

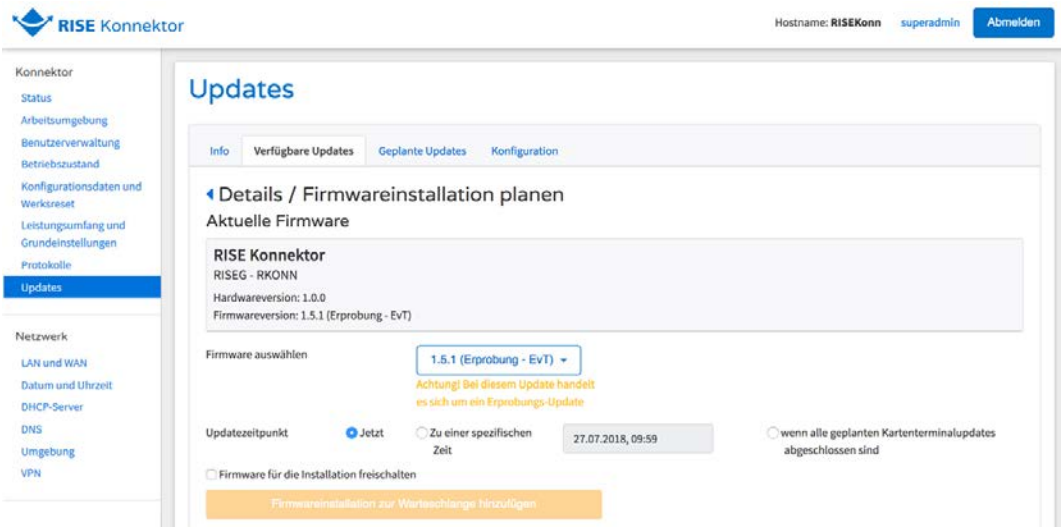


Abbildung 34: RISE Konnektor Updates - Verfügbare Updates - Details/Firmwareinstallation planen

Folgende Informationen stehen zur Verfügung:

- **Aktuelle Firmware:** Informationen über die aktuell installierte Firmwareversion
- **Firmware auswählen:** eine Liste über alle zur Verfügung stehenden Versionen bzw. Bezeichner bei Kartenterminal-Updates. Bei der Auswahl der gewünschten Version/Bezeichnung werden auch die Details sichtbar.
- Information, ob die installierte Software und die Software-Updates zum Online-Produktivbetrieb oder zur Erprobung gedacht sind.
- **Updatezeitpunkt:**
  - "Jetzt": die Firmware wird unmittelbar nach dem Hinzufügen des Updates in die Warteschlange aktualisiert. Der RISE Konnektor ist dann für die nächsten 6 Minuten nicht verfügbar.
  - "Zu einer spezifischen Zeit": wählen Sie die Uhrzeit aus, wann das Update durchgeführt werden soll.
  - "Wenn alle geplanten Kartenterminalupdates abgeschlossen sind": diese Option startet das Update unmittelbar nach dem Updateprozess der Kartenterminals.

Warnung: Planen Sie Updates nur in enger Abstimmung mit dem Personal des Leistungserbringers. Während des Updateprozesses, stehen sämtliche Funktionen des RISE Konnektors (inkl. Kartenterminals) nicht zur Verfügung (Dauer des Updateprozesses ohne Download: ca. 6 Minuten).

Hinweis: Die Option "Wenn alle geplanten Kartenterminalupdates abgeschlossen sind" startet das Konnektor-Update nur, wenn auch alle zu aktualisierenden Kartenterminals verfügbar sind.

- Details des ausgewählten Firmwarepakets
  - Reiter "Zusammenfassung" (verfügbar für RISE Konnektor- und Kartenterminalupdates):
    - **Update-ID:** Eindeutige Kennung des Updates bzw. Bezeichnung.

- **Hersteller-ID:** Eindeutiges Kürzel des Herstellers.
- **Produktkürzel:** Kürzel des Produkts, für welches das Update geeignet ist.
- **Hardwareversion:** Hardware, für die das Update geeignet ist.
- **Erstellungsdatum:** Datum, an dem das Updatepaket erstellt wurde.

– Reiter "Zusammenfassung" (verfügbar nur für RISE Konnektor-Updates):

- **Gültigkeitsbereich:** Enthält u.a. Information für den Administrator bezüglich der Installation; beispielsweise wann das Update frühestens oder spätestens durchgeführt werden sollte.
- **Firmwaregruppe:** Identifikation der Firmware-Gruppe.
- **Firmwarebeschreibung:** Enthält Information zur Firmware selbst wie z.B. Beschreibungen und Dokumentationen zu dem Update.
- **Firmwaregruppenbeschreibung:** Durch den Hersteller erstellte Beschreibung der Firmware-Gruppe. Falls es Abhängigkeiten zwischen Update-Paketen gibt, werden sie hier beschrieben.

– Reiter "Dateien": Es werden die im Updatepaket enthaltenen Dateien inkl. Dateigröße angezeigt.

– Reiter "Dokumentation": Es wird eine Dokumentation zum Updatepaket angezeigt bzw. Hinweise gegeben, wo eine detaillierte Beschreibung zu finden ist.

- "Firmware für die Installation freischalten": nachdem Sie sich überzeugt haben, dass die ausgewählte Firmware-Version installiert werden soll, schalten Sie die Firmware frei, indem Sie das Häkchen setzen.

Sicherheitshinweis: Schalten Sie ein Softwareupdate nur frei, wenn Sie ausreichend Informationen über den Inhalt des Softwareupdates erhalten haben (u.a. im Menü "Dokumentation"), die Ihnen eine bewusste Entscheidung bei der Freischaltung ermöglichen. Falls Sie sich nicht sicher sind, kontaktieren Sie bitte den Händlersupport (siehe Abschnitt 2).

- Mit der Auswahl "Firmwareinstallation zur Warteschlange hinzufügen" bestätigen Sie Ihre Eingaben. Die Installation ist nun im Reiter "Geplante Updates" aufgelistet.

Hinweis: Die Firmwareinstallation kann nur dann zur Warteschlange hinzugefügt werden, wenn die ausgewählte Firmware zuvor freigeschaltet wurde.

Hinweis: Sollte für Kartenterminals noch kein Username und Passwort vergeben worden sein, so sind diese vor dem Hinzufügen zur Warteschlange anzugeben (siehe Abschnitt 6.3.4.1.3, Abbildung 115). Dieser Umstand ist durch den Protokolleintrag "Download nicht aller UpdateFiles möglich" zu identifizieren.

6.1.3.3 Geplante Updates

Abbildung 35 zeigt an, wann Updates geplant sind. Diese werden beim Erreichen des geplanten Zeitpunktes durchgeführt.

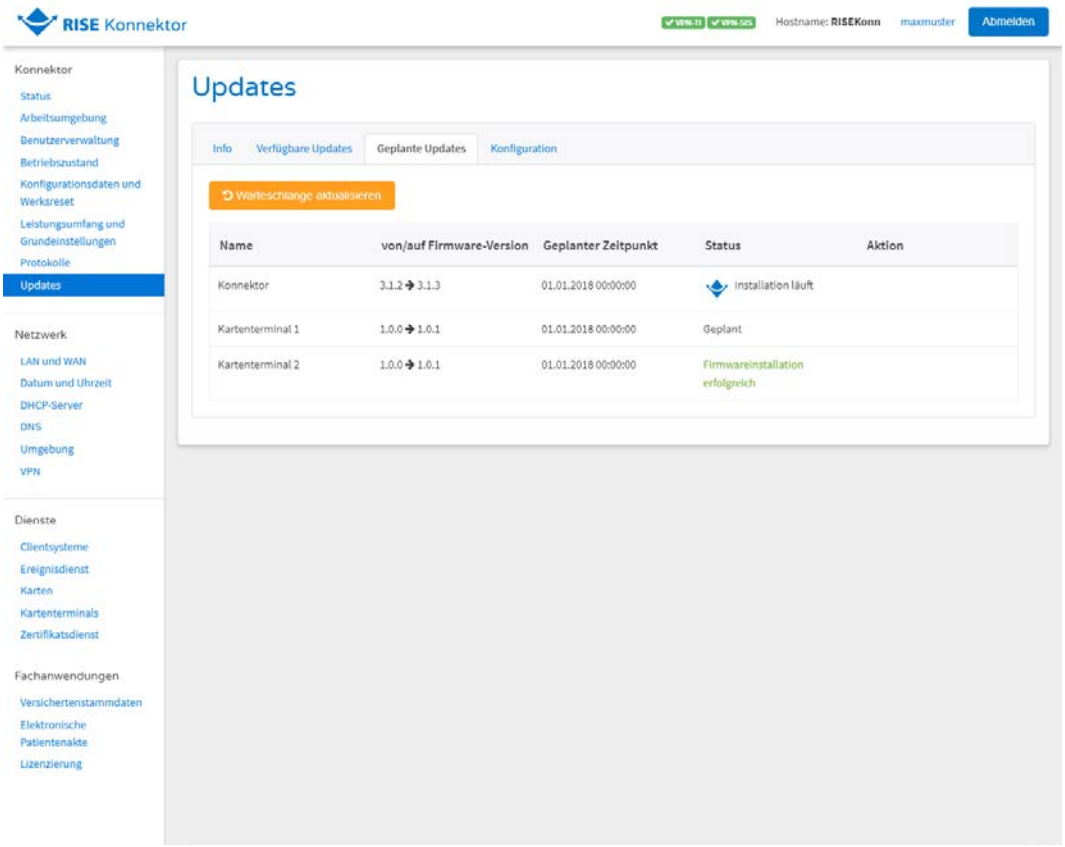


Abbildung 35: RISE Konnektor Updates "Geplante Updates"

Um die Liste der geplanten Updates zu aktualisieren, wählen Sie "Warteschlange aktualisieren".

Hinweis: Der Konnektor bzw. das Kartenterminal führen automatisch eine Integritätsprüfung von Update-Paketen durch. Pakete, welche nicht integer sind, können nicht installiert werden.

Der Administrator kann ein gesammeltes Update für die Liste der markierten Geräteeinträge auslösen.

Ist kein Ausführungszeitpunkt gesetzt, wird die Aktualisierung der Kartenterminals sofort durchgeführt. Wurde ein Ausführungszeitpunkt festgelegt, wird das Update durchgeführt, sobald der Ausführungszeitpunkt erreicht ist, oder, sofern der Konnektor zum Ausführungszeitpunkt nicht in Betrieb war, überschritten wurde. Konnte das Kartenterminal nicht erreicht werden, bleibt das gesetzte Update für eine spätere Anwendung erhalten und wird ereignisgesteuert neu ausgelöst.

Sofern die Konnektor-Update-Abhängigkeit von Kartenterminal-Updates nicht gesetzt wurde oder wenn alle vorgesehenen Kartenterminal-Updates durchgeführt wurden, wird das Update des RISE Konnektors (in Abhängigkeit des

Ausführungszeitpunktes) durchgeführt: Wurde kein Ausführungszeitpunkt gesetzt, wird das Update des RISE Konnektors sofort durchgeführt. Wurde ein Ausführungszeitpunkt gesetzt, wird das Update durchgeführt, sobald dieser erreicht ist, oder, sofern der Konnektor zum Ausführungszeitpunkt nicht in Betrieb war, überschritten wurde.

Warnung: Trennen Sie während des gesamten Updateprozesses auf keinen Fall das Gerät von der Stromversorgung! Es kann dadurch zu irreparablen Schäden kommen.

Sicherheitshinweis: Überzeugen Sie sich nach dem abgeschlossenen Update-Prozess, dass die korrekte Firmware-Version auf Ihren Geräten installiert wurde (siehe Abbildung 35). Sollte die Prüfung nach mehrmaligen Versuchen fehlschlagen, kontaktieren Sie umgehend den Händlersupport (siehe Abschnitt 2).

Sicherheitshinweis: Überprüfen Sie nach einem Update, ob die Firmware-Version der vom BSI zugelassenen Version entspricht (siehe Abschnitt 1.4).

Sicherheitshinweis: Während des automatischen Firmware-Updates ist der Schutz von Kartenterminals nicht sichergestellt. Der Administrator ist daher verpflichtet, in dem Zeitraum, in dem Firmware-Updates durchgeführt werden, entsprechende organisatorische Schutzmaßnahmen durchzusetzen.

Hinweis: Nach erfolgreichem Update findet eine Migration der Protokoll-Einträge statt. Die Migration ist nach spätestens 24 Stunden abgeschlossen. Sollte während diesem Vorgang ein Fehler auftreten (z.B. Trennung des Konnektors von der Stromversorgung), werden die betroffenen Einträge mit "Fehler beim Parsen des Protokolleintrags (30042)" gekennzeichnet.

Hinweis: Ein Erprobungs-Update sollte nur dann installiert werden, wenn die Institution oder Organisation an der Erprobung teilnehmen. Während dieses Updates wird der Administrator mittels Warnhinweis informiert, für welche Erprobung es vorgesehen ist. Wird das Update installiert, kann dies zu funktionalen Einschränkungen des Konnektors führen.

6.1.3.4 Konfiguration

Der Reiter "Konfiguration" ermöglicht das Einsehen und Setzen der Einstellungen, wie der RISE Konnektor mit verfügbaren Update-Paketen verfährt (siehe Abbildung 36).

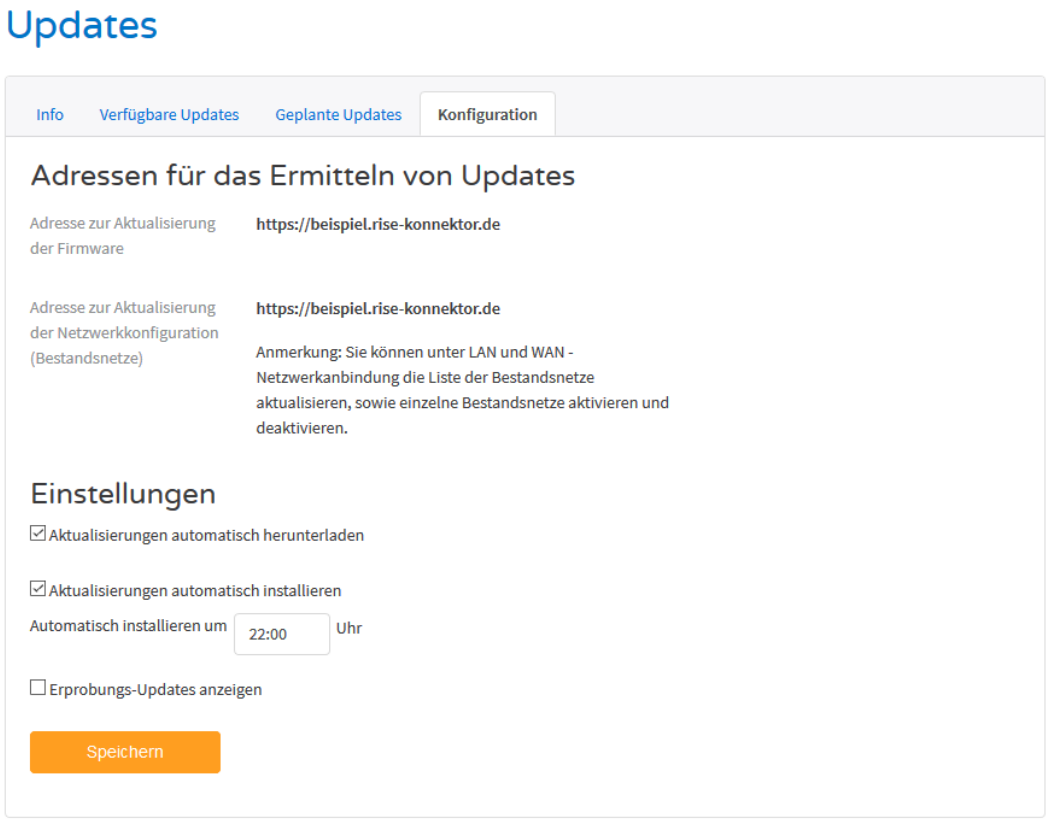


Abbildung 36: RISE Konnektor Updates "Konfiguration"

ReferenzID	Belegung	Bedeutung
Adresse zur Aktualisierung der Firmware (MGM_KSR_FIRMWARE_URL)	URL	SOAP-Endpunkt des Konfigurationsdienstes zum Download der Firmware
Adresse zur Aktualisierung der Netzwerkkonfiguration (Bestandsnetze) (MGM_KSR_KONFIG_URL)	URL	SOAP-Endpunkt des Konfigurationsdienstes zum Download von Konfigurationsdaten
Aktualisierungen automatisch herunterladen (MGM_KSR_AUTODOWNLOAD)	Enabled / Disabled; Standard-Wert: Enabled	Sofern Aktualisierungen automatisch gesucht werden, kann der Administrator den automatischen Download verfügbarer Update-Pakete an- und abschalten.
Aktualisierungen automatisch installieren (FW_AUTO_UPDATE_ENABLED)	Enabled / Disabled; Standard-Wert: Disabled	Der Administrator kann das automatische Installieren verfügbarer RISE Konnektor Update-Pakete an- und abschalten. Ist FW_AUTO_UPDATE_ENABLED aktiv so ist automatisch auch MGM_KSR_AUTODOWNLOAD

ReferenzID	Belegung	Bedeutung
		aktiv.
Uhrzeit der automatischen Installation der RISE Konnektor Update-Pakete	Uhrzeit. Standard-Wert: 22:00 Uhr	Uhrzeit, an dem verfügbare RISE Konnektor Update-Pakete automatisch installiert werden. Sollte der RISE Konnektor zu dieser Zeit gerade beschäftigt sein, so wird das Update-Paket installiert, sobald der RISE Konnektor wieder verfügbar ist.
Erprobungsupdates anzeigen (MGM_KSR_SHOW_TRIAL_UPDATES)	Enabled / Disabled; Standard-Wert: Disabled	Der Administrator kann zusätzlich zur Anzeige von Update-Paketen für den Online-Produktivbetrieb auch die Anzeige von Erprobungs-Update-Paketen aktivieren. Wird dieser Schalter gesetzt, erscheint ein Warnhinweis, dass die Installation von Erprobungs-Update-Paketen nur für Teilnehmer der Erprobungen vorgesehen ist.

Tabelle 14: Parameter der Update Konfiguration

6.1.3.4.1 Aktualisierung der Bestandsnetze

Sind die Netzwerk-Routen eingerichtet (siehe Abschnitt 6.2.1.1.1) und ist eine Verbindung zum VPN-Konzentrator der Telematikinfrastruktur aufgebaut (siehe Abschnitt 6.2.6), können die Bestandsnetze aktualisiert, aktiviert bzw. deaktiviert werden.

6.1.3.4.2 Aktualisierung automatisch herunterladen

Wenn die Konfiguration "Aktualisierungen automatisch herunterladen" ausgewählt wurde, wird auch der Download der aktuellsten Software-Versionen sowohl für den RISE Konnektor als auch für Kartenterminals automatisch durchgeführt.

6.1.3.5 Aktualisierungen automatisch installieren

Wenn die Konfiguration "Aktualisierungen automatisch installieren" ausgewählt wurde, wird nach erfolgreichem Download und Prüfung der Integrität der aktuellesten RISE Konnektor Software-Version, diese zu einer konfigurierbaren Uhrzeit automatisch installiert.

Sicherheitshinweis: Beim Aktivieren der automatischen Installation ist eine Registrierung des Clientsystems auf die KSR/UPDATE-Ereignisse verpflichtend.

Hinweis: Software-Updates werden nur durchgeführt, wenn der RISE Konnektor zur angegeben Uhrzeit eingeschaltet ist. Es ist daher sicherzustellen, dass ein Software-Update zur eingestellten Uhrzeit möglich ist. Beachten Sie dabei auch die Hinweise und Warnungen aus Abschnitt 6.1.3.2.4 und Abschnitt 6.1.3.3.

Hinweis: Die Funktion "Aktualisierungen automatisch installieren" wird ausschließlich für Firmware-Updates des RISE Konnektors angewendet.

6.1.3.5.1 Erprobungsupdates anzeigen

Wählen Sie die Option "Erprobungsupdates anzeigen", wenn Ihr Institut an Erprobungen teilnimmt.

Warnung: Aktivieren Sie die Anzeige von Erprobungsupdates nur, wenn Ihr Institut an Erprobungen teilnimmt.

6.1.4 RISE Konnektor Arbeitsumgebung

Im Menüpunkt "Arbeitsumgebung" ist die Arbeitsumgebung einzurichten, in der der Konnektor betrieben wird. Bitte definieren Sie für Ihren konkreten Einsatzfall die Arbeitsumgebung. Dabei sind in einem ersten Schritt folgende Informationen zu geben:

- **Mandanten** entspricht einem Arzt/einer Ärztin/einem Krankenhaus.
- **Clientsysteme** entspricht einem Computer mit einer Primärsystem-Software.
- **Arbeitsplätze** entspricht einem physischen Ort, an dem Kartenterminals aufgestellt sind.

Der Konnektor kann im Minimalfallfall mit nur jeweils einem Mandanten, einem Clientsystem und einem Arbeitsplatz betrieben werden.

Sicherheitshinweis: Die Seriennummer Ihrer SMC-B (ICCSN) wird bei der Einrichtung der Arbeitsumgebung protokolliert. Diese Protokollierung kann verhindert werden, wenn das Log-Level vor der Einrichtung auf "Warning" (default), "Error" oder "Fatal" gestellt wird (siehe Abschnitt 6.1.2.8). Ein erzeugter Protokolleintrag kann gelöscht werden, indem nach der Einrichtung das Systemlog gelöscht wird (siehe Abschnitt 6.1.2.4).

6.1.4.1 Einrichtungsassistent

Um die Einrichtung zu vereinfachen (siehe Abbildung 37) kann der Assistent "Vereinfachte Arbeitsumgebung einrichten" eingesetzt werden, um genau einen Mandanten, einen Arbeitsplatz und ein Clientsystem einzurichten.

Hinweis: Vergewissern Sie sich, dass eine SMC-B Karte im Kartenterminal steckt, da der Assistent ansonsten wieder abgebrochen werden muss (siehe Abbildung 39).

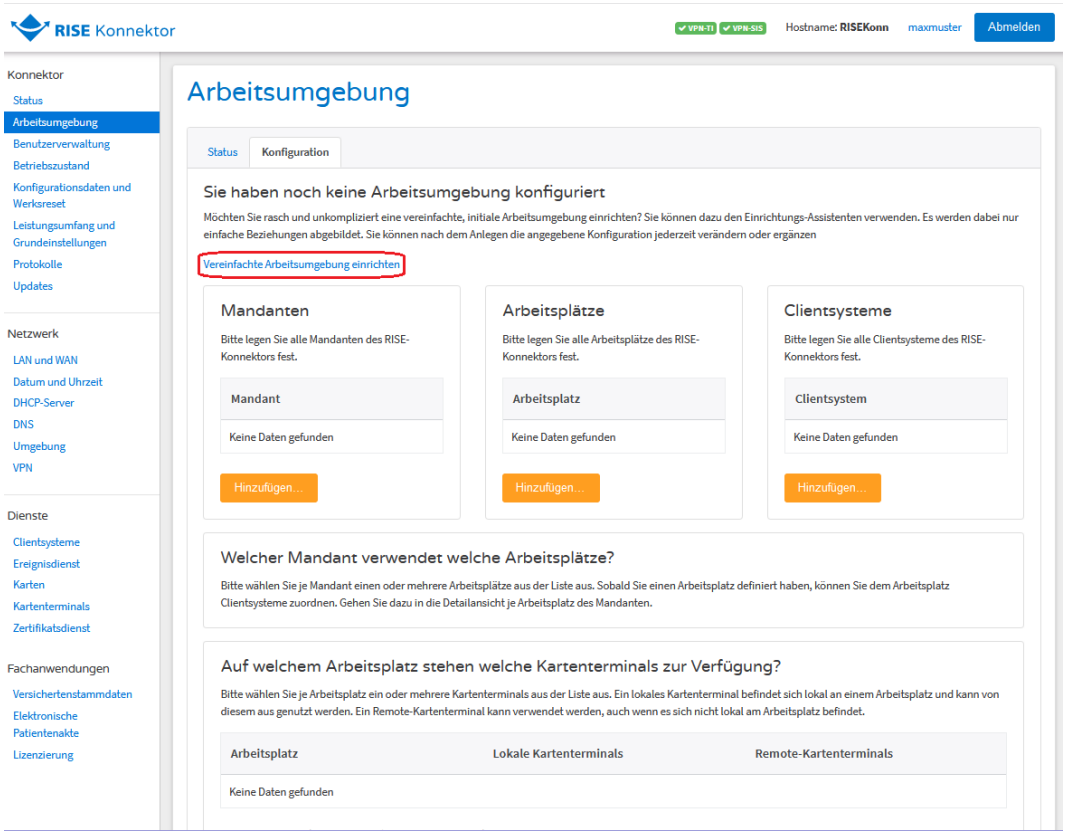


Abbildung 37: Konfiguration - Einrichtungsassistent

Führen Sie den Assistenten nur aus, wenn Sie keine bereits vorhandene Konfiguration überschreiben wollen, wie in Abbildung 38 dargestellt.

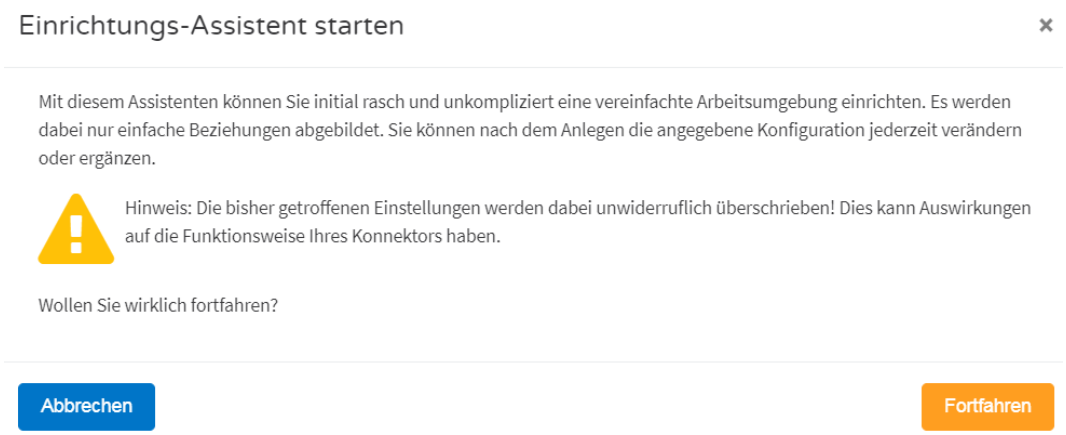


Abbildung 38: Konfiguration - Einrichtungsassistent starten

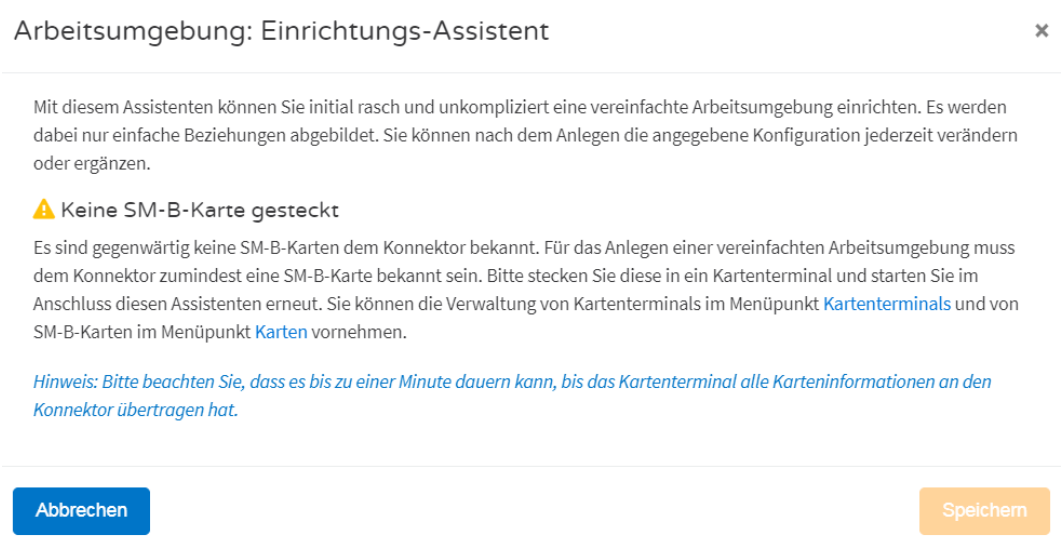


Abbildung 39: Konfiguration - Einrichtungsassistent mit gesteckter SMC-B starten

Abbildung 40 zeigt eine mögliche initiale Konfiguration mit Hilfe des Einrichtungsassistenten und gesteckter SMC-B Karte. Es können damit nur einfache Beziehungen eingerichtet werden, im Anschluss daran können anhand der Beschreibung in Abschnitt 6.1.4.2 komplexere Beziehungen abgebildet werden, wo dies anhand eines Beispiels gezeigt wird. Mit abschließendem Speichern wird die Konfiguration persistiert.

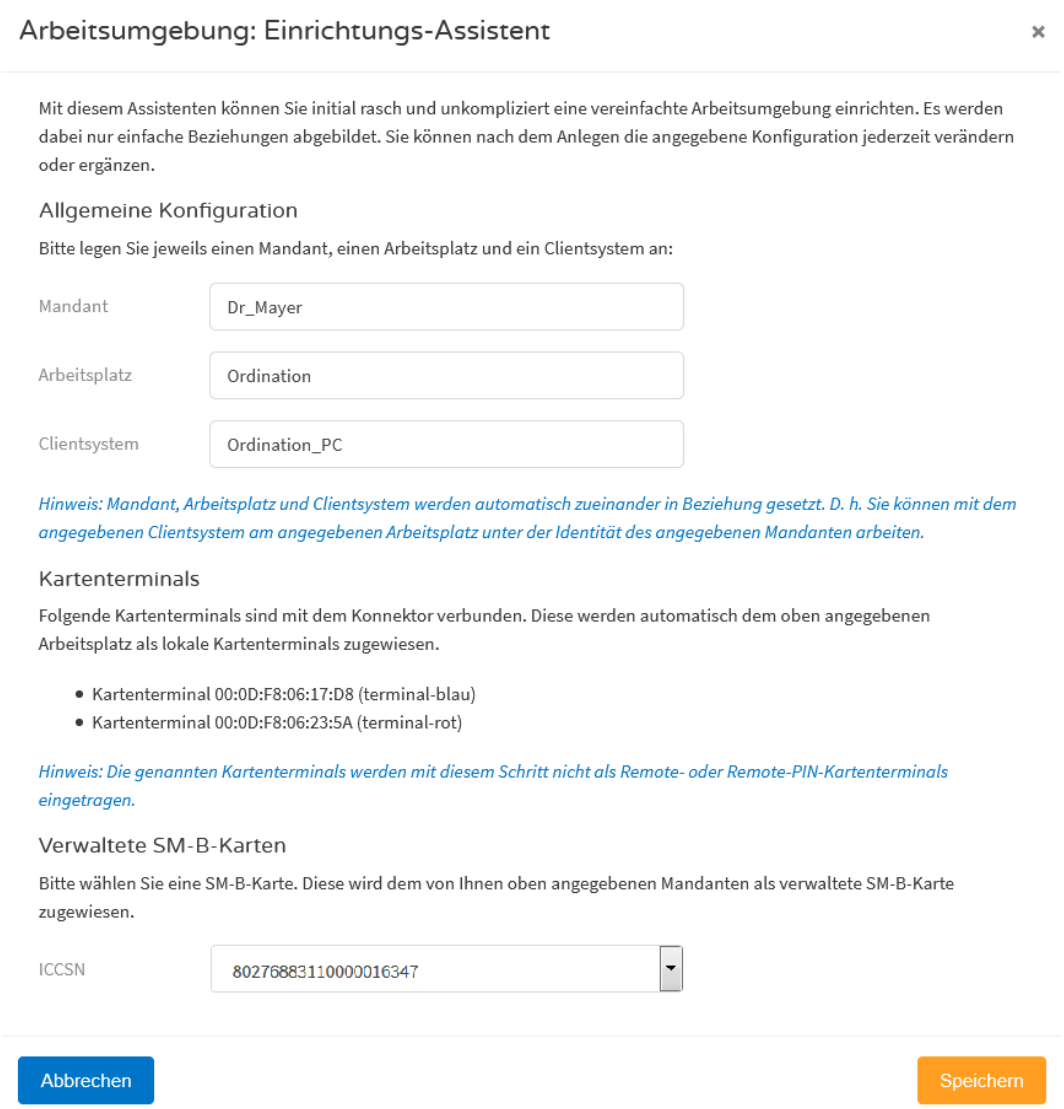


Abbildung 40: Konfiguration - Einrichtungsassistent finalisieren.

6.1.4.2 Arbeitsumgebung – Basiskonfiguration an Hand eines Beispiels

Annahme: In einer Ordination arbeitet ein Arzt/eine Ärztin zusammen mit einer Sprechstundenhilfe. Es müssen daher im System ein Mandant (für den Arzt/die Ärztin), zwei Clientsysteme und zwei Arbeitsplätze angelegt werden (jeweils einer für den Arzt/die Ärztin und einer für die Sprechstundenhilfe).

Sowohl der Arzt/die Ärztin als auch die Sprechstundehilfe haben je ein Kartenterminal. Im Kartenterminal des Arztes/der Ärztin steckt die SMC-B Karte und mittels Remote-PIN-Eingabe kann das Kartenterminal des Arztes/der Ärztin vom Kartenterminal der Sprechstundenhilfe angesteuert werden.

6.1.4.2.1 Konfiguration Mandanten, Arbeitsplätze und Clientsysteme

Die Standardansicht, wenn weder Mandant, Arbeitsplatz noch Clientsystem konfiguriert sind, ist in Abbildung 41 zu sehen.

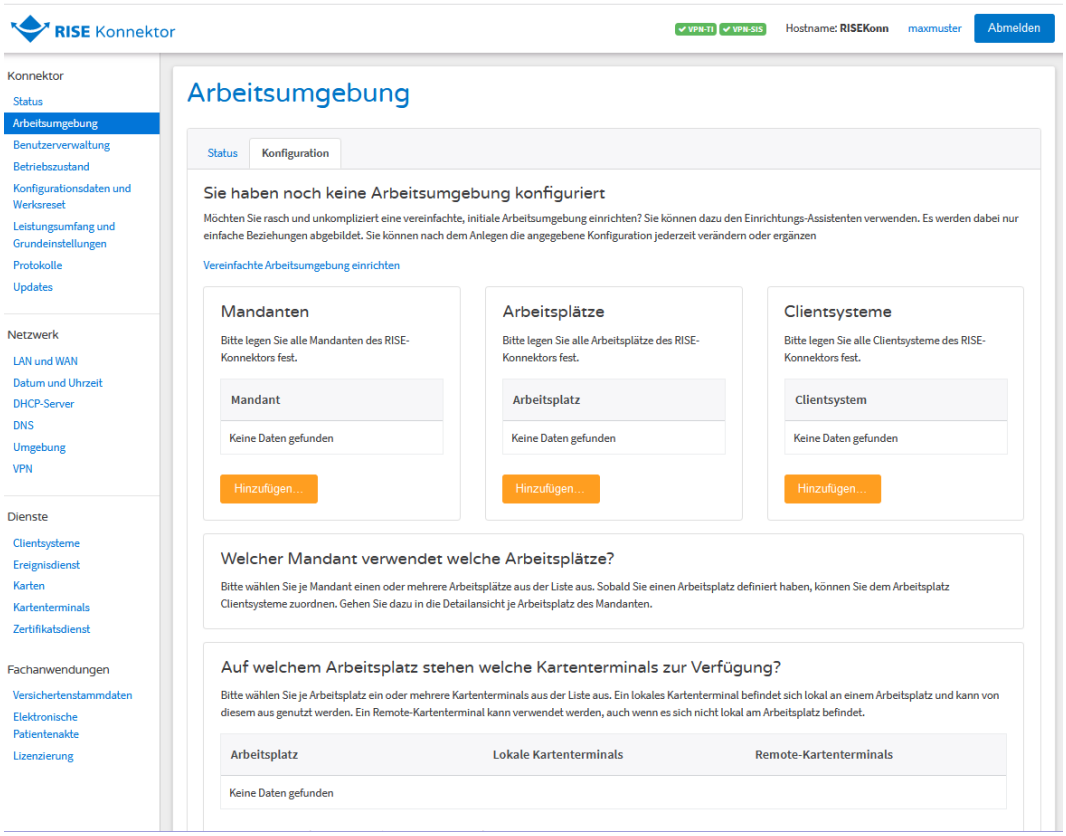


Abbildung 41: Konfiguration - Mandanten, Arbeitsplätze, Clientsysteme

Im ersten Schritt können jetzt über den Button "Hinzufügen..." jeweils ein Mandant, zwei Arbeitsplätze und zwei Clientsysteme hinzugefügt werden (vgl. Abbildung 42).

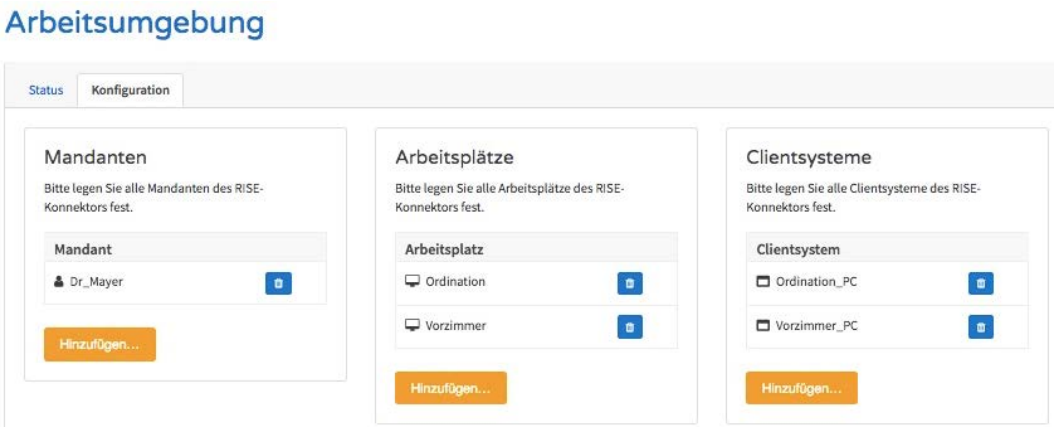


Abbildung 42: Beispiel: 1 Mandant, 2 Arbeitsplätze, 2 Clientsysteme

Als nächstes können darunter Verknüpfungen zwischen Mandanten, Arbeitsplätzen und Clientsystemen hergestellt werden.

Unter dem Punkt "Welcher Mandant verwendet welche Arbeitsplätze?" werden alle konfigurierten Mandanten aufgelistet (im Rahmen dieses Beispiels nur "Dr_Mayer") und diesem können dann mittels "Arbeitsplatz hinzufügen..." alle ihm zuordenbaren Arbeitsplätze zugewiesen werden (siehe Abbildung 43).

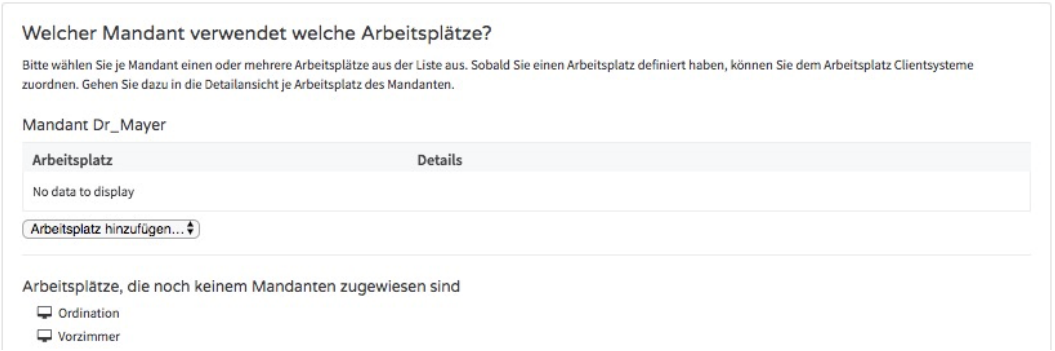


Abbildung 43: Konfiguration – Zuweisung zwischen Mandanten und Arbeitsplätzen

Da beide konfigurierten Arbeitsplätze der Ordination von Dr. Mayer angehören, werden auch beide mittels "Arbeitsplatz hinzufügen…" diesem zugeordnet (siehe Abbildung 44).

Anmerkung: Jedem Mandanten muss mindestens ein Arbeitsplatz zugewiesen werden.

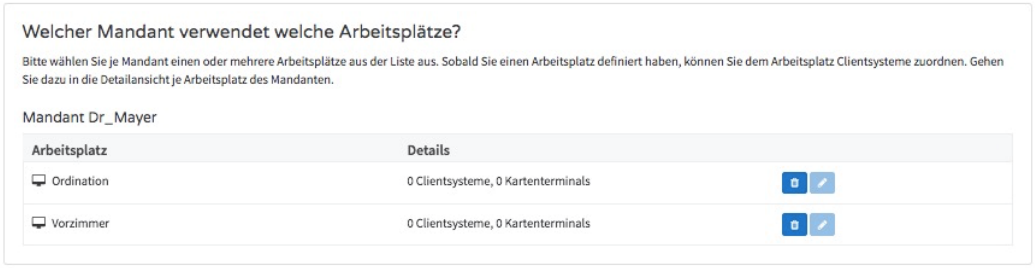


Abbildung 44: Beispiel – Zuweisung 2 Arbeitsplätze zu einem Mandanten

Anmerkung: Derselbe Arbeitsplatz kann auch mehreren Mandanten hinzugefügt werden. Das wäre z.B. ein Szenario, bei dem in einer Ordination zwei verschiedene Ärzte arbeiten, aber gemeinsam eine Sprechstundenhilfe haben. In diesem Szenario gäbe es zwei Mandanten (einen pro Arzt), drei Arbeitsplätze und 3 Clientsysteme (2x Arzt, 1x Sprechstundehilfe). Den beiden Mandanten werden jetzt jeweils zwei Arbeitsplätze zugewiesen (einmal ihr eigener und einmal der gemeinsame der Sprechstundenhilfe):

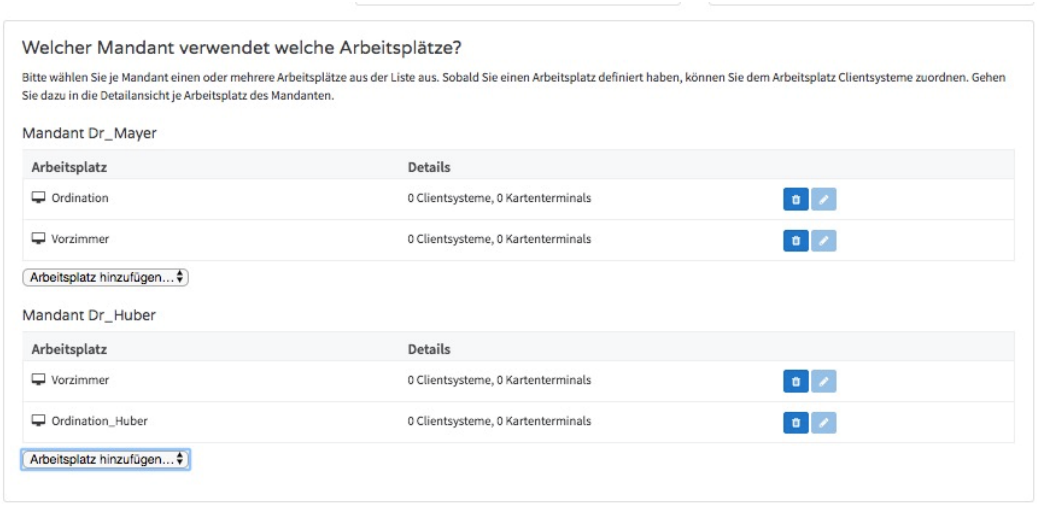


Abbildung 45: Weiterführendes Beispiel – 2 Mandanten, geteilter Arbeitsplatz

Wichtig: Nach dem Hinzufügen von Arbeitsplätzen (mittels "Arbeitsplatz hinzufügen...) muss der"Speichern" Button am Ende der Seite geklickt werden, damit die Änderungen auch tatsächlich übernommen werden. Erst ab diesem Zeitpunkt sind die Details (Stift-Symbol) des jeweiligen Arbeitsplatzes einzusehen und auch zu konfigurieren. Vergleiche hierzu Abbildung 44 (vor dem Speichern ist das Stift-Symbol deaktiviert) und Abbildung 46 (nach dem Speichern).

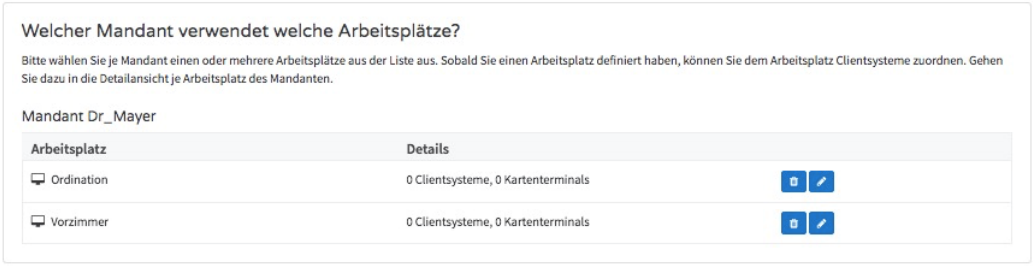


Abbildung 46: Beispiel – Nach dem Speichern ist die Detailansicht aktiviert

In der Detailansicht (Mandant "Dr_Mayer" und Arbeitsplatz "Ordination") können jetzt Clientsysteme zugewiesen werden (siehe Abbildung 47).

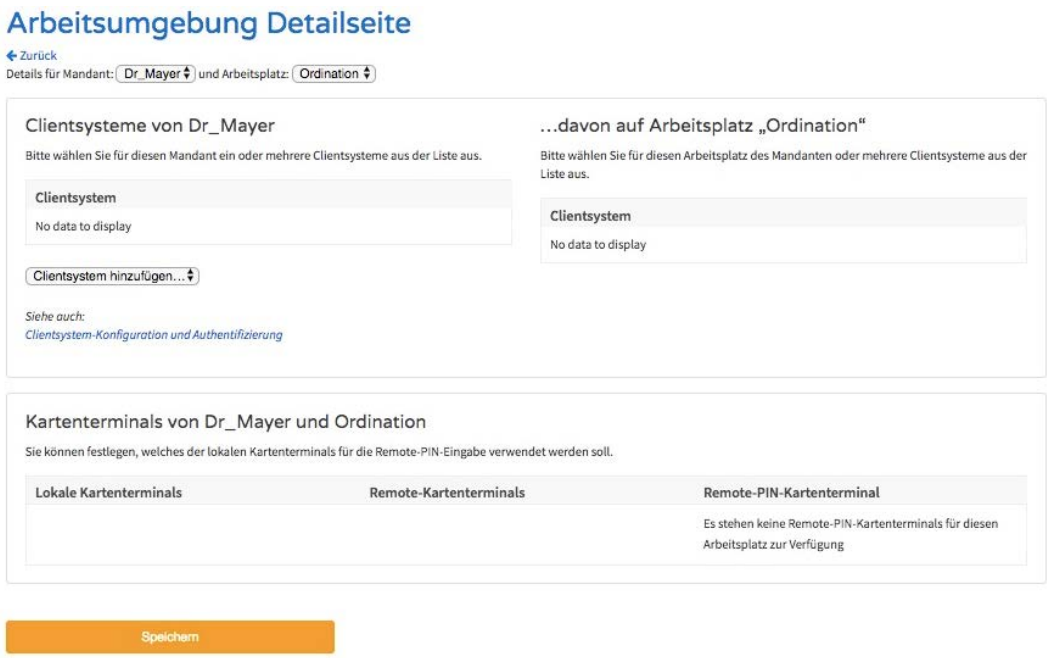


Abbildung 47: Beispiel – Detailseite für Mandant und Arbeitsplatz

Hierbei können mittels “Clientsystem hinzufügen…” generell Clientsysteme einem Mandanten zugewiesen werden (siehe Abbildung 48).

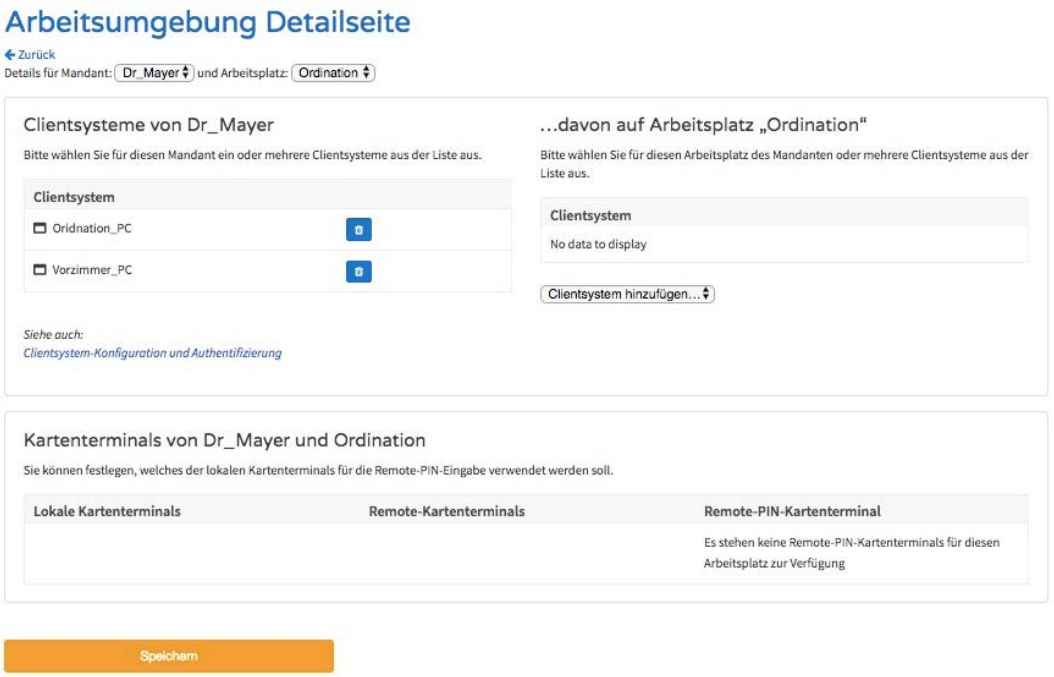


Abbildung 48: Beispiel – Clientsysteme einem Mandanten zuordnen

In einem nächsten Schritt kann dann auch entschieden werden, welche dieser Clientsysteme jetzt dem konkret ausgewählten Arbeitsplatz zugewiesen werden sollen (siehe Abbildung 49).

Abbildung 49: Beispiel – Clientsysteme zusätzlich einem Arbeitsplatz zuordnen

Wichtig: Nach dem Hinzufügen von Clientsystemen muss der “Speichern” Button am Ende der Seite geklickt werden, damit die Änderungen auch tatsächlich übernommen werden. Um auch dem Arbeitsplatz “Vorzimmer” ein Clientsystem hinzufügen zu können, kann auch einfach in der Menüleiste oben gewechselt werden (siehe Abbildung 50) und anschließend das entsprechende Clientsystem dem Arbeitsplatz zugewiesen werden.

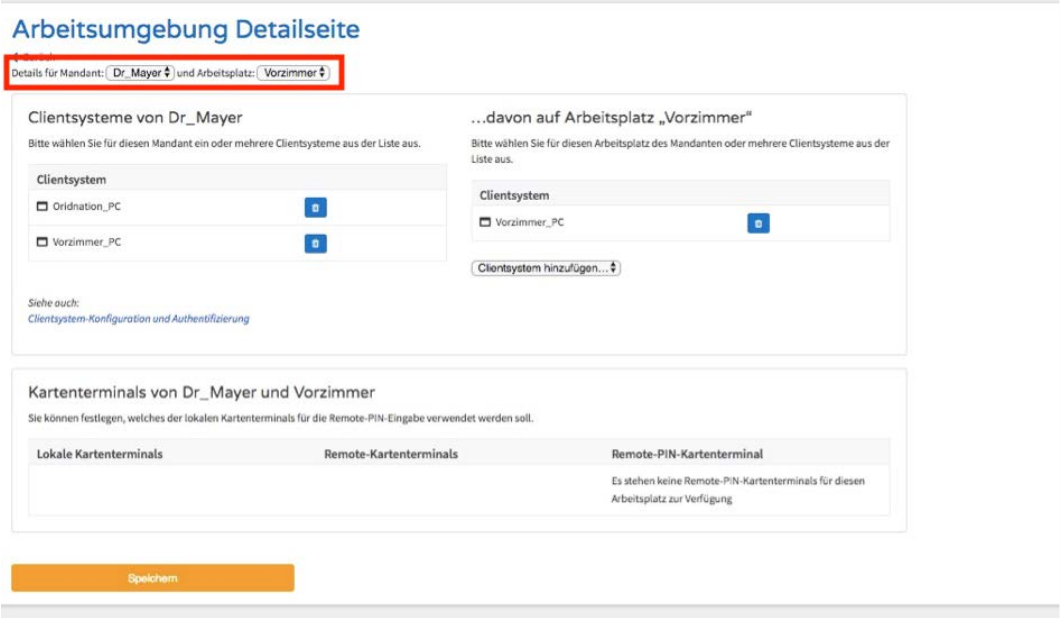


Abbildung 50: Detailansicht – schneller Wechsel zwischen Mandanten und Arbeitsplätzen

6.1.4.2.2 Zuweisung Kartenterminals zu Arbeitsplätzen

Um die nachfolgenden Schritte durchführen zu können, ist es einerseits erforderlich, dass die zu konfigurierenden Kartenterminals bereits mit dem RISE Konnektor gepaired wurden (siehe Abschnitt 6.3.4.1.1) und andererseits eine SMC-B Karte (Erklärung zu den verschiedenen Kartentypen - siehe Abschnitt 6.3.3) im System bekannt ist.

Prinzipiell gibt es drei Arten, wie ein Kartenterminal mit einem Arbeitsplatz (bzw. Arbeitsplatz und Mandanten) verknüpft werden kann:

- Lokale Kartenterminals: Ein lokales Kartenterminal befindet sich lokal an einem Arbeitsplatz und kann von diesem aus genutzt werden.

- Remote Kartenterminals: Ein Remote-Kartenterminal befindet sich nicht lokal an einem Arbeitsplatz, kann aber von diesem Arbeitsplatz aus (mit Hilfe eines Remote-PIN-Kartenterminals) verwendet werden.
- Remote-PIN-Kartenterminals: Ist ein lokales Kartenterminal (d.h. ein Kartenterminal, welches lokal auf einem Arbeitsplatz steht), das verwendet wird, um ein Remote-Kartenterminal (in dem z.b. die SMC-B Karte des Mandanten steckt) anzusteuern. Ein Remote-PIN-Kartenterminal kann allerdings immer nur für die Kombination Mandant + Arbeitsplatz konfiguriert werden.

Zur Abbildung des zu Beginn von Abschnitt 6.1.4.2 beschriebenen Szenarios müssen die Kartenterminals dem jeweiligen Arbeitsplatz zugewiesen werden. Das Beispiel aus Abschnitt 6.1.4.2.1 wird hierbei fortgesetzt.

Das Kartenterminal (Endung :D8, terminal-blau), das in der Ordination lokal vor Ort steht (lokales Kartenterminal), soll vom Vorzimmer aus auch angesteuert werden können (Remote Kartenterminal) (siehe Abbildung 51).

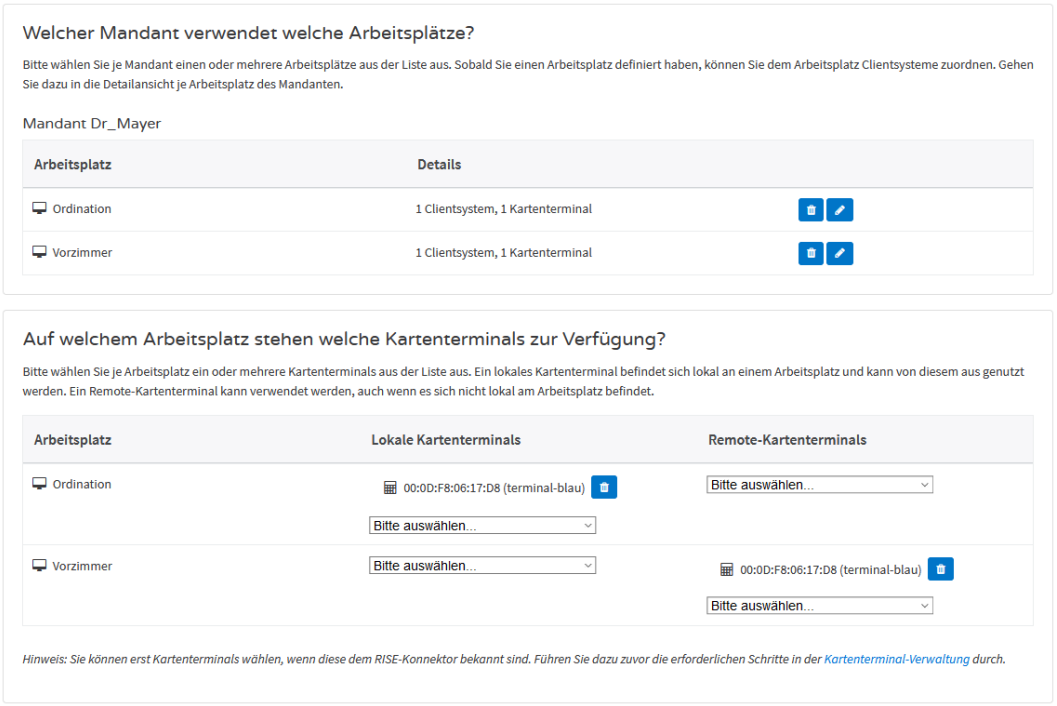


Abbildung 51: Beispiel – Ordinationsterminal, steht dem Vorzimmer auch Remote zur Verfügung

Zusätzlich gibt es noch das Kartenterminal (Endung :5A, terminal-rot), das lokal im Vorzimmer steht (siehe Abbildung 52).

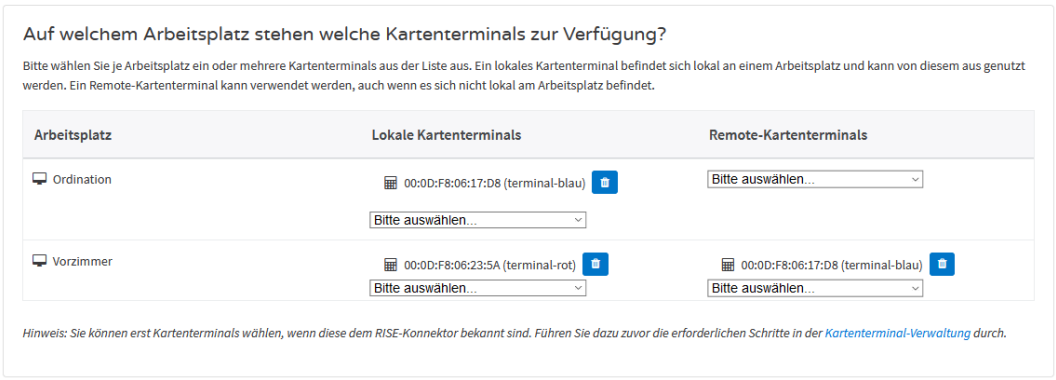


Abbildung 52: Beispiel – Zusätzliches lokales Kartenterminal im Vorzimmer

Damit aber das lokale Vorzimmer-Kartenterminal als Remote-PIN-Kartenterminal das Kartenterminal in der Ordination ansteuern kann, muss dies in der Detailansicht des Vorzimmer-Arbeitsplatzes konfiguriert werden (siehe Abbildung 53 und Abbildung 54).

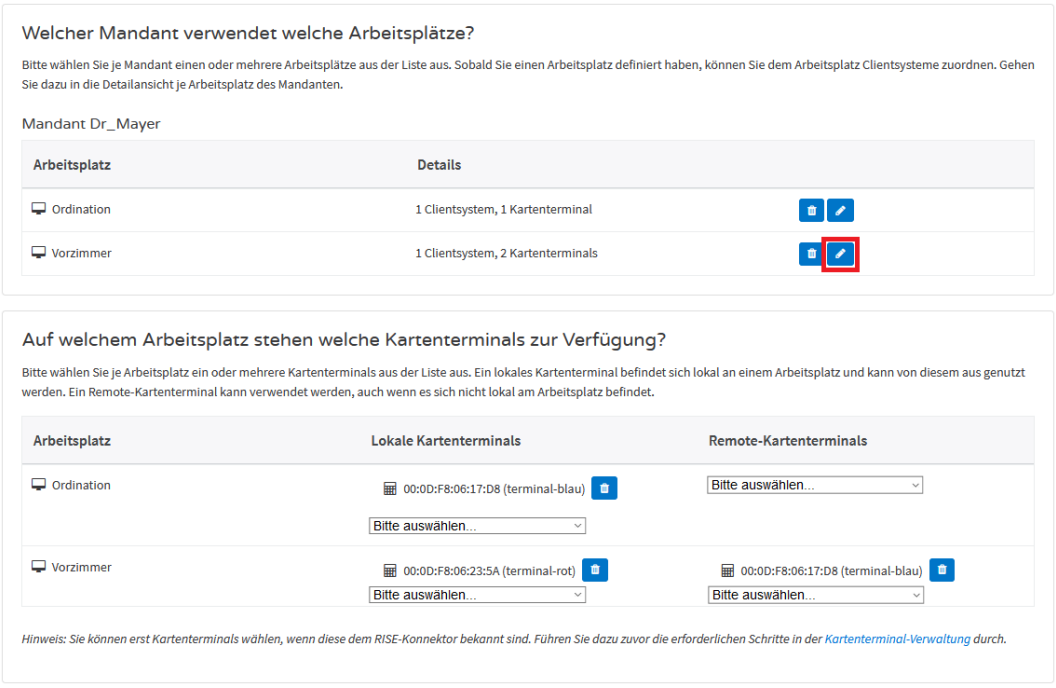


Abbildung 53: Beispiel – Klick auf Stift-Symbol um in die Detailansicht des Vorzimmers zu wechseln

In der Detailansicht (siehe Abbildung 54) kann jetzt das sich lokal im Vorzimmer befindliche Kartenterminal (Endung :5A, terminal-rot) als Remote-PIN-Kartenterminal konfiguriert werden, um das lokal am Ordinations-Arbeitsplatz befindliche Kartenterminal (Endung :D8, terminal-blau) ansteuern zu können.

Hinweis: Ein Kartenterminal kann nicht an einem Arbeitsplatz exklusiv einem Mandanten zugewiesen werden.

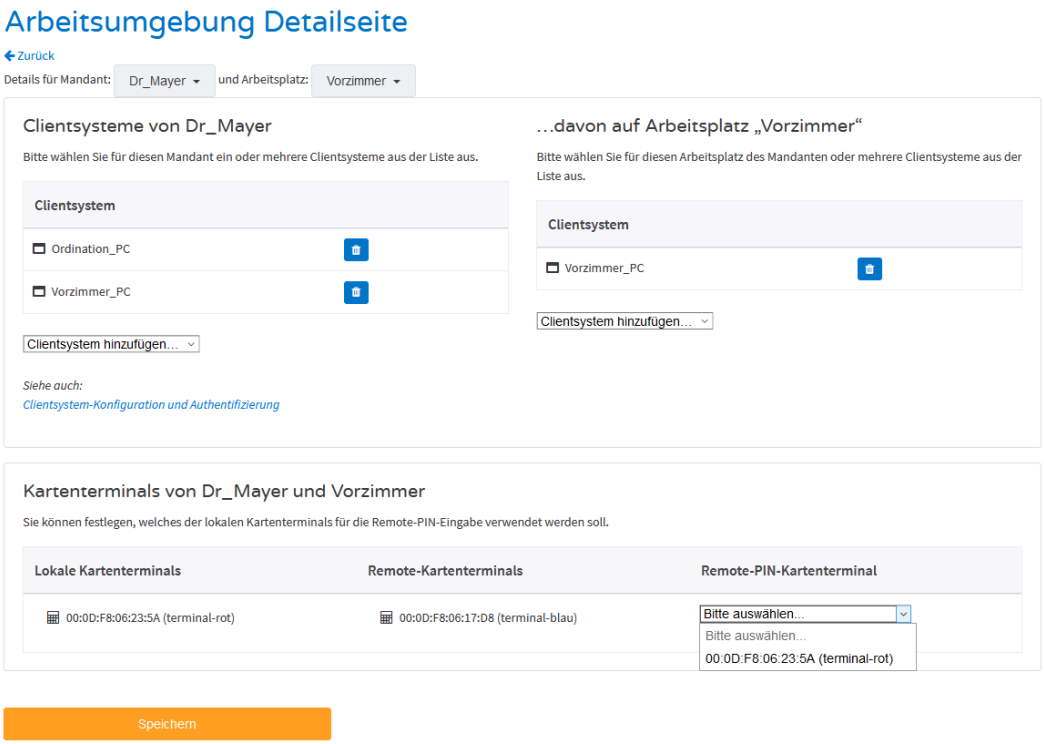


Abbildung 54: Beispiel – Auswahl des lokalen Kartenterminals, das als Remote-PIN-Kartenterminal dienen soll um das Remote-Kartenterminal anzusteuern

Die Konfiguration der Kartenterminals für das beschriebene Szenario ist somit abgeschlossen.

Anmerkung: Pro Arbeitsplatz können auch mehrere lokale Kartenterminals sowie Remote-Kartenterminals konfiguriert werden. In der Detailansicht (je Mandant und Arbeitsplatz) muss dann jeweils wiederum festgelegt werden, welches lokale Kartenterminal für die Remote-PIN-Eingabe verwendet werden soll.

6.1.4.2.3 Zuweisung SMC-B zu Mandanten

Im Menü “Arbeitsumgebung”, Reiter “Konfiguration” können die SMC-B Identitätskarten den einzelnen Mandanten zugewiesen werden (siehe Abbildung 55).

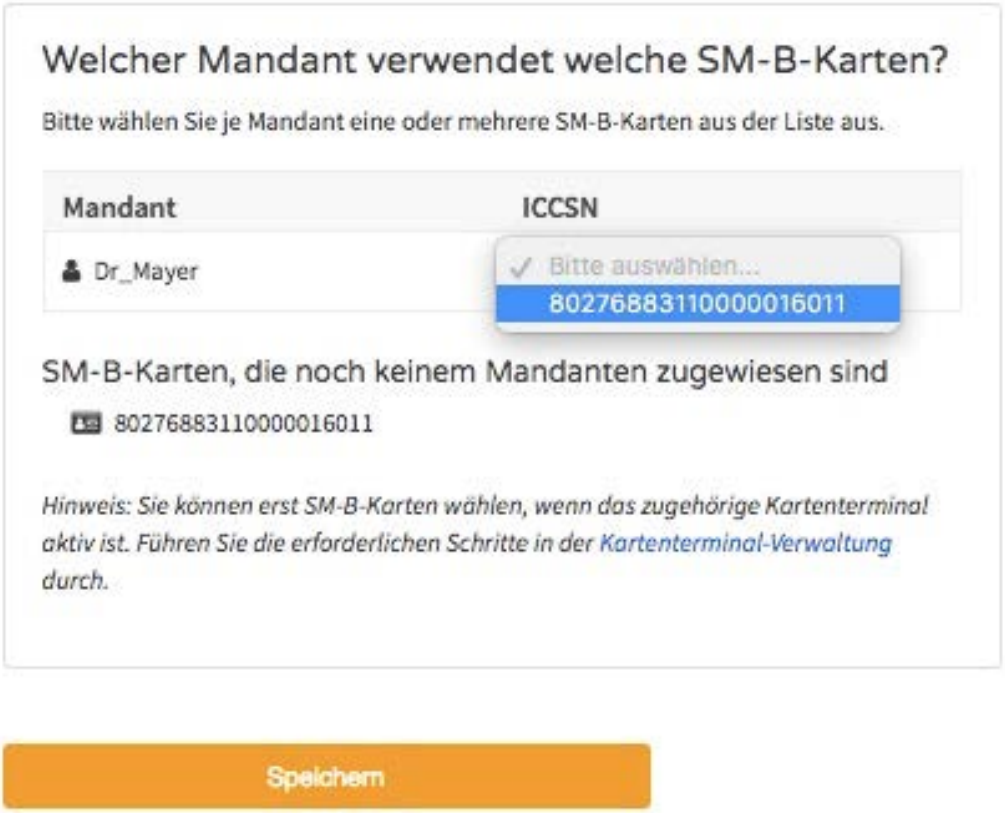


Abbildung 55: Zuweisung SMC-B zu Mandanten

6.1.4.3 Arbeitsumgebung – Konfiguration

Der Reiter "Konfiguration" in der Arbeitsumgebung bietet die Möglichkeit Mandanten, Arbeitsplätze und Clientsysteme zu konfigurieren und miteinander sowie mit Kartenterminals in Verbindung zu bringen.

Die prinzipielle Funktionsweise der Konfiguration wurde in Abschnitt 6.1.4.2 an Hand eines Beispiels erläutert. Der Konnektor ist aber auch für komplexere Anwendungsfälle konzipiert. Das heißt, er kann auch getrennt mit mehreren Mandanten, Clientsystemen und Arbeitsplätzen betrieben werden. Es ist auch zulässig, dass mehrere Arbeitsplätze von unterschiedlichen Clientsystemen bzw. Mandanten genutzt werden.

Um Kartenterminals einem Arbeitsplatz bzw. einem Arbeitsplatz in Kombination mit einem Mandanten zuweisen zu können muss dieses Kartenterminal bereits mit dem RISE Konnektor gepaired worden sein. Erklärungen zu lokalen Kartenterminals, Remote Kartenterminals und Remote-PIN-Kartenterminals sind in Abschnitt 6.1.4.2.2 zu finden. Um eine SMC-B Karte einem Mandanten zuweisen zu können, muss diese ebenfalls dem RISE Konnektor bekannt sein (Erklärung zu den verschiedenen Kartentypen - siehe Abschnitt 6.3.3).

Hinweis: Der Konnektor kann nur mit einer vollständigen, in sich stimmigen Definition im vollen Umfang in Betrieb genommen werden. Bitte überprüfen Sie, ob

Sie auch alle Beziehungen und Definitionen korrekt vorgenommen haben. Hierbei kann auch die Status-Ansicht behilflich sein (siehe Abschnitt 6.1.4.4).

Sicherheitshinweis: Der Administrator ist jederzeit für die korrekte Zuordnung von Kartenterminals und Clientsystemen verantwortlich.

6.1.4.4 Arbeitsumgebung – Status

Der Reiter "Status" in der Arbeitsumgebung soll eine Übersicht über alle Einstellungen betreffend der Arbeitsumgebung geben, die im Reiter "Konfiguration" vorgenommen wurden. Die Ansicht kann hierbei nach unterschiedlichen Systemteilen gruppiert werden (siehe Abbildung 56).

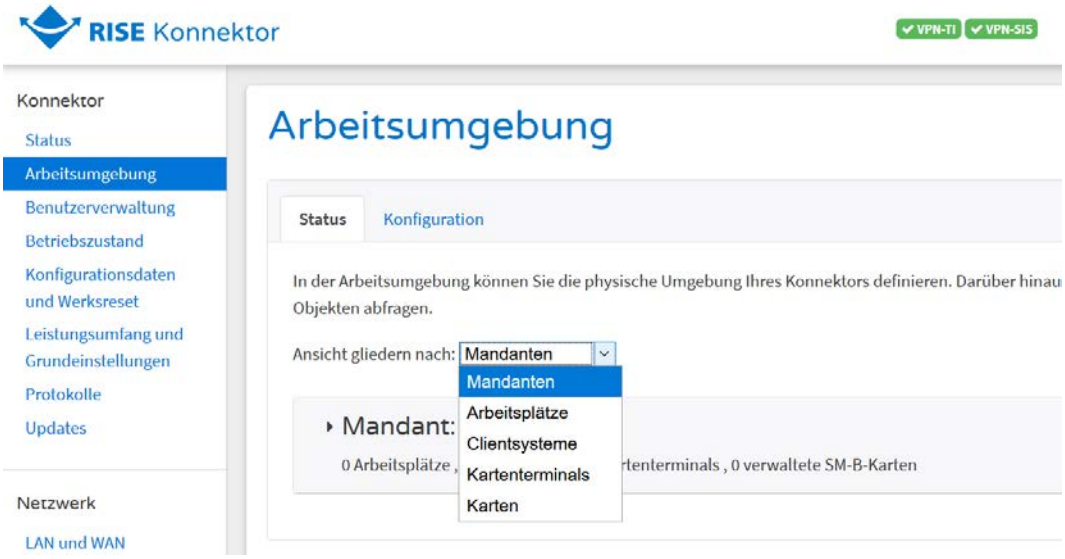


Abbildung 56: Arbeitsumgebung – Status – Gliederung der Ansicht

Wird beispielsweise die Gruppierung nach Arbeitsplätzen gewählt, werden in einer Liste alle konfigurierten Arbeitsplätze angezeigt (siehe Abbildung 57).

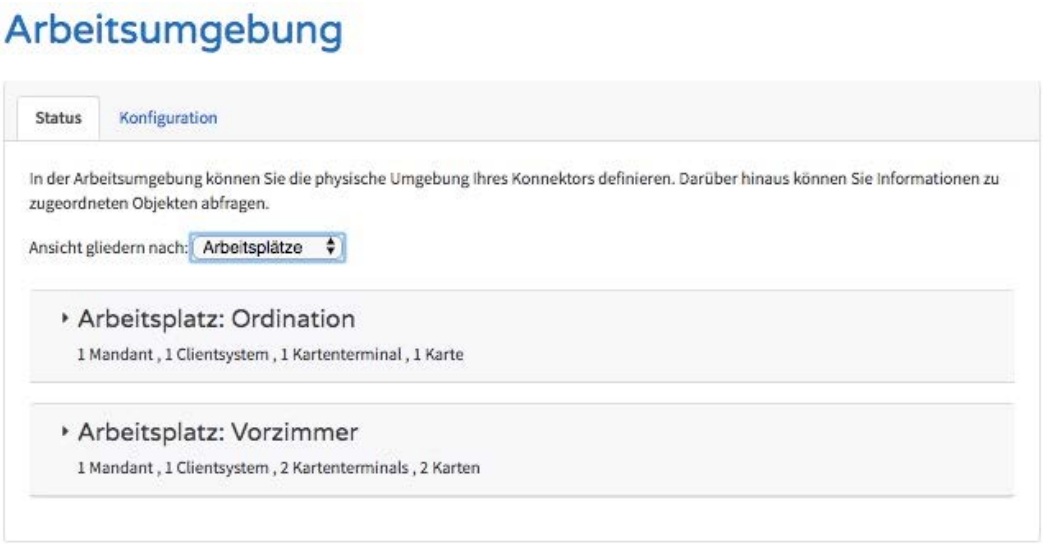


Abbildung 57: Arbeitsumgebung – Status – Gliederung nach Arbeitsplatz

Mithilfe eines Klicks auf einen der Listeneinträge werden im Detail alle Einstellungen zu dem jeweiligen Objekt angezeigt (siehe Abbildung 58). Das gibt eine Übersicht über alle Konfigurationswerte und Zusammenhänge des jeweiligen Objektes und erleichtert die Fehlersuche im Fall von falscher oder unvollständiger Konfiguration.

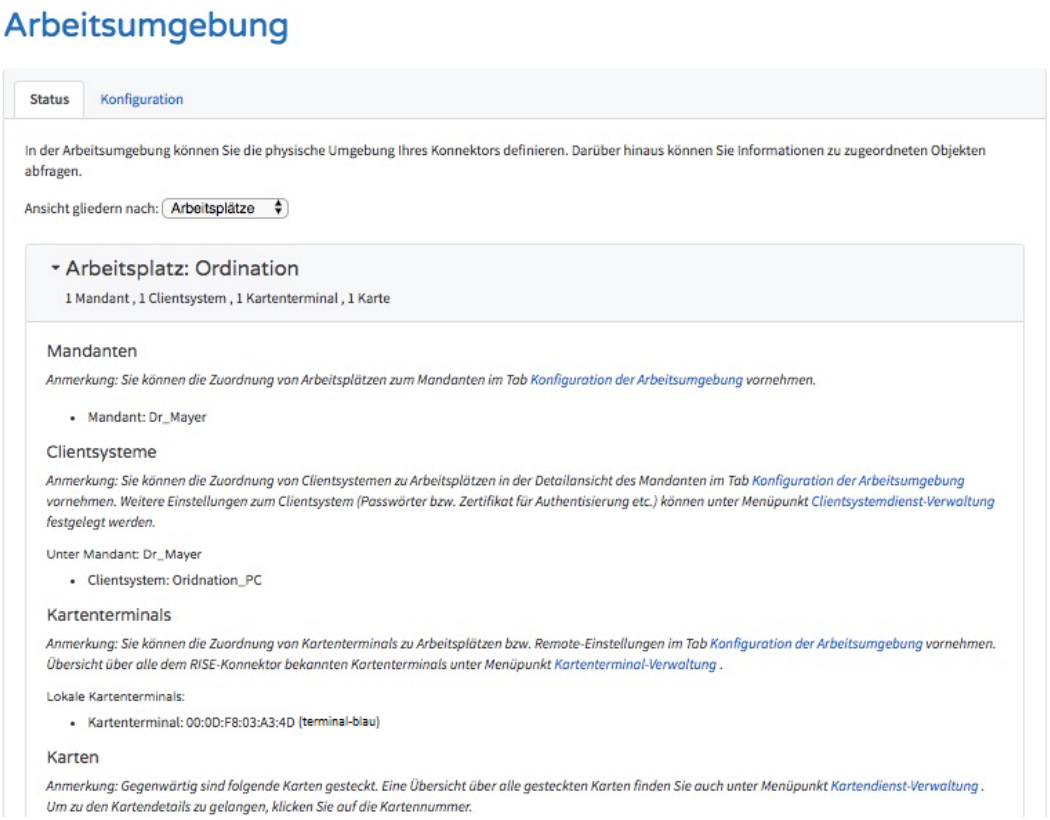


Abbildung 58: Arbeitsumgebung – Status – Details eines Arbeitsplatzes

6.1.5 RISE Konnektor Benutzerverwaltung

Im Menü "Benutzerverwaltung" kann die Administration der Benutzer des RISE Konnektors durchgeführt werden. Wie bereits in Abschnitt 5.4 beschrieben, ist diese Möglichkeit einem Super-Administrator vorbehalten. Wie in Abbildung 59 ersichtlich werden in einer Liste zunächst alle bereits konfigurierten Benutzer angezeigt. Pro Benutzer wird angezeigt:

- **Benutzername:** Benutzername des Users beim Login; Groß- und Kleinschreibung wird berücksichtigt.
- **Name:** Vollständiger Name des Benutzers.
- **Rolle:** "Lokaler Administrator" bzw. "Super-Administrator" (siehe auch Beschreibung der Benutzerrollen in Abschnitt 5).
- Bleistift-Symbol: Button, um die Einstellungen eines Benutzers zu ändern.
- Schlüssel-Symbol: Button, um das Passwort für den Benutzer neu zu setzen (siehe Abbildung 64).

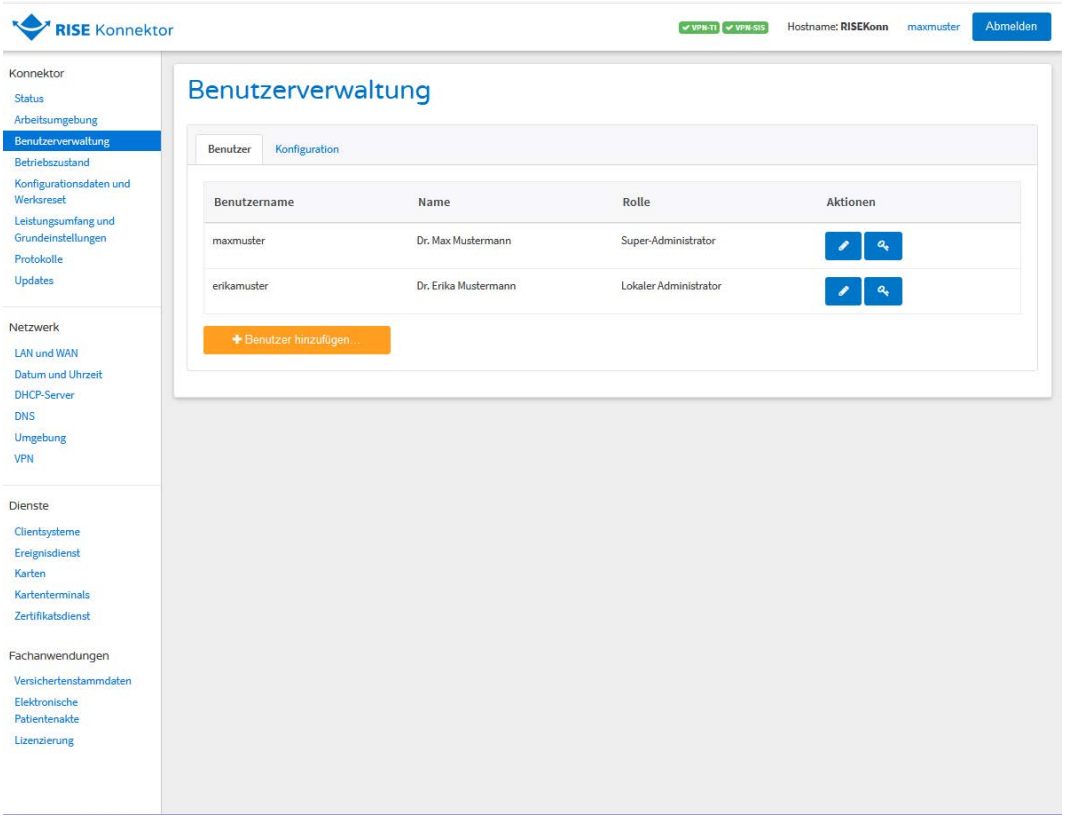


Abbildung 59: RISE Konnektor Benutzerverwaltung

Über den Button “Benutzer hinzufügen” können weitere Benutzer hinzugefügt werden (Abbildung 61).

6.1.5.1 Konfiguration

Über den Reiter “Konfiguration” im Menü “Benutzerverwaltung” können Sie die Gültigkeit von Passwörtern von Benutzern einstellen, wie in Abbildung 60 dargestellt ist.

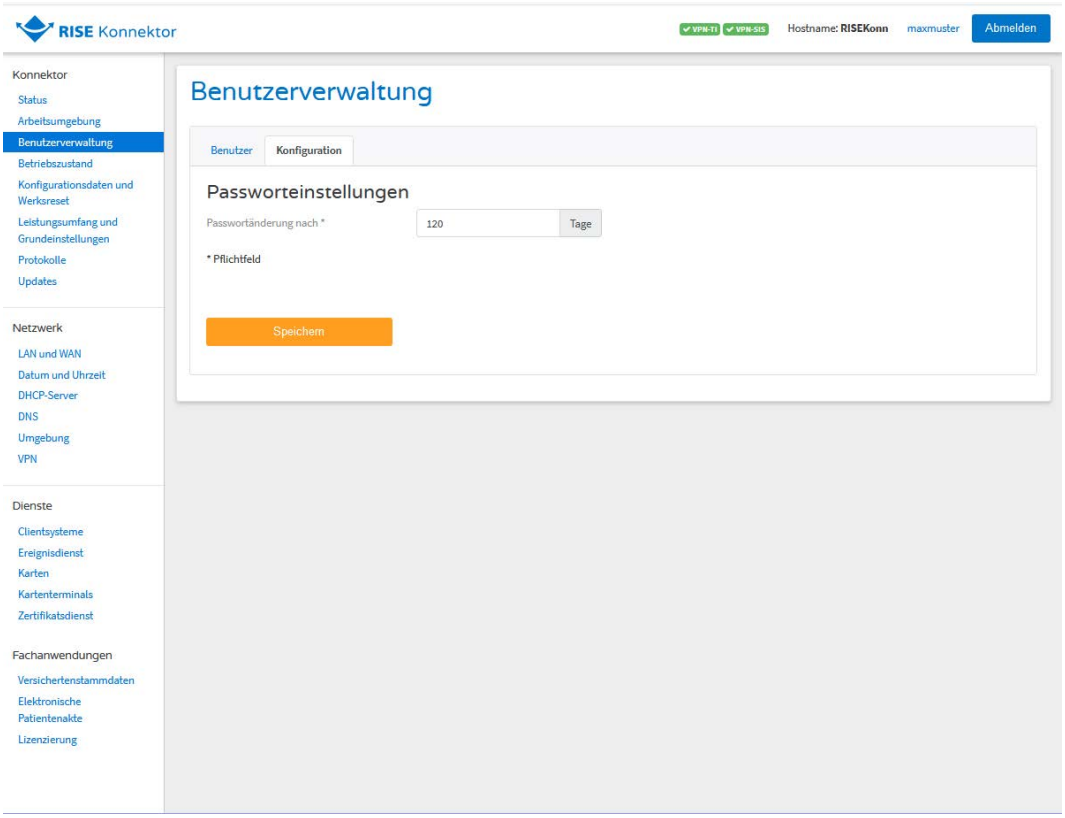


Abbildung 60: Gültigkeitsdauer von Benutzerpasswörtern

6.1.5.2 Benutzer hinzufügen

Durch Klick auf den Button "Benutzer hinzufügen" können Sie einen neuen Benutzer anlegen. Vergeben Sie hier die geforderten Daten, wie Benutzername, Rolle, Passwort, Kontaktdaten und Berechtigungen.

Der angeführte Benutzername muss eindeutig im System sein (Unterscheidung auch auf Groß- und Kleinschreibung). Es ist nicht möglich, einen bereits bestehenden Benutzernamen nochmals zu vergeben.

Bitte wählen Sie ein Passwort für den von Ihnen angelegten Benutzer. Dieses ist ein Einmalpasswort, d.h. der Benutzer wird nach dem ersten Login gebeten, sein Passwort selbst zu ändern. Bitte teilen Sie ihm das von Ihnen gewählte Passwort mit.

Hinweis: Bitte beachten Sie, dass das Passwort entsprechend den Sicherheitsrichtlinien gewählt werden muss. Diese sind in Abschnitt 4.1 beschrieben.

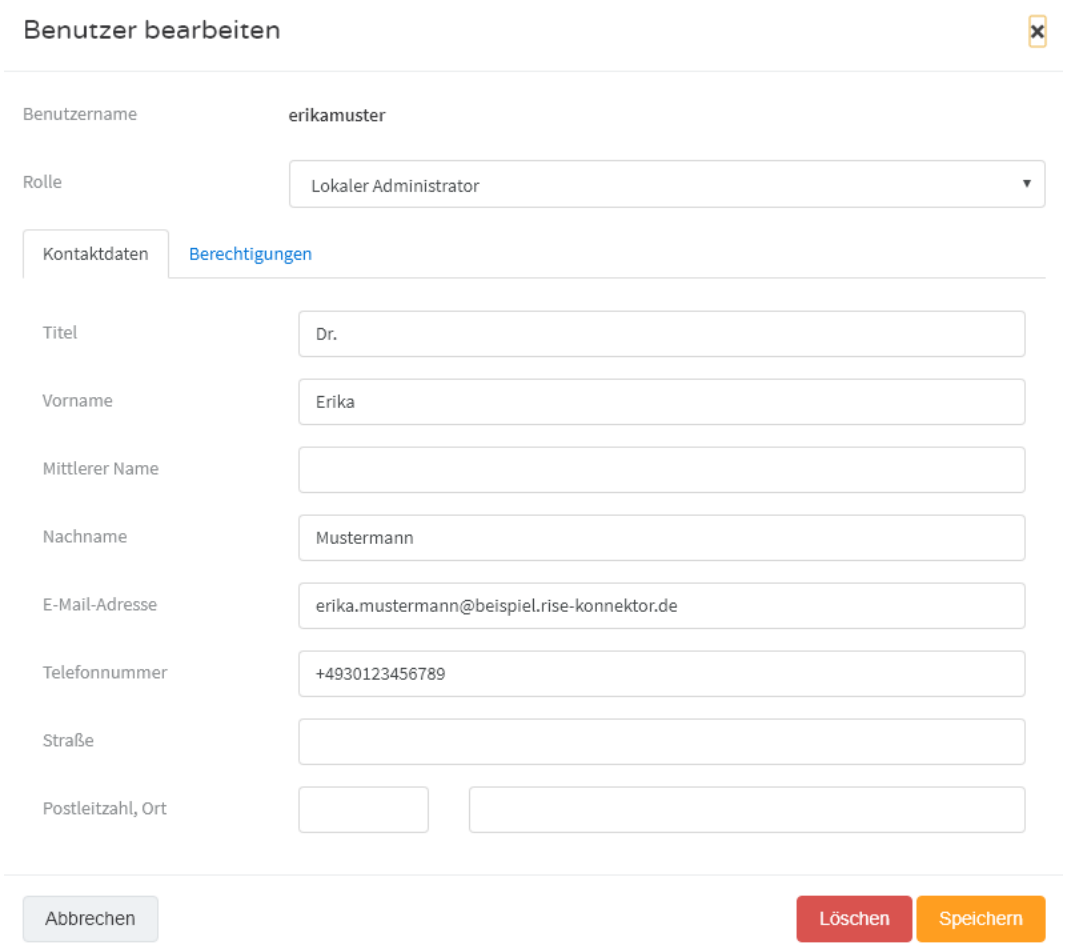


Abbildung 61: Benutzer hinzufügen

Im Reiter “Berechtigungen” werden abhängig von der gewählten Rolle die Standard-Berechtigungen der jeweiligen Rolle angezeigt (siehe hierzu auch Abschnitt 5 bzw. Abschnitt 6.1.5.3).

6.1.5.3 Berechtigungsverwaltung eines Benutzers

Die Benutzerrechte können in der Benutzerverwaltung bei jedem Benutzer im Reiter “Berechtigungen” individuell vergeben werden (siehe Abbildung 62 und Abbildung 63). Wenn das Häkchen bei einem Recht gesetzt ist, hat der jeweilige Benutzer dieses Recht. Dies bedeutet, dass er auf diese Seite gelangen kann beziehungsweise die entsprechenden Aktionen in der Management-Oberfläche durchführen kann. Bei Gruppen von Rechten bezieht sich das gesetzte Recht stets auf die unterste Ebene; die Gruppenbezeichnung darüber dient nur der besseren Lesbarkeit.

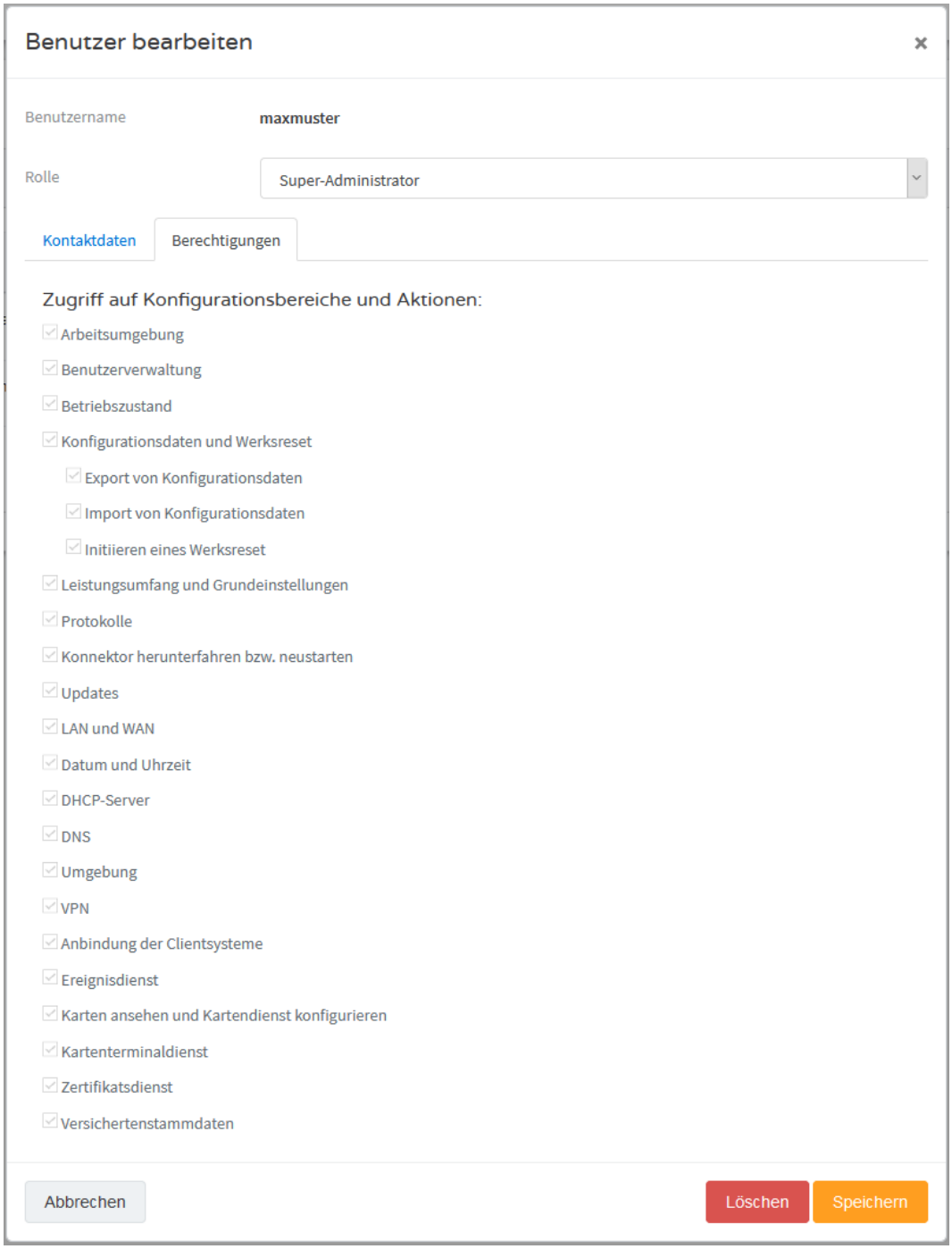


Abbildung 62: Berechtigungen eines Super-Administrators

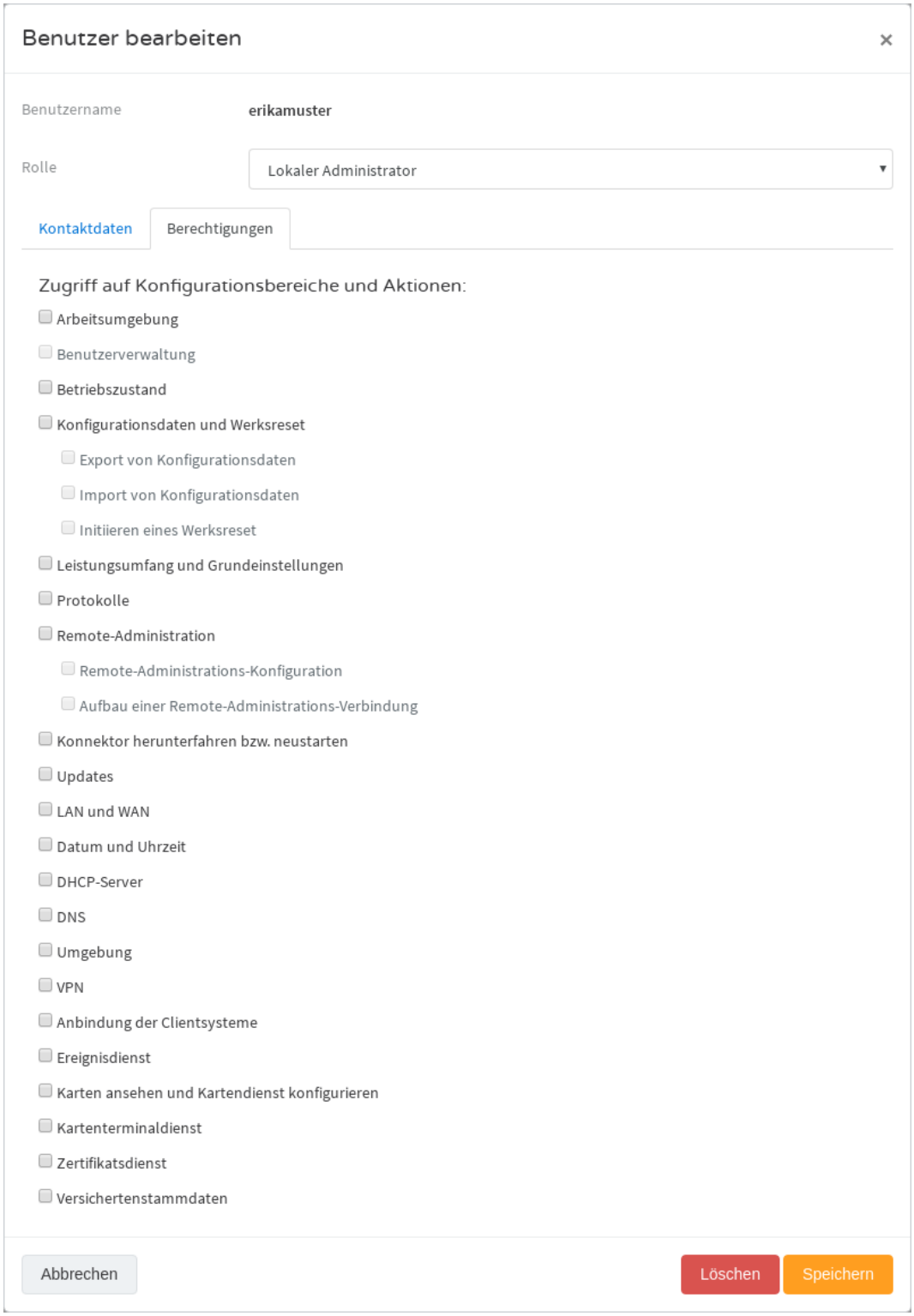


Abbildung 63: Standard-Berechtigungen eines Administrators

Hinweis: Es können nur jene Rechte vergeben werden, die eine entsprechende Rolle auch ausüben darf. Andernfalls ist ein Häkchen in der Rechteverwaltung ausgegraut und nicht anwählbar.

Hinweis: Grundsätzlich hat ein neu angelegter lokaler Administrator alle Rechte, die standardmäßig für ihn vorgesehen sind. Das Entfernen einzelner Rechte führt zur

Entfernung der entsprechenden Menüpunkte – kann aber auch Einfluss auf andere Funktionen haben. Daher sollen, um unbeabsichtigten Funktionseinschränkungen vorzubeugen, nur im Ausnahmefall die Berechtigungen eingeschränkt werden. Der Super-Administrator muss nach Anpassung einzelner Rechte prüfen, ob noch alle Funktionalitäten, wie von ihm gewünscht, vorhanden sind.

6.1.5.4 Passwort zurücksetzen

Durch Klicken auf das Schlüsselsymbol in der rechten Spalte der Benutzerverwaltungs-Liste, lassen sich Passwörter der jeweiligen Benutzer neu setzen (Abbildung 64).

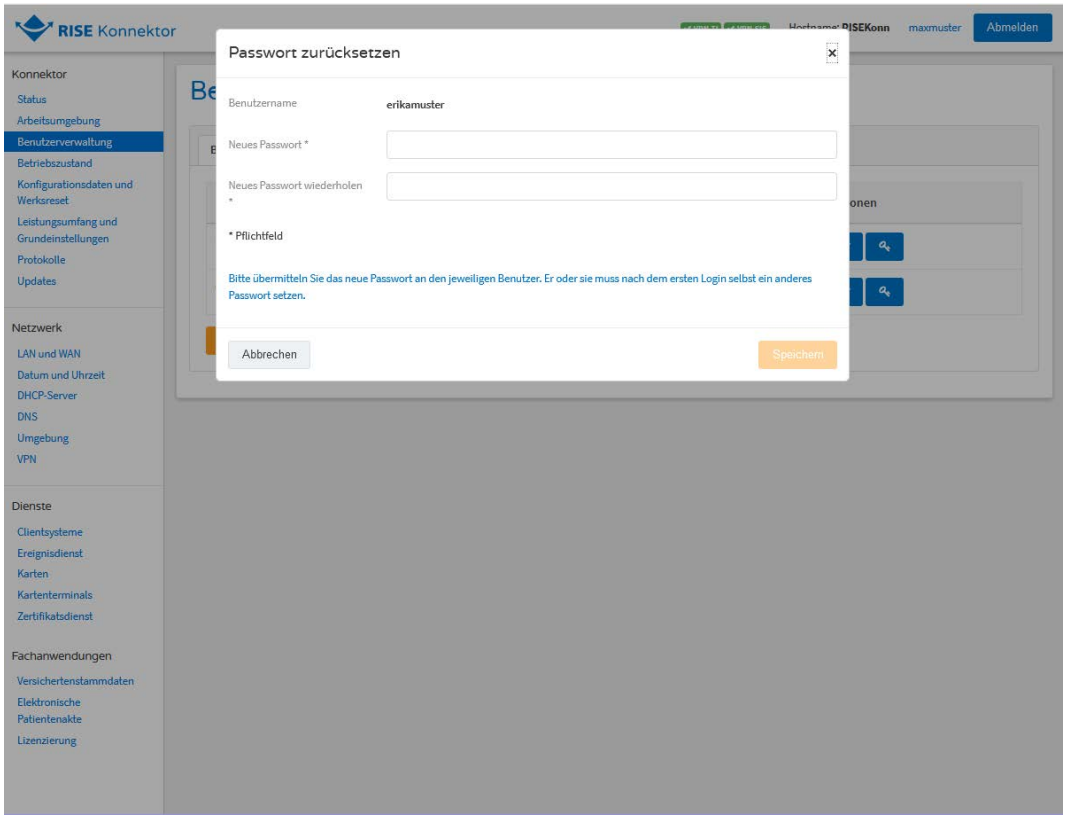


Abbildung 64: Passwort ändern

Warnung: Der Administrator ist verantwortlich, dass das neu gesetzte Passwort auf einem sicheren Weg zum Benutzer gelangt und zu jedem Zeitpunkt vor dem Missbrauch Dritter geschützt wird.

Hinweis: Bitte beachten Sie, dass das Passwort entsprechend den Sicherheitsrichtlinien gewählt werden muss. Diese sind in Abschnitt 4.1 beschrieben.

6.1.5.5 Benutzer bearbeiten oder löschen

Durch Klicken auf den Button “Bearbeiten” in der Benutzertabelle gelangen Sie zur Detailansicht des Benutzers. Dort können Sie die Kontaktdaten des jeweiligen Benutzers bearbeiten (Reiter “Kontaktdaten”) oder ihn löschen. Des Weiteren

können Sie die Benutzerrolle des Benutzers ändern bzw. ihm eingeschränkten Zugriff zur Wegnahme von bestimmten, vordefinierten Rechten geben (Reiter "Berechtigungen", vgl. auch Abschnitt 5 bzw. Abschnitt 6.1.5.3).

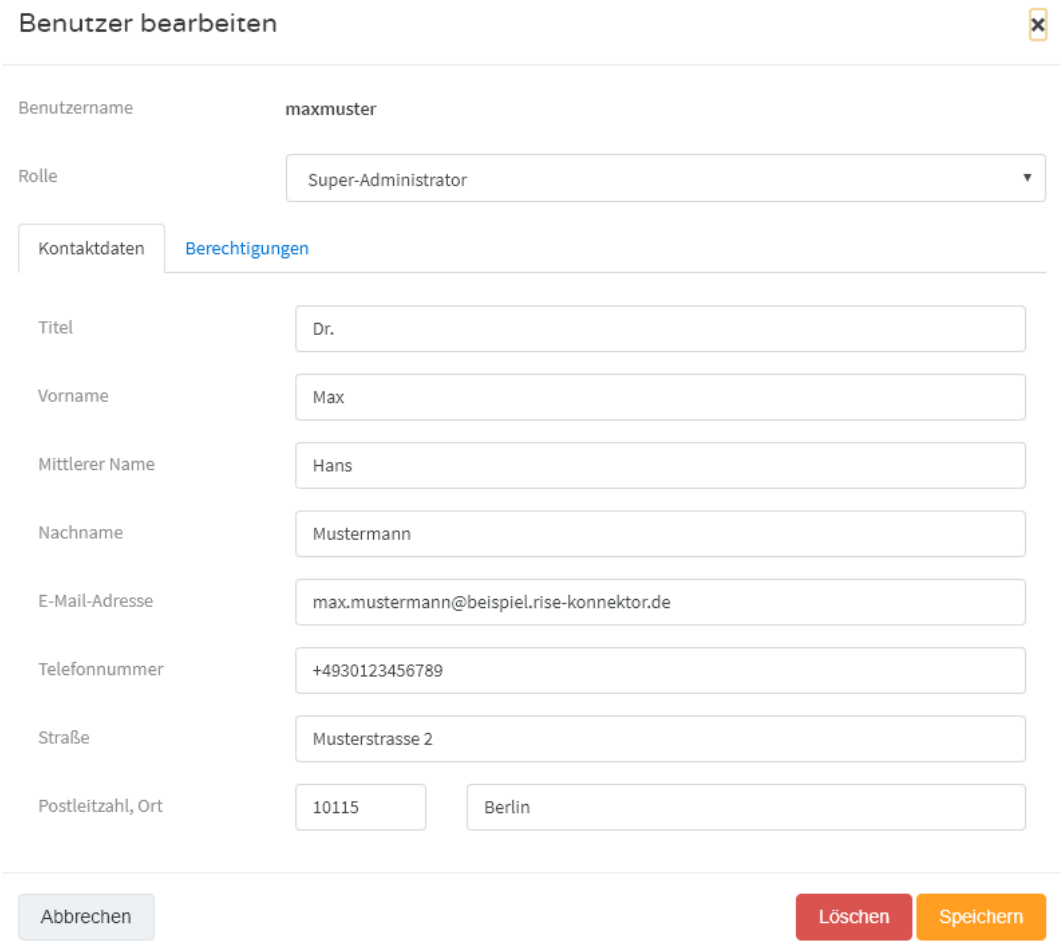


Abbildung 65: Benutzer bearbeiten oder löschen

Um die neuen Einstellungen zu übernehmen, wählen Sie den Button "Speichern".

Um einen Benutzer zu löschen, wählen Sie den Button "Löschen".

Warnung: Nach dem Löschvorgang kann sich der jeweilige Benutzer nicht mehr am RISE Konnektor anmelden.

Hinweis: Beachten Sie, dass es immer einen Benutzer mit der Rolle "Super-Administrator" geben muss. Sollte auf Ihrem System nur mehr ein Benutzer mit der Rolle "Super-Administrator" existieren, wird das Löschen unterbunden. Wenn Sie auch diesen Benutzer löschen möchten, führen Sie einen Werksreset durch (siehe Abschnitt 3.4.1).

6.1.6 RISE Konnektor Betriebszustand

Im Menüpunkt "Betriebszustand" sind Betriebs- und Fehlerzustände des RISE Konnektors tabellarisch dargestellt. Eine Übersicht zu allen, potentiell auftretenden

Fehler- und Betriebszuständen ist in Abschnitt 4.7 gegeben. Die Tabelle ist in der Management-Oberfläche (vgl. Abbildung 66) ersichtlich. Für eine Beschreibung der einzelnen Felder in der Tabelle siehe auch Abschnitt 4.7.

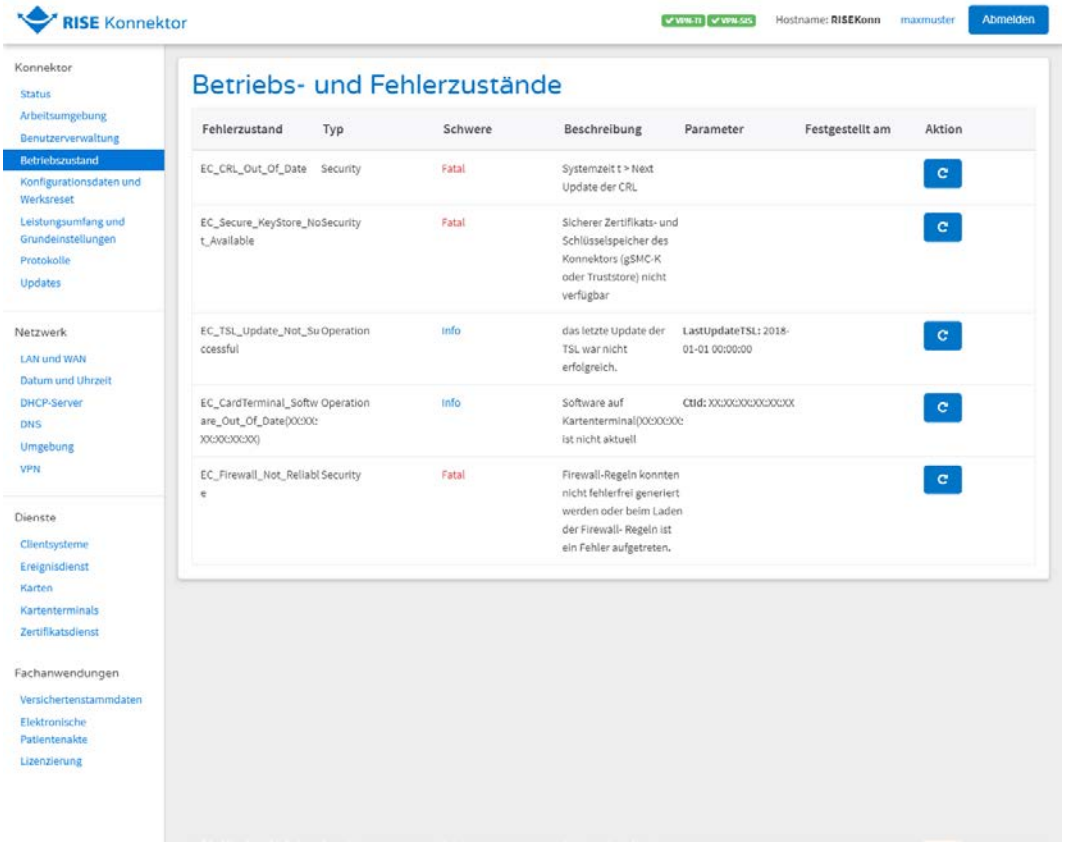


Abbildung 66: RISE Konnektor Betriebszustand

Ein Zurücksetzen des Fehlerzustandes ist für den Administrator nur dann möglich, wenn diese Funktionalität bei dem jeweiligen Fehlerzustand auch technisch erlaubt ist. Das bedeutet, die Software verhindert von selbst ein Zurücksetzen eines Fehlers, der anderswertig behoben werden muss (z.B. Fehler mit dem Status “fatal”).

Warnung: Das Zurücksetzen eines Fehlerzustandes zieht unter Umständen einen automatischen Neustart des RISE Konnektors nach sich. Sollte dies der Fall sein, wird ein entsprechender Hinweis in der Management-Oberfläche angezeigt. Während der RISE Konnektor neu startet, stehen dem Leistungserbringer sämtliche Funktionen nicht mehr zur Verfügung. Informieren Sie daher das Personal des Leistungserbringers rechtzeitig, wenn Sie planen, einen Fehlerzustand zurückzusetzen.

Um den Fehlerzustand zurückzusetzen, wählen Sie den Link im Abfragefenster, um zu den fehlerhaften Einstellungen zu gelangen (siehe Abbildung 67).

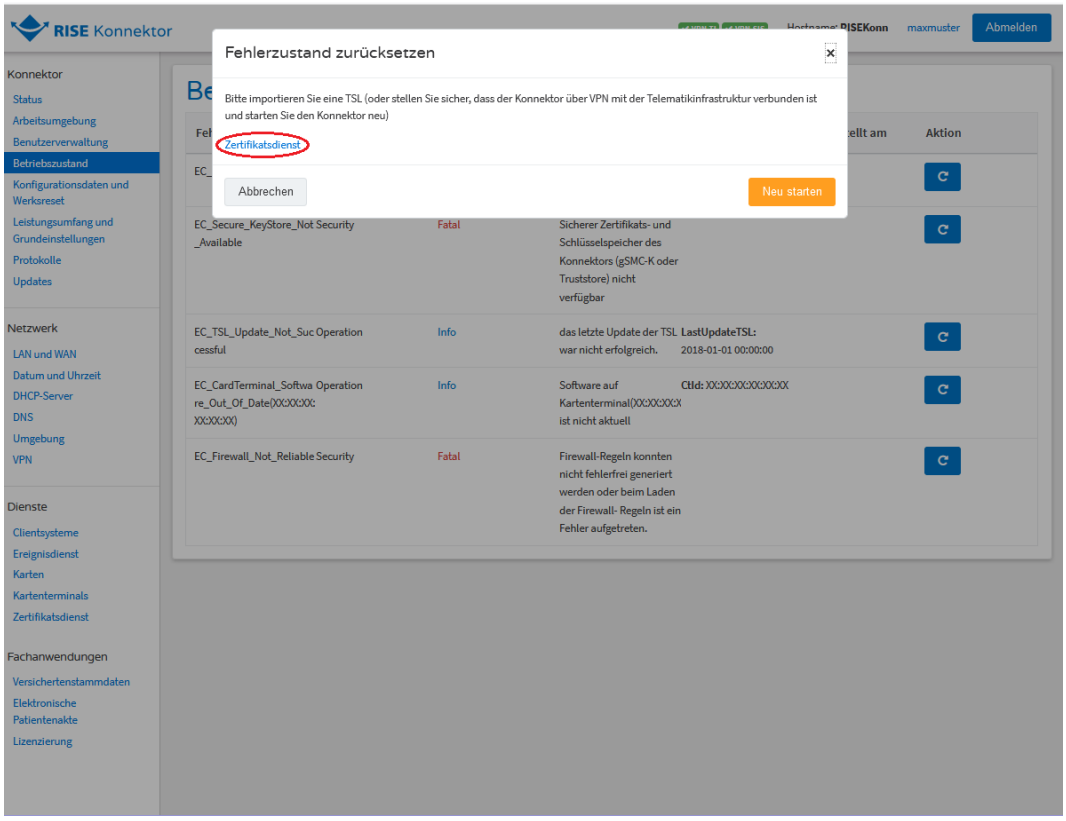


Abbildung 67: Fehlerzustand zurücksetzen

6.1.7 RISE Konnektor Konfigurationsdaten und Werksreset

Unter dem Menüpunkt “Konfigurationsdaten und Werksreset” befinden sich die Funktionalitäten, die gesamtheitlich auf die gesetzten Einstellungen Ihres RISE Konnektors wirken:

- Export von Konfigurationsdaten
- Import von Konfigurationsdaten
- Durchführung eines Werksresets (siehe Abschnitt 3.4.1)

6.1.7.1 Export Konfigurationsdaten

Der Export von Konfigurationsdaten (enthalten alle aktuellen Konfigurationsparameter des Konnektors) kann von allen Administratorrollen (die das entsprechende Recht besitzen) durchgeführt werden. Zum Schutz der Integrität, Authentizität und Nichtabstreitbarkeit der exportierten Daten wird eine Signatur mit der Hilfe einer SMC-B erstellt und mit den Konfigurationsdaten mitgeliefert. Des Weiteren wird eine Zeitangabe zum Signaturzeitpunkt in die Signatur integriert.

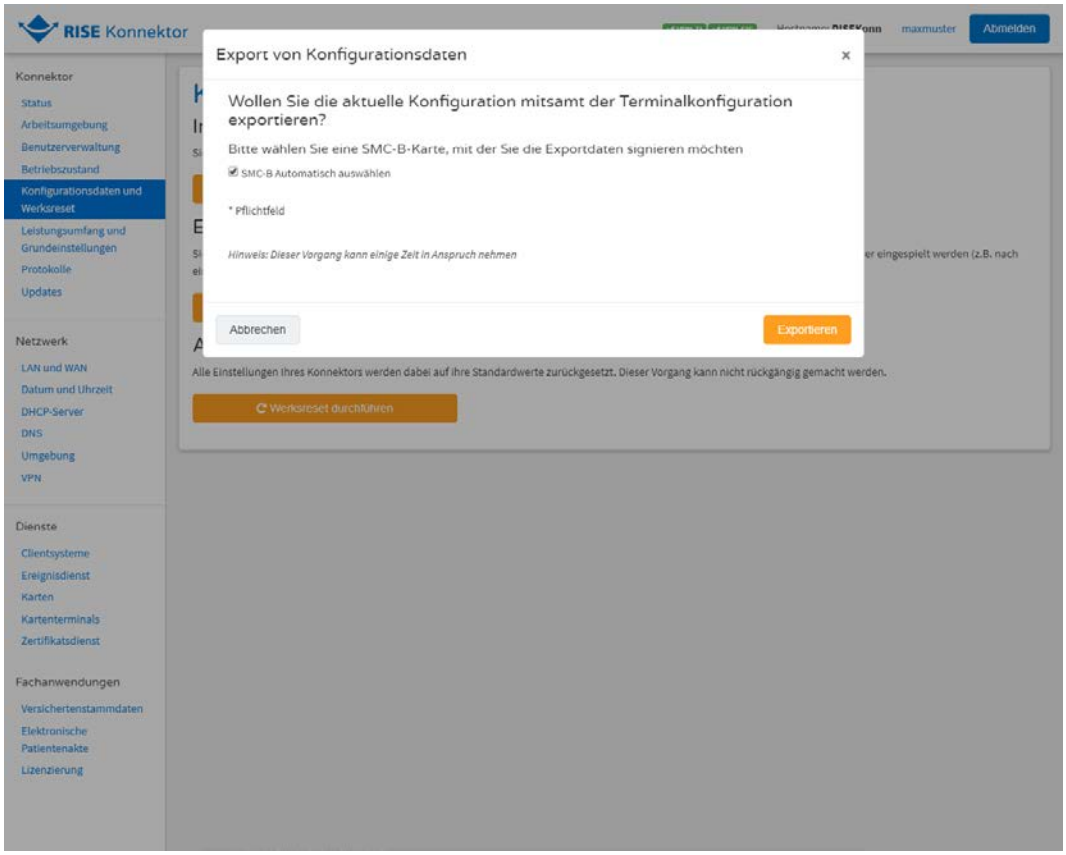


Abbildung 68: Export von Konfigurationsdaten: Schritt 1 - Automatische Auswahl einer SMC-B

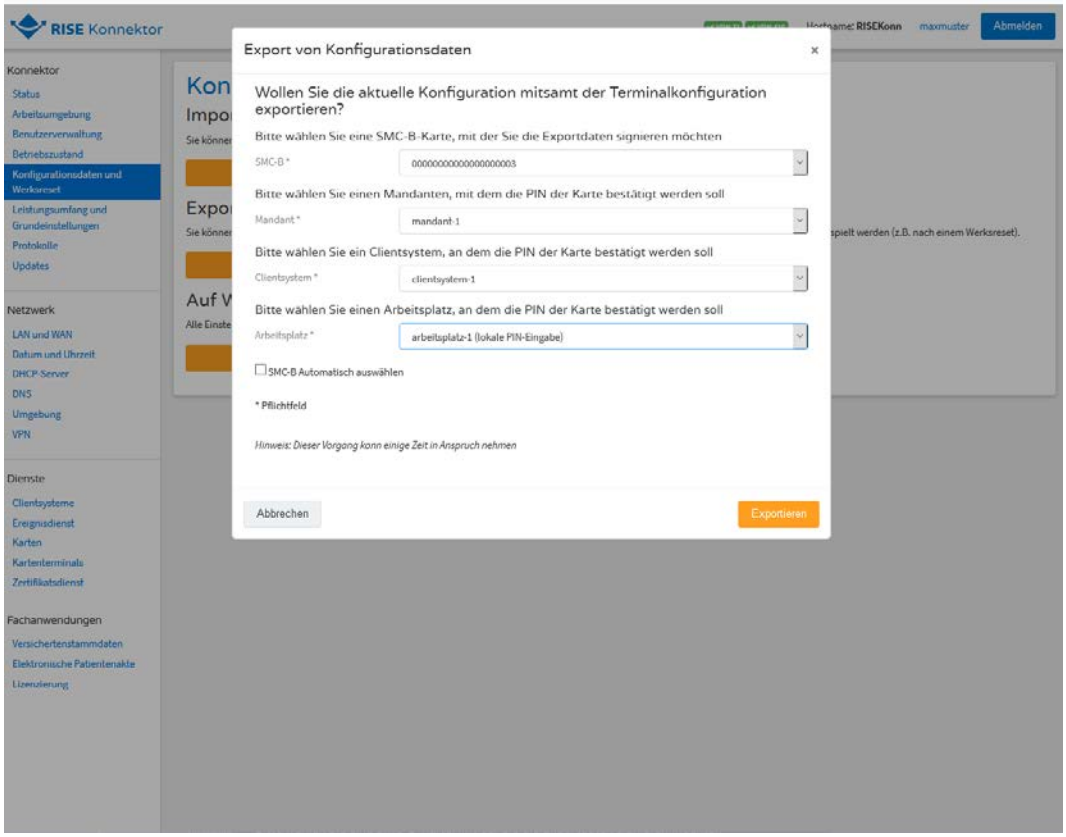


Abbildung 69: Export von Konfigurationsdaten: Schritt 1 - Manuelle Auswahl einer SMC-B

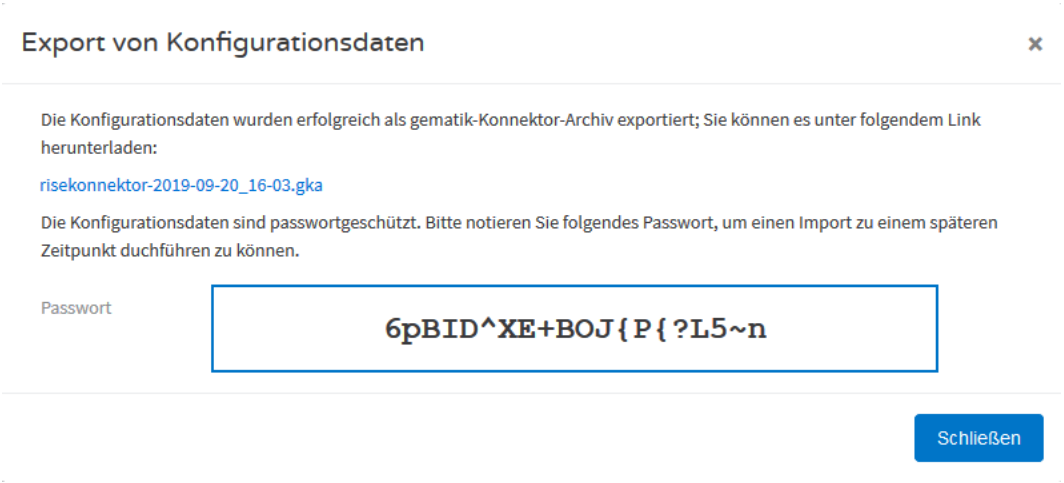


Abbildung 70: Export von Konfigurationsdaten: Schritt 2: Downloaddialog

Zum Exportieren der Konfigurationsdaten kann eine passende SMC-B, mit der die Daten signiert werden, entweder automatisch durch den Konnektor, oder manuell durch den Benutzer aufgewählt werden. Um die automatische Auswahl zu verwenden, wählen Sie im Dialogfeld für den Export (siehe Abbildung 68) das Feld SMC-B Automatisch auswählen aus. Der RISE Konnektor prüft dann für die vorhandenen SMC-Bs aller Mandanten in jedem möglichen Kontext, ob die PIN verifiziert ist. Wird auf diese Weise eine passende SMC-B gefunden, so wird diese für die Signatur des Exports verwendet. Ist dies nicht der Fall, so liefert das System die Fehlermeldung 30091 - "Automatische Auswahl einer freigeschalteten SMC-B für den Export der Konfigurationsdaten fehlgeschlagen. Manuelle Auswahl erforderlich." und die Auswahl muss manuell getätigt werden. Für die manuelle Auswahl entfernen Sie das Häkchen im Feld SMC-B Automatisch auswählen. Anschließend können eine SMC-B, ein Mandant, ein Clientsystem und ein Arbeitsplatz ausgewählt (siehe Abbildung 69) und der Export mit diesem Kontext durchgeführt werden.

Von dem Arbeitsplatz aus, welcher entweder im Zuge der automatischen Ermittlung einer SMC-B oder manuell ausgewählt wurde, muss die PIN der Karte bestätigt werden. Wenn ein Arbeitsplatz gewählt wird, dem nicht das Kartenterminal als lokales Kartenterminal zugeordnet ist, in dem die Karte steckt, muss die PIN am Remote-PIN-Kartenterminal des Arbeitsplatzes eingegeben werden.

Das Ergebnis des Exports ist ein verschlüsseltes Archiv (enthält Konfigurationsdaten und Signatur) und ein Passwort, das dem Administrator zur Verfügung gestellt wird. Bitte laden Sie dieses durch Klicken auf die Datei mit der Endung *.gka aus dem Download-Dialog (siehe Abbildung 68) herunter und notieren Sie sich das angezeigte Passwort. Im Zuge des Exports werden auch der Benutzername mitsamt den eingetragenen Kontaktdaten sowie der Zeitpunkt des Exports exportiert. Dies ist erforderlich, damit im Zuge des Imports aus Sicherheitsgründen festgestellt werden kann, wer den Export durchgeführt hat.

Beim Import werden immer die Daten des Benutzers, der den Export durchführt unter dem Bereich “Herkunft” angezeigt. Bitte prüfen Sie daher, ob Ihre Benutzereinstellungen aktuell sind. Falls nicht, sollten Sie diese aktualisieren (siehe Abschnitt 6.1.9).

Sicherheitshinweis: Der Administrator ist für die sichere Verwahrung und den sicheren Transport der exportierten Konfigurationsdaten (verschlüsseltes Archiv und Passwort) verantwortlich.

Sicherheitshinweis: Bitte beachten Sie, dass der Benutzer, der den Export durchführt, möglicherweise Zugriff auf Einstellungen erhält, die auf Grund seiner Berechtigungseinstellung gem. Abschnitt 6.1.5.3 für ihn über die Administrationsoberfläche nicht direkt einsehbar sind.

Hinweis: Nach Abschluss der Konfiguration des RISE Konnektors wird ein Export sämtlicher Konfigurationen empfohlen, um diesen Betriebszustand jederzeit wiederherstellen zu können.

6.1.7.2 Import Konfigurationsdaten

Der Import von Konfigurationsdaten obliegt ausschließlich einem Benutzer mit der Rolle Super-Administrator. Hierfür sind ein verschlüsseltes Archiv (enthält zuvor exportierte Konfigurationsdaten inkl. Signatur) sowie ein Passwort (wurde beim Export der Konfigurationsdaten angezeigt) erforderlich.

Für den Import muss das Archiv hochgeladen werden bzw. das Passwort angegeben werden.

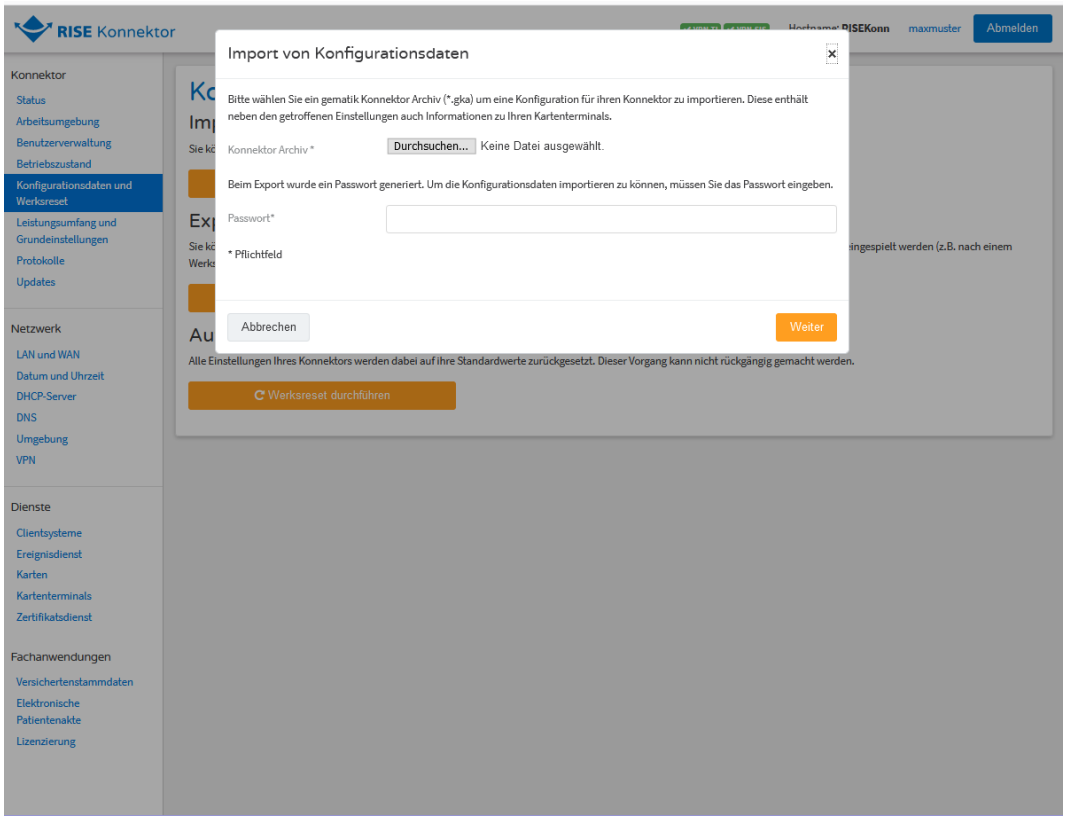


Abbildung 71: Import von Konfigurationsdaten: Schritt 1

Nach erfolgreichem Upload wird dem Super-Administrator der Zeitpunkt der Erstellung der exportierten Konfigurationsdaten, das Zertifikat, das Ergebnis der Validierung der Signatur, Informationen zum Benutzer, der den Export durchgeführt hat, und eine Kartenterminalliste angezeigt. Weiterhin muss der Super-Administrator die gewünschten eHealth-Kartenterminals auswählen, deren Einstellungen ebenfalls mit importiert werden sollen und bestätigen, dass er diese Konfigurationsdaten importieren möchte. Erst dann erfolgt der tatsächliche Import der Konfigurationsdaten (siehe Abbildung 72).

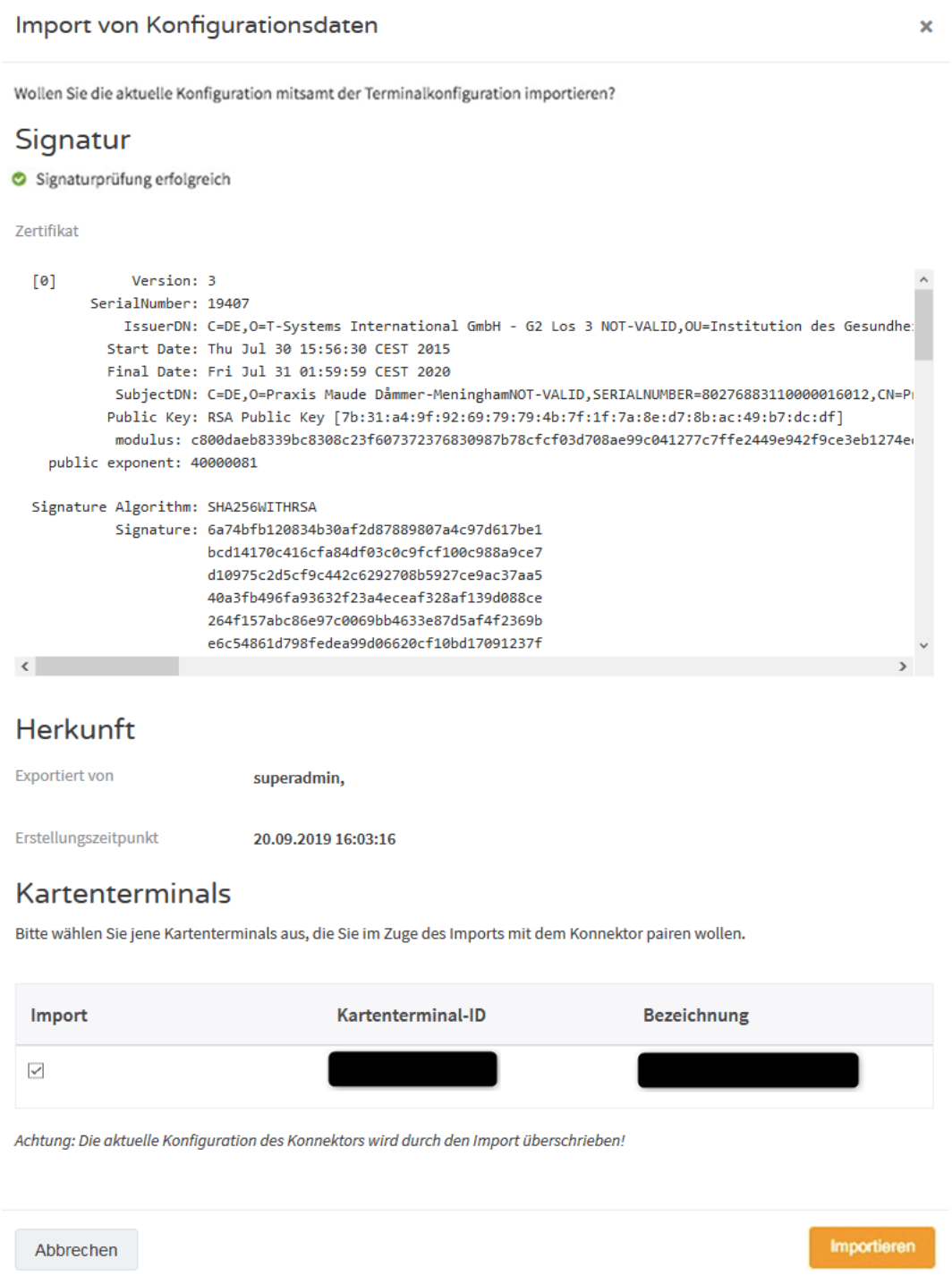


Abbildung 72: Import von Konfigurationsdaten: Signatur-, Herkunfts- und Kartenterminalprüfung

Sicherheitshinweis: Der Administrator ist verantwortlich, dass ein Import nach expliziter Bestätigung nur dann durchgeführt wird, wenn die Herkunft, der Erstellungszeitpunkt und das Zertifikat des Archivs korrekt sind.

Sicherheitshinweis: Prüfen Sie nach einem erfolgreichen Import sorgfältig, ob alle Einstellungen wie erwartet übernommen wurden, insbesondere die Konfiguration im Bereich Netzwerk (siehe Abschnitt 6.2).

Warnung: Ein Import von Konfigurationsdaten überschreibt die bisherige Konfiguration Ihres RISE Konnektors. Etwaige nach einem Export getroffene Einstellungen gehen dabei verloren. Dies kann den Betrieb Ihres RISE Konnektors beeinträchtigen. Führen Sie einen Import nur durch, wenn Sie sich den Folgen der neuen Einstellungen bewusst sind!

Warnung: Im Zuge eines Imports von Konfigurationsdaten startet der Konnektor automatisch neu. Während der RISE Konnektor neu startet, stehen dem Leistungserbringer sämtliche Funktionen nicht mehr zur Verfügung. Informieren Sie daher das Personal des Leistungserbringers rechtzeitig, wenn Sie planen, einen Import von Konfigurationsdaten am RISE Konnektor durchzuführen.

6.1.8 RISE Konnektor Leistungsumfang und Grundeinstellungen

Im Menü "Leistungsumfang und Grundeinstellungen" können, wie in Abbildung 73 zu sehen ist, Basis-Einstellungen für die Konfiguration des Konnektors getroffen werden (Leistungsumfang, Grundeinstellungen und Komfortsignatur). Eine Beschreibung der einzelnen Einstellungen ist in Tabelle 15 zu finden.

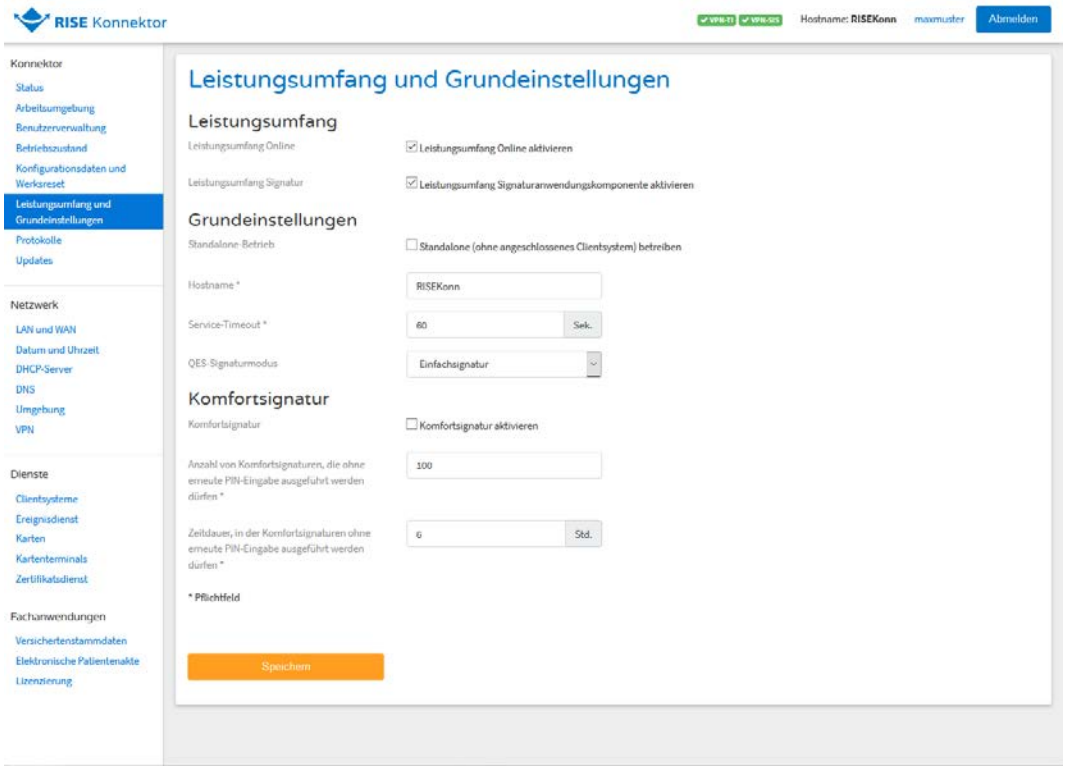


Abbildung 73: RISE Konnektor Leistungsumfang und Grundeinstellungen

Eine Beschreibung der einzelnen Einstellungen ist in Tabelle 15 zu finden.

ReferenzID	Belegung	Bedeutung
Leistungsumfang Online	Enabled /	Der Administrator kann den

ReferenzID	Belegung	Bedeutung
(MGM_LU_ONLINE)	Disabled; Standard-Wert: Enabled	"Leistungsumfang Online" aktivieren und deaktivieren (siehe auch Abschnitt 4.5.1 und Abschnitt 4.5.2).
Leistungsumfang Signatur (MGM_LU_SAK)	Enabled / Disabled; Standard-Wert: Enabled	Der Administrator kann den "Leistungsumfang Signaturanwendungskomponente" aktivieren und deaktivieren. Dieser Konfigurationsparameter wirkt hauptsächlich in dem Funktionsmerkmal "Signaturdienst".
Standalone-Betrieb (MGM_STANDALONE_KON)	Enabled / Disabled; Standard-Wert: Disabled	Der Administrator kann den Konnektor als alleinstehend konfigurieren.
Hostname (MGM_KONN_HOSTNAME) 12 Zeichen	Standard-Wert: "RISEKonn"	Der Hostname des Konnektors muss folgende Anforderungen erfüllen: Verwendung der Buchstaben "A bis Z" und "a bis z", Verwendung der Ziffern "0 bis 9", Verwendung von "–" als Sonderzeichen (Minus; nicht als erstes oder letztes Zeichen), sowie eine maximale Länge von 12 Zeichen. Die Verwendung weiterer Sonderzeichen sowie des Leerzeichens ist nicht möglich.
Service-Timeout (ANLW_SERVICE_TIMEOUT)	X Sekunden; Standard-Wert: 60 Sekunden	Der Administrator kann die maximale Zeit konfigurieren, in der ein Service antworten muss, bevor das System einen Timeout-Fehler meldet.
QES-Signaturmodus (SAK_SIMPLE_SIGNATURE_MODE)	Einfachsignatur / Stapelsignatur; Standard-Wert: Einfachsignatur	Der Administrator kann auswählen, ob für alle HBAx Einfachsignaturen im SecurityEnvironment #1 (SE#1) für Dokumentenstapel der Größe 1 durchgeführt werden sollen, oder die Verwendung des SE#2 zu bevorzugen ist. Dieser Wert ist nur relevant wenn SAK_COMFORT_SIGNATURE = Disabled

ReferenzID	Belegung	Bedeutung
Komfortsignatur (SAK_COMFORT_SIGNATURE)	Enabled / Disabled; Standard-Wert: Disabled	Der Administrator kann die Komfortsignatur aktivieren oder deaktivieren. Die Komfortsignaturfunktion kann nur aktiviert werden, wenn ANCL_TLS_MANDATORY = Enabled und ANCL_CAUT_MANDATORY = Enabled
Anzahl von Komfortsignaturen, die ohne erneute PIN-Eingabe ausgeführt werden dürfen (SAK_COMFORT_SIGNATURE_MAX)	X Signaturen (1 - 250); Standard-Wert: 100	Der Administrator kann die Anzahl von Komfortsignaturen, die ohne erneute PIN-Eingabe ausgeführt werden dürfen festlegen. Dieser Wert ist nur relevant wenn SAK_COMFORT_SIGNATURE = Enabled
Zeitdauer, in der Komfortsignaturen ohne erneute PIN-Eingabe ausgeführt werden dürfen (SAK_COMFORT_SIGNATURE_TIMER)	X Stunden (1 - 24); Standard-Wert: 6	Der Administrator kann das Zeitintervall, in dem Komfortsignaturen ohne erneute PIN-Eingabe ausgeführt werden dürfen festlegen. Der Timer startet mit Eingabe der PIN.QES für die Komfortsignatur. Dieser Wert ist nur relevant wenn SAK_COMFORT_SIGNATURE = Enabled

Tabelle 15: Parameter des Leistungsumfanges und der Grundeinstellungen

Sicherheitshinweis: Das Primärsystem leistet einen unverzichtbaren Beitrag zur Sicherheit der Komfortsignatur, indem es die sichere Nutzer-Authentisierung des HBA-Inhabers vornimmt und dabei durch Prüfung auf Länge und Format eine starke UserID sicherzustellen hat. Der RISE Konnektor geht davon aus, dass das Primärsystem UserIDs mit entsprechend hoher Entropie verwendet, sodass ein Angreifer diese nicht in praktikabler Zeit erraten kann. Die TR-03116-1 ist zu beachten. Das Geheimnis UserID darf ausschießlich vom berechtigten Nutzer verwendet werden und darf auch nur diesem bekannt sein.

Hinweis: Wenn Sie den "Leistungsumfang Online" deaktivieren möchten, dann muss zuvor der Internetmodus auf "Keiner" gesetzt werden (siehe Abschnitt 6.2.1.2).

Hinweis: Im deaktivierten "Leistungsumfang Online" ist der WAN-Adapter ebenfalls deaktiviert.

Hinweis: Wird der "Leistungsumfang Online" wieder aktiviert, bleibt der Internetmodus "Keiner" bestehen. Passen Sie danach die Einstellung wieder wie gewünscht an (siehe Abschnitt 6.2.1.2).

6.1.9 RISE Konnektor Benutzereinstellungen

Nach Klick auf den Benutzernamen in der rechten oberen Ecke können die Einstellungen des aktuell eingeloggten Benutzers eingesehen bzw. auch geändert werden:

- Meine Benutzerdaten (Abschnitt 6.1.9.1)
- Berechtigungen (Abschnitt 6.1.9.2)
- Passwort (Abschnitt 6.1.9.3)

6.1.9.1 Meine Benutzerdaten

Im Reiter "Meine Benutzerdaten" können der Benutzername sowie die aktuelle Rolle des Benutzers eingesehen werden und die Kontaktdaten geändert werden (siehe Abbildung 74).

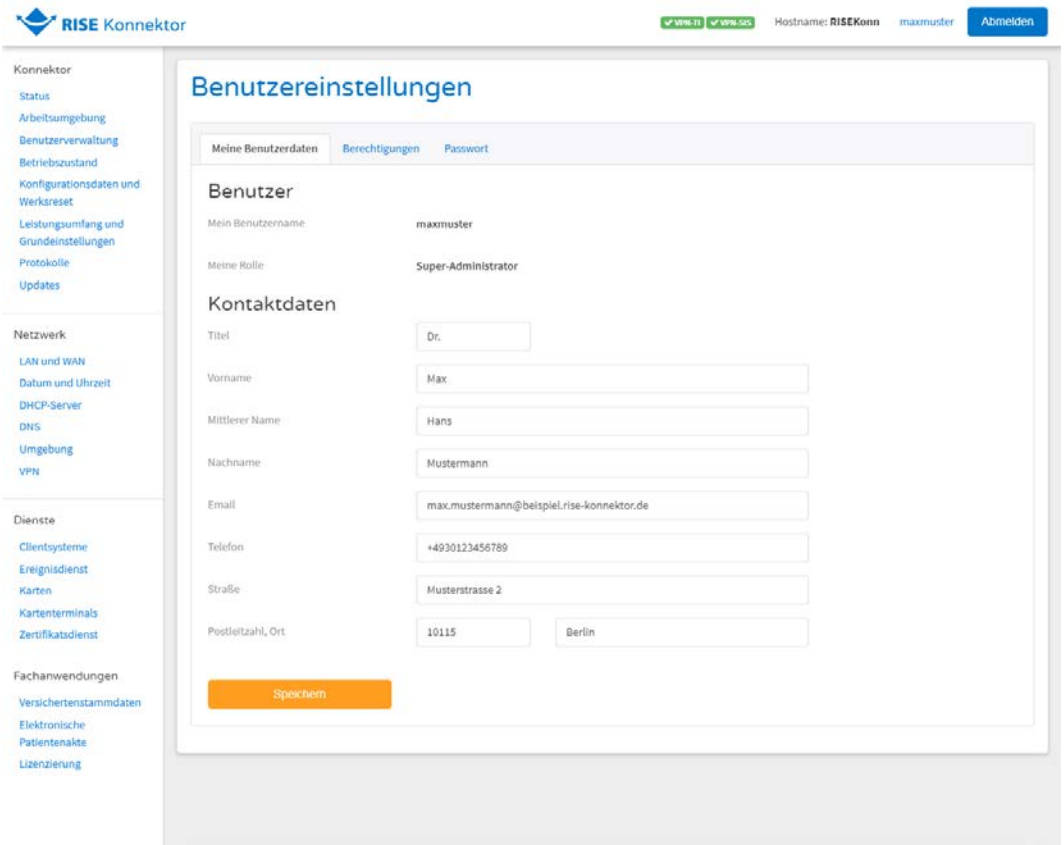


Abbildung 74: Meine Benutzerdaten

6.1.9.2 Berechtigungen

Im Reiter “Berechtigungen” können die Berechtigungen des aktuellen Benutzers eingesehen werden (siehe Abbildung 75). Diese Berechtigungen wurden zuvor durch einen Super-Administrator vergeben und können nur durch einen Super-Administrator im Menüpunkt “Benutzerverwaltung” (siehe Abschnitt 6.1.5) geändert werden.

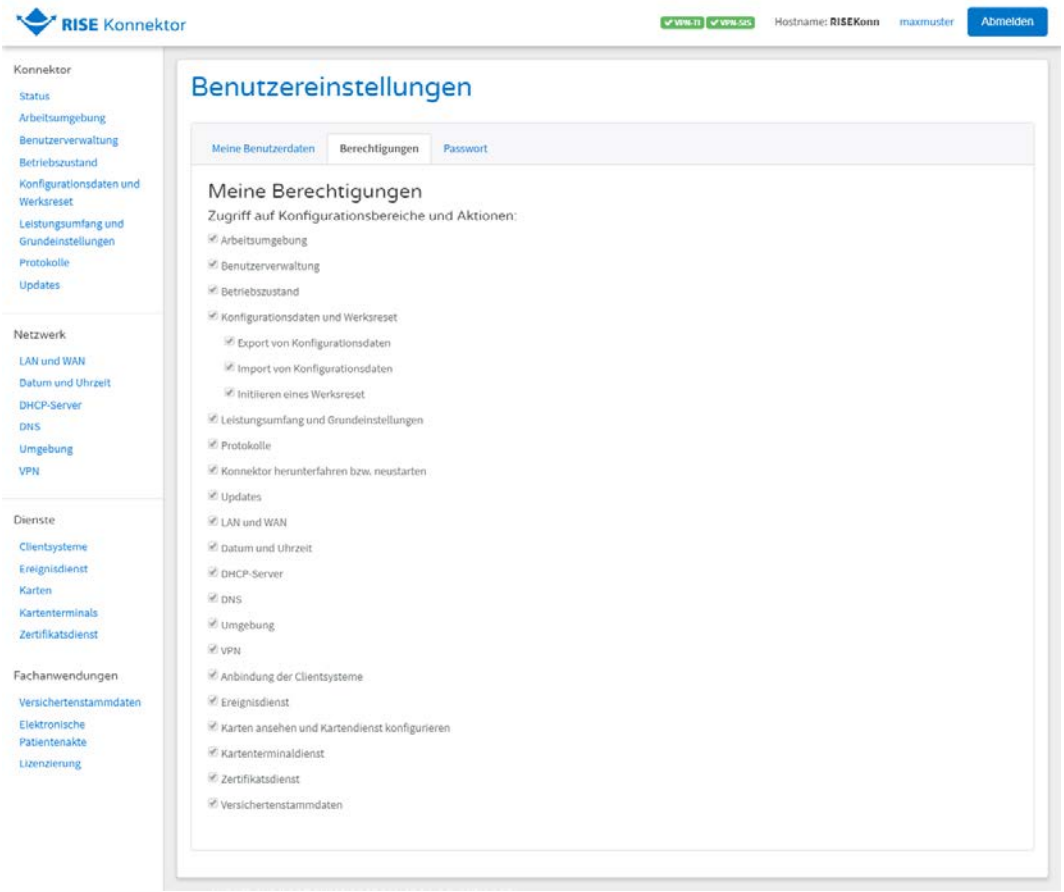


Abbildung 75: Berechtigungen (eines Super-Administrators)

6.1.9.3 Passwort

Im Reiter “Passwort” kann der eingeloggte Benutzer durch Eingabe des aktuellen Passworts und der zweimaligen Eingabe eines neuen Passworts sein Passwort ändern (siehe Abbildung 76).

Die Sicherheitsrichtlinien für Passwörter sind in Abschnitt 4.1 zu finden.

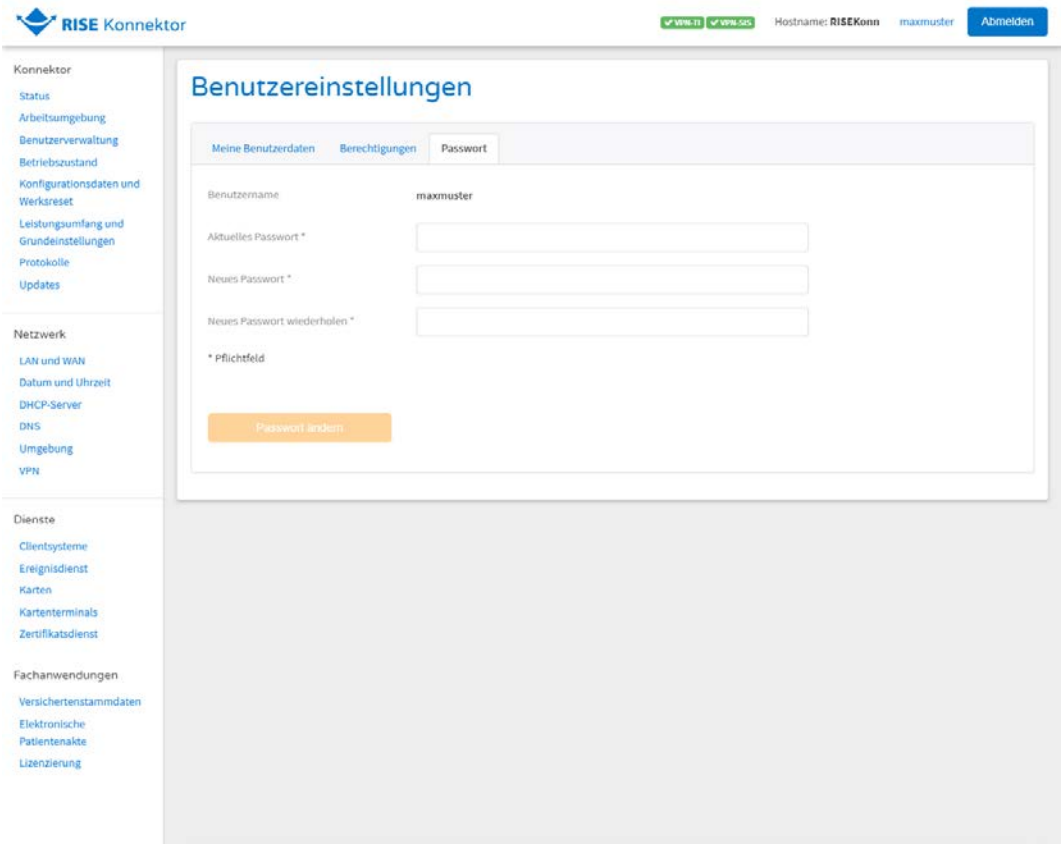


Abbildung 76: Passwort

6.2 Netzwerk

Das Netzwerk-Hauptmenü setzt sich aus den Unterpunkten zusammen, die in Abschnitt 6.2.1 bis Abschnitt 6.2.6 im Detail erläutert werden:

- LAN/WAN Anbindung (Abschnitt 6.2.1)
- Datum & Uhrzeit (Abschnitt 6.2.2)
- DHCP-Server (Abschnitt 6.2.3)
- DNS (Abschnitt 6.2.4)
- RISE Konnektor Umgebung (Abschnitt 6.2.5)
- VPN (Abschnitt 6.2.6)

6.2.1 LAN/WAN Anbindung

Die Konfigurationen der LAN/WAN Anbindung variieren je nach Art des angebundenen Netzwerkes. Prinzipiell wird zwischen folgenden Anbindungen unterschieden:

- LAN Netzwerk des Leistungserbringers: Konfigurationen an der LAN-Anbindung werden vom Administrator vorgenommen.

- WAN Anbindung an Bestandsnetze der zentralen Telematikinfrastruktur: Im Rahmen der Anbindung der Bestandsnetze und der zentralen Telematikinfrastruktur Plattform besitzt der Administrator keinerlei Konfigurationsrechte. Diese Konfiguration kann lediglich durch Hersteller-Updates verändert werden.
- WAN Anbindung an den Sicheren Internet Service der Telematikinfrastruktur: Für die Konfiguration der WAN-Anbindung des Sicheren Internet Service sind dem Administrator nur eingeschränkte Konfigurationsoptionen zugänglich.

6.2.1.1 LAN/WAN Status

Abbildung 77 zeigt die Benutzermaske und die Konfigurationsparameter der LAN- beziehungsweise WAN-Anbindung.

- Status: Aktueller Anbindungsmodus (Parallel oder InReihe)
- LAN: MAC-Adresse, IP-Adresse und Netzwerk-Segment der LAN-Schnittstelle
- WAN: MAC-Adresse, IP-Adresse und Netzwerk-Segment der WAN-Schnittstelle
- Ping: Möglichkeit, die Erreichbarkeit einer IP-Adresse oder eines FQDNs zu prüfen
- Aktuell verwendete Routen

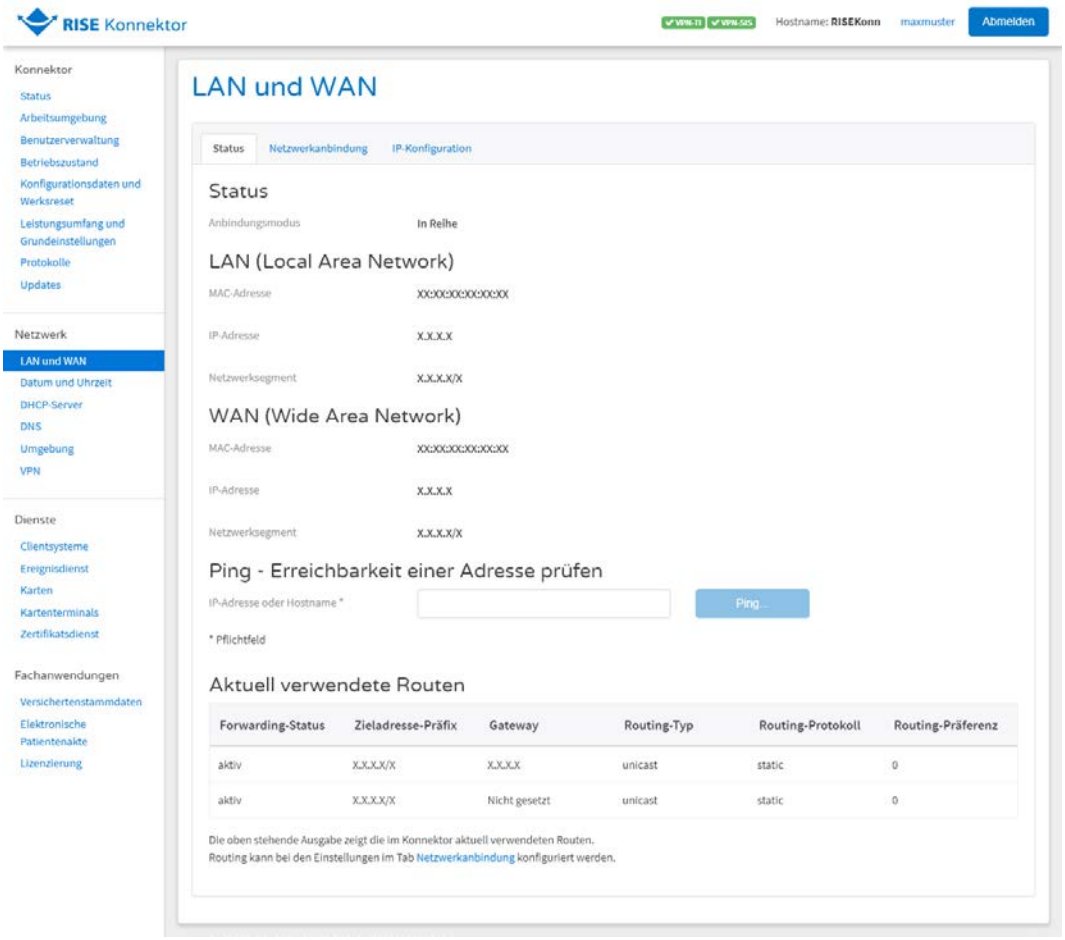


Abbildung 77: LAN/WAN Status

ReferenzID	Belegung	Bedeutung
Anbindungsmodus (ANLW_ANBINDUNGS_MODUS)	InReihe	Der Konnektor ist in Reihe zu dem IAG der Einsatzumgebung geschaltet. Wenn der WAN-Adapter aktiviert ist (ANLW_WAN_ADAPTER_MODUS = Enabled) befindet sich der Konnektor in diesem Anbindungsmodus. Der Administrator kann diesen Parameter lediglich einsehen, aber nicht verändern.
	Parallel	Der Konnektor ist parallel (zu allen bestehenden Systemen) in das Netzwerk der Einsatzumgebung angebunden. Wenn der WAN-Adapter deaktiviert ist (ANLW_WAN_ADAPTER_MODUS= DISABLED) befindet sich der Konnektor in diesem Anbindungsmodus. Der Administrator kann diesen Parameter lediglich einsehen, aber nicht verändern.
LAN – MAC Adresse, IP-Adresse und Netzwerksegment	MAC-Adresse, IP-Adresse oder Netzwerksegment	MAC-Adresse, IP-Adresse und Netzwerk-Segment der LAN-Schnittstelle
WAN – MAC Adresse, IP-Adresse und Netzwerksegment	MAC-Adresse, IP-Adresse oder Netzwerksegment	MAC-Adresse, IP-Adresse und Netzwerk-Segment der WAN-Schnittstelle
Aktuell verwendete Routen	Liste aller aktuell verwendeten Routen	In Abhängigkeit davon, ob VPN verwendet wird oder nicht, welche Bestandnetzrouten oder Intranet Routen zur Verfügung stehen ändert sich die angezeigt Liste an Routen dynamisch. D.h. hier wird eine Übersicht über alle derzeit für den Konnektor aktuelle Routen gegeben. Die einzelnen Spalten pro Listeneintrag werden in den nachfolgenden Zeilen beschrieben.
Forwarding Status	Aktiv	In der Liste werden ausschließlich aktive Routen angezeigt.

ReferenzID	Belegung	Bedeutung
Zieladresse-Präfix	Netzwerksegment Default: 0.0.0.0/0	Zieladresse-Präfix - definiert das Netzwerk, in dem sich die Zieladresse befindet.
Gateway	IP-Adresse	Ein Paket, das für das Ziel-Adressen-Netzwerk gedacht ist, wird über dieses Gateway weitergeroutet.
Routing-Typ	"unicast"	Falls Zieladressen-Präfix gesetzt, ist der Routing Typ immer "unicast". Route zu einem Zielnetz über ein bestimmtes Gateway.
Routing-Protokoll	"kernel" oder "static"	Gibt das verwendete Protokoll an, wobei "static" der Standard ist und "kernel" für ICMP redirect messages verwendet wird.
Routing-Präferenz	Zahl zwischen 0 und 4.294.967.295	Gibt die Wichtigkeit einer Route an – niedrigere Routen werden bevorzugt.

Tabelle 16: LAN/WAN Status

Hinweis: Die Ping-Funktion zu den Downloadadressen für die CRL (vgl. Tabelle 49) ist erst nach dem ersten Herunterladen einer CRL erfolgreich.

6.2.1.1.1 Anbindungsmodus

Der Anbindungsmodus kann vom Administrator in der Management-Oberfläche nur eingesehen werden. Eine Änderung ist möglich, indem der RISE Konnektor im Netz des Leistungserbringers entsprechend angeschlossen wird und die Einstellungen für die Internetanbindung (siehe Abschnitt 6.2.1.2), den WAN-Adapter (siehe Abschnitt 6.2.1.3) und den Leistungsumfang Online (siehe Abschnitt 6.1.8) angepasst werden. Tabelle 17 zeigt mögliche Einstellungsvarianten.

Anbindungsmodus	Bedeutung	WAN-Adapter	Leistungsumfang Online	Internetanbindung
InReihe	Der Konnektor ist in Reihe zu dem IAG der Einsatzumgebung geschaltet.	Aktiviert	Aktiviert	SIS/Keiner
Parallel	Der Konnektor ist	Deaktiviert	Aktiviert	SIS/IAG/Keiner

Anbindungsmodus	Bedeutung	WAN-Adapter	Leistungsumfang Online	Internetanbindung
	parallel (zu allen bestehenden Systemen) in das Netzwerk der Einsatzumgebung angebunden.			

Tabelle 17: Anbindungsmodus

6.2.1.2 LAN/WAN-Netzwerkanbindung

Abbildung 78 zeigt die Benutzermaske und Konfigurationsmöglichkeiten der Netzwerkanbindungen des RISE Konnektors:

- Internetanbindung
- Bestandsnetze
- Intranet Routing

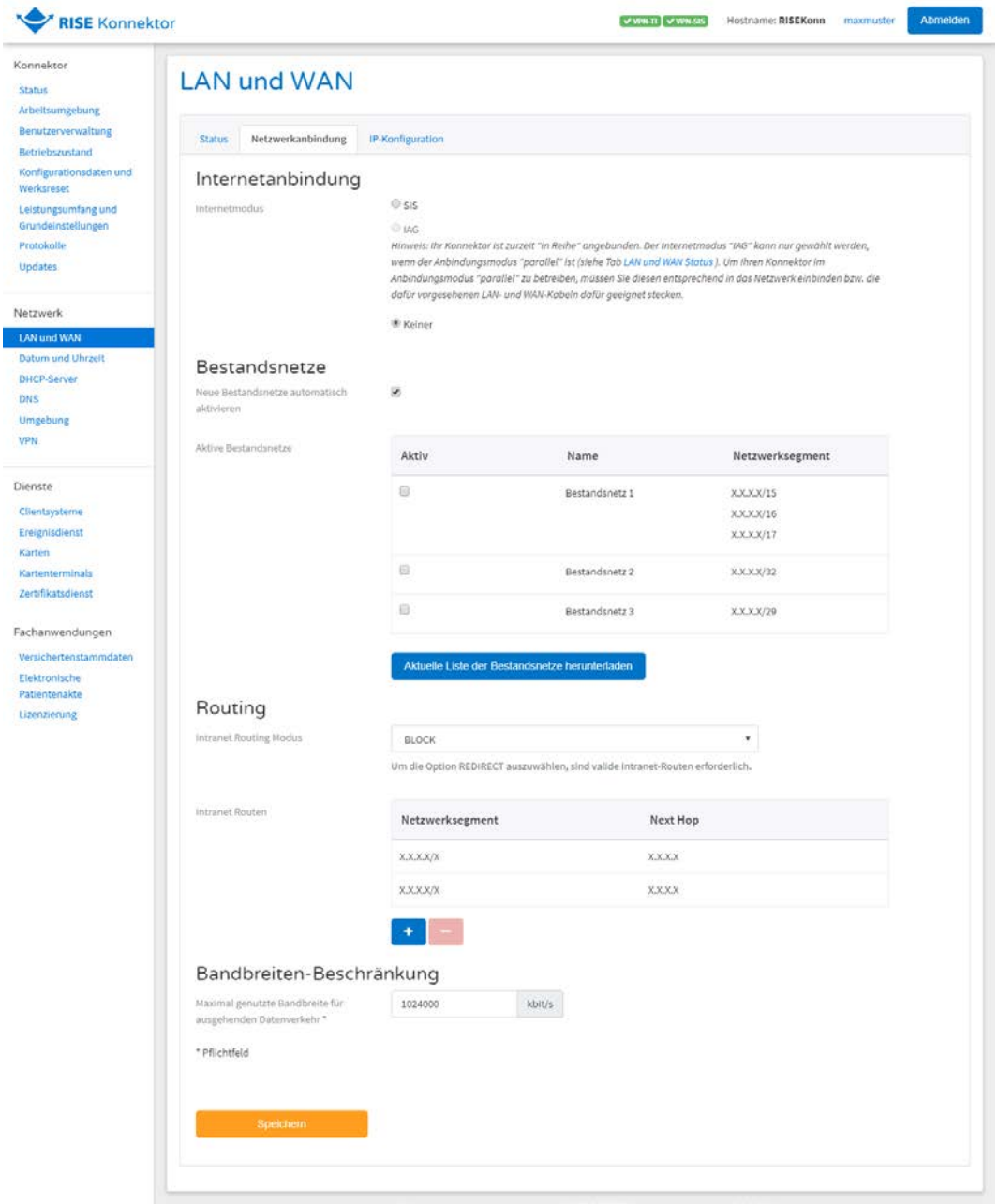


Abbildung 78: LAN/WAN-Netzwerkanbindung

Tabelle 18 beschreibt Konfigurationsparameter der LAN/WAN Netzwerkanbindung.

ReferenzID	Belegung	Bedeutung
Internetmodus (ANLW_INTERNET_MODUS)	SIS	Dieser Konfigurationsparameter bestimmt den Modus des Umgangs mit Zugriffen aus dem LAN des Leistungserbringers zum Internet. Bei Konfiguration als “SIS”-Modus wird der (am Konnektor LAN-seitig ankommende) Internet-Traffic per VPN an den SIS geschickt.

ReferenzID	Belegung	Bedeutung
	IAG	Bei Konfiguration als “IAG”-Modus wird der Aufrufer bei Internet-Anfragen per ICMP-Redirect (Type 5) auf die Route zum IAG verwiesen. Wenn (ANLW_ANBINDUNGS_MODUS = InReihe) kann ein Administrator diesen Wert nicht auswählen – stattdessen muss dann der Wert SIS verwendet werden.
	KEINER	Bei Konfiguration als “KEINER”-Modus wird kein Traffic ins Internet geroutet
Neue Bestandsnetze automatisch aktivieren (ANLW_IA_BESTANDSNETZE)	AN / AUS; Standard-Wert: AN	Ist diese Option gewählt (AN), aktiviert der Konnektor alle übermittelten und angeschlossenen Netze des Gesundheitswesens mit aAdG-NetG. Bei Abwahl der Option (AUS) werden zwar alle übermittelten und angeschlossenen Netze des Gesundheitswesens mit aAdG-NetG angeboten, aber nicht aktiviert.
Aktive Bestandsnetze (ANLW_AKTIVE_BESTANDSNETZE)	Liste von IP-Address Segmenten	Der Administrator kann manuell aus der empfangenen Liste der zur Verfügung stehenden Bestandsnetze einzelne freischalten oder deaktivieren. Standardmäßig sind alle Bestandsnetze aktiviert. Nur die freigegebenen Bestandsnetze werden in dieser Variablen erfasst und sind aus den Netzwerken der Einsatzumgebung erreichbar. Wird eine Änderung an der Liste der freigegebenen Bestandsnetze vorgenommen, hinterlegt der Konnektor für jedes freigegebene Bestandsnetz in DNS_SERVERS_BESTANDSNETZE einen DNS-Referer-Eintrag für jede der dazugehörigen Domains mit allen zugehörigen DNS-Servern im Konnektor.
Internet Routing Modus (ANLW_INTRANET_ROUTES_MODU	REDIRECT	Dieser Konfigurationswert bestimmt den Routing Modus bei

ReferenzID	Belegung	Bedeutung
S)		einem oder mehreren Intranets. Der "REDIRECT"-Wert kann nur dann ausgewählt werden, wenn der Administrator zuvor ein oder mehrere Intranets (ANLW_LEKTR_INTRANET_ROUTES) definiert hat.
	BLOCK	Bei Auswahl des "BLOCK"-Wertes werden alle IP-Pakete für ein Intranet (gemäß ANLW_LEKTR_INTRANET_ROUTES) abgelehnt.
Intranet Routen (ANLW_LEKTR_INTRANET_ROUTES)	Tupel aus Netzwerksegment und dazugehörigem Next-Hop	Dieser Konfigurationsparameter enthält eine Liste von Routen zur Erreichung der Clientsysteme und Kartenterminals vom Konnektor; jeweils mit IP-Netzwerksegment und dazugehörigem Next-Hop. Der Administrator kann in diese Liste Einträge hinzufügen, editieren und löschen. Die Netzwerksegmente dürfen nicht mit den Netzbereichen der Telematikinfrastruktur, des sicheren Internetservices sowie der Fachdienste und Bestandsnetze kollidieren.
Maximal genützten Bandbreite für ausgehenden Datenverkehr	mbit/sec	Für die Priorisierung von Datenpaketen und die Schonung der Internetbandbreite kann der Administrator die maximal genutzte Bandbreite des Konnektors beschränken. Dabei wird klassenbasiertes Queuing nach dem "Hierarchical Token Bucket" (HTB) Algorithmus verwendet.

Tabelle 18: LAN/WAN-Netzwerkanbindung

Hinweis: Falls der RISE Konnektor für den Parallel-Betrieb konfiguriert wurde (ANLW_ANBINDUNGS_MODUS=Parallel bzw. ANLW_WAN_ADAPTER_MODUS=DISABLED) ist im Unterschied zum InReihe-Betrieb (ANLW_ANBINDUNGS_MODUS=InReihe bzw. ANLW_WAN_ADAPTER_MODUS=ENABLED) die Verwendung des Internets über den SIS optional. Das bedeutet, dass ein Client, je nach individuellem Anforderungsprofil,

den sicheren Internetzugang über den Konnektor nutzt oder alternativ auch den direkten Internetzugang über ein bereits bestehendes Internet Access Gateway.

Hinweis: Wenn Einstellungen in der LAN/WAN Anbindung geändert werden und VPN aktiviert ist, kann der Fehler 4001 auftreten, da die VPN-Verbindung nach den Änderungen nicht mehr aufgebaut werden kann. Die geänderten Einstellungen wurden dabei gespeichert. Der Fehler kann ebenso auftreten, wenn keine VPN-Verbindung aufgebaut wurde, die VPN-Parameter (Leistungsumfang Online für TI bzw. Internetmodus SIS) gesetzt sind und die VPN-Verbindung nicht aufgebaut werden kann.

6.2.1.3 LAN/WAN-IP-Konfiguration

Abbildung 78 zeigt die Benutzermaske und Konfigurationsparameter der LAN/WAN-IP-Konfiguration.

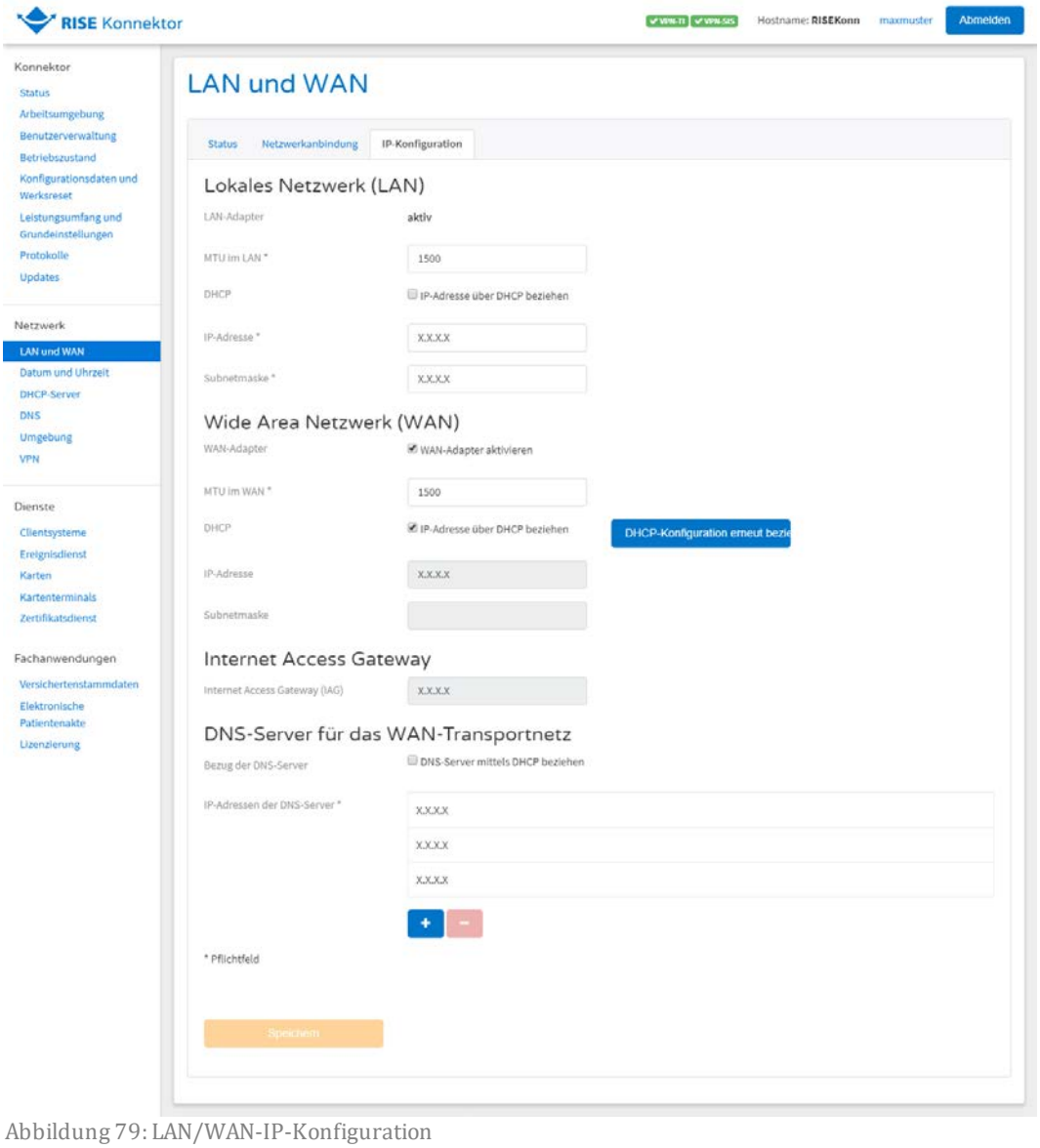


Abbildung 79: LAN/WAN-IP-Konfiguration

Die Konfigurationsparameter der LAN-Anbindung in Tabelle 19 können bei deaktiviertem DHCP-Client (DHCP_CLIENT_LAN_STATE=Disabled) verändert werden. Sollte der DHCP-Client jedoch aktiviert sein (DHCP_CLIENT_LAN_STATE=Enabled), sind die Werte der Tabelle 19 lediglich einsehbar.

ReferenzID	Belegung	Bedeutung
MTU im LAN (ANLW_LAN_MTU)	Nummer; Standard-Wert: 1400	Der Administrator kann mittels dieses Konfigurationsparameters die Maximum Transmission Unit (MTU) setzen. Hierbei muss der konfigurierte Wert innerhalb der Grenzen von 576 bis 9000 liegen.
IP-Adresse im LAN über DHCP beziehen (DHCP_CLIENT_LAN_STATE)	Enabled / Disabled; Standard-Wert: Enabled	Der Administrator kann den DHCP-Client an der LAN Schnittstelle aktivieren oder deaktivieren.
LAN – IP-Adresse (ANLW_LAN_IP_ADDRESS)	IP-Adresse	Dieser Parameter repräsentiert die IP-Adresse des LAN-Adapters. Nur wenn der DHCP-Client deaktiviert ist (DHCP_CLIENT_LAN_STATE=Disabled), kann der Administrator die LAN-seitige IP-Adresse des Konnektors setzen. Ist hingegen der DHCP-Client des Konnektors für das LAN-Interface aktiviert (DHCP_CLIENT_LAN_STATE=Enabled), kann der Administrator die IP-Adresse lediglich auslesen.
LAN – Subnetmaske (ANLW_LAN_SUBNETMASK)	Subnetzmaske	Dieser Parameter repräsentiert die zu ANLW_LAN_IP_ADDRESS gehörende Subnetzmaske. Wie auch ANLW_LAN_IP_ADDRESS ist dieser Parameter nur bei deaktiviertem DHCP-Client (DHCP_CLIENT_LAN_STATE=Disabled) veränderbar.

Tabelle 19: LAN Konfigurationsparameter

Hinweis: Nach dem Ändern der IP-Adresse im LAN (ANLW_LAN_IP_ADDRESS) bzw. beim Aktivieren des DHCP-Clients (DHCP_CLIENT_LAN_STATE=Enabled), ist der RISE Konnektor möglicherweise unter der im Browser eingegebenen IP-Adresse nicht mehr erreichbar. Ändern Sie daher in der Adresszeile die IP-Adresse auf den manuell gesetzten bzw. vom DHCP-Server vergebenen Wert (siehe Abschnitt 3.3.1.2).

Die Konfiguration der WAN-Anbindung kann, ähnlich der LAN-Anbindung, unter nachfolgend beschriebenen Bedingungen mittels der hier beschriebenen Parameter verändert werden.

Tabelle 20 beschreibt die WAN Konfigurationsparameter:

- Ist der DHCP-Client aktiviert (DHCP_CLIENT_WAN_STATE=Enabled) sind die Konfigurationsparameter nur einsehbar.
- Ist der DHCP-Client deaktiviert sind die Konfigurationsparameter der WAN-Anbindung (DHCP_CLIENT_WAN_STATE=DISABLED) konfigurierbar.

ReferenzID	Belegung	Bedeutung
WAN-Adapter (ANLW_WAN_ADAPTER_MODUS)	Enabled / Disabled; Standard-Wert: Enabled	Dieser Parameter ändert den Interface-Status des WAN-Adapters. Hiermit wird festgelegt, ob der WAN-Adapter aktiviert oder deaktiviert ist. Der "Enabled"-Wert aktiviert den Adapter. Der Administrator kann diesen Wert sowohl einsehen als auch ändern.
MTU im WAN (ANLW_WAN_MTU)	Nummer; Standard-Wert: 1400	Der Administrator kann mittels dieses Konfigurationsparameters die Maximum Transmission Unit (MTU) setzen. Hierbei muss der konfigurierte Wert innerhalb der Grenzen von 576 bis 9000 liegen.
IP-Adresse im WAN über DHCP beziehen (DHCP_CLIENT_WAN_STATE)	Enabled / Disabled; Standard-Wert: Enabled	Der Administrator kann den DHCP-Client an der WAN-Schnittstelle aktivieren oder deaktivieren.
WAN – IP-Adresse (ANLW_WAN_IP_ADDRESS)	IP-Adresse	Dieser Parameter repräsentiert die IP-Adresse des WAN-Adapters. Nur wenn der DHCP-Client deaktiviert ist (DHCP_CLIENT_WAN_STATE=Disabled) und der WAN-Adapter aktiviert ist (ANLW_WAN_ADAPTER_MODUS=Enabled), kann der Administrator die WAN-seitige IP-Adresse des Konnektors setzen. Ist hingegen der DHCP-Client des Konnektors für das WAN-Interface aktiviert (DHCP_CLIENT_WAN_STATE=Enabled) oder der WAN-Adapter deaktiviert (ANLW_WAN_ADAPTER_MODUS=Disabled), kann der Administrator die IP-Adresse lediglich auslesen.
WAN – Subnetmaske	Subnetzmask	Dieser Parameter repräsentiert die zu

ReferenzID	Belegung	Bedeutung
(ANLW_WAN_SUBNETMASK)	e	ANLW_WAN_IP_ADDRESS gehörende Subnetzmaske. Wie auch ANLW_WAN_IP_ADDRESS ist dieser Parameter nur bei deaktiviertem DHCP-Client (DHCP_CLIENT_WAN_STATE=Disabled) und aktiviertem WAN-Adapter (ANLW_WAN_ADAPTER_MODUS=Enabled) veränderbar.

Tabelle 20: WAN Konfigurationsparameter

Darüber hinaus gibt es noch weitere LAN/WAN Konfigurationsparameter (siehe Tabelle 21).

ReferenzID	Belegung	Bedeutung
Internet Access Gateway (ANLW_IAG_ADDRESS)	IP-Adresse	Das IAG ist das Standardgateway des RISE Konnektors. Sämtliche erlaubte Datenpakete, die nicht über andere Routen abgedeckt sind, werden an das Standardgateway gesendet. Die Einstellung kann je nach Anbindungsmodus im WAN oder LAN Segment liegen. Die Adresse wird entweder über den aktivierten DHCP automatisch (DHCP_CLIENT_WAN_STATE=enabled) oder (ANLW_WAN_ADAPTER_MODUS= Disabled und DHCP_CLIENT_LAN_STATE=enabled) oder manuell durch den Administrator konfiguriert. Bei automatischer Konfiguration per DHCP kann der Administrator den Wert von ANLW_IAG_ADDRESS ausschließlich einsehen.
DNS-Server für das WAN Transportnetz – IP-Adressen der DNS-Server (DNS_SERVERS_INT)	IP-Adresse(n)	Im Internet erreichbare DNS-Server für die Namensauflösung. Diese werden entweder über DHCP bezogen oder manuell gesetzt. Für Benutzer des Sicheren Internet Service (SIS) werden automatisch die SIS-DNS-Server verwendet.
Bezug der DNS-Server für das WAN-Transportnetz (DNS_SERVERS_INT_STATIC)	Enabled / Disabled; Standard-Wert: Enabled	Dieser Parameter gibt an, ob die DNS-Server des WAN-Transportnetzes statisch konfiguriert sind oder via DHCP von der WAN-Schnittstelle übernommen werden sollen. Die DNS-Server müssen statisch konfiguriert sein, wenn bei deaktivierter WAN-Schnittstelle (ANLW_WAN_ADAPTER_MODUS=DISABLED) das LAN-Interface statisch konfiguriert ist

ReferenzID	Belegung	Bedeutung
		(DHCP_CLIENT_LAN_STATE=DISABLED) oder die WAN-Schnittstelle aktiviert und statisch konfiguriert ist.

Tabelle 21: Weitere LAN/WAN Konfigurationsparameter

6.2.1.4 Fehlermeldungen

Im Zuge der Einstellungen der LAN/WAN-Anbindung können Fehler gem. Tabelle 22 auftreten.

Fehlercode	Fehlertyp	Severity	Fehlertext
4001	Technical	Error	Änderungen wurden verarbeitet. Fehler beim Aufbau der VPN Verbindung TI.
4001	Technical	Error	Änderungen wurden verarbeitet. Fehler beim Aufbau der Verbindung SIS.
4162	Technical	Error	Es liegt eine fehlerhafte LAN IP-Konfiguration vor.
4163	Technical	Error	Es liegt eine fehlerhafte WAN-IP-Konfiguration vor.
4168	Technical	Error	Der DHCP-Server des Konnektors konnte nicht gestartet werden.
4170	Technical	Error	Konnektor besitzt identische IP-Adressen am WAN und LAN Interface.
4169	Technical	Error	Konnektor erhält keine DHCP-Informationen (wird nur direkt nach Neustart protokolliert).
4164	Technical	Fatal	Beim Aktualisieren oder Aktivieren der Firewall-Regeln ist es zu einem Fehler gekommen.
4167	Technical	Fatal	CreateRoutes: Ein oder mehrere Adressen sind ungültig.
4160	Technical	Fatal	Public-IP: Zu einem DNS Namen konnte keine IP-Adresse gefunden werden.
4161	Technical	Fatal	Public-IP: Ein oder mehrere IP-Adressen sind ungültig.

Tabelle 22: WAN/LAN Fehlermeldungen

6.2.2 Datum & Uhrzeit

Der Zeitdienst schafft die Grundlage einer gleichen Systemzeit für alle in der TI eingesetzten Systeme. Die Management-Oberfläche bietet dem Administrator die Möglichkeit, eine Synchronisation mit dem zentralen Zeitdienst explizit anzustoßen (Button "Jetzt synchronisieren").

Darüber hinaus hat der Administrator die Möglichkeit die Konfigurationsparameter des Zeitdienstes zu konfigurieren bzw. einzusehen. Mittels des Buttons "Zeit setzen" kann die Zeit auch manuell durch einen Administrator festgelegt werden.

Warnung: Beim Setzen der Zeit wird ein Neustart des RISE Konnektors durchgeführt. Bitte beachten Sie dabei die Hinweise in Abschnitt 6.1.1.

Abbildung 80 zeigt die Benutzermaske und Konfigurationsparameter zu den Datums- & Uhrzeiteinstellungsoptionen des RISE Konnektors (Zeitdienst).

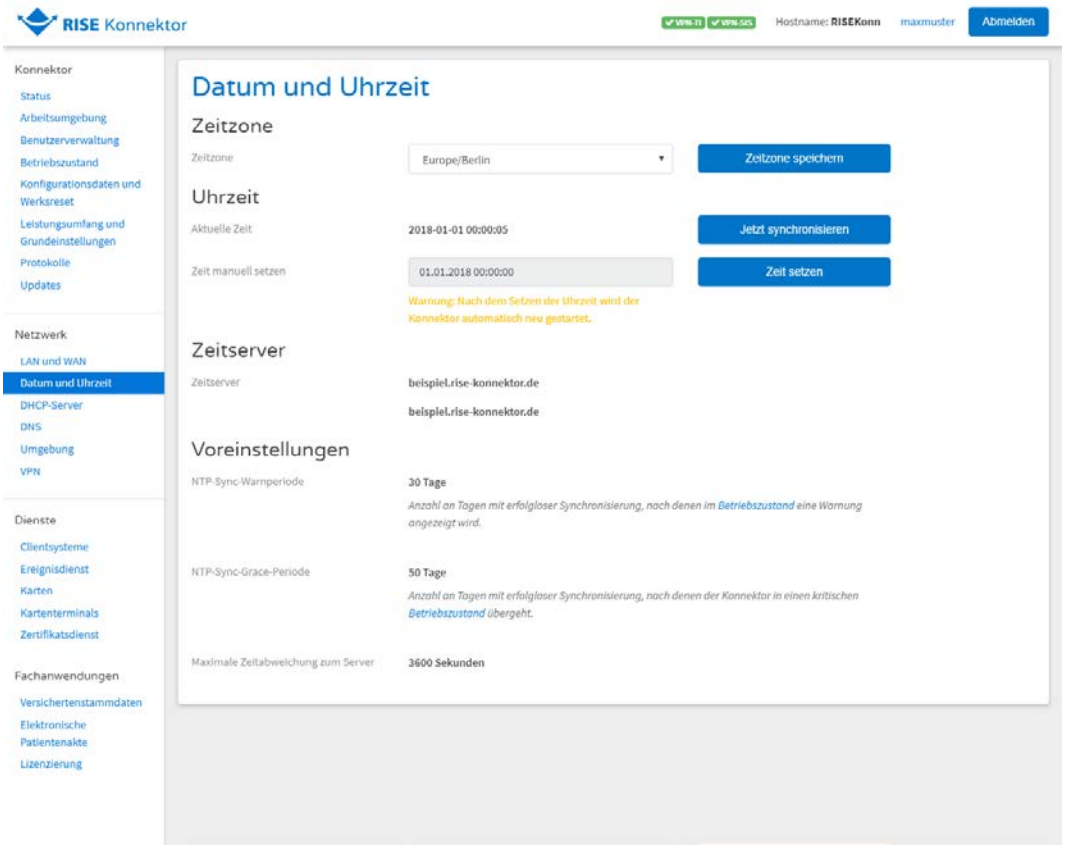


Abbildung 80: LAN/WAN-IP-Konfiguration

6.2.2.1 Zeitdienst Konfiguration

Tabelle 23 gibt Auskunft über die Konfigurationsparameter des Zeitdienstes.

ReferenzID	Belegung	Bedeutung
Zeitzone (NTP_TIMEZONE)	Zeitzone; Standard-Wert: Central European Time/Mitteleuropäische	Der Administrator kann die Zeitzone des

ReferenzID	Belegung	Bedeutung
	Zeit (CET/MEZ)	Konnektors einstellen.
Uhrzeit – Zeit manuell setzen	Zeit	Der Administrator kann die Zeit des Konnektors (NTP_TIME) über die Management-Oberfläche manuell einstellen.

Tabelle 23: Konfigurationsparameter des Zeitdienstes

Tabelle 24 beschreibt die einsehbaren Parameter des Zeitdienstes.

ReferenzID	Belegung	Bedeutung
Uhrzeit – aktuelle Zeit	Zeit	Aktuelle Zeit am Konnektor.
Zeitserver (NTP_SERVER_ADDR)	IP-Adressen / DNS-Namen	Die Adressen des primären und sekundären Stratum-2-Zeitservers der zentralen Telematikinfrastruktur-Plattform für die Synchronisation mit dem NTP-Server des Konnektors.
NTP-Sync-Warnperiode	30 Tage	Liegt die letzte erfolgreiche Synchronisation mit dem Zeitserver der TI länger als 30 Tage zurück, wird eine Warnungsmeldung angezeigt und der Konnektor befindet sich im Fehlerzustand “EC_Time_Sync_Pending_Warning” (siehe auch Abschnitt 4.7.2).
NTP-Sync-Graceperiode	50 Tage	Liegt die letzte erfolgreiche Synchronisation mit dem Zeitserver der TI länger als 50 Tage zurück, befindet sich der Konnektor im kritischen Fehlerzustand “EC_Time_Sync_Pending_Critical” (siehe auch Abschnitt 4.7.1).
Maximale Zeitabweichung zum Server	3600 Sekunden	Zeitspanne, die die Konnektor-Zeit maximal von der vom Zeitserver der TI vorgegebenen Zeit abweichen darf. Ist die Zeitspanne größer, befindet sich der Konnektor im kritischen Fehlerzustand “EC_Time_Difference_Intolerable” (siehe auch Abschnitt 4.7.1).

Tabelle 24: Einsehbare Parameter des Zeitdienstes

Hinweis: Hat seit zu langer Zeit (Tageszähler) keine erfolgreiche Zeitsynchronisation mit der Telematikinfrastruktur stattgefunden, befindet sich der Konnektor im Zustand EC_Time_Sync_Pending_Critical.

Hinweis: Ist die Abweichung zwischen der lokalen Zeit und der mit der Zeitsynchronisation empfangenen Zeit größer als erlaubt, befindet sich der Konnektor im Zustand EC_Time_Difference_Intolerable.

Hinweis: Nach dem Ändern der Systemzeit werden die Protokolleinträge eventuell nicht mehr chronologisch angezeigt.

Sicherheitshinweis: Wenn Sie den RISE Konnektor offline betreiben, muss ein manueller Abgleich der Uhrzeit mindestens einmal jährlich durchgeführt werden.

Sicherheitshinweis: Sollten Sie den RISE Konnektor zwei Monate oder länger ohne Stromversorgung gelagert haben, ist ebenfalls ein manuelles Setzen der korrekten Uhrzeit empfohlen.

In allen Hinweisfällen muss der Administrator eine Korrektur der Systemzeit vornehmen und auch bestätigen (Button "Zeit setzen"). Ist die Zeitdifferenz zwischen aktueller und neuer Uhrzeit größer als eine Stunde, muss zuvor die Option "Leistungsumfang online" deaktiviert werden (siehe Abschnitt 6.1.8). Im Anschluss wird der Tagezähler im Konnektor wieder auf 0 zurückgesetzt und die kritischen Sicherheitszustände nach einem Neustart aufgehoben.

Hinweis: Weicht die neu gesetzte Zeit mehr als 20 Minuten von der ursprünglichen Uhrzeit ab, kann es sein, dass Sie sich aus Sicherheitsgründen erneut einloggen müssen.

6.2.2.2 Fehlermeldungen

Im Zuge der Einstellungen des Zeitdienstes können Fehler gem. Tabelle 25 auftreten.

Fehlercode	Fehlertyp	Severity	Fehlertext
4177	Technical	Warning	Der NTP-Server des Konnektors konnte nicht synchronisiert werden.
4178	Technical	Error	Das Fachmodul konnte die aktuelle Systemzeit des Konnektors nicht abrufen.

Tabelle 25: Fehlermeldungen des Zeitdienstes

6.2.3 DHCP-Server

Der RISE Konnektor bietet unter anderem die Möglichkeit mittels eines DHCP-Servers, ähnlich eines konventionellen Routers, IP-Adressen dynamisch an angebundene Geräte zu verteilen. Diese DHCP-Serverkomponente des Konnektors ist durch die Benutzerrolle des Administrators konfigurierbar.

Hinweis: Der DHCP-Server ist standardmäßig deaktiviert und kann durch einen Administrator über den Konfigurationsparameter in Tabelle 26 aktiviert/deaktiviert werden.

6.2.3.1 DHCP-Server Aktivierung

Abbildung 81 zeigt die Benutzermaske für die DHCP-Server Aktivierung.

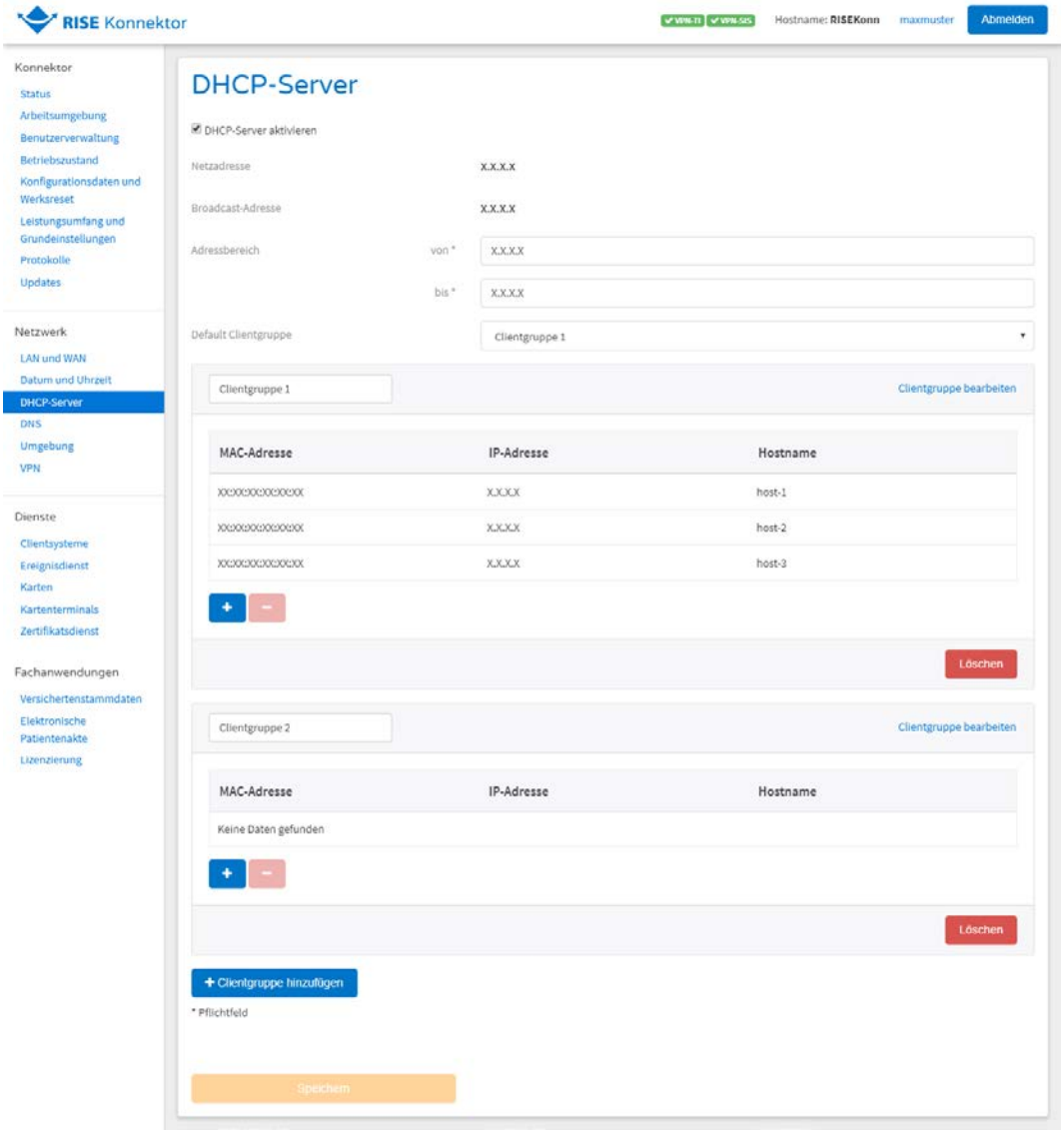


Abbildung 81: DHCP-Server Status

Tabelle 26 beschreibt den DHCP-Server Aktivierungs- bzw. Deaktivierungs-Konfigurationsparameter.

ReferenzID	Belegung	Bedeutung
DHCP Server aktivieren (DHCP_SERVER_STATE)	Enabled / Disabled; Standard-Wert: Disabled	Dieser Konfigurationsparameter steuert die Aktivierung/Deaktivierung des DHCP-Servers des Konnektors.

Tabelle 26: Aktivierung/Deaktivierung des DHCP-Servers

Hinweis: Bei aktiviertem DHCP-Server erhalten Komponenten, welche als Netzwerkkomponenten auf der LAN-Schnittstelle des RISE Konnektors auftreten, ihre Adressen per Zuweisung.

6.2.3.2 DHCP-Server

Die Konfiguration des DHCP-Servers setzt sich aus unterschiedlichen Konfigurationsparametern zusammen und kann in zwei unterschiedliche Kategorien unterteilt werden:

- Die "Basiskonfiguration" für den Betrieb des DHCP-Servers (siehe Abbildung 82).
- Die "Client-Gruppen" über welche Konfigurationsparameter anhand ihrer Zugehörigkeit zusammengefasst werden (siehe Abbildung 83 und Abbildung 84).

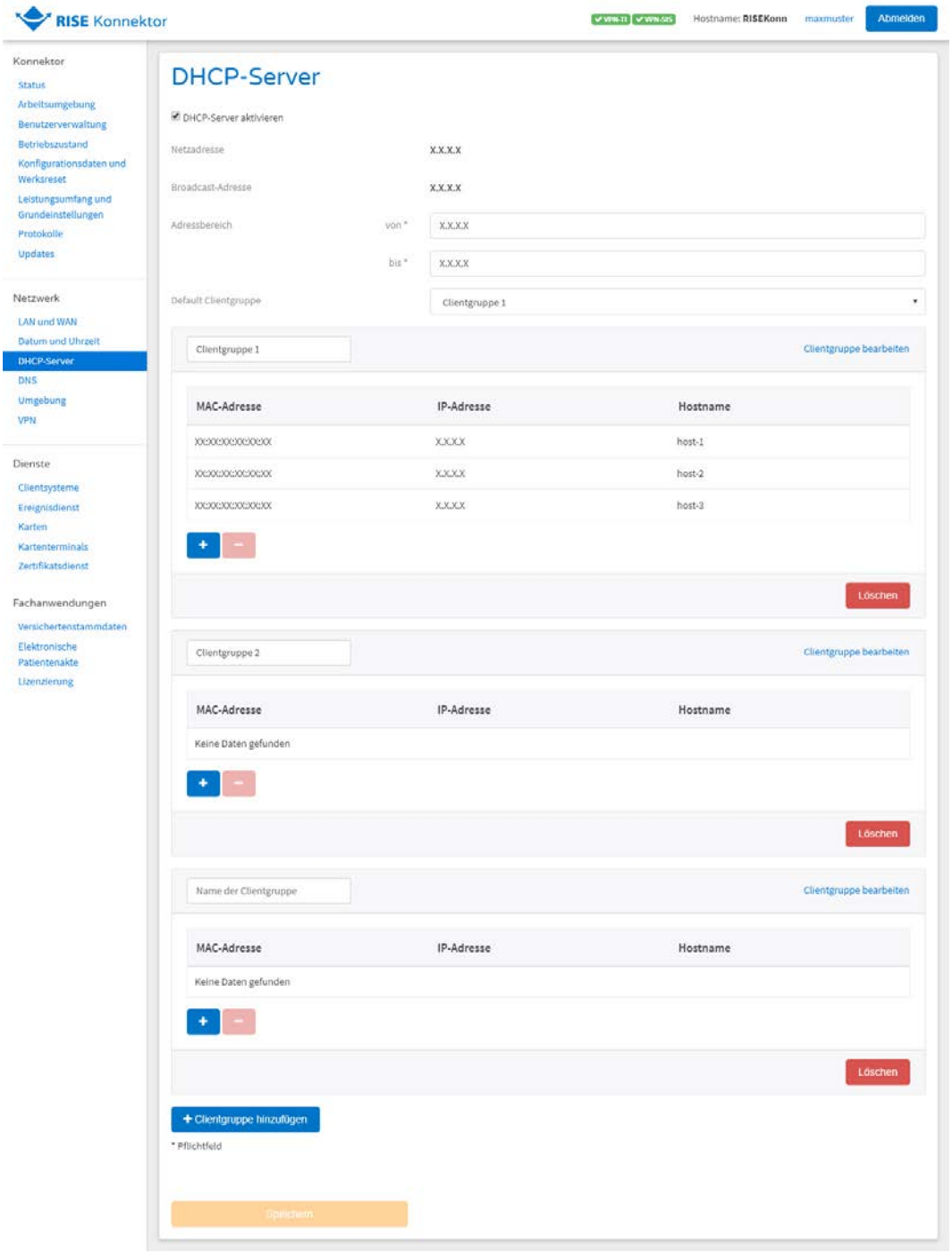


Abbildung 82: DHCP-Server Einstellungen

Tabelle 27 beschreibt jene DHCP-Server Einstellungsparameter, welche für die Basiskonfiguration für den Betrieb eines DHCP-Servers gelten.

ReferenzID	Belegung	Bedeutung
Netzadresse (DHCP_SERVER_NETWORK)	IP-Adresse	Dieser Konfigurationsparameter enthält das IP-Netzwerk der Einsatzumgebung.

ReferenzID	Belegung	Bedeutung
		Dieser Parameter kann jederzeit durch den Administrator gesetzt werden.
Broadcast-Adresse (DHCP_SERVER_BROADCAST)	IP-Adresse	Dieser Konfigurationsparameter enthält die Broadcast-Adresse des Konnektors am LAN-Interface. Dieser Parameter kann jederzeit durch den Administrator gesetzt werden.
Adressbereich (DHCP_SERVER_DYNAMIC_RANGE)	von – bis IP-Adresse	Dieser Konfigurationsparameter enthält den Adressbereich für Adressen, die dynamisch vergeben werden dürfen. Dieser Parameter kann jederzeit durch den Administrator gesetzt werden.
Clientgruppen (DHCP_SERVER_CLIENTGROUPS)	Name der Clientgruppe; Liste an MAC-Adressen	Über diesen Konfigurationsparameter bietet der Konnektor dem Administrator die Möglichkeit mehrere Client-Gruppen zu verwalten.Dieser Parameter kann jederzeit durch den Administrator gesetzt werden.
Default Clientgruppe (DHCP_SERVER_DEFAULT_CLIENTGROUP)	Client-Gruppe	Dieser Konfigurationsparameter legt die Default-Client-Gruppe fest. Diese wird verwendet, falls der Client keiner anderen Gruppe zugeordnet ist. Dieser Parameter kann jederzeit durch den Administrator gesetzt werden.
Hostname und MAC-Adresse der Clients einer Clientgruppe (DHCP_HOSTNAME)	Liste von Tupel aus Hostname	Der Administrator kann über diesen Parameter

ReferenzID	Belegung	Bedeutung
	und MAC-Adresse	eine Liste von Clients konfigurieren (Einträge einfügen, ändern, löschen).
IP-Adresse und MAC-Adresse der Clients einer Clientgruppe (DHCP_STATIC_LEASE)	Liste von Tupel aus IP- und MAC-Adresse	Der Administrator kann über diesen Parameter für jede MAC-Adresse Static Leases konfigurieren.

Tabelle 27: DHCP Server Einstellungen

Hinweis: Der Adressbereich muss im gleichen IP-Segment liegen wie die aktuelle IP-Adresse des RISE Konnektors.

Hinweis: Bei der Eingabe der MAC-Adressen wird eine Trennung der Oktette durch Doppelpunkte (":") erwartet.

Mittels "Clientgruppe bearbeiten" können Konfigurationen pro Clientgruppe vorgenommen werden (siehe Abbildung 83 und Abbildung 84).

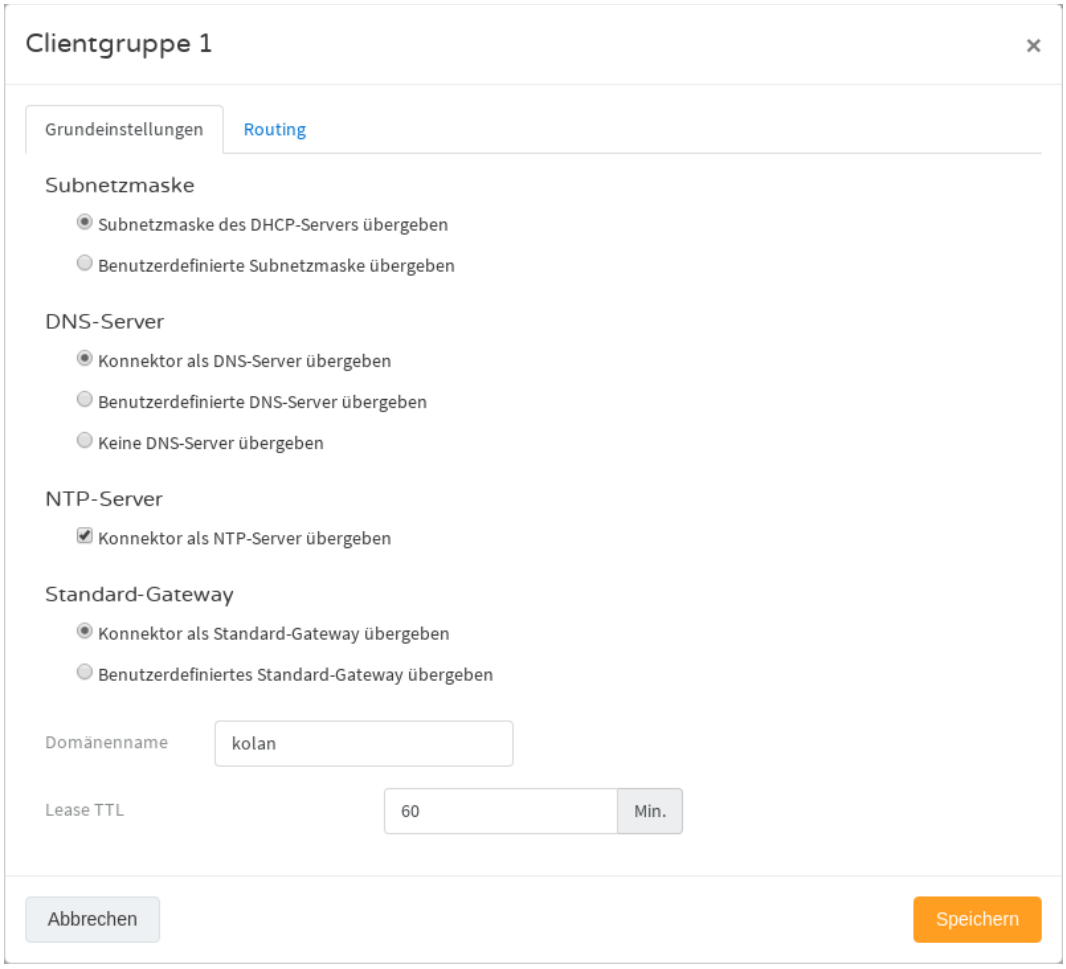


Abbildung 83: Client Group Grundeinstellungen

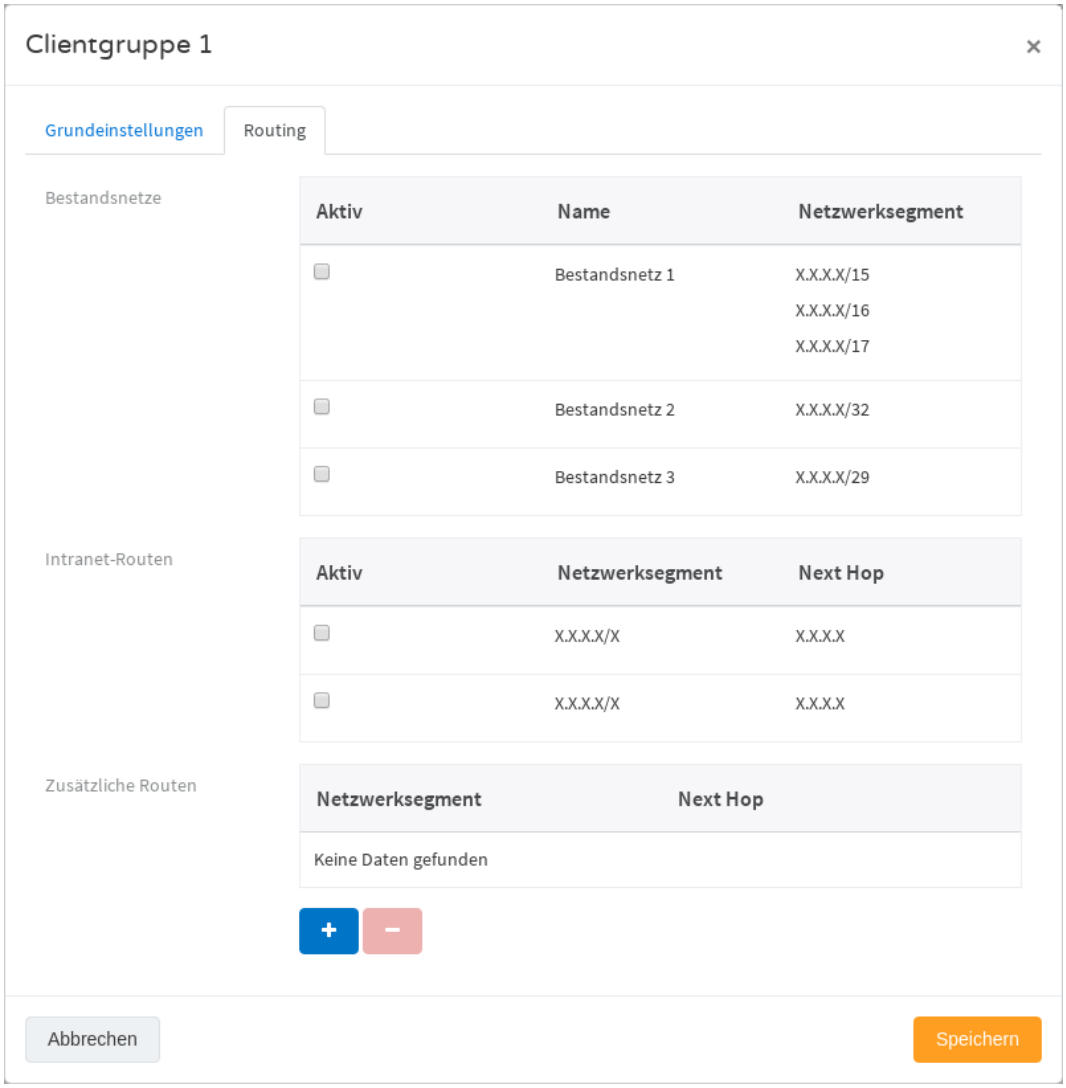


Abbildung 84: Client Group Routing

Tabelle 28 beschreibt die gruppenspezifischen Konfigurationsparameter des DHCP-Servers, welche für jede Clientgruppe spezifisch zusammengefasst sind.

ReferenzID	Belegung	Bedeutung
Subnetzmaske (DHCP_IP_NETMASK)	Netzmaske	Der Administrator kann über diesen Parameter die Netzmaske des Clients konfigurieren.
Konnektor als DNS übergeben (DHCP_OWNDNS_ENABLED)	Enabled / Disabled; Standard-Wert: Disabled	Dieser Konfigurationsparameter erlaubt es dem Administrator zu konfigurieren, ob der Konnektor-eigene DNS-Server als Parameter übergeben wird.
Benutzerdefinierten DNS-Server	IP-Adressen der	Falls der Konnektor-eigene

ReferenzID	Belegung	Bedeutung
übergeben – Liste von DNS-Servern (DHCP_DNS_ADDR)	DNS-Server	DNS-Server nicht übergeben werden soll, müssen die Adressen externer aus dem Netz der Einsatzumgebung erreichbaren DNS-Server als Parameter übergeben werden. Der Administrator kann diese Adressen konfigurieren: Wenn "Benutzerdefinierte DNS-Server übergeben" ausgewählt ist, erscheint eine Liste, in der DNS-Server hinzugefügt werden können.
Keine DNS-Server übergeben	Enabled / Disabled; Standard-Wert: Enabled	Der Administrator kann konfigurieren, dass kein DNS-Server übergeben wird.
Konnektor als NTP Server übergeben (DHCP_NTP)	Enabled / Disabled; Standard-Wert: Enabled	Der Administrator kann über diesen Parameter konfigurieren, ob der Konnektor die Adresse des Konnektor- internen NTP-Servers per DHCP an die Clients sendet.
Konnektor als Standard-Gateway übergeben (DHCP_OWNDGW_ENABLED)	Enabled / Disabled; Standard-Wert: Enabled	Der Administrator kann über diesen Parameter konfigurieren, ob der Konnektor beim Client als Standard-Gateway gesetzt werden soll.
Benutzerdefiniertes Standard-Gateway übergeben (DHCP_DGW_ADDR)	IP-Adresse des Standard-Gateways	Falls der Konnektor nicht als Standard-Gateway gesetzt werden soll, muss die Adresse des zu verwendenden Standard-Gateway als Parameter übergeben werden. Der Administrator kann über diesen Parameter die Adresse des Standard-Gateways konfigurieren.
Kein Standard-Gateway übergeben	Enabled / Disabled; Standard-Wert: Disabled	Der Administrator kann über diesen Parameter konfigurieren, dass dem Client kein Standard-Gateway übergeben wird.
Domänenname (DHCP_DOMAINNAME)	Domainname	Der Administrator kann über

ReferenzID	Belegung	Bedeutung
		diesen Parameter den Domainnamen des Clients konfigurieren.
Lease TTL (DHCP_LEASE_TTL)	X Minuten	Der Administrator kann über diesen Parameter die Lease-Dauer der dynamischen Adressen konfigurieren.
Bestandsnetze (DHCP_AKTIVE_BESTANDSNETZE_ROUTES)	Liste von Tupel: Netzwerksegment je INTRANET und Adresse für Next-Hop je freigegebenem Bestandsnetz	Der Administrator kann über diesen Parameter je freigegebenem Bestandsnetz (aus ANLW_AKTIVE_BESTANDSNETZE) den an den Client zu übermittelnden Routen-Eintrag aktivieren oder deaktivieren.
Intranet Routen (DHCP_INTRANET_ROUTES)	Liste von Tupel: Netzwerksegment je INTRANET und Adresse für Next-Hop in die definierten Intranets	Der Administrator kann über diesen Parameter je Intranet Tupel (aus ANLW_LEKTR_INTRANET_ROUTES) den an den Client zu übermittelnden Routen-Eintrag aktivieren oder deaktivieren.
Zusätzliche Routen (DHCP_ROUTES)	Tupel Netzwerksegment und Adresse für Next-Hop	Der Administrator kann über diesen Parameter Routen zur Verteilung an die Clients frei konfigurieren. Hierbei dürfen diese Listeneinträge keine Überschneidungen mit folgenden Netzwerksegmenten haben: WAN-, LAN-, den Bestandsnetz-, und den Intranet Routen. Die Routen werden über DHCP Option 121 (Windows Vista oder höher) bzw. DHCP Option 249 (Windows XP und darunter) verteilt.

Tabelle 28: DHCP Gruppenspezifische Konfigurationsparameter

6.2.3.2.1 Routing – Neue zusätzliche Route einrichten

Mit der Auswahl des “Plus”-Symbols in Abbildung 84 (über dem “Speichern”-Button), können Sie eine neue zusätzliche Route einrichten, wie in Abbildung 85 dargestellt.

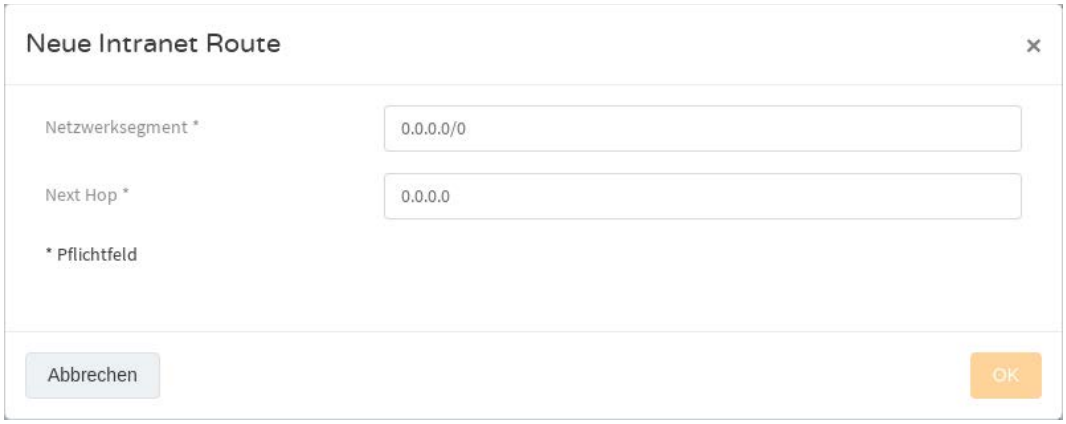


Abbildung 85: Neue zusätzliche Route einrichten

6.2.4 DNS

Das Domain Name System (DNS) (siehe Abbildung 86) erfüllt im lokalen Netzwerk des Leistungserbringers die Aufgaben der Namensauflösung durch die Auflösung von Records (siehe Abbildung 88). Er führt Validierungen mit dem DNS-Vertrauensanker (siehe Abbildung 89) durch.

Hinweis: Durchgeführte Änderungen am autoritativen Namensserver bzw. am Caching-Nameserver sind unmittelbar sichtbar.

6.2.4.1 DNS-Server

Abbildung 86 zeigt die Benutzermaske und die Konfigurationsparameter der DNS-Server.

- DNS-Server (TI)
- DNS-Server (SIS)
- DNS-Server (Bestandsnetze)
- DNS-Server (Einsatzumgebung)
- DNS-Domänenname (Zugangsdienste)

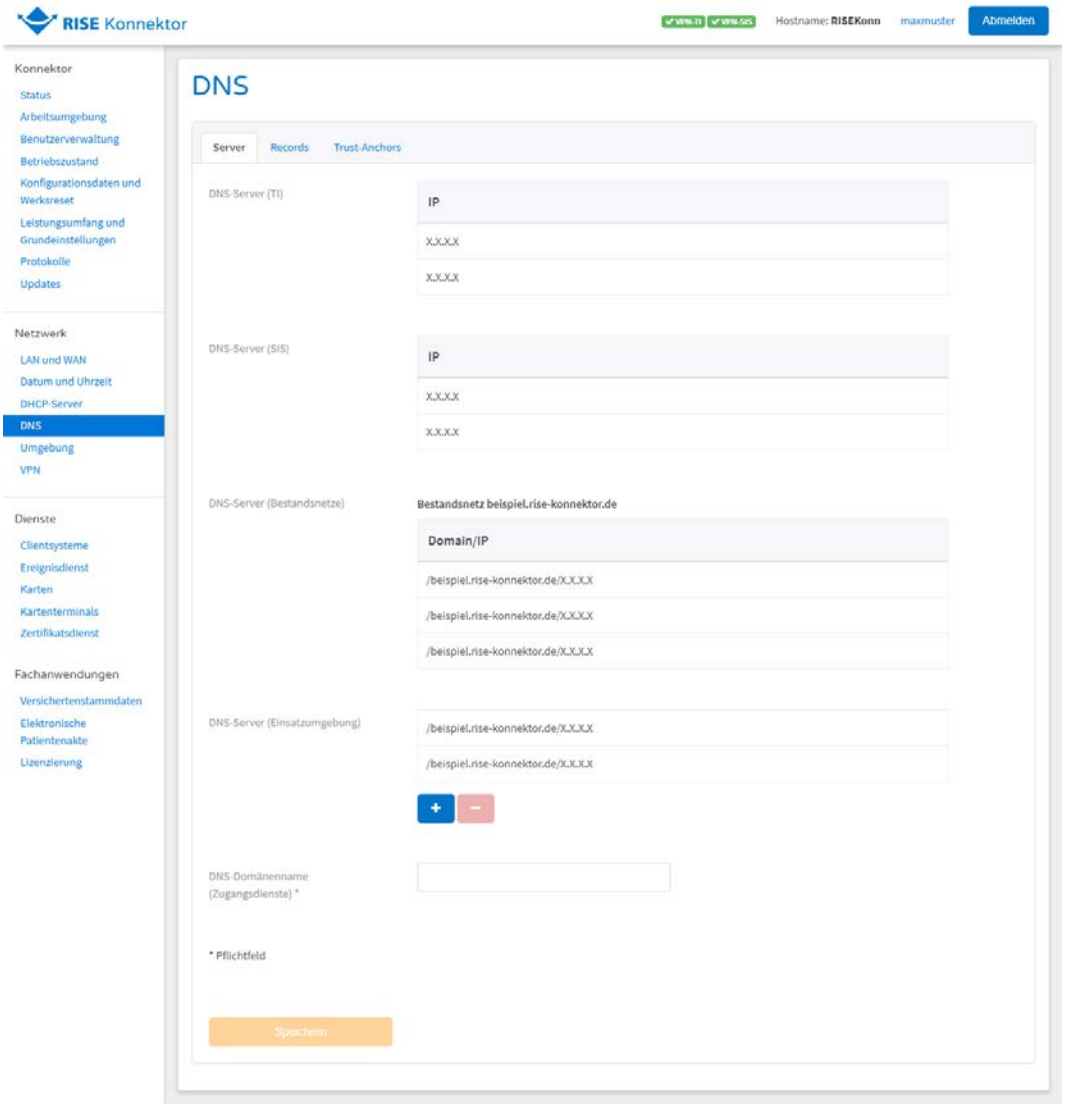


Abbildung 86: DNS-Server

Tabelle 29 beschreibt die Statusparameter der DNS-Serverkonfiguration.

ReferenzID	Belegung	Bedeutung
DNS-Server (TI) (DNS_SERVERS_TI)	Liste von IP-Adressen der DNS-Server	Liste von DNS-Servern, die zur Namensauflösung des Namensraums der Telematikinfrastruktur verwendet werden. **Hinweis:** Die Telematikinfrastruktur DNS-Server Liste wird erst nach erfolgreichem Aufbau eines VPN-Kanals in die Telematikinfrastruktur bereitgestellt.
DNS-Server (SIS) (DNS_SERVERS_SIS)	Liste von IP-Adressen der DNS-Server	Liste von DNS-Servern, die zur Namensauflösung des

ReferenzID	Belegung	Bedeutung
		Namensraums Internet bei Nutzung des SIS verwendet werden. **Hinweis:** Die SIS DNS-Server Liste wird erst nach erfolgreichem Aufbau eines VPN-Kanals zum Sicheren Internet Service bereitgestellt.
DNS-Server (Bestandsnetze) (DNS_SERVERS_BESTANDSNETZE)	Liste von IP-Adressen der DNS-Server je Domäne je freigegebenem Bestandsnetz	Liste von DNS-Servern je Domain eines freigegebenen Bestandsnetzes.
DNS-Server (Einsatzumgebung)	Liste von IP-Adressen der DNS-Server	Liste von DNS-Servern in der Einsatzumgebung. Mittels des Plus-Symbols können neue DNS-Server hinzugefügt werden.
DNS Domänenname (Zugangsdienste) (DNS_DOMAIN_VPN_ZUGD_INT)	DNS-Domainname	DNS-Domainname für die Service Discovery der VPN-Konzentratoren des VPN-Zugangsdienstes

Tabelle 29: DNS-Server Konfiguration

Durch das Auswählen des Plus-Symbols können Sie die Adresse eines weiteren DNS-Servers für die Einsatzumgebung hinzufügen (siehe Abbildung 87).

Sicherheitshinweis: Konfigurieren Sie nur DNS-Server, denen Sie vertrauen.

Hinweis: Aus technischen Gründen kann es bei einer Unterbrechung des VPN-Tunnels zum SIS dazu kommen, dass DNS-Anfragen des Clientsystems an den konfigurierten DNS-Server des WAN Transportnetzes geroutet werden (siehe Abschnitt 6.2.1.3). Damit können Namen von Servern in das Transportnetz übertragen werden, keinesfalls jedoch Inhaltsdaten der Webseiten.

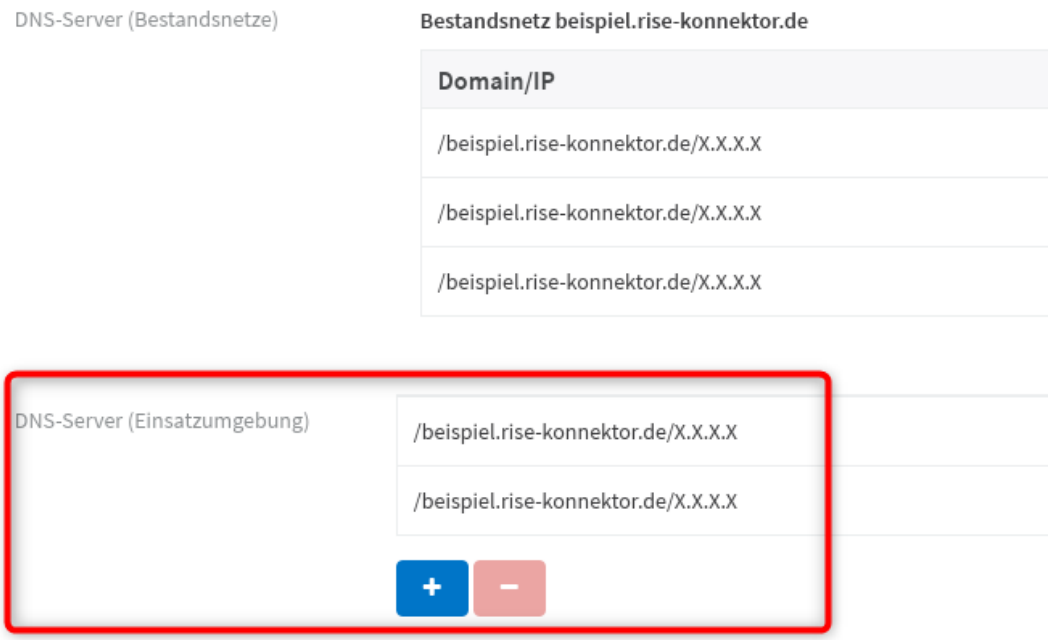


Abbildung 87: Hinzufügen eines neuen DNS-Servers

6.2.4.2 DNS-Records

Abbildung 88 zeigt die Benutzermaske und die Konfigurationsparameter der DNS-Records.

- Statische Records
- Weitere Records

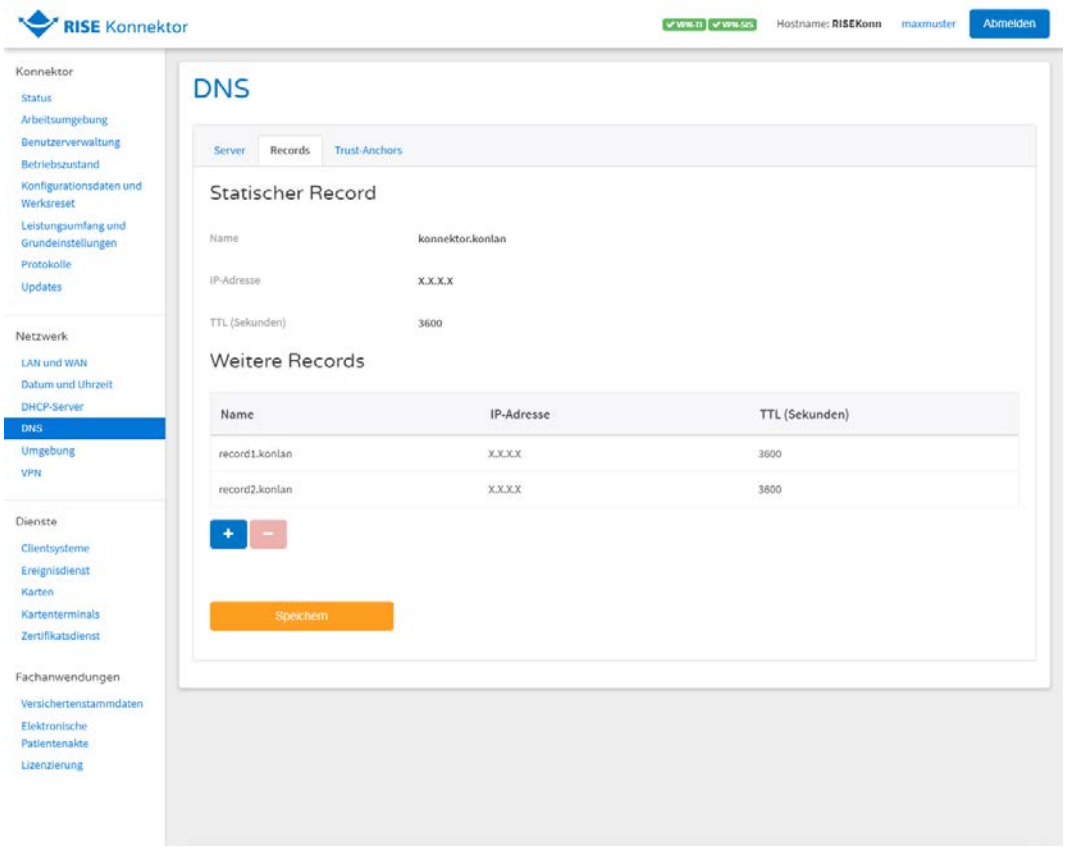


Abbildung 88: DNS-Records

Tabelle 30 beschreibt die Status- und Konfigurationsparameter des DNS-Namensdienstes.

ReferenzID	Belegung	Bedeutung
Weitere Records (DNS_KONLAN_RR)	Liste von DNS Resource Records der Zone “konlan.”.	Der Administrator kann die einzelnen Resource Records (RR) der Domain “konlan.” bearbeiten (erzeugen, lesen, löschen). Davon ausgenommen sind die “konlan.” SOA und NS RR, der “konnektor.konlan.” A RR, sowie der zum NS RR zugehörige A RR.

Tabelle 30: Konfigurationsparameter der DNS Records

6.2.4.3 DNS-Vertrauensanker

Abbildung 89 zeigt die Benutzermaske und Konfigurationsparameter der verwendeten Vertrauensanker für DNSSEC.

Hinweis: IPv6-Adressen können nicht verwendet werden.

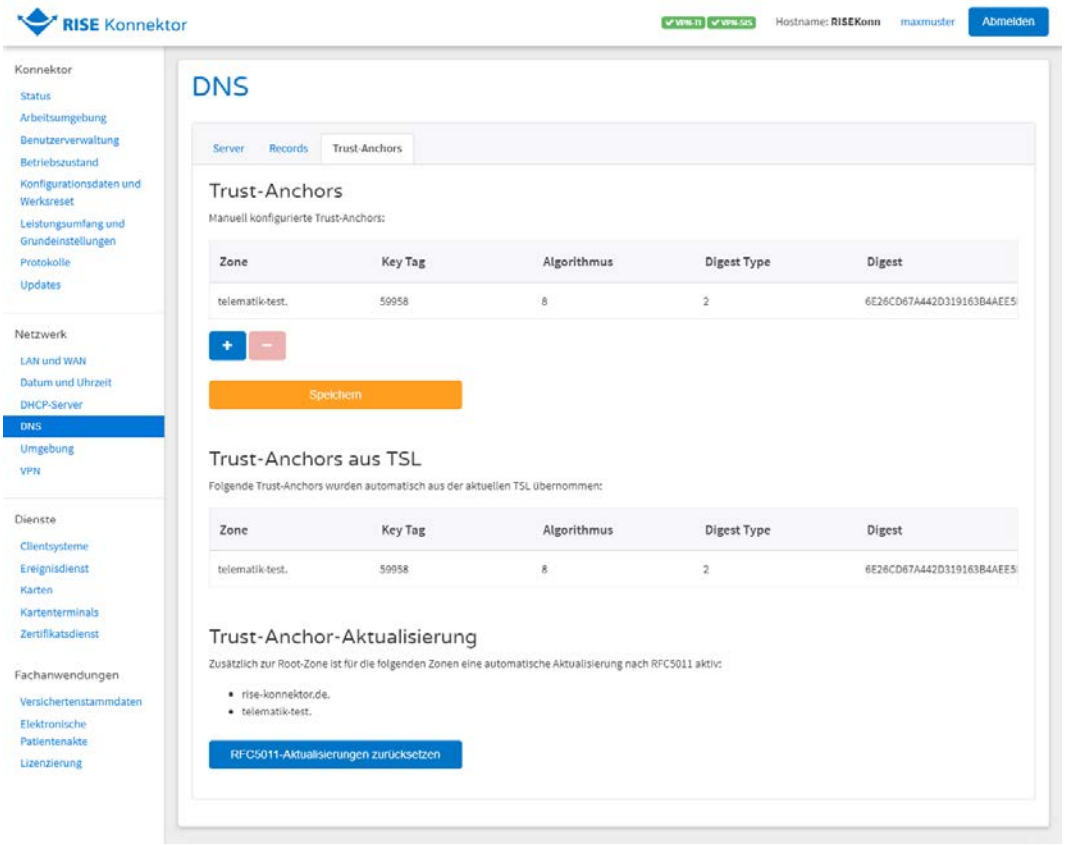


Abbildung 89: DNS Trust-Anchors

Hinweis: Sollte eine DNS-Auflösung bzw. die DNSSEC-Validierung nicht funktionieren, dann kann mit "RFC5011-Aktualisierungen zurücksetzen" die automatische DNSSEC-Vertrauensanker-Aktualisierung zurückgesetzt werden. Die automatische Aktualisierung wird mit den aktuell konfigurierten und aus der TSL übernommenen Vertrauensankern neu gestartet.

ReferenzID	Belegung	Bedeutung
Trust-Anchors (DNS_TA_CONFIG)	Vertrauensanker	Der Administrator kann die aktuellen DNSSEC-Vertrauensanker für den Namensraum Internet zum Konnektor hinzufügen, verändern oder löschen.
Zone	String	Das Zonen Element im Trust-Anchor gibt an, auf welche DNS Zone er anzuwenden ist. Ein "." (ohne Hochkomma) ist die Root Zone.
KeyTag	String	Das KeyTag Element enthält den Key Tag des DNSKEY records. Ein Beispiel hierfür ist "31406".
Algorithmus	Zahl	Das Algorithmus Element enthält den signing algorithm identifier des DNSKEY records. Ein Beispiel hierfür ist "8".

ReferenzID	Belegung	Bedeutung
DigestType	Zahl	Das DigestType Element enthält den digest algorithm identifier des DNSKEY records. Ein Beispiel hierfür ist “2”.
Digest	String	Das Digest Element enthält den Hash des DNSKEY records.

Tabelle 31: Konfigurationsparameter der DNS Trust Anchors

6.2.4.4 Trust-Anchor-Aktualisierung

In diesem Bereich sind zusätzlich zur Root-Zone aktive Namenszonen und der Gültigkeitsstatus gelistet (automatische Aktualisierung nach RFC5011).

Sicherheitshinweis: Wird bei mindestens einer Zone “ungülig” angezeigt, wählen Sie “RFC5011-Aktualisierungen zurücksetzen”. Bleibt der Status “ungülig” bestehen, informieren Sie bitte den Händlersupport (siehe Abschnitt 2).

6.2.4.5 Fehlermeldungen

Im Zuge der Einstellungen des DNS können Fehler gem. Tabelle 32 auftreten.

Fehlercode	Fehlertyp	Severity	Fehlertext
4179	Technical	Error	DNS: Anfrage wurde abgebrochen, da das Timeout von ANLW_SERVICE_TIMEOUT Sekunden überschritten wurde.
4180	Technical	Fatal	DNS: Es ist ein Fehler bei der Namensauflösung aufgetreten. Prüfen Sie ggf. Ihre Firewall, ob diese DNSSEC korrekt handhabt.

Tabelle 32: Fehlermeldungen DNS

6.2.5 RISE Konnektor Umgebung

Abbildung 90 zeigt die Benutzermaske und die Konfigurationsparameter der RISE Konnektor Netzwerkumgebung, in der die Subnetze der Zonen für zentrale Dienste TI, offene Fachdienste TI und gesicherte Fachdienste TI definiert werden.

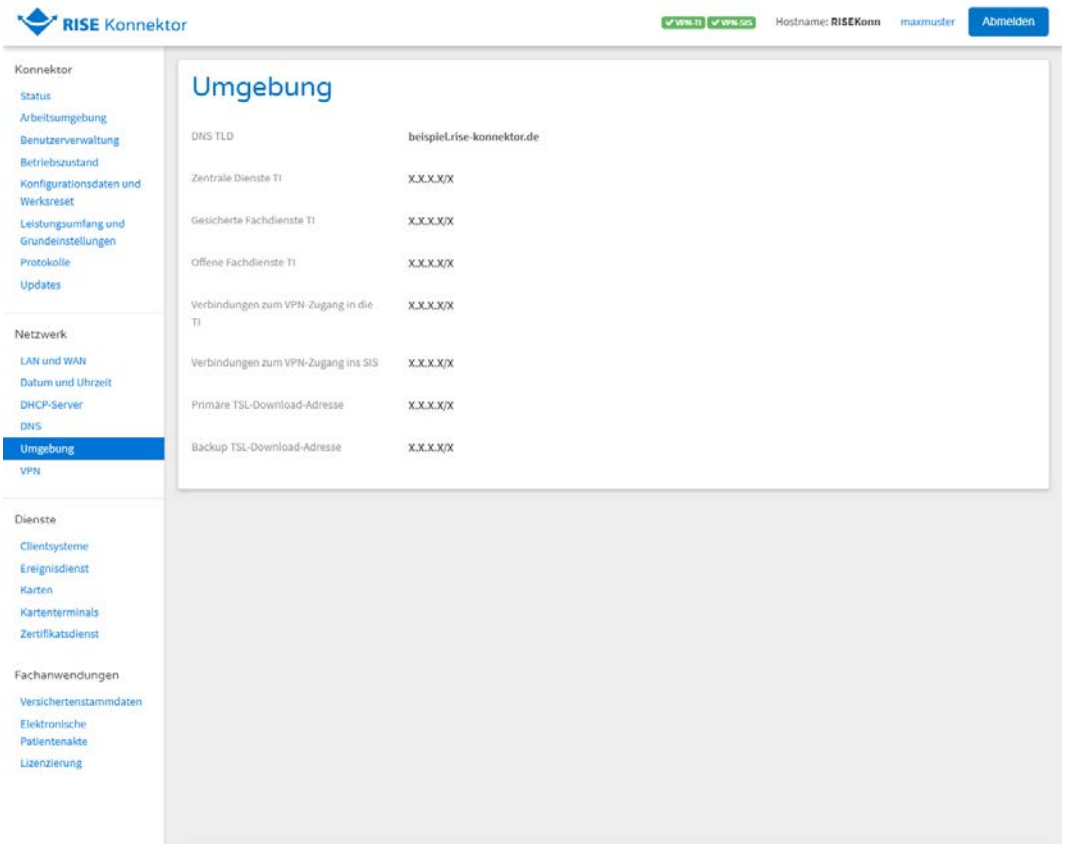


Abbildung 90: RISE Konnektor Netzwerkumgebung

ReferenzID	Belegung	Bedeutung
DNS TLD (DNS_TOP_LEVEL_DOMAIN_TI)	Adresse des DNS-Servers der Telematikinfrastruktur	Dieser Wert ist für den Administrator über die Management-Oberfläche einsehbar, kann aber nicht verändert werden.
Zentrale Dienste TI (NET_TI_ZENTRAL)	IPv4	Adressbereich für Zentrale Dienste der TI. Dieser Wert ist für den Administrator über die Management-Oberfläche einsehbar, kann aber nicht verändert werden.
Gesicherte Fachdienste TI (NET_TI_GESICHERTE_FD)	IPv4	Adressbereich für die gesicherten Fachdienste der TI. Dieser Wert ist für den Administrator über die Management-Oberfläche einsehbar, kann aber nicht verändert werden.

ReferenzID	Belegung	Bedeutung
Offene Fachdienste TI (NET_TI_OFFENE_FD)	IPv4	Adressbereich für offene Fachdienste der TI. Dieser Wert ist für den Administrator über die Management-Oberfläche einsehbar, kann aber nicht verändert werden.
Verbindungen zum VPN Zugang in die TI	IPv4	Adressbereich für VPN-Konzentratoren der TI. Dieser Wert ist für den Administrator über die Management-Oberfläche einsehbar, kann aber nicht verändert werden.
Verbindungen zum VPN Zugang ins SIS (NET_SIS)	IPv4	Adressbereich für VPN-Konzentratoren der SIS. Dieser Wert ist für den Administrator über die Management-Oberfläche einsehbar, kann aber nicht verändert werden.
Primäre TSL-Download-Adresse	URL in der Telematikinfrastruktur (ECC-TSL)	Dieser Wert ist für den Administrator über die Management-Oberfläche einsehbar, kann aber nicht verändert werden.
Backup TSL-Download-Adresse	URL in der Telematikinfrastruktur (ECC-TSL)	Dieser Wert ist für den Administrator über die Management-Oberfläche einsehbar, kann aber nicht verändert werden.

Tabelle 33: Parameter der RISE Konnektor Netzwerkumgebung

6.2.6 VPN

Der VPN-Client dient zur Erstellung und Verwaltung ausgehender VPN-Kommunikationskanäle. Dabei kann sowohl der Status der Verbindung zur Telematikinfrastruktur als auch zum Sicheren Internet Service eingesehen und verändert als auch die Einstellungen der VPN-Verbindung angepasst werden (siehe Abbildung 91).

Hinweis: Auf Grund von technischen Anforderungen wird die nicht-öffentliche IP-Adresse beim Verbindungsaufbau an den VPN-Konzentrator mitgeschickt.

Hinweis: Den Spezifikationen der gematik folgend unterstützt der RISE Konnektor für die VPN-Kanäle den Mechanismus Traffic Flow Confidentiality nicht.

Hinweis: Aus technischen Gründen kommt es beim An- und Abstecken der Netzwerkkabel sowohl am LAN- als auch am WAN-Interface automatisch zu einem Ab- und Aufbau der zuvor bestehenden VPN-Verbindungen.

6.2.6.1 VPN-Status

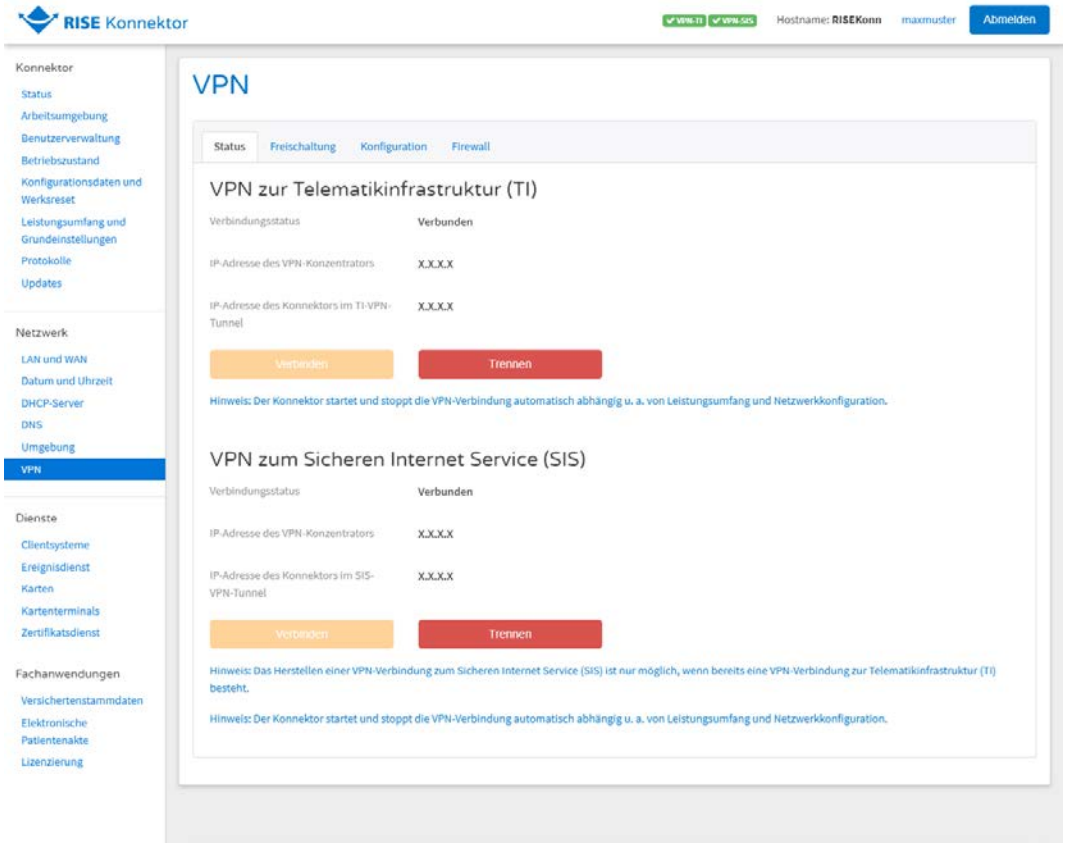


Abbildung 91: VPN-Status

Abbildung 91 zeigt die Benutzermaske und die Konfigurationsparameter zum Status des VPN-Dienstes.

- VPN zur Telematikinfrastruktur (TI)
- VPN zum Sicheren Internet Service (SIS)

Hinweis: Trennen Sie VPN-Verbinungen nicht, während die Verbindung aufgebaut wird (Status "Verbindung wird hergestellt …").

Tabelle 34 zeigt die Parameter des VPN-Clients, welche nur eingesehen werden können.

ReferenzID	Belegung	Bedeutung
IP-Adresse des VPN Konzentrators (TI)	IP-	IP-Adresse des VPN-

ReferenzID	Belegung	Bedeutung
(VPN_KONZENTRATOR_TI_IP_ADDRESS)	Adresse	Konzentrators TI im Transportnetz, zu dem der IPsec-Tunnel VPN_TI aufgebaut wird. Dieser Wert ist nur bei aktivem Tunnel zur Telematikinfrastruktur verfügbar.
IP-Adresse des Konnektors im TI-VPN-Tunnel (VPN_TUNNEL_TI_INNER_IP)	IP-Adresse	IP-Adresse des RISE Konnektors als Endpunkt der IPSec-Kanäle mit den VPN-Konzentratoren der Telematikinfrastruktur.
IP-Adresse des VPN Konzentrators (SIS) (VPN_KONZENTRATOR_SIS_IP_ADDRESS)	IP-Adresse	IP-Adresse des VPN-Konzentrators SIS im Transportnetzt zu dem der IPsec-Tunnel VPN_SIS aufgebaut wird. Dieser Wert ist nur bei aktivem Tunnel zum Sicheren Internet Service verfügbar.
IP-Adresse des Konnektors im SIS-VPN-Tunnel (VPN_TUNNEL_SIS_INNER_IP)	IP-Adresse	IP-Adresse des RISE Konnektors als Endpunkt der IPSec-Kanäle mit den VPN-Konzentratoren des Sicheren Internet Service.

Tabelle 34: Einsehbare Parameter des VPN-Clients

6.2.6.2 VPN-Konfiguration

Der VPN-Client dient zur Absicherung der Verbindung des RISE Konnektors zur Telematikinfrastruktur.

Abbildung 92 zeigt die Benutzermaske und die Konfigurationsparameter der VPN-Konfiguration.

- Maximum Transmission Unit (MTU)
- Verhalten bei Inaktivität der VPN-Verbindungen
- Keep-Alive Einstellungen für NAT
- Hash&URL Verfahren für den Zertifikatsaustausch

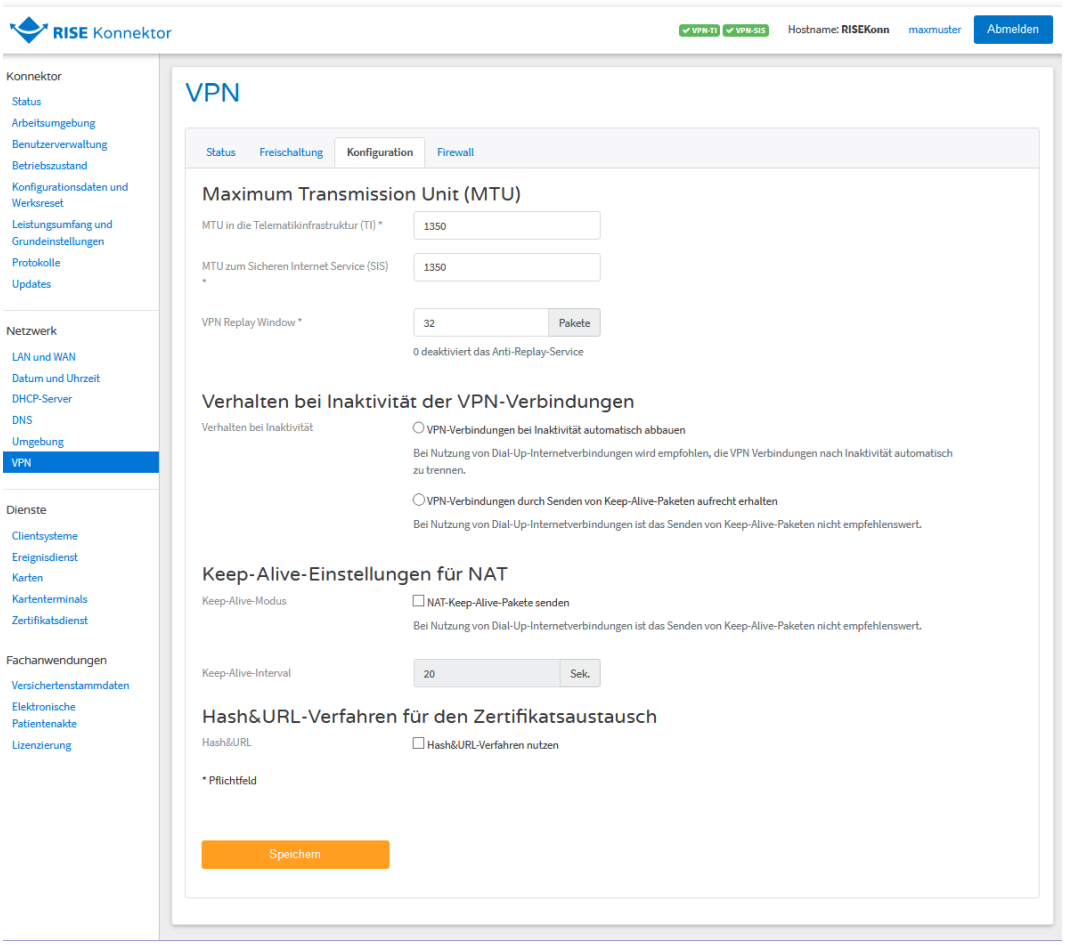


Abbildung 92: VPN-Konfiguration

Abbildung 92 beschreibt die Status- und die Konfigurationsparameter des VPN-Dienstes.

ReferenzID	Belegung	Bedeutung
MTU in die Telematikinfrastruktur (VPN_TI_MTU)	Paketgröße in Byte; Standard-Wert: 1350	Der Administrator kann die MTU für ESP-Pakete zur Telematikinfrastruktur (exkl. ESP-Header-Size) in den Grenzen von 576 bis 8076 konfigurieren. Für eine spezifikationskonformen Betrieb ist die VPN MTU auf 1318 zu ändern.
MTU zum Sicheren Internet Service (VPN_SIS_MTU)	Paketgröße in Byte; Standard-Wert: 1350	Der Administrator kann die MTU für ESP-Pakete zum Sicheren Internet Service (exkl. ESP-Header-Size) in den Grenzen von 576 bis 8076 konfigurieren. Für eine spezifikationskonformen Betrieb ist die VPN MTU auf 1318 zu ändern.
VPN-Verbindung bei Inaktivität automatisch abbauen (VPN_IDLE_TIMEOUT_MODUS)	Enabled / Disabled; Standard-Wert: Disabled	Der Administrator kann einstellen, ob nach Inaktivität die VPN-Verbindung automatisch abgebaut wird. Bei der Nutzung von Dial-Up-Verbindungen ist “Enabled” empfehlenswert.

ReferenzID	Belegung	Bedeutung
Timeout (VPN_IDLE_TIMEOUT)	X Sekunden; Standard-Wert: 600	Wenn "VPN-Verbindung bei Inaktivität automatisch abbauen" aktiviert ist, dann kann der Administrator die Zeit in Sekunden angeben, nach der eine inaktive VPN-Verbindung abgebaut wird.
VPN-Verbindungen durch Senden von Keep-Alive Paketen aufrecht erhalten (IKE_KEEPALIVE_MODUS)	Enabled / Disabled; Standard-Wert: Enabled	Der Administrator kann einstellen, ob IKE Keep-Alive-Pakete gesendet werden. Dies ist bei der Nutzung von Dial-Up-Verbindungen allerdings nicht zu empfehlen, weil bei der Nutzung eines Internetzugangs ohne Flatrate in diesem Fall Kosten entstehen können.
Verhalten bei Inaktivität der VPN-Verbindungen – Keep-Alive-Interval (IKE_KEEPALIVE_INTERVAL)	X Sekunden; Standard-Wert: 30	Wenn "VPN-Verbindungen durch Senden von Keep-Alive Paketen aufrecht erhalten" aktiviert ist, kann der Administrator die Zeit in Sekunden angeben, nach der ein neues IKE Keep-Alive-Paket gesendet wird.
Verhalten bei Inaktivität der VPN-Verbindungen – Keep-Alive Retries (IKE_KEEPALIVE_RETRY)	X Versuche; Standard-Wert: 3	Wenn "VPN-Verbindungen durch Senden von Keep-Alive Paketen aufrecht erhalten" aktiviert ist, kann der Administrator angeben, nach wie vielen IKE Keep-Alive-Paketen ohne Acknowledge Message die VPN-Verbindung beendet wird.
NAT – Keep-Alive Modus (NAT_KEEPALIVE_MODUS)	Enabled / Disabled; Standard-Wert: Enabled	Der Administrator kann einstellen, ob NAT Keep-Alive-Pakete gesendet werden. Dies ist bei der Nutzung von Dial-Up-Verbindungen allerdings nicht zu empfehlen, weil bei der Nutzung eines Internetzugangs ohne Flatrate in diesem Fall Kosten entstehen können.
NAT – Keep-Alive-Interval (NAT_KEEPALIVE_INTERVAL)	X Sekunden; Standard-Wert: 20	Der Administrator kann die Zeit in Sekunden angeben, nach der ein neues NAT Keep-Alive-Paket gesendet wird.
Hash&Url-Verfahren nutzen (HASH_AND_URL)	Enabled / Disabled; Standard-Wert: Disabled	Der Administrator kann die Nutzung des Hash&URL-Verfahrens zum Zertifikatsaustausch konfigurieren. Wenn HASH_AND_URL = ENABLED gesetzt ist, wird die URL für das Hash&URL-Verfahren automatisch durch DNS SRV- und TXT-Anfragen mit Owner "_hashandurl._tcp.<DNS_DOMAIN_VPN_ZU_GD_INT>" ermittelt.

Tabelle 35: Konfiguration des VPN-Dienstes

Des Weiteren besteht die Möglichkeit, die Sequenznummern-Auswertung empfängerseitig im Rahmen des Anti Replay Service abzuschalten ("VPN Replay Window"), sowie das Fenster für die Auswertung der Sequenznummern zu konfigurieren.

Sicherheitswarnung: Eine Änderung des Anti Replay Services wird nicht empfohlen und darf nur in begründeten Fällen (z.B. zur Fehleranalyse) vorübergehend durchgeführt werden, da der RISE Konnektor in dieser Konfiguration nicht mehr den Sicherheitsanforderungen der Telematikinfrastruktur entspricht.

6.2.6.3 VPN-Firewall

Der RISE Konnektor verfügt über eine Firewall. Der Administrator hat über die Management-Oberfläche die Möglichkeit, einschränkende Firewall-Regeln ausschließlich zum SIS zu setzen und den Internet-Zugang der Rechner im LAN zu steuern. Die Regeln werden basierend auf folgenden Parametern gesetzt: Absender IP-Adresse, Absender Port, Empfänger IP-Adresse, Empfänger Port und Übertragungsprotokoll.

Administratoren haben auch die Möglichkeit, bestehende einschränkende Regeln zu editieren oder zu löschen.

Hinweis: Administratoren können nur eingehende Netzwerkverbindungen aus dem LAN konfigurieren.

Im Reiter "Firewall" (siehe Abbildung 93) erhält der Administrator eine Übersicht über die derzeitige Konfiguration der Firewall.

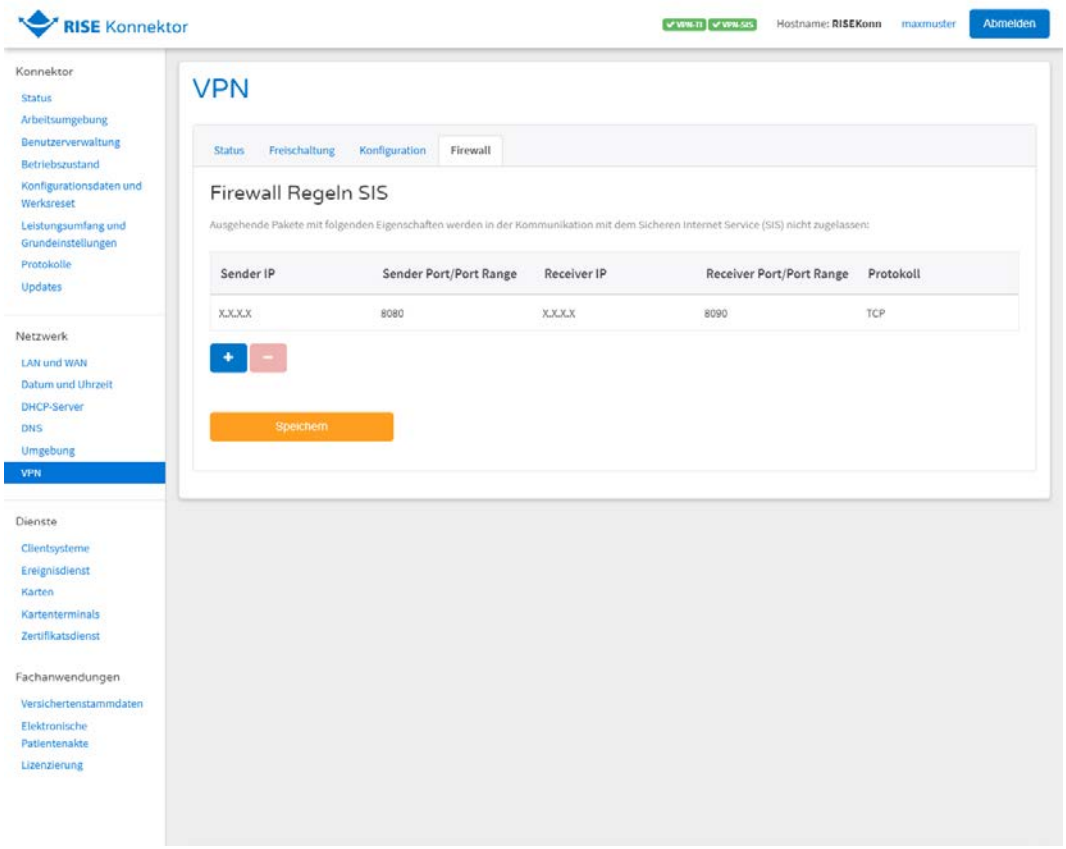


Abbildung 93: Firewall-Konfiguration für SIS

Um eine neue einschränkende Firewall-Regel zu erstellen, klicken Sie auf das "Plus"-Symbol. Sie können nun eine neue Regel erstellen (siehe Abbildung 94).

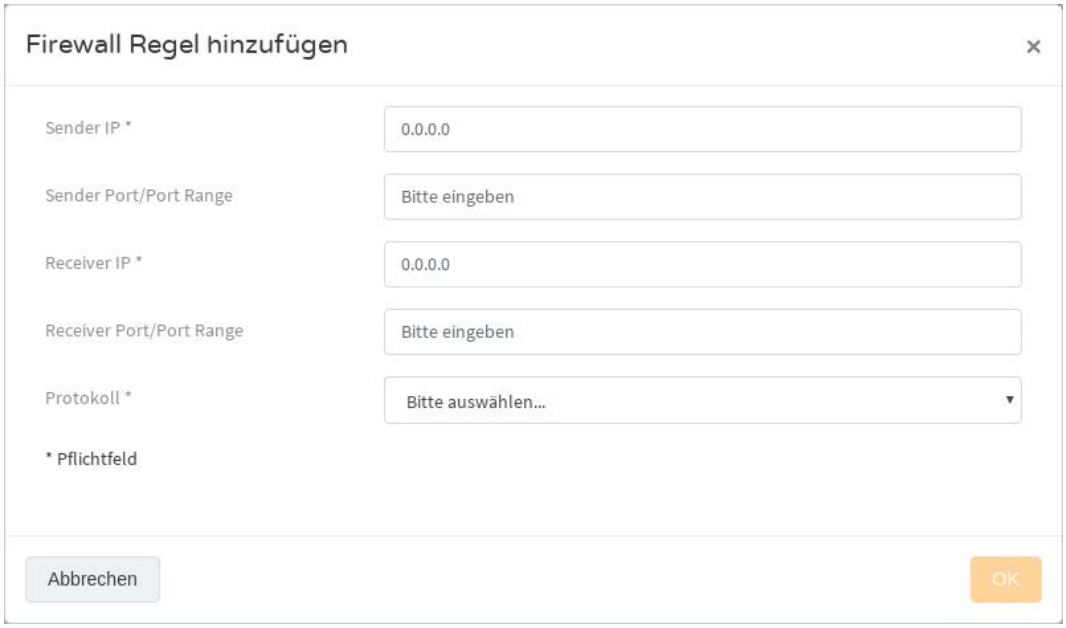


Abbildung 94: Erstellen einer neuen Firewall-Regel

ReferenzID	Belegung	Bedeutung

ReferenzID	Belegung	Bedeutung
Firewall Regeln SIS (ANLW_FW_SIS_ADMIN_RULES)	Firewall Regelset	Der Administrator kann Firewall-Regeln für den einschränkenden Zugriff auf die SIS, auf Grundlage der Parameter Absender-IP-Adresse, Empfänger-IP-Adresse, Protokoll, Absender-Port und Empfänger-Port einfügen, editieren und löschen.

Tabelle 36: Konfiguration von Firewall Regeln

Sicherheitshinweis: Durch das Erstellen neuer Firewall-Regeln schränken Sie den Internetzugriff auf den Client-PCs, und damit Dienste, die möglicherweise für den reibungslosen Betrieb beim Leistungserbringer erforderlich sind, ein. Stimmen Sie sich daher vor dem Erstellen neuer Firewall-Regeln mit dem Personal der Leistungserbringer-Organisation ab.

Hinweis: Es können nur ausgehende Firewall-Regeln gesetzt werden.

6.2.6.4 VPN-Freischaltung

Im Reiter "Freischaltung" zeigt die Benutzermaske Einstellungen der RISE Konnektor Registrierung beim Zugangsdienstprovider. Der Anbieter des VPN-Zugangsdienstes stellt dem Leistungserbringerinstitut die erforderliche Vertragsnummer (Contract-ID) für die Registrierung zur Verfügung.

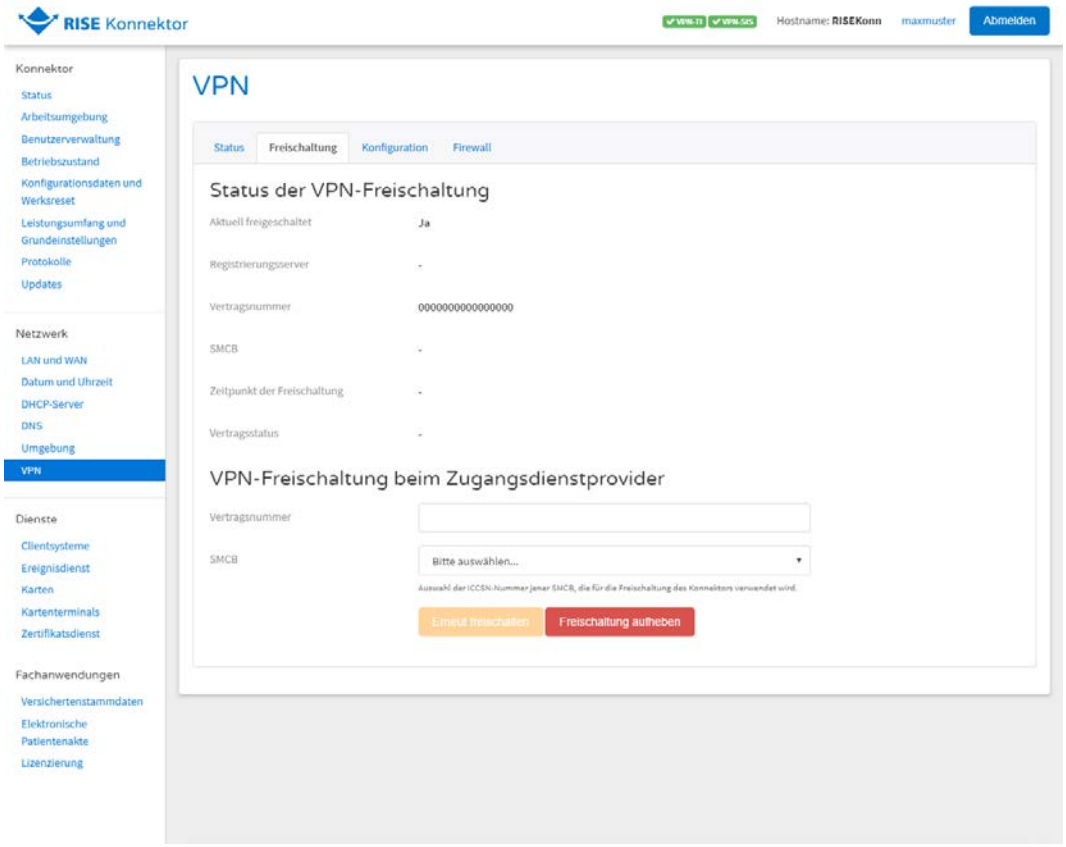


Abbildung 95: VPN-Freischaltung der Zugangsdienstbetreiber

ReferenzID	Belegung	Bedeutung
Vertragsnummer (MGM_ZGDP_CONTRACTID)	Für die Admin-Rollen (Super- & lokaler Admin) einsehbar/veränderbar Wertebereich: Contract-ID - gültiger String	Dieser Konfigurationsparameter enthält die vom Zugangsdienst erhaltene Contract-ID, welche von einem Administrator zur Freischaltung des RISE Konnektors eingetragen werden muss.
SMCB (MGM_ZGDP_SMCB)	Für die Admin-Rollen (Super- & lokaler Admin) einsehbar/veränderbar Wertebereich: Gültige ICCSN	Dieser Konfigurationsparameter enthält die ICCSN der zur Freischaltung des RISE Konnektors zu verwendenden SMC-B.

Tabelle 37: Registrierung beim Zugangsdienstprovider

Nach erfolgreicher Registrierung ist der Status der Registrierung inklusive aller Informationen im Bereich “Status der VPN-Freischaltung” einsehbar.

6.2.6.5 Fehlermeldungen

Im Zuge der Einstellungen von VPN können Fehler gem. Tabelle 38 auftreten.

Fehlercode	Fehlertyp	Severity	Fehlertext
4171	Technical	Fatal	Der VPN-Tunnel zur TI konnte nicht beendet werden.
4172	Technical	Fatal	Es ist keine Online-Verbindung zulässig.
4173	Technical	Fatal	Die CRL ist nicht mehr gültig (outdated).
4174	Technical	Fatal	TI VPN-Tunnel: Verbindung konnte nicht aufgebaut werden.
4175	Technical	Fatal	Der VPN-Tunnel zum SIS konnte nicht beendet werden.
4176	Technical	Fatal	SIS VPN-Tunnel: Verbindung konnte nicht aufgebaut werden.

Tabelle 38: Fehlermeldungen des VPN-Dienstes

6.3 RISE Konnektor Dienste

Das Dienste-Hauptmenü setzt sich aus den Unterpunkten zusammen, die in Abschnitt 6.3.1 bis Abschnitt 6.3.5 im Detail erläutert werden:

- Anbindung der Clientsysteme (Abschnitt 6.3.1)
- Ereignisdienst (Abschnitt 6.3.2)
- Karten (Abschnitt 6.3.3)
- Kartenterminal (Abschnitt 6.3.4)
- Zertifikatsdienst (Abschnitt 6.3.5)

6.3.1 Anbindung der Clientsysteme

Die Anbindung der Clientsysteme erfolgt optional mittels TLS. Dabei können am Clientsystem Konfigurationen (siehe Abschnitt 6.3.1.2), Passwörter (siehe Abschnitt 6.3.1.3) und Zertifikate (siehe Abschnitt 6.3.1.4) modifiziert werden. Bitte beachten Sie, dass Sie Clientsysteme zuvor in der Arbeitsumgebung definieren müssen (siehe Abschnitt 6.1.4.2.1). Der in der Arbeitsumgebung vergebene Name (entspricht der ID eines Clientsystems) wird an dieser Stelle weiter verwendet.

6.3.1.1 Anforderung an Clientsysteme

Bitte beachten Sie, dass für die im Clientsystem konfigurierten Felder (User-ID, Mandanten-ID, Workplace-ID, Clientsystem-ID) folgende Zeichen erlaubt sind:

- Wortzeichen (A-Z, a-z)
- Ziffern (0-9)
- Umlaute, “ß”
- Sonderzeichen bis ASCII-Code 0x7E
- Abstand/Space (ASCII-Code 0x20), jedoch nicht zu Beginn oder am Ende des Wertes
- Unicode von U+00A1 bis U+00FF (Latin-1 Supplement)
- Unicode von U+0100 bis U+017F (Latin Extended-A)

Dabei müssen die Felder jeweils mindestens ein Zeichen enthalten und dürfen eine Länge von 64 Zeichen nicht überschreiten.

6.3.1.2 Clientsystem-Konfiguration

Im Reiter “Konfiguration” zeigt die Benutzermaske die Konfigurationsparameter der Clientsysteme (siehe Abbildung 96). Hierbei können Konfigurationen vorgenommen werden, um die Kommunikation mit den Clients mittels TLS abzusichern bzw. um

die verpflichtende Authentifizierung von Clientsystemen zu aktivieren bzw. zu deaktivieren.

Ist TLS aktiviert, so authentifiziert sich der Konnektor gegenüber Clientsystemen mit dem Konnektor-Zertifikat. Um eine TLS-Verbindung zwischen dem PVS und dem Konnektor zu konfigurieren, kann das Konnektor-Zertifikat manuell heruntergeladen werden:

- Rufen Sie dazu die Addresse https://<IP-Adresse des RISE Konnektors>/connector.sds auf
- Laden Sie das Zertifikat, beispielsweise durch Anzeigen der Seiteninformationen im Browser, herunter. Dies ist abhängig vom genutzten Browser, daher ist ggf. in der entsprechenden Browser-Anleitung nachzusehen, wie Zertifikate (.pem-Datei) von einer Website heruntergeladen werden kann.
- Importieren Sie das Zertifikat anschließend in das PVS-System, welches auf den Konnektor zugreift. Ziehen Sie dafür ggf. das Handbuch für Ihr PVS-System heran.

Sicherheitshinweis: Aus Sicherheitsgründen soll die Kommunikation der Clientsysteme mit dem Konnektor und dessen Fachmodule verschlüsselt erfolgen. Dies erfolgt, indem das Häkchen bei "Verpflichtend TLS verwenden" gesetzt ist (ANCL_TLS_MANDATORY=Enabled). Falls diese Kommunikation unverschlüsselt erfolgt (Häkchen nicht gesetzt bzw. ANCL_TLS_MANDATORY=Disabled), übernimmt der Administrator und somit der Leistungserbringer die Verantwortung für die Sicherstellung der vertraulichen Übertragung.

Sicherheitshinweis: Ohne Authentisierung des Konnektors durch das Clientsytsem (d.h. TLS-Client-Authentication über X.509-Zertifikate) können CETP-Nachrichten möglicherweise nicht authentisch, integer und vertraulich empfangen werden. Für die Authentisierung muss ein X.509-Zertifikat am Clientsystem eingebracht werden.

Sicherheitshinweis: Eine ungesicherte Verbindung zwischen Clientsystem und Konnektor bietet keinen Schutz gegen Man-in-the-Middle Angriffe.

Sicherheitshinweis: Der Administrator muss die Nutzer darüber informieren, welche Art von Verbindung zwischen Clientsystem und Konnektor existiert.

Sicherheitshinweis: Keine oder einseitige authentisierte TLS-Verbindungen des Konnektors können dazu führen, dass unbemerkt qualifizierte Signaturn über von Angreifern vorgegeben Dokumente erstellt werden.

Sicherheitshinweis: Wird ANCL_TLS_MANDATORY von Disabled auf Enabled gesetzt, so ist anschließend ein Reboot des Konnektors notwendig, um sicherzustellen, dass bestehende nicht verschlüsselte Verbindungen abgebaut werden.

Hinweis: Wurde eine passwortbasierte Authentifizierung gewählt, findet keine Authentisierung des LDAP-Clients statt.

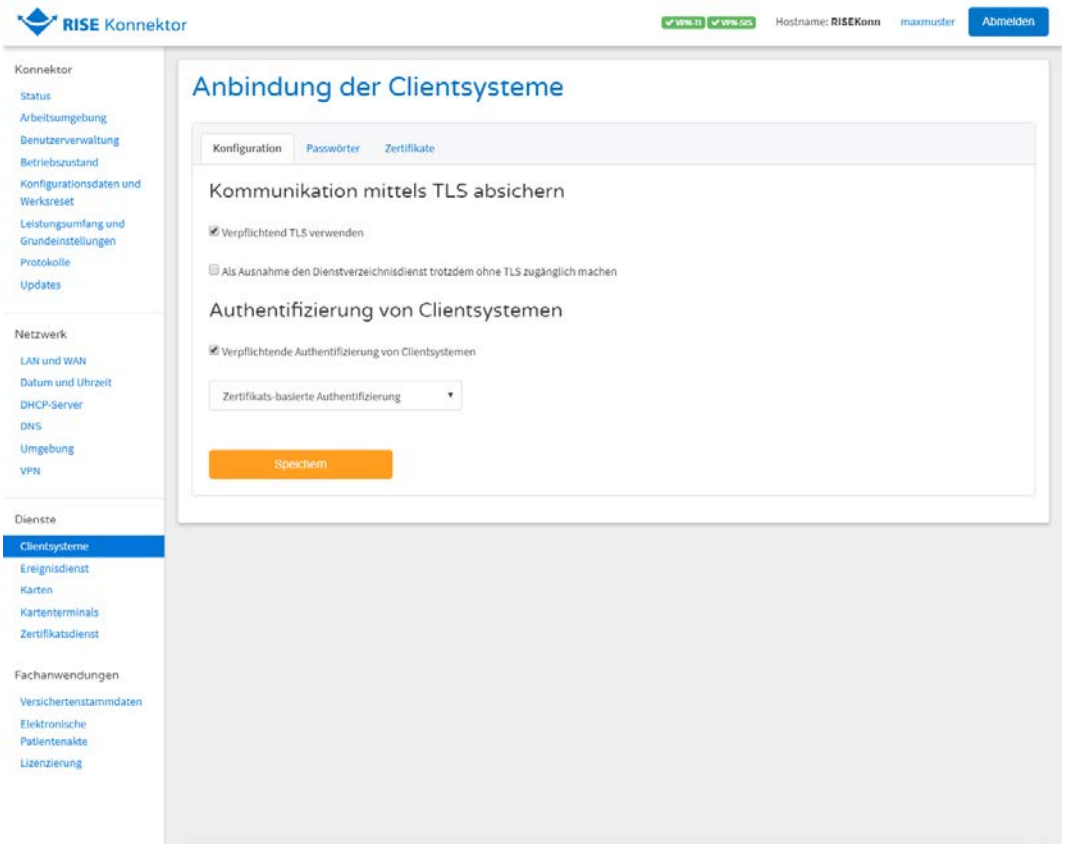


Abbildung 96: Clientsystem Konfiguration

ReferenzID	Belegung	Bedeutung
Verpflichtend TLS verwenden (ANCL_TLS_MANDATORY)	Enabled / Disabled; Standard-Wert: Enabled	Der Administrator kann die verpflichtende Verwendung eines mittels TLS gesicherten Übertragungskanals an- oder abschalten. Wenn ANLW_ANBINDUNGS_MODUS =Parallel konfiguriert ist, erscheint vor dem Deaktivieren von ANCL_TLS_MANDATORY ein Warnhinweis, der über die mit der Abschaltung verbundenen Risiken informiert und darlegt, dass in diesem Fall der Administrator die Verantwortung für die Sicherstellung der vertraulichen Übertragung übernimmt.
Als Ausnahme den	Enabled / Disabled; Standard-	Der Administrator kann

ReferenzID	Belegung	Bedeutung
Dienstverzeichnisdienst trotzdem ohne TLS zugänglich machen (ANCL_DVD_OPEN)	Wert: Enabled	konfigurieren, ob der Zugriff auf den Dienstverzeichnisdienst auch dann über einen ungesicherten HTTP-Kanal erfolgen kann, wenn TLS verpflichtend verwendet werden muss.
Verpflichtende Authentifizierung von Clientsystemen (ANCL_CAUT_MANDATORY)	Enabled / Disabled; Standard-Wert: Enabled	Der Administrator kann die verpflichtende Authentifizierung der Clientsysteme an- oder abschalten.
Authentifizierung (ANCL_CAUT_MODE)	Zertifikatsbasierte Authentifizierung/Passwortbasierte Authentifizierung; Standard-Wert: Zertifikatsbasierte Authentifizierung	Der Administrator kann konfigurieren, welcher Client Authentifizierungsmodus genutzt werden muss.

Tabelle 39: Konfiguration des Clientsystems

6.3.1.3 Clientsystem-Passwörter

Im Reiter “Passwörter” zeigt die Benutzermaske Einstellungsmöglichkeiten zu den Passwortkonfigurationen des Clientsystems. Bitte beachten Sie, dass Sie Clientsysteme zuvor in der Arbeitsumgebung definieren müssen (siehe Abschnitt 6.1.4.2.1)

Sicherheitshinweis: Das Passwort muss eine Mindestlänge von 20 Zeichen aufweisen. Passwörter müssen für jedes Clientsystem unterschiedlich sein und zufällig mit ausreichender Entropie (also auch voneinander unabhängig) gewählt werden.

Bitte beachten Sie, dass für den Benutzernamen folgende Regeln gelten:

- Maximale Länge: 500 Zeichen
- Der Benutzername muss global eindeutig sein.
- Erlaubte Zeichen:
  - Wortzeichen (A-Z, a-z), keine Umlaute oder “ß”
  - Ziffern (0-9)
  - Unterstrich (Underscore) ("_")
  - Bindestrich (“-”)

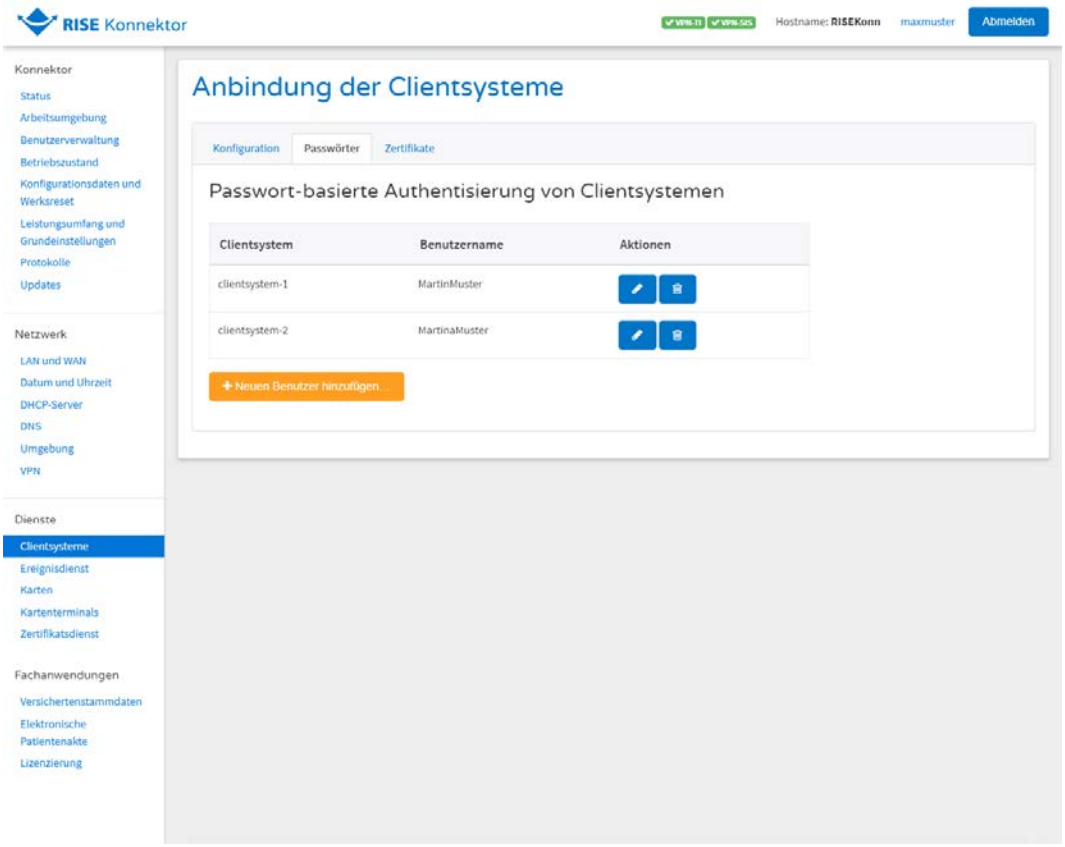


Abbildung 97: Passwörter des Clientsystems

ReferenzID	Belegung	Bedeutung
Passwort-basierte Authentisierung von Clientsystemen (ANCL_CUP_LIST)	Liste von Benutzer/Passwort-Kombinationen, zugeordnet zu ClientID	Liste an Anmeldeinformationen und dazugehörenden Client-system IDs. Der Administrator kann eine Liste von Anmeldeinformationen und zugehörendem Clientsystem verwalten. Bei diesen Benutzer-/Passwortkombinationen handelt es sich nicht um personenbezogene Anmeldeinformationen, sondern um clientbezogene.

Tabelle 40: Passwörter des Clientsytems

6.3.1.4 Clientsystem-Zertifikate

Im Reiter “Zertifikate” zeigt die Benutzermaske Einstellungsmöglichkeiten der zertifikatsbasierten Authentisierung von Clientsystemen. Als Client-Zertifikate werden nur Self-Signed Zertifikate unterstützt.

Zunächst sind alle Clientsysteme aufgelistet, für welche Zertifikate im Konnektor gespeichert sind. In dieser Liste befindet sich einerseits der Name des Clientsystems, neben einem “Auge”-Symbol (Details zum Zertifikat können damit angezeigt

werden) sowie einem “Mülleimer”-Symbol (damit kann der Eintrag gelöscht werden – siehe auch Abschnitt 6.3.1.4.1).

Mittels des Buttons “Neues Zertifikat hinzufügen” können weitere Zertifikate für Clientsysteme hinzugefügt/generiert werden (siehe auch Abschnitt 6.3.1.4.2) bzw. können auch bereits bestehende Zertifikate importiert werden (siehe auch Abschnitt 6.3.1.4.3).

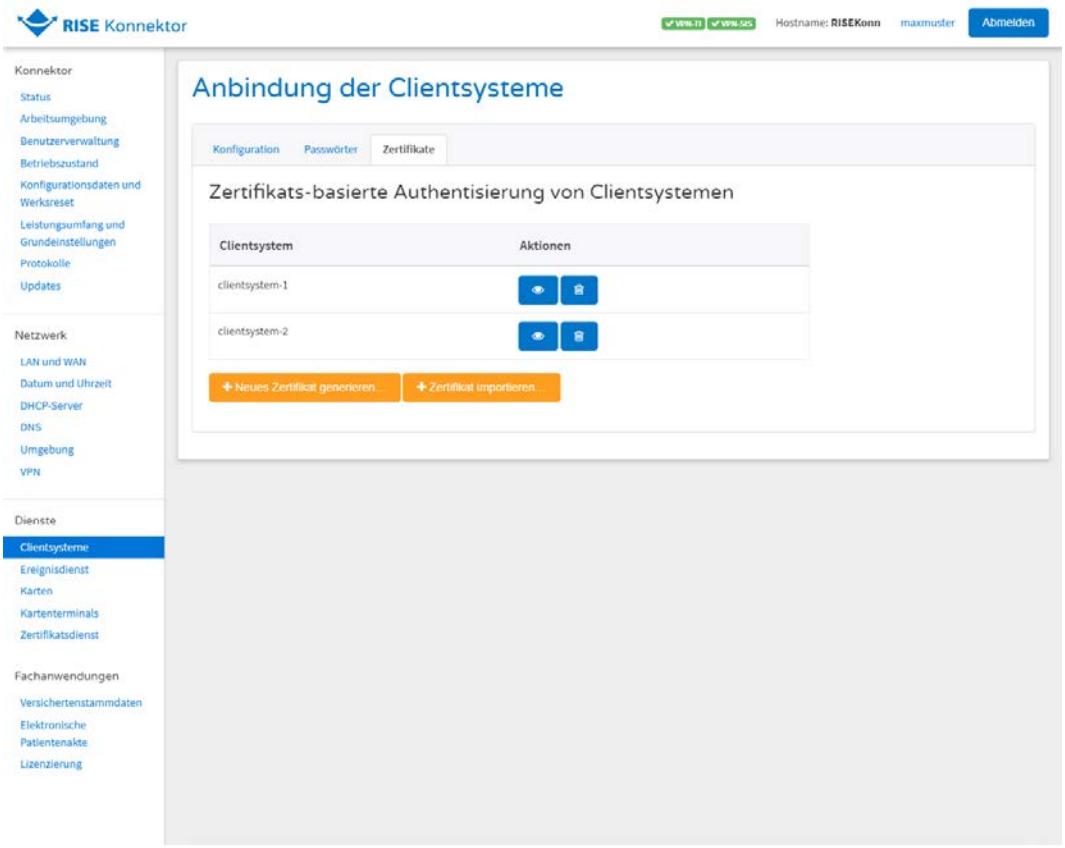


Abbildung 98: Clientsystem Zertifikate

ReferenzID	Belegung	Bedeutung
Zertifikats-/Passwort-basierte Authentisierung von Clientsystemen (ANCL_CCERT_LIST)	Liste von X.509-Zertifikaten zugeordnet zu ClientID	Whitelist an importierten oder vom Konnektor erzeugten X.509-Zertifikaten und dazu gehörenden Clientsystem IDs. Der Administrator kann die Liste der Zertifikate und den zugehörenden Clientsystemen verwalten.

Tabelle 41: Zertifikate des Clientsystems

Sicherheitshinweis: Der RISE Konnektor führt eine vollständige Prüfung[12] des Clientsystem-Zertifikats beim Importieren durch. Diesem Zertifikat wird solange vertraut, bis das Zertifikat abläuft oder der Administrator das Zertifikat wieder entfernt oder ersetzt.

Sicherheitshinweis: Der Administrator ist dafür verantwortlich, dass abgelaufene Clientsystem-Zertifikate ersetzt werden.

Sicherheitshinweis: Die verwendeten Zertifikate sollen eine Schlüssellänge von mind. 2048 bit aufweisen und die Extension "X509v3 Subject Key Identifier" und "X509v3 Authority Key Identifier" enthalten.

Sicherheitshinweis: Ergibt die vollständige Prüfung durch den Konnektor beim Import eines Clientsystem-Zertifikats, dass dessen Algorithmen und/oder Schlüssellängen nicht konform den Signaturrichtlinien (siehe Abschnitt 8) sind, so ist der Client in diesem Fall praktisch nicht authentifiziert.

6.3.1.4.1 Zertifikate löschen

Bevor Sie ein Zertifikat löschen, müssen Sie eine Sicherheitsabfrage bestätigen (siehe Abbildung 99).

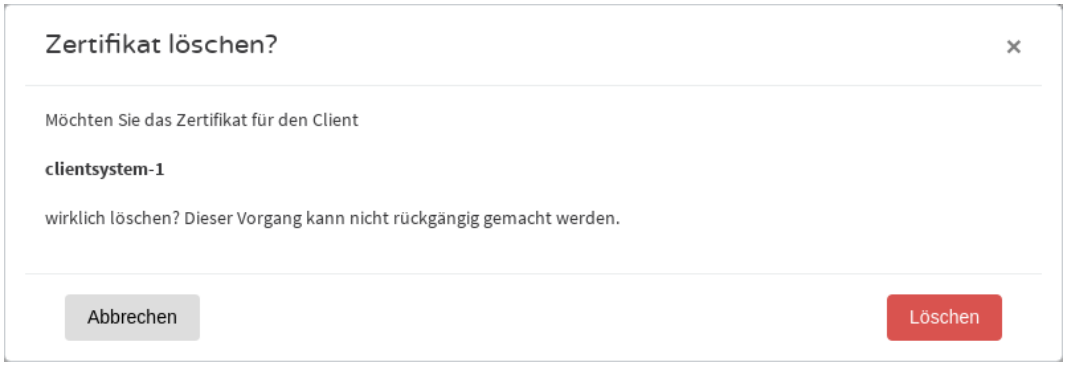


Abbildung 99: Sicherheitsabfrage beim Löschen eines Zertifikats

Warnung: Das Löschen von Zertifikaten kann nicht mehr rückgängig gemacht werden! Durch das Fehlen von Zertifikaten kann es zu einer Einschränkung im Betrieb des RISE Konnektors kommen, da möglicherweise die Vertrauenswürdigkeit von Gegenstellen nicht mehr überprüft werden kann.

6.3.1.4.2 Zertifikat hinzufügen

Mit Hilfe des Buttons "Neues Zertifikat hinzufügen" können neue Zertifikate für Clientsysteme generiert werden. Hierfür muss zunächst im ersten Schritt ein Clientsystem ausgewählt werden (siehe Abbildung 100).

[12] Vollständig heißt an der Stelle, dass das Zertifikat folgende Eigenschaften aufweisen muss: gültige Signatur, self-signed, nicht abgelaufen, die Extensions subjectKeyIdentifier und authorityKeyIdentifier müssen vorhanden sein.

Abbildung 100: Hinzufügen eines Zertifikats – Auswahl Clientsystem

Nach Drücken auf "Weiter" wird das Zertifikat generiert und kann über den angezeigten Link heruntergeladen werden. Des Weiteren wird noch das dazugehörige Passwort angezeigt (siehe Abbildung 101).

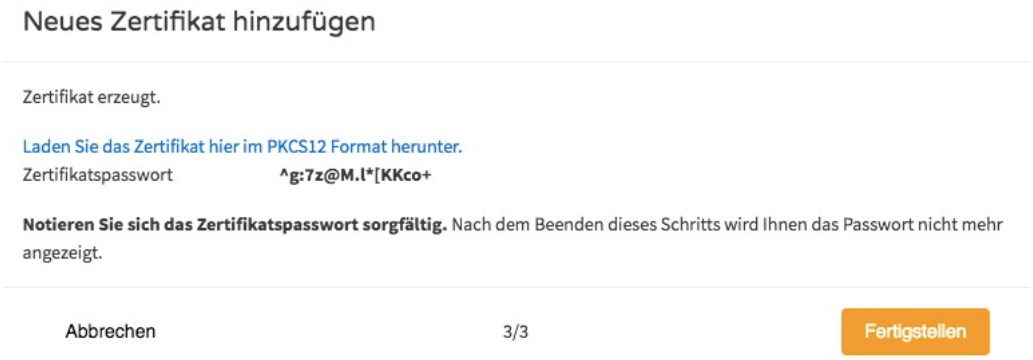


Abbildung 101: Hinzufügen eines Zertifikats – Downloadlink und Passwort

6.3.1.4.3 Client-Zertifikat importieren

Mit Hilfe des Buttons "Zertifikat importieren" können bereits bestehende Zertifikate eines Clientsystems in den Konnektor eingebracht werden. Hierfür muss zunächst das gewünschte Clientsystem ausgewählt werden, und dann das jeweilige Zertifikat (.pem-Datei) hochgeladen werden.

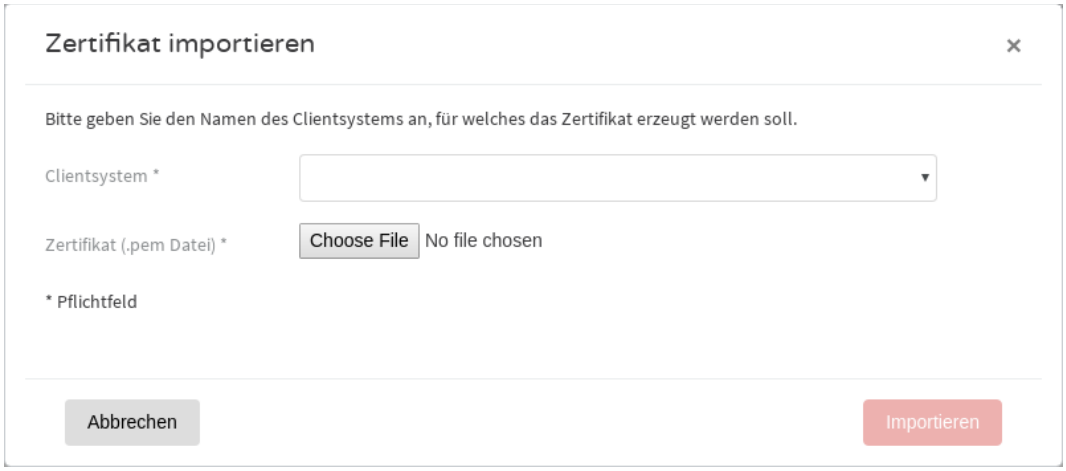


Abbildung 102: Importieren eines Zertifikats

6.3.2 Ereignisdienst

Mit Hilfe des Ereignisdienstes können einerseits Einstellungen bzgl. Zustellungen von Ereignissen an Clientsysteme und andererseits bzgl. der Überwachung kryptographischer Operationen vorgenommen werden.

6.3.2.1 Ereignisdienst – Konfiguration

Im Reiter "Konfiguration" kann der Administrator Einstellungen zu der Benachrichtigung von Clientsystemen vornehmen.

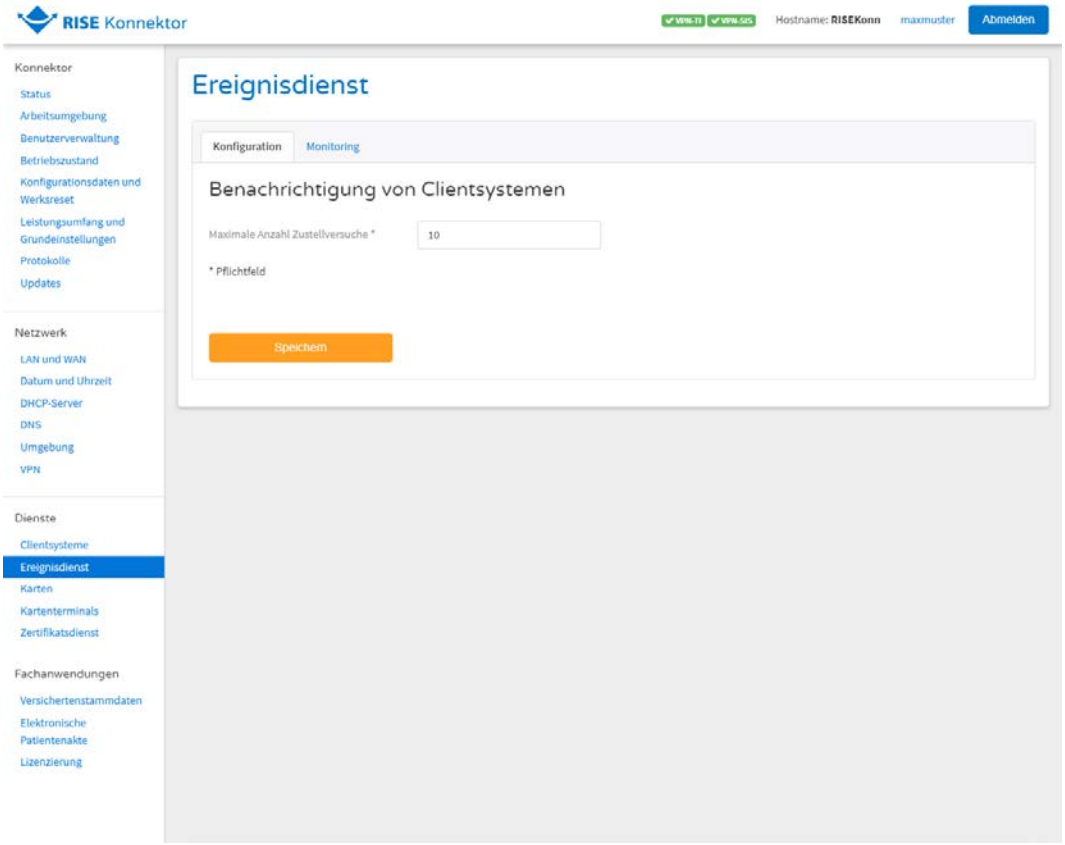


Abbildung 103: Ereignisdienst - Konfiguration - Benachrichtigungen von Clientsystemen

ReferenzID	Belegung	Bedeutung
Maximale Anzahl Zustellversuche	X Versuche; Standardwert: 3	Die Anzahl der maximalen Zustellversuche gibt an, wie oft der Konnektor versucht, eine Ereignisbenachrichtigung an das Clientsystem zuzustellen.

Tabelle 42: Konfigurationswerte des Ereignisdienstes

6.3.2.2 Ereignisdienst – Monitoring

Im Reiter "Monitoring" können Einstellungen getroffen werden, um kryptographische Operationen zu überwachen.

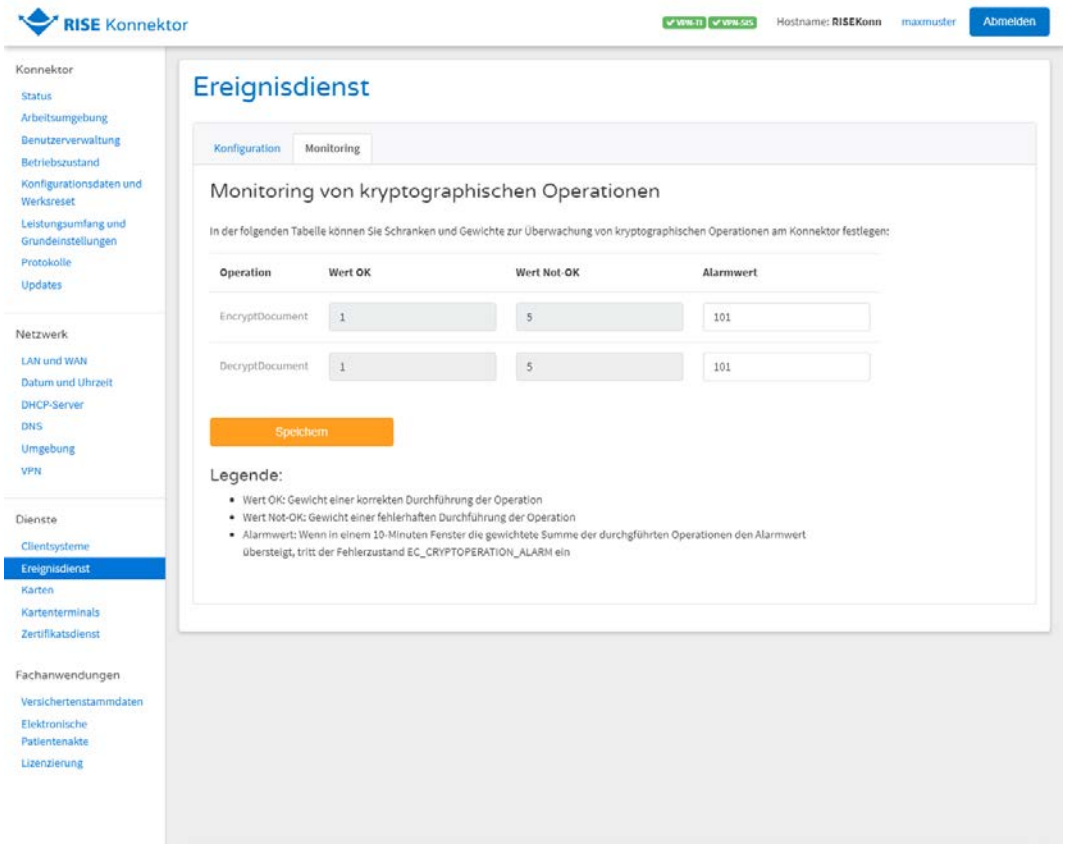


Abbildung 104: Ereignisdienst - Monitoring

6.3.3 Karten

Grundsätzlich kann der RISE Konnektor verschiedene Kartentypen verwalten:

- eGK (G1+ und G2): Die elektronische Gesundheitskarte.
- HBA-qSig: HBA-Vorläuferkarte.
- HBA: Der elektronische Heilberufsausweis (HBA).
- SMC-B: Die Institutionskarte Typ B.
- HSM-B: HSM-Variante einer SMC-B. Das HSM-B wird in dieser Fassung als ein oder mehrere virtuelle Kartenterminals verstanden, in denen virtuelle Karten stecken.
- gSMC-KT: Gerätespezifische Secure Module Card Typ KT.
- KVK: Die Krankenversichertenkarte.
- ZOD_2.0: HBA-Vorläuferkarte.

In der Folge können auch Kartentypen zusammengefasst bezeichnet werden. Die zugehörigen Aussagen und Festlegungen gelten für die jeweils betroffenen Kartentypen.

- HBA-VK: Adressiert die HBA-Vorläuferkarten HBA-qSiq und ZOD_2.0.
- HBAx: Adressiert sowohl den HBA, als auch die HBA-Vorläuferkarten (HBA-VK).

- SM-B: Adressiert sowohl eine echte SMC-B als auch eine in einem HSM-B enthaltene virtuelle SMC-B.

Falls eine Karte unlesbar bzw. nicht erkennbar ist, kann diese als UNKNOWN interpretiert und dargestellt werden.

Sicherheitshinweis: Der Leistungserbringer hat sicherzustellen, dass nur authentische Karten mit dem Typ HBA und SMC-B verwendet warden.

Sicherheitshinweis: Für einen zertifizierten Betrieb des Konnektors und dessen Fachmodule muss ein HBA der Produktiv-Umgebung benutzt werden. Dabei ist die Verwendung eines HBA mit abgelaufenem Zertifikat unzuläsig.

Sicherheitshinweis: Der Versicherte darf seine eGK nur dann und nur dort einem HBA-Inhaber oder einem seiner Mitarbeiter aushändigen, wenn er diesem Zugriff auf seine Daten gewähren will. Nach Abschluss der Konsultation nimmt er seine eGK wieder an sich. Schulen Sie das Personal beim Leistungserbringer diesbezüglich.

6.3.3.1 Kartenverwaltung

Das Menü “Karten” gibt im Reiter “Status” eine Übersicht über alle durch den RISE Konnektor verwalteten Karten (siehe Abbildung 105). In dieser ersten Übersicht sind Informationen zum Kartentyp, der ICCSN der Karte und dem Karteninhaber gegeben. Darüber hinaus wird gelistet, an welchem Kartenterminal, in welchem Slot die Karte unter welchem Hostname gesteckt ist. Ebenso ist der Einsteckzeitpunkt der Karte angeführt. Es können zudem Detailinformationen zu den jeweiligen Karten abgerufen werden. Ebenso befindet sich das PIN-Management (siehe Abschnitt 6.3.3.1.1) in der Detailseite der Kartenverwaltung (bei Karten vom Typ SM-B). Um diese Detailseite zu öffnen, klicken Sie auf das Stift-Symbol in der jeweiligen Kartenzeile.

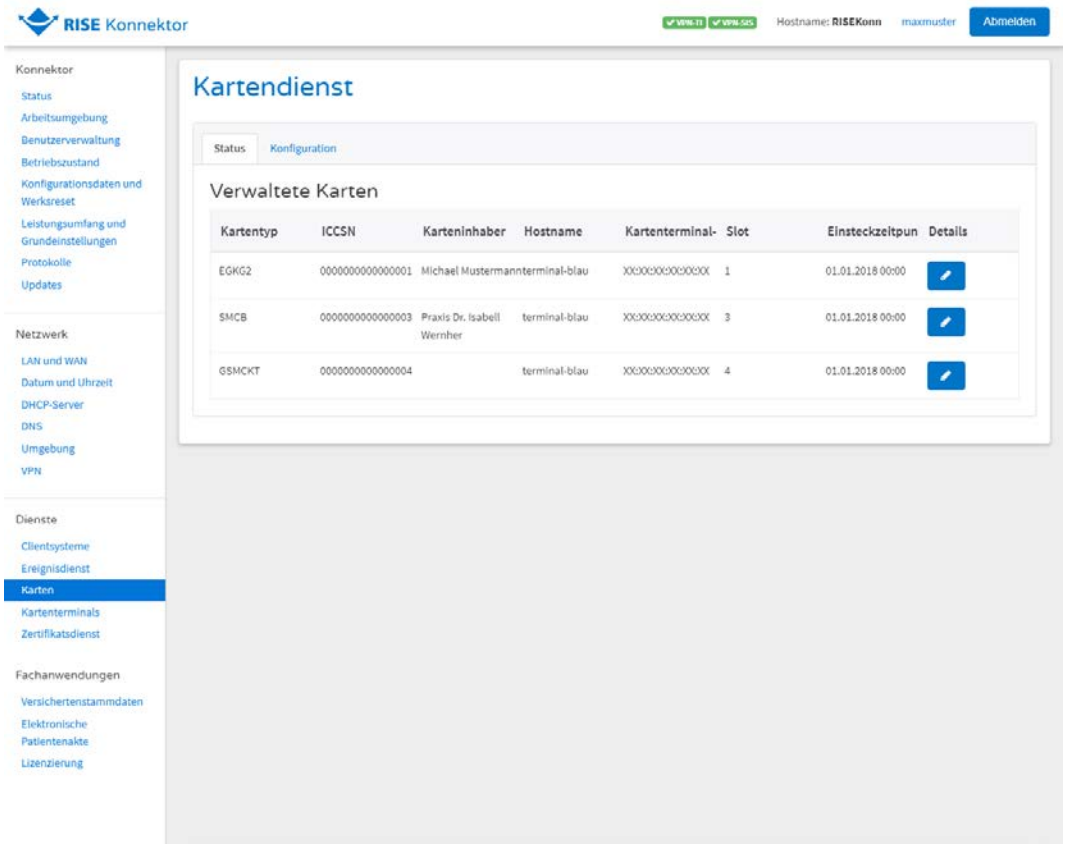


Abbildung 105: Übersicht über verwaltete Chipkarten

ReferenzID	Belegung	Bedeutung
Verwaltete Karten (CM_CARD_LIST)	Liste von Card-Objekten	Eine Liste von Repräsentanzen (CardObjects) der dem Konnektor bekannten Karten. Die Attribute der Card-Objekte sind im Folgenden gelistet.

Tabelle 43: Übersicht über verwaltete Karten

In der Detailseite zur Karte (siehe Abbildung 106) sind im Reiter "Karte" alle Informationen gelistet, die zu einer Karte bekannt sind. Dies sind im Wesentlichen drei Bereiche:

- Versicherteninformationen: Hier werden, wenn verfügbar, der Name des Karteninhabers bzw. der Institution / Organisation, die Versichertennummer sowie das Ablaufdatum des AUT-Zertifikates dargestellt.
- Allgemeine Karteninformationen: Hier werden kartenspezifische, technische Informationen dargestellt. Dies ist etwa die ICCSN, eine Nummer, anhand der die Karte identifiziert wird. Des Weiteren wird der CardHandle ausgegeben. Dies ist ebenfalls ein eindeutiges, technisches Identifikationsmerkmal der Karte. Darüber hinaus sind Kartentyp und Kartenversion mitsamt Detailinformationen angeführt.
- Terminalinformation: Hier werden Informationen zum Kartenterminal gegeben, in dem die Karte gesteckt wurde: Kartenterminal-ID, Kartenterminal-Hostname, Slot, an dem die Karte steckt, sowie der Einsteckzeitpunkt.

Im Reiter “Sessions” befindet sich eine Auflistung der aktuellen Sitzungen einer Karte, welche neben Informationen zur Art der Authentisierung auch die Parameter Mandant-ID, Clientsystem-ID und User-ID des entsprechenden Kartenkontexts enthält. Da die User-ID ein schützenswertes Datum ist, wird dieser Wert allerdings ausgeblendet und durch den Platzhalter "***" ersetzt.

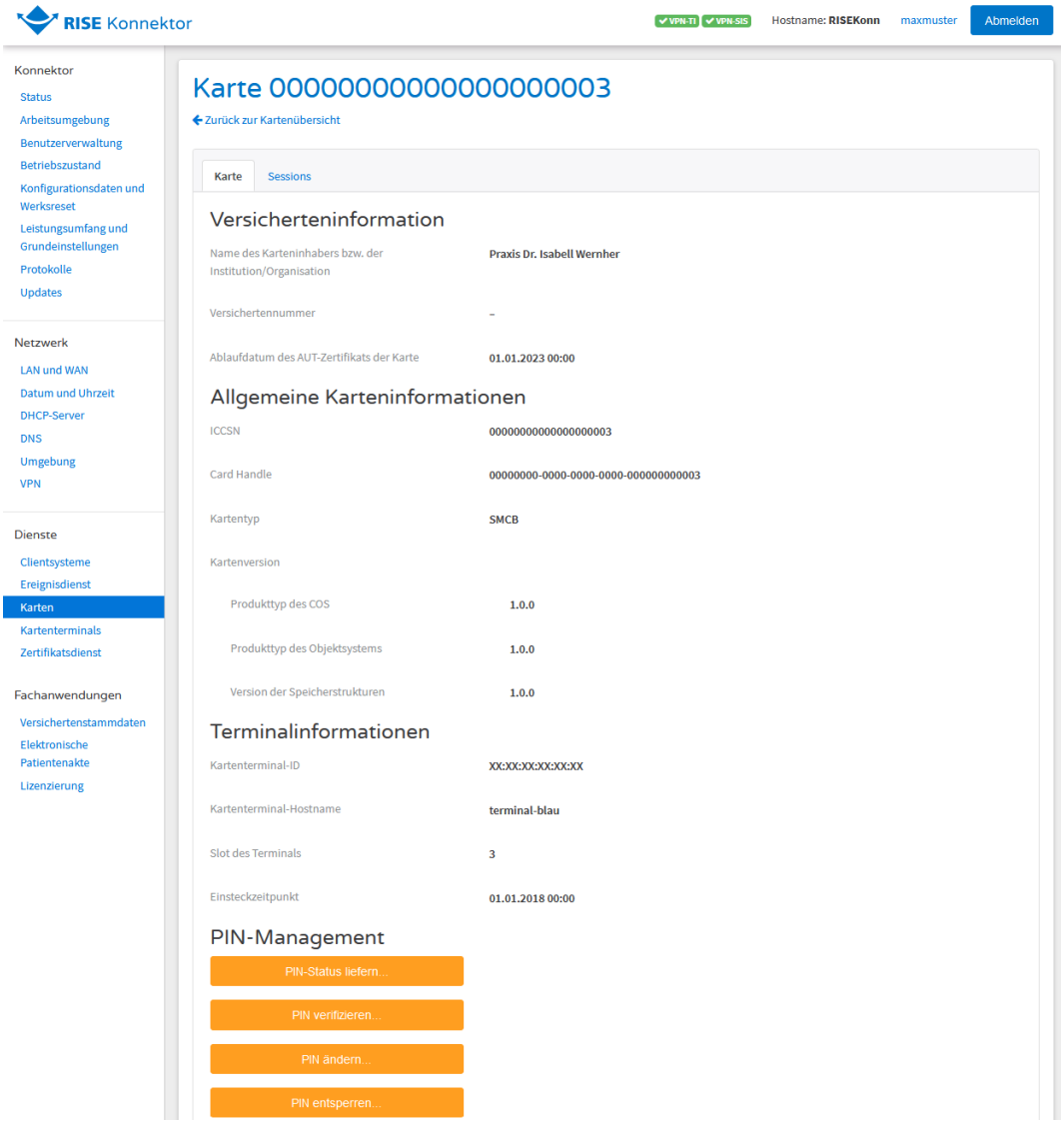


Abbildung 106: Karten-Detailansicht

6.3.3.1.1 PIN-Management

Sofern es sich um eine Karte des Typs SM-B handelt (d.h. sowohl eine echte SMC-B als auch eine in einem HSM-B enthaltene virtuelle SMC-B), ist es möglich, PIN-Management-Aktionen durchzuführen. Der gesamte Block erscheint automatisch in der Detailansicht zur Karte, sofern die Karte PIN-Management zulässt. Folgende vier Optionen sind verfügbar:

- PIN-Status liefern
- PIN verifizieren

- PIN ändern
- PIN entsperren

Sicherheitshinweis: Die SMC-B darf nur freigeschaltet sein, so lange sich die Karte und der Konnektor unter der Kontrolle des Karteninhabers befinden. Wenn der Karteninhaber keine Kontrolle mehr über den Konnektor oder die SMC-B hat, muss die Freischaltung der SMC-B zurückgesetzt werden (z.B. durch Ausschalten des Kartenterminals oder Ziehen der Chipkarte).

Sicherheitshinweis: Der Chipkarteninhaber darf seine PIN nur dann an einem Kartenterminal eingeben, wenn der initiierte Anwendungsfall dies erfordert und das Kartenterminal dem Chipkarteninhaber einen sicheren PIN-Eingabemodus anzeigt. Wird der Chipkarteninhaber von einem Kartenterminal zur PIN-Eingabe aufgefordert, ohne dass das Kartenterminal gleichzeitig den sicheren PIN-Eingabemodus anzeigt, muss der Chipkarteninhaber den Vorgang abbrechen und darf seine PIN nicht eingeben. Der Chipkarteninhaber kontrolliert, dass die PIN-Eingabe-Aufforderung (einschließlich Jobnummer) konsistent sowohl in seiner Clientsoftware, als auch auf dem PIN-Kartenterminal angezeigt wird.

Abbildung 107: PIN-Management

Bei den jeweiligen PIN-Management-Aktionen ist eine Interaktion mit dem Karten-Terminal, an dem die Karte gesteckt wurde, oder einem Remote-PIN-Kartenterminal erforderlich. Die Eingabe der PIN oder ggf. PUK erfolgt dabei nicht in der Management-Oberfläche selbst, sondern am Karten-Terminal oder Remote-PIN-Kartenterminal. Um eine PIN-Management-Aktion auszuführen, klicken Sie in der Detailansicht zur Karte den jeweiligen Button. Es erscheint danach ein Dialog, der Sie durch die gesamte Aktion führt. Wählen Sie den Kontext, unter dem die PIN-Eingabe erfolgen soll (Mandant, Clientsystem und Arbeitsplatz) bzw. jenen Arbeitsplatz, an dem die PIN-Eingabe erfolgen soll. Wenn an dem Arbeitsplatz ein Remote-PIN-Kartenterminal eingetragen ist, hat die PIN- oder PUK-Eingabe bzw. Bestätigung an diesem Terminal zu erfolgen – ausgenommen, das Kartenterminal, in dem die Karte gesteckt wurde, befindet sich am gewählten Arbeitsplatz.

- Durch Auswahl der Aktion "PIN-Status liefern" können Sie nach der Auswahl eines Aufrufkontexts (Mandant, Clientsystem und Arbeitsplatz) den Status der Karte und die Anzahl der verbleibenden Eingabe-Versuche der PIN anzeigen (siehe Abbildung 108).
- Wird die Aktion "PIN verifizieren" (siehe Abbildung 109) ausgewählt, so haben Sie im nachfolgenden Dialog die Möglichkeit, die PIN für alle Mandanten, Clientsysteme und Arbeitsplätze der eingesteckten Karten zu verifizieren. Wählen Sie dafür direkt die Option "Für alle Mandanten, Clientsysteme und Arbeitsplätze freischalten" aus. Des Weiteren ist es möglich, einen bestimmten Aufrufkontext (Mandant, Clientsystem und Arbeitsplatz) auszuwählen, für den die PIN verifiziert werden soll. Wählen Sie dafür zusätzlich den gewünschten Kontext mittels Dropdown-Menü für Mandant, Clientsystem und/oder Arbeitsplatz aus.
- Um die PIN zu ändern wählen Sie die Aktion "PIN ändern". Nach der Auswahl eines Aufrufkontexts (Mandant, Clientsystem und Arbeitsplatz) können Sie entweder im lokalen Kartenterminal, in dem die Karte gesteckt ist, oder im Remote-PIN-Kartenterminal des ausgewählten Arbeitsplatzes die neue PIN eingeben.
- Um eine gesperrte PIN zu entsperren, muss eine neue PIN gewählt werden. Diese kann durch die Aktion "PIN entsperren", nach der Auswahl eines Aufrufkontexts (Mandant, Clientsystem und Arbeitsplatz), entweder im lokalen Kartenterminal, in dem die Karte gesteckt ist, oder im Remote-PIN-Kartenterminal des ausgewählten Arbeitsplatzes gesetzt werden.

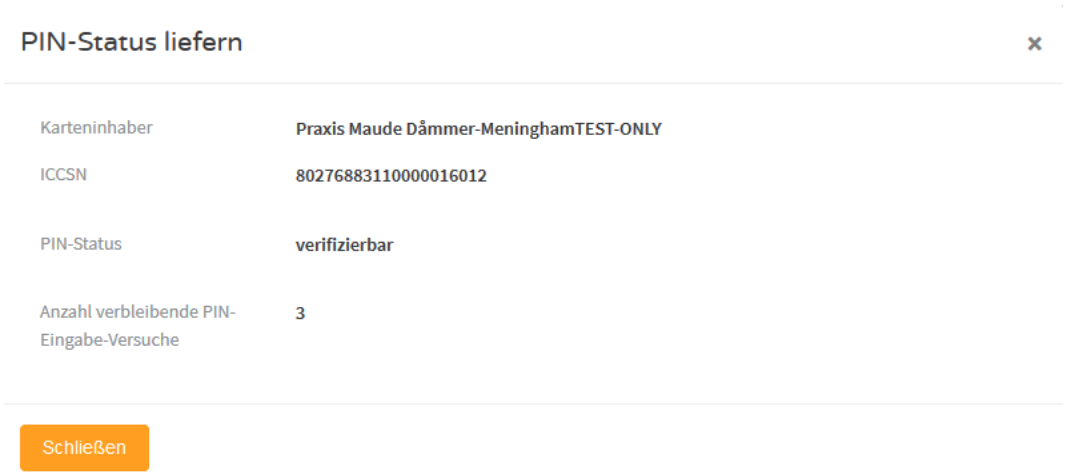


Abbildung 108: PIN-Management - PIN-Status liefern

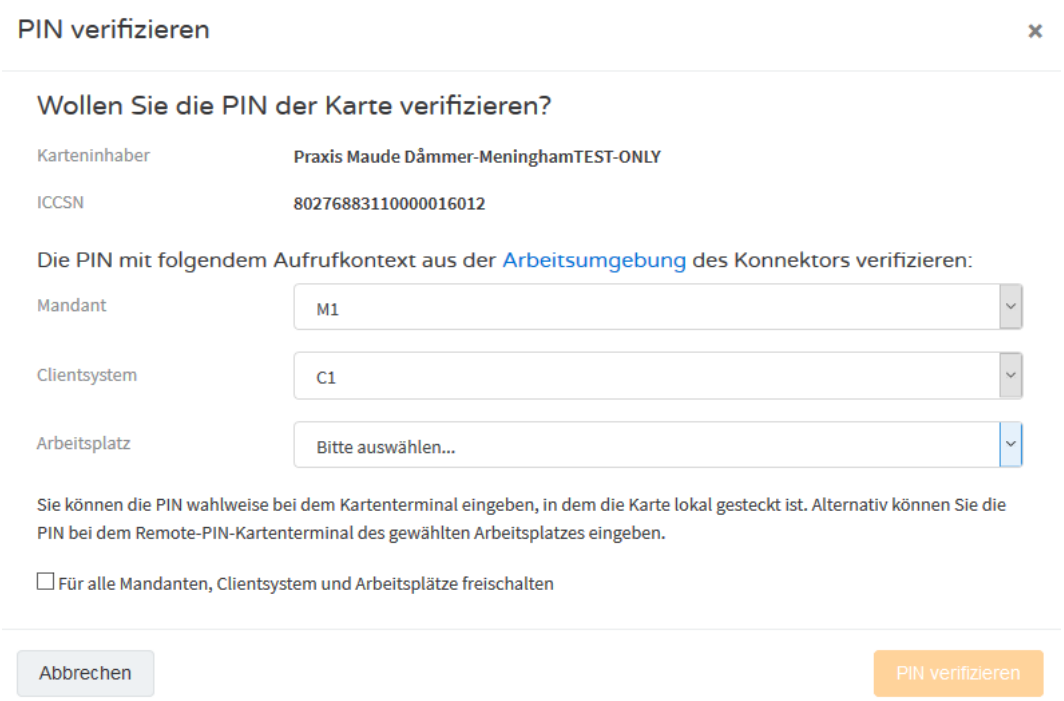


Abbildung 109: PIN-Management - PIN verifizieren

Sie bekommen die erfolgreiche PIN-Aktion als Ergebnis angezeigt. Bitte beachten Sie, dass die Rückmeldung unterschiedliche Status haben kann und abhängig von der jeweiligen Karte ist.

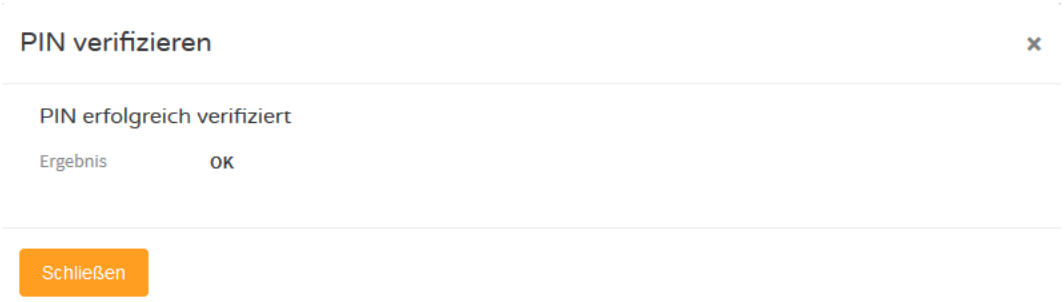


Abbildung 110: PIN-Management - Ergebnisdialog PIN-Verifikation

6.3.3.2 Kartendienstkonfiguration

Im Reiter “Konfiguration” (siehe Abbildung 111) kann die maximale Zeit für ein Karten-Timeout spezifiziert werden. Dies stellt die maximale Zeit eines Aufrufs einer Kartenoperation dar. Einstellungen zu Karten-Zertifikaten bzw. des Ablaufs von Karten-Zertifikaten kann in der Zertifikatsdienst-Konfiguration (vgl. Abschnitt 6.3.5.2) vorgenommen werden.

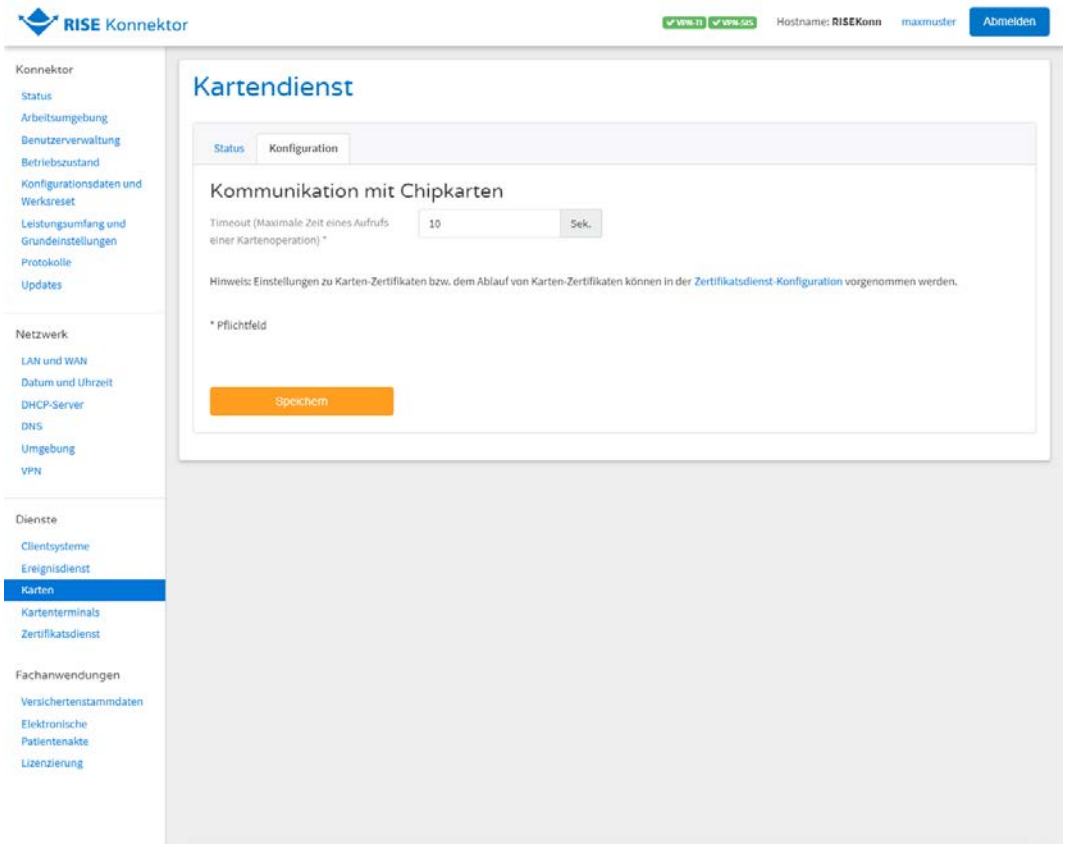


Abbildung 111: Kartendienst – Kommunikation mit Chipkarten

ReferenzID	Belegung	Bedeutung
Timeout (Maximale Zeit eines Aufrufs einer Kartenoperation) (CARD_TIMEOUT_CARD)	Sekunden	Maximale Zeit, die ein Aufruf einer Kartenoperation dauern darf, bevor der Aufruf abgebrochen wird.

Tabelle 44: Konfigurationsparameter Karten

6.3.3.3 Fehlercodes

Im Rahmen der Administration von Karten, die der RISE Konnektor verwaltet, können Fehlercodes, wie in Tabelle 45 dargestellt, auftreten.

Fehlercode	Fehlertyp	Severity	Fehlertext
4043	Technical	Warning	Timeout bei der PIN-Eingabe

Tabelle 45: Fehlercodes im Zusammenhang mit der Administration von Karten

6.3.4 Kartenterminals

Das Menü Kartenterminals bietet einerseits eine Übersicht über alle Kartenterminals und die Möglichkeit weitere Kartenterminals hinzufügen (siehe

Abschnitt 6.3.4.1) und andererseits diverse Konfigurationsmöglichkeiten (siehe Abschnitt 6.3.4.2).

Sicherheitshinweis: Sollte Ihnen eine Unregelmäßigkeit am Kartenterminal auffallen, so ist die Unversehrtheit des Gehäuses zu überprüfen.

Hinweis: Bei Frage- oder Problemstellungen in Verbindung mit Kartenterminals lesen Sie bitte auch die Bedienungsanleitung(en) Ihrer eingesetzten Kartenterminals.

6.3.4.1 Kartenterminals - Status

Der Reiter "Status" gibt eine Übersicht über alle durch den RISE Konnektor verwalteten Kartenterminals (siehe Abbildung 112).

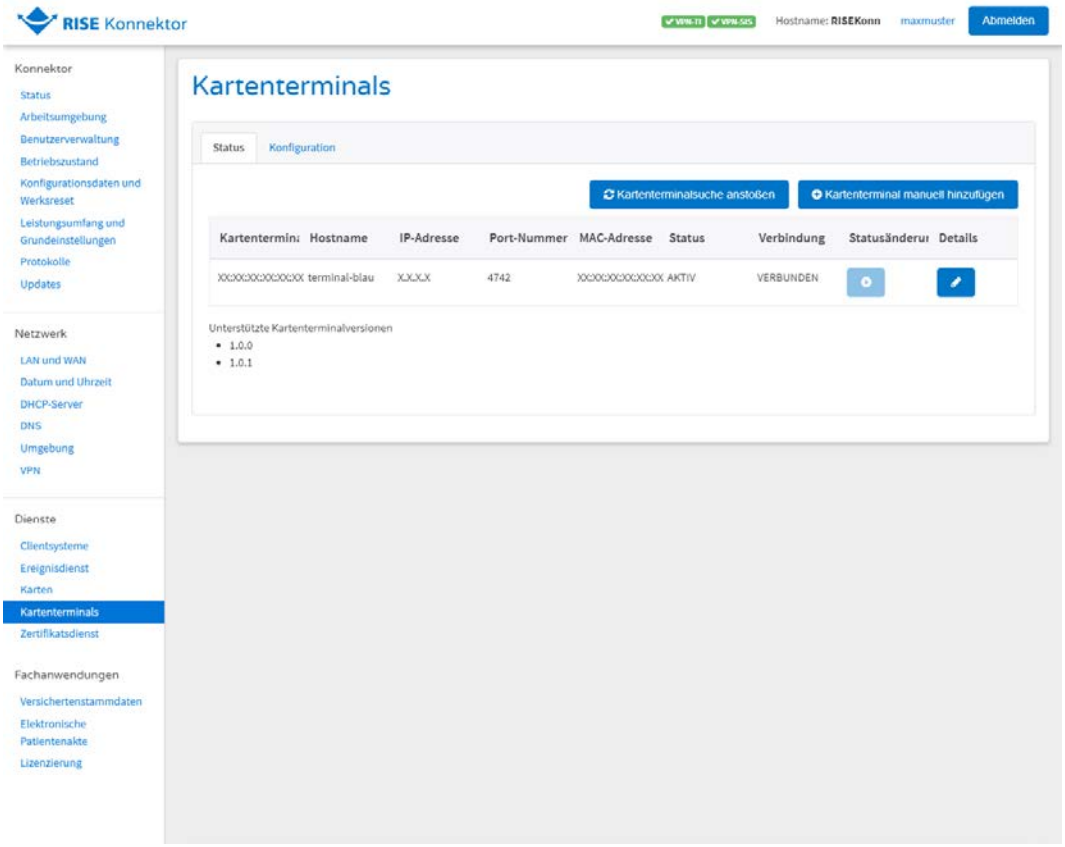


Abbildung 112: Übersicht über verwaltete Kartenterminals

ReferenzID	Belegung	Bedeutung
Verwaltete Kartenterminals (CTM_CT_LIST)	Liste von Kartenterminal-Objekten	Eine Liste von der dem RISE Konnektor bekannten Kartenterminals.

Tabelle 46: Übersicht über verwaltete Kartenterminals

Durch das Auswählen von "Kartenterminalsuche anstoßen" kann unabhängig von den Einstellungen der automatischen Suche eine Aktualisierung der Liste durchgeführt werden.

Hinweis: Wenn Sie den RISE Konnektor LAN-seitig als DHCP-Client betreiben und trotz korrekt zugewiesener IP-Konfiguration die Kartenterminalsuche erfolglos ist, führen Sie bitte erneut eine manuelle Aktualisierung der DHCP-Konfiguration durch (siehe Abschnitt 6.2.1.3, Funktion "DHCP-Konfiguration erneut beziehen").

Durch Auswahl von "Kartenterminal manuell hinzufügen" kann ein neues Kartenterminal hinzugefügt werden. Dabei müssen die Eigenschaften des Terminals manuell eingegeben werden (siehe Abbildung 113).

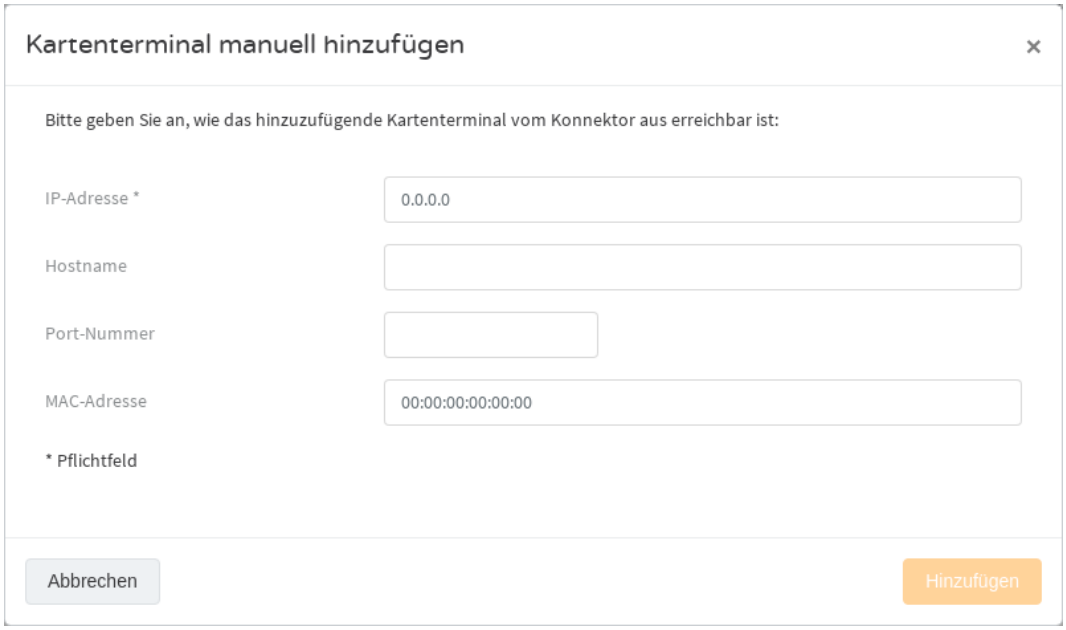


Abbildung 113: Kartenterminal manuell hinzufügen

Zu jedem Kartenterminal können Details, Statusinformationen und Eigenschaften (Stift-Symbol) angezeigt werden, die in Abbildung 114 veranschaulicht sind (siehe Abschnitt 6.3.4.1.3).

6.3.4.1.1 Pairing / Inbetriebnahme von Kartenterminals

Das initiale Pairing zwischen einem Kartenterminal und dem RISE Konnektor besteht aus zwei Schritten:

Schritt 1, Einbringen des Kartenterminals im dezentralen Netzwerk: Der Administrator prüft die Unversehrtheit und Authentizität des Kartenterminals, bevor dieses mit einem LAN-Kabel mit dem Netzwerk verbunden wird. Eine Beschreibung hierzu entnehmen Sie bitte dem Handbuch Ihres Kartenterminals. Der Terminalname und/oder die MAC-Adresse des Kartenterminals sowie der Fingerprint einer noch nicht zugeordneten gSMC-KT werden zur Überprüfung vom Administrator notiert, bevor dieser die gSMC-KT in das Kartenterminal einbringt.

Schritt 2, Inbetriebnahme eines Kartenterminals am RISE Konnektor: In der Kartenterminalverwaltung (siehe Abbildung 112) scheint das neue Kartenterminal (erkennbar anhand der Kartenterminal-ID, d.h. der MAC-Adresse) automatisch auf.

(Sollte dies nicht der Fall sein, kann es mittels “Kartenterminalsuche anstoßen” bzw. “Kartenterminal manuell hinzufügen” hinzugefügt werden.) Der Status des neu eingebrachten Kartenterminals ist “BEKANNT”. Mittels Plus-Symbol kann das Kartenterminal dem Konnektor zugewiesen werden und befindet sich dann im Status “ZUGEWIESEN”. Anschließend kann es durch Klick auf das Kette-Symbol gepaired werden. Der RISE Konnektor baut danach eine TLS-Verbindung zum Kartenterminal auf und erhält das Komponentenzertifikat der gSMC-KT. Ist das Zertifikat gültig, wird dem Administrator der Fingerprint des Zertifikates angezeigt. Im Fehlerfall bricht der RISE Konnektor den Verbindungsaufbau ab. Stimmt der Fingerprint mit jenem aus Schritt 1 überein, bestätigt dies der Administrator, wodurch ein Austausch eines Shared Secret erfolgt. Das Terminal zeigt eine Displaymeldung an, welche abhängig vom jeweiligen Kartenterminal-Typ ist. Diese muss innerhalb von kurzer Zeit entsprechend der herstellerabhängigen Anweisung am Kartenterminal bestätigt werden, ansonsten wird der Pairing-Vorgang abgebrochen. Nach Bestätigung prüft der RISE Konnektor die Antwort des Kartenterminals und speichert Identifikationsmerkmal, Kartenterminalzertifikat und Shared Secret ab. Die Inbetriebnahme des Kartenterminals ist hiermit abgeschlossen.

Hinweis: Kartenterminals können im Regelfall nur eine begrenzte Anzahl an Pairing-Informationen speichern. Falls ein etwaiges Pairing mit anderen Geräten nicht ordnungsgemäß aufgehoben wurde (z.B. nur durch Abstecken), können unter Umständen noch Pairing-Informationen zu diesen Geräten im internen Speicher des Kartenterminals vorliegen. Falls ein Pairing mit dem RISE Konnektor durch einen derartigen Fehler verhindert wird, wird ein entsprechender Fehler in der Administrationsoberfläche ausgegeben: “Fehlercode 4041, Fehler im Pairing, SICCT-Fehler: 6900”. Setzen Sie infolge dieser Fehlermeldung den internen Speicher Ihres Kartenterminals (im Regelfall “Pairing-Cache”) gemäß der Bedienungsanleitung Ihres Kartenterminals zurück. Wiederholen Sie anschließend das Pairing mit dem RISE Konnektor.

6.3.4.1.2 Kartenterminals – Statusänderung

Pro Kartenterminal gibt es die Möglichkeit, Statusänderungen durchzuführen. Abhängig davon, in welchem Status sich das Kartenterminal derzeit befindet, sind unterschiedliche Aktionen möglich:

- Befindet sich das Kartenterminal im Zustand “BEKANNT”, dann besteht mit dem “Plus”-Symbol die Möglichkeit, das Kartenterminal dem Konnektor zuzuweisen.
- Befindet sich das Kartenterminal im Zustand “ZUGEWIESEN”, dann besteht mit dem “Kette”-Symbol die Möglichkeit, das Kartenterminal mit dem Konnektor zu pairen. Mehr Informationen zum Pairing ist in Abschnitt 6.3.4.1.1 zu finden.
- Befindet sich das Kartenterminal im Zustand “GEPAIRED”, besteht mit dem “Play”-Symbol die Möglichkeit, eine TLS-gesicherte Verbindung zum Kartenterminal aufzubauen und somit in den Status “AKTIV” zu wechseln.

Sicherheitshinweis: Sobald ein Kartenterminal in den Status "AKTIV" wechselt, muss das Kartenterminal regelmäßig auf Auffälligkeiten (gebrochene Siegel, etc.) überprüft werden, um jederzeit mögliche Manipulationsversuche zu erkennen.

Sicherheitshinweis: Ein nicht vertrauenswürdiges/unerwünschtes Kartenterminal muss nach erfolgter Aufhebung des Pairings aus der Liste der Kartenterminals entfernt werden. Dies ist in der Detailansicht des Kartenterminals möglich, siehe Abschnitt 6.3.4.1.3.

Hinweis: Es kann bis zu 30 Sekunden dauern, bis das Pairing tatsächlich abgeschlossen wurde und erste Abfragen getätigt werden können.

6.3.4.1.3 Kartenterminal – Details

Zu jedem bekannten Kartenterminal können im Reiter "Kartenterminal" verschiedene Details eingesehen werden (siehe Abbildung 114):

- Statusinformationen
- Produktinformationen
- Benutzerinformationen

Im Reiter "Einstellungen" können Konfigurationen (IP-Adresse, Port, Passwort, etc.) vorgenommen werden (siehe Abbildung 115).

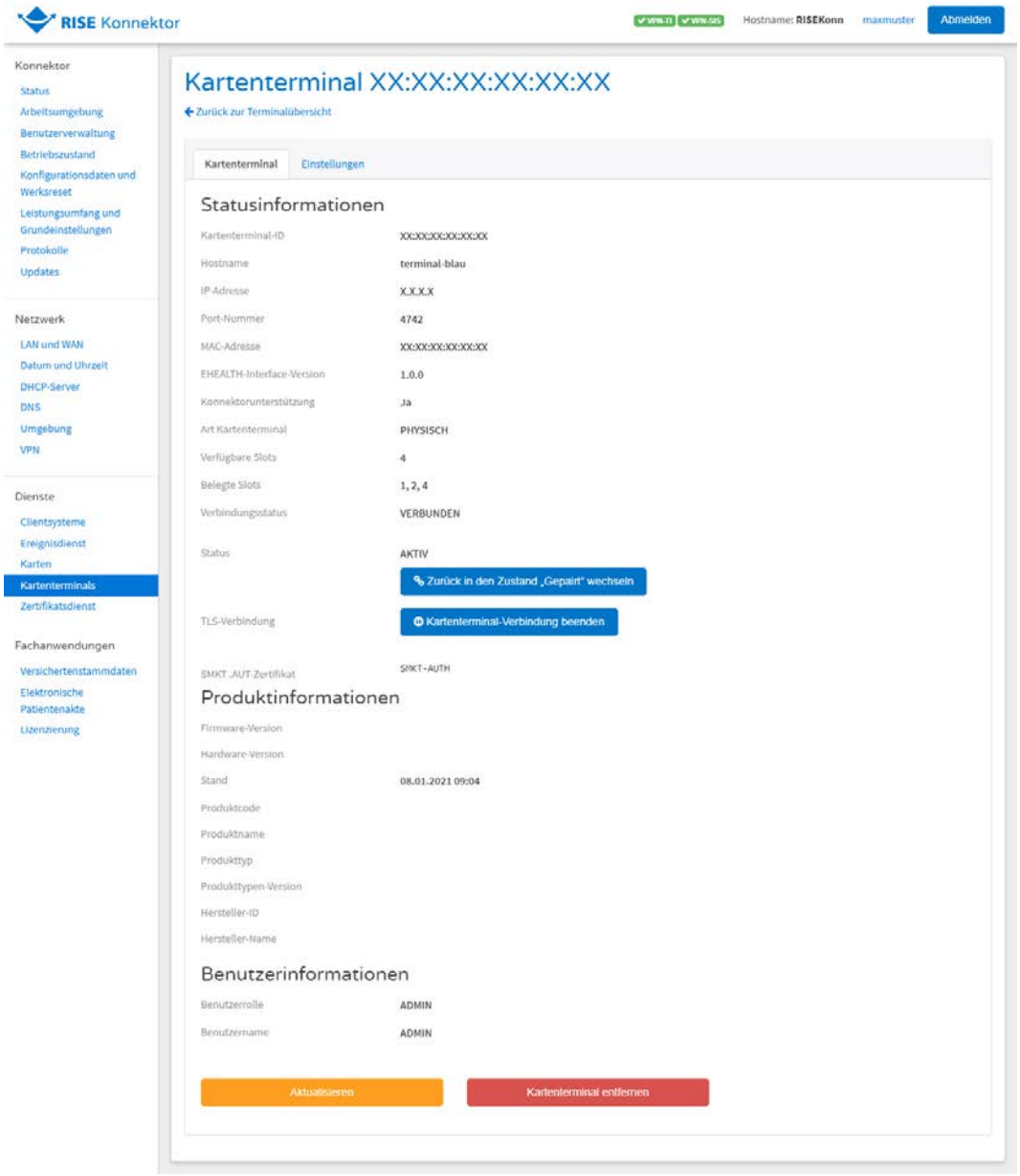


Abbildung 114: Statusinformationen des Kartenterminals

Im Bereich "Statusinformationen" – "Status" befindet sich wieder (abhängig vom Status, in dem sich das Kartenterminal aktuell befindet) ein Button für die Statusänderung analog zu Abschnitt 6.3.4.1.2 ("Plus"-Symbol mit "Kartenterminal zuweisen", "Ketten"-Symbol mit "Pairen" und "Play"-Symbol mit "Kartenterminal verbinden"). Im Unterschied zur Kartenterminal-Übersicht (Abbildung 112) ist es in der Detail-Ansicht auch möglich in vorherige Zustände zurück zu wechseln.
Abhängig vom aktuellen Status gibt es folgende Möglichkeiten:

- Wenn eine TLS-Verbindung zum Kartenterminal besteht: "Pause"-Symbol mit "Kartenterminal-Verbindung beenden" um TLS-Verbindung zum Kartenterminal zu beenden
- Wenn das Kartenterminal gepaired wurde: "getrennte Kette"-Symbol mit "Pairing aufheben" um das Pairing zum Kartenterminal wieder aufzuheben

- Wenn das Kartenterminal dem Konnektor zugewiesen ist: “Minus”-Symbol mit “Kartenterminal Zuweisung aufheben” um die Zuweisung des Kartenterminals zum Konnektor wieder aufzuheben. In Folge dessen befindet sich das Kartenterminal wieder im Zustand “BEKANNT”.

Des Weiteren besteht in dieser Detailansicht die Möglichkeit, das entsprechende Kartenterminal mittels des roten Buttons “Kartenterminal entfernen” aus der internen Liste der Kartenterminals und damit aus der Ansicht der Kartenterminals zu entfernen (siehe Abbildung 114).

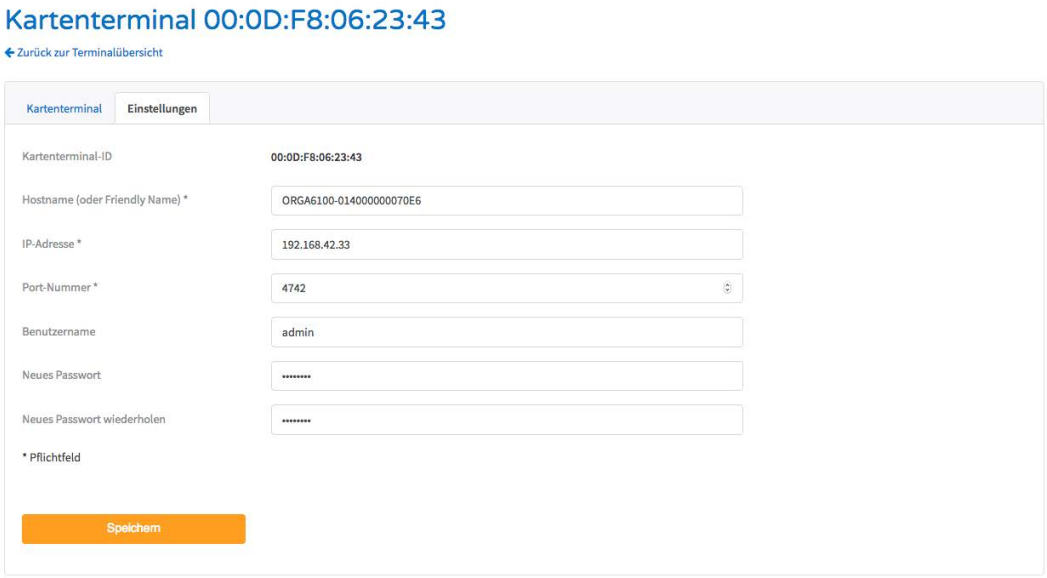


Abbildung 115: Einstellungen des Kartenterminals

Hinweis: Es wird empfohlen, Benutzername und Passwort des Kartenterminals sofort zu setzen.

6.3.4.2 Kartenterminals - Konfiguration

Einstellungen zu den Kartenterminals werden im Reiter “Konfiguration” vorgenommen (siehe Abbildung 116). Dort können neben der Anzahl an Keep-Alive-Versuchen und -Intervall bzw. TLS-Handshake Timeout auch Service Discovery Timeout, Zyklus und Port an dieser Stelle administriert werden. Kartenterminals, die für den Betrieb mit dem RISE Konnektor vorgesehen sind, müssen mit diesem gepaired werden, um eine sichere Kommunikation zwischen RISE Konnektor und Kartenterminal zu ermöglichen (siehe Abschnitt 6.3.4.1.1).

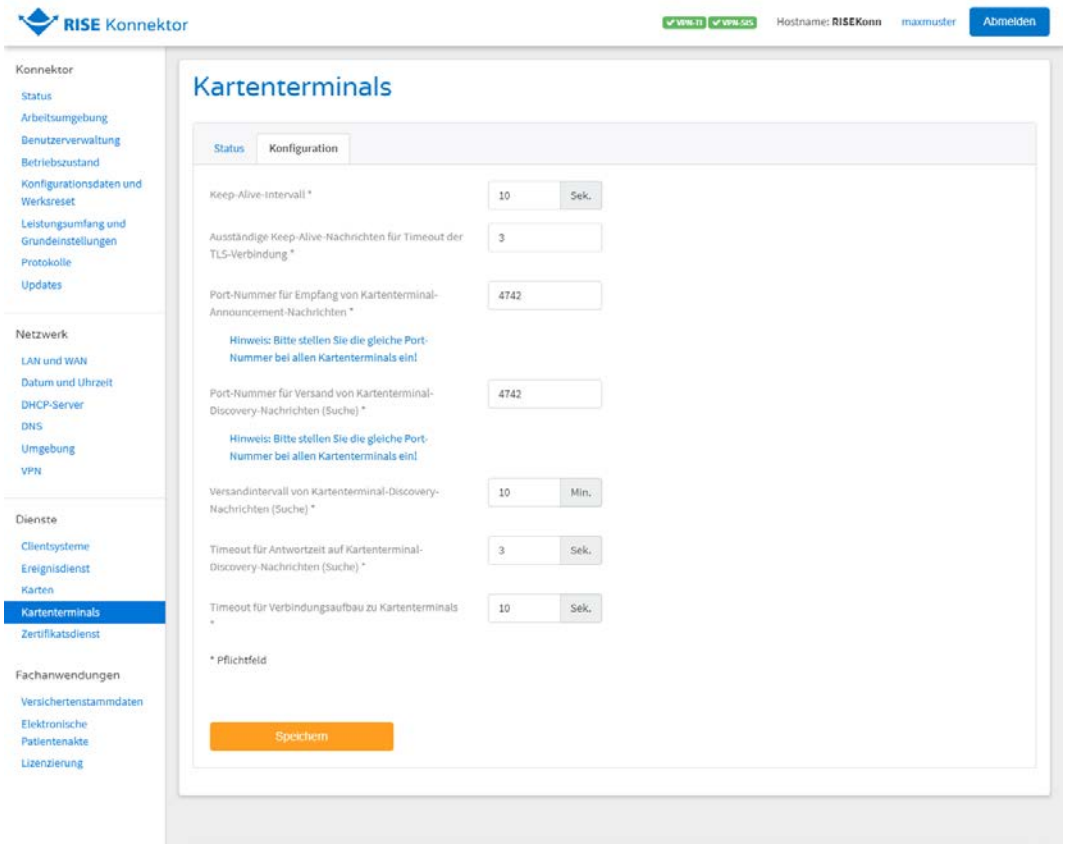


Abbildung 116: Konfiguration von Kartenterminals

ReferenzID	Belegung	Bedeutung
Keep-Alive-Interval (CTM_KEEP_ALIVE_INTERVAL)	X Sekunden; Standard-Wert: 10 Sek.	Intervall in Sekunden in dem Keep-Alive Nachrichten an das Kartenterminal gesendet werden. Der Administrator kann diesen Wert im vorgegebenen Bereich anpassen (1-10).
Ausständige Keep-Alive-Nachrichten für Timeout der TLS-Verbindung (CTM_KEEP_ALIVE_TRY_COUNT)	Anzahl der Versuche; Standard-Wert: 3	Anzahl der Versuche von aufeinander folgenden, nicht beantworteten Keep-Alive Nachrichten, nachdem ein Timeout der TLS-Verbindung festgestellt wird. Der Administrator kann diesen Wert im vorgegebenen Bereich (3-10) anpassen.
Port-Nummer für Empfang von	Portnummer;	Der Administrator kann

ReferenzID	Belegung	Bedeutung
Kartenterminal-Announcement-Nachrichten (CTM_SERVICE_DISCOVERY_PORT)	Standard-Wert: 4742	die Portnummer eingeben, auf der die Kartenterminals im lokalen Netz auf Dienstanfragen hören.
Port-Nummer für Versand von Kartenterminal-Discovery-Nachrichten (Suche) (CTM_SERVICE_DISCOVERY_PORT)	Portnummer; Standard-Wert: 4742	Der Administrator kann die Portnummer eingeben, auf der die Kartenterminals im lokalen Netz für den Versand von Kartenterminal-Discovery-Nachrichten hören.
Versandintervall von Kartenterminal-Discovery-Nachrichten (Suche) (CTM_SERVICE_DISCOVERY_CYCLE)	X Minuten; Standard-Wert: 10 Minuten	Der Administrator kann die Anzahl Minuten einstellen, in denen der Konnektor wiederholt Service Discovery Nachrichten absetzt. Der Wert 0 deaktiviert die Suche komplett.
Timeout für Antwortzeit auf Kartenterminal-Discovery-Nachrichten (Suche) (CTM_SERVICE_DISCOVERY_TIMEOUT)	X Sekunden; Standard-Wert: 3 Sek.	Der Administrator kann die Anzahl Sekunden eingeben, die der Konnektor auf Antworten zu Service-Discovery-Anfragen wartet.
Timeout für Verbindungsaufbau zu Kartenterminals (CTM_TLS_HS_TIMEOUT)	X Sekunden; Standard-Wert: 10 Sek.	Der Administrator kann die Anzahl Sekunden eingeben, die der Konnektor auf den TLS-Verbindungsaufbau zum Kartenterminal wartet (Handshake-Timeout). Der eingegebene Wert muss zwischen 1 und 60 liegen.

Tabelle 47: Konfigurationswerte der Kartenterminals

6.3.4.3 Fehlercodes

Im Rahmen der Verbindung des RISE Konnektors mit Kartenterminals können Fehlercodes wie in Tabelle 48 dargestellt auftreten.

Fehlercode	Fehlertyp	Severity	Fehlertext
4028	Technical	Error	Fehler beim Versuch eines Verbindungsaufbaus zum Kartenterminal.
4029	Security	Error	Fehler bei der Kartenterminal-Authentisierung. Prüfen Sie die Kartenterminal-Konfiguration, insb. die TSL.
4030	Security	Error	Admin-Werte für Kartenterminal fehlerhaft.
4032	Technical	Error	Verbindung zu HSM konnte nicht aufgebaut werden.
4033	Technical	Error	Kartenterminal antwortet nicht, Hinzufügen fehlgeschlagen.
4034	Technical	Error	Es ist bereits ein Kartenterminal mit gleichem Hostname in der Liste der Kartenterminals vorhanden. Bitte Hostname des Kartenterminals ändern.
4035	Technical	Error	Die angegebene IP-Adresse gehört zu einer anderen MAC-Adresse als die, die übergeben wurde. Angaben zur MAC prüfen.
4036	Technical	Error	Die angegebene IP-Adresse gehört zu einem anderen Hostnamen als der, der übergeben wurde. Angaben zum Hostnamen prüfen.
4037	Technical	Error	Verwaltung der Kartenterminals inkonsistent.
4039	Technical	Error	Kartenterminal durch andere Nutzung aktuell belegt.
4040	Security	Error	Fehler beim Versuch eines Verbindungsaufbaus zum Kartenterminal.
4042	Technical	Error	Die Version des Kartenterminals wird nicht unterstützt.
4041	Technical	Error	Fehler im Pairing, SICCT-Fehler: <SICCT-Fehler>
4044	Technical	Error	Fehler beim Zugriff auf das Kartenterminal.

Tabelle 48: Fehlercodes im Zusammenhang mit Kartenterminals

6.3.5 Zertifikatsdienst

Durch den Zertifikatsdienst besteht die Möglichkeit, Zertifikate zu importieren und Downloadadressen für den CRL-Import einzustellen.

Hinweis: Der Administrator übernimmt die Verantwortung für die Verlässlichkeit der importierten Zertifikate. Die Auswahl der zu importierenden Zertifikate wird von der

gematik unterstützt, indem diese Informationen über CA-Betreiber veröffentlicht, die den Sicherheitsanforderungen der gematik entsprechen.

6.3.5.1 Zertifikatsdienst Status

Der Reiter “Status” des Zertifikatsdienstes in Abbildung 117 zeigt die CRL Downloadadressen, den TSL Vertrauensraumstatus und den Status der Bundesnetzagentur-Vertrauensliste (BNetzA-VL). Des Weiteren besteht die Möglichkeit, das Ablaufdatum von Zertifikaten zu ermitteln und OCSP Tests durchzuführen.

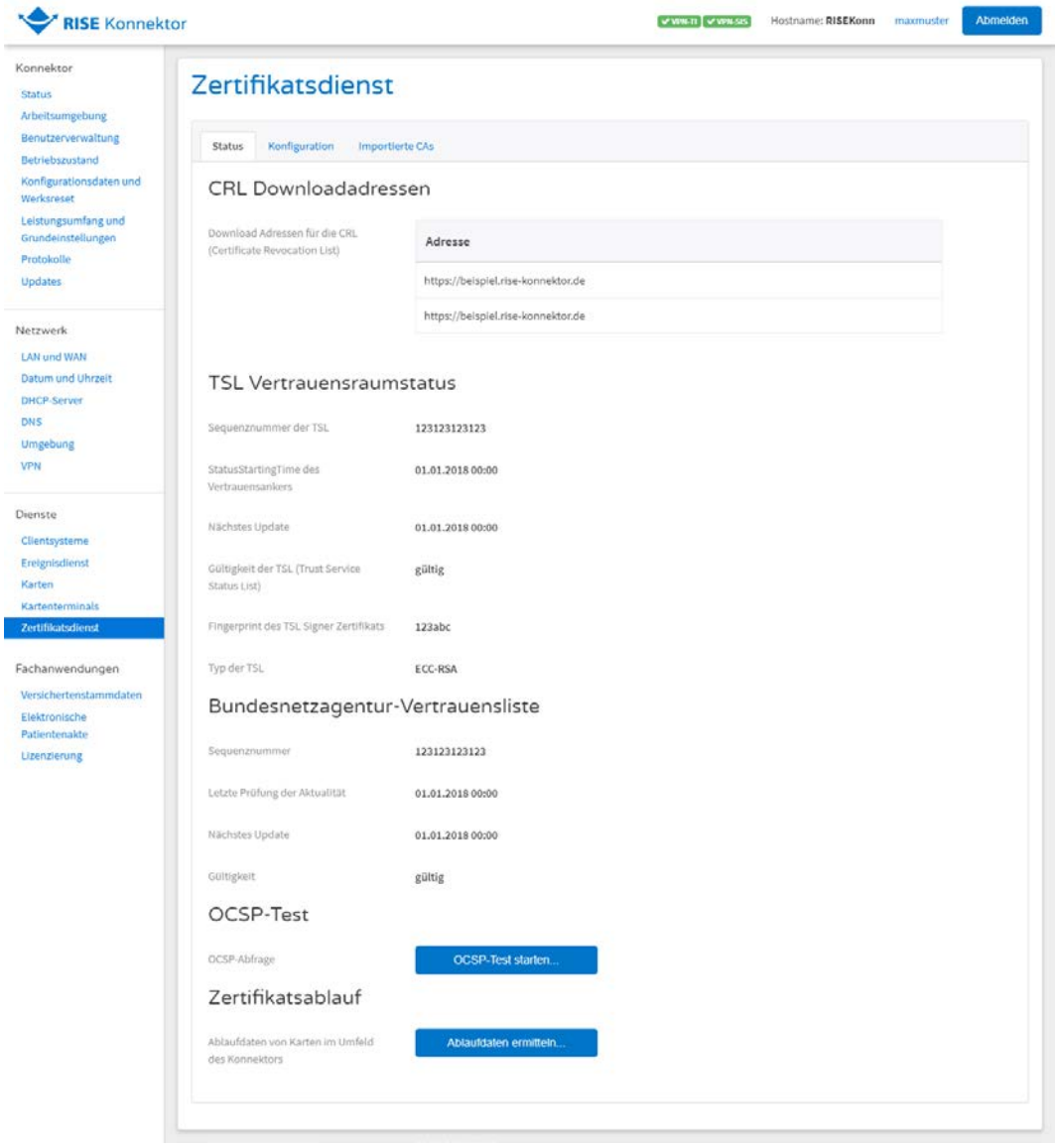


Abbildung 117: Zertifikatsdienst – Status

ReferenzID	Belegung	Bedeutung
Download-Adressen für die CRL (CERT_CRL_DOWNLOAD_ADDRESS)	2 URIs	Download-Adressen für die CRL; werden automatisch aus der TSL

ReferenzID	Belegung	Bedeutung
		ausgelesen.
Sequenznummer der TSL	Nummer	Eindeutige Nummer der TSL.
StatusStartingTime des Vertrauensankers	Datum	Startdatum des Gültigkeitszeitraums des aktuellen Vertrauensankers (TSL-Signer-CA-Zertifkates).
Nächstes Update	Datum	Datum, an dem das nächste TSL-Update durchgeführt wird.
Gültigkeit der TSL	gültig/ungültig	Es wird angezeigt, ob die TSL aktuell gültig oder ungültig ist.
Fingerprint des TSL Signer Zertifikats	Fingerprint	Fingerprint der TSL.
Sequenznummer	Nummer	Eindeutige Nummer der BNetzA-VL.
Letzte Prüfung der Aktualität	Datum	Zeitpunkt der letzten Prüfung der Aktualität der BNetzA-VL.
Nächstes Update	Datum	Zeitpunkt der nächsten Aktualisierung der BNetzA-VL.
Gültigkeit	gültig/ungültig	Gültigkeitsstatus der BNetzA-VL.
TSL-Typ	keine TSL vorhanden / ECC-RSA / RSA	Art des Vertrauensraums der etabliert ist

Tabelle 49: Zertifikatsdienst - Status

6.3.5.1.1 OCSP Abfrage - OCSP Test starten

Abbildung 118: Zertifikatsdienst – OCSP Test Ergebnis

Mit Klick auf den Button "OCSP Test starten…" kann der Administrator überprüfen ob, ein in der TSL enthaltener OCSP Server erreichbar ist. Das Ergebnis eines erfolgreichen OCSP Tests ist in Abbildung 118 ersichtlich.

6.3.5.1.2 Ablaufdaten ermitteln

Die Ablaufdaten von Karten im Umfeld des Konnektors können ermittelt werden (siehe Abbildung 119). Wird das Zertifikat demnächst ablaufen, wird ein Warnungs-Symbol angezeigt. Wie viele Tage vor dem Zertifikatsablauf es zu einer Warnung kommt, kann im Reiter "Konfiguration" definiert werden (siehe Abschnitt 6.3.5.2).

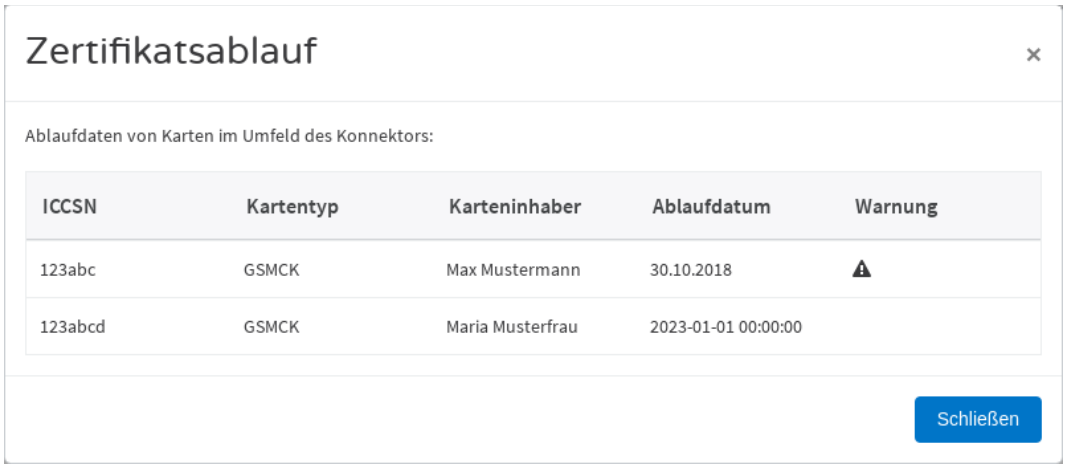


Abbildung 119: Zertifikatsdienst – Zertifikatsablauf

6.3.5.2 Zertifikatsdienst Konfiguration

Abbildung 120 zeigt die Benutzermaske zur Konfiguration des Zertifikatsdienstes, mit dem CRL- und TSL-Zertifikate und die BNetzA-Vl manuell importiert werden können. Wie viele Tage vor Ablauf eines Zertifikates eine Warnung erscheint kann ebenso konfiguriert werden wie die Grace Periods für TSL und OCSP. Für Letzteres kann des Weiteren ein Forwarder Port und eine Timeout Zeit definiert werden.

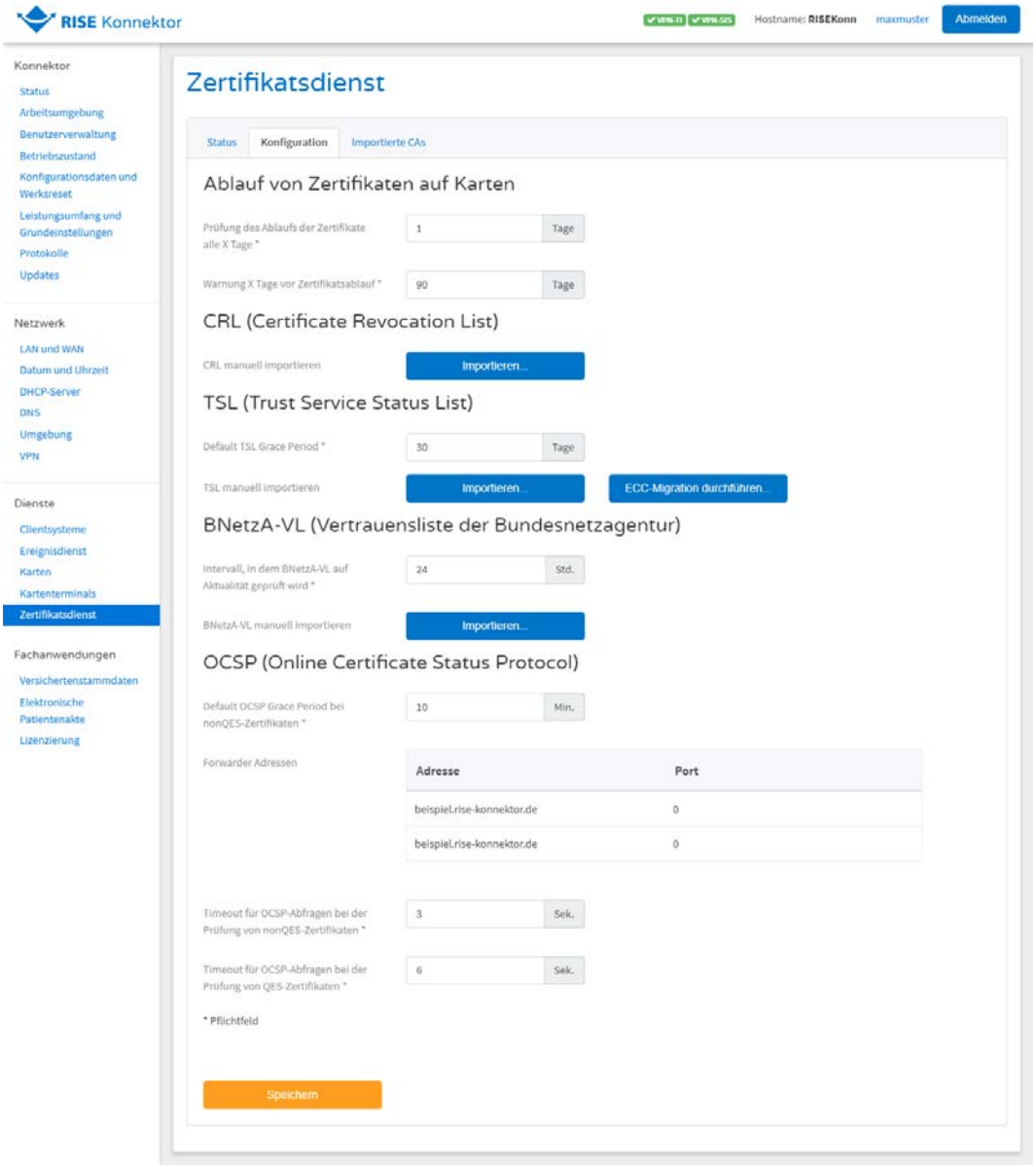


Abbildung 120: Zertifikatsdienst - Konfiguration

ReferenzID	Belegung	Bedeutung
Prüfung des Ablaufs der Zertifikate alle X Tage (CERT_EXPIRATION_CARD_CHECK_DAYS)	X Tag(e); Standard-Wert: 1	Alle X Tage wird der Ablauf aller gesteckten Karten überprüft. Der Wert muss zwischen 0

ReferenzID	Belegung	Bedeutung
		und 365 liegen (0=kein Check).
Warnung X Tage vor Zertifikatsablauf (CERT_EXPIRATION_WARN_DAYS)	X Tag(e); Standard-Wert: 90 Tage	Warnung X Tage vor Ablauf von Zertifikaten in der Management-Oberfläche und per Ereignis. Der Wert muss zwischen 0 und 180 Tagen (0=keine Warnung) liegen.
Default TLS Grace Period (CERT_TSL_DEFAULT_GRACE_PERIOD_DAYS)	X Tage; Standard-Wert: 30 Tage	Default Grace Period TSL in Tagen gibt an, wie viele Tage der Konnektor mit einer zeitlich abgelaufenen TSL weiter betrieben werden kann. Der Wert MUSS zwischen 1 und 30 Tagen liegen.
Intervall, in dem BNetzA-VL auf Aktualität geprüft wird (CERT_BNETZA_VL_UPDATE_INTERVAL)	X Stunden; Standard-Wert: 24 Stunden	Intervall, in dem die BNetzA-VL auf Aktualität geprüft werden muss. Der Wert muss zwischen 1 und 168 Stunden (= 7 Tage) liegen.
Default OCSP Grace Period bei non-QES-Zertifikaten (CERT_OCSP_DEFAULT_GRACE_PERIOD_NONQES)	X Minuten; Standard-Wert: 10 Minuten	Die Default Grace Period OCSP für nonQES Zertifikate in Minuten ist jene Zeit, die OSCP-Antworten zwischengespeichert werden. Der Wert muss zwischen 0 und 20 Minuten liegen.
Forwarder Adressen (CERT_OCSP_FORWARDER_ADDRESS)	2 FQDNs	Adressen der OCSP-Forwarder (HTTPS-Proxy) beim Zugangsdienstprovider. Der Administrator kann einen Test auslösen, ob einer der Server per ICMP-Echo (ping) erreichbar ist (siehe Abbildung 77) und ob

ReferenzID	Belegung	Bedeutung
		ein (beliebiger) OCSP-Request zu einer erhaltenen OCSP-Antwort führt (siehe Abbildung 117).
Forwarder Port (CERT_OCSP_FORWARDER_PORT)	TCP-Port	TCP-Port des OCSP-Forwarders (HTTPS-Proxy) beim Zugangsdienstprovider
Timeout für OCSP Abfragen bei Prüfung von non-QES-Zertifikaten (CERT_OCSP_TIMEOUT_NONQES)	X Sekunden; Standard-Wert: 10 Sekunden	Timeout für OCSP-Abfragen bei der Prüfung von non-QES-Zertifikaten. Der Wert muss zwischen 1 und 120 Sekunden liegen.
Timeout für OCSP Abfragen bei Prüfung von QES-Zertifikaten (CERT_OCSP_TIMEOUT_QES)	X Sekunden; Standard-Wert: 10 Sekunden	Timeout für OCSP-Abfragen bei der Prüfung von QES-Zertifikaten. Der Wert muss zwischen 1 und 120 Sekunden liegen.

Konfigurationsparameter Zertifikatsdienst - Konfiguration

Um auch ECC (Elliptic Curve Cryptography)-Zertifikate prüfen zu können, kann durch Klick auf den Button "ECC-Migration durchführen…" manuell von Vertrauensraum (RSA) zu Vertrauensraum (ECC-RSA) gewechselt werden. Dafür benötigt wird

- ein TSL-Signer-CA-Zertifikat (Vertrauensanker)
- ein TSL-Signer-CA Cross-Zertifikat (für den Vertrauensraum-Wechsel von RSA nach ECC-RSA)
- eine ECC-TSL

Abbildung 121 zeigt die Maske zum Hochladen dieser Dateien. Anschließend werden diese Dateien geprüft und der Wechsel vollzogen. Kann dieser Vorgang nicht erfolgreich abgeschlossen werden, so antwortet der Konnektor mit dem Fehler 4255 (siehe Tabelle 51). Der Konnektor befindet sich nach erfolgreicher Migration im ECC-Vertrauensraum, in dem sowohl RSA- als auch ECC-Zertifikate überprüft werden können. Nachdem diese Migration einmal durchgeführt wurde, befindet sich der Konnektor permanent im ECC-Vertrauensraum.

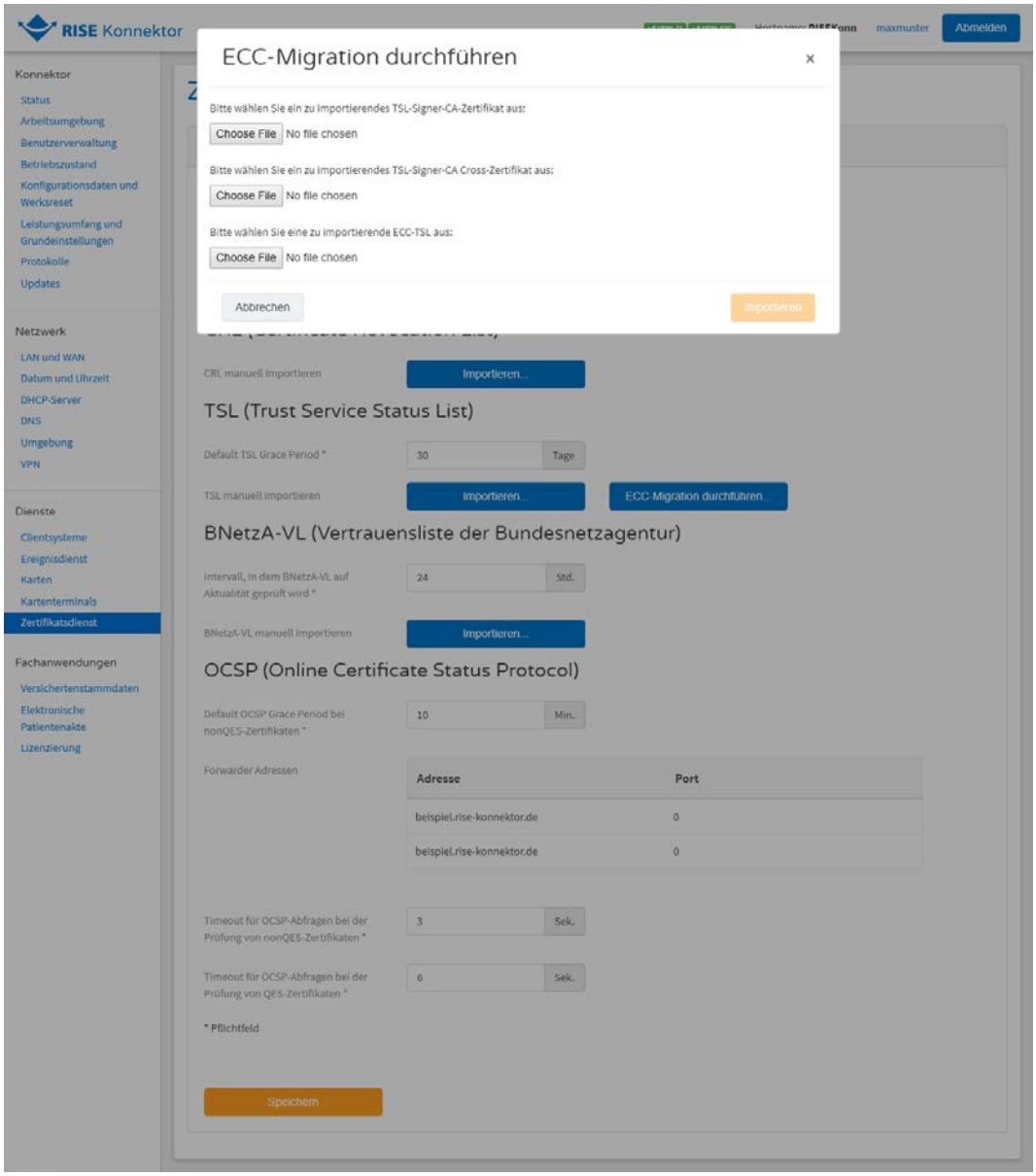


Abbildung 121: Zertifikatsdienst - ECC-Migration

Kommt es bei einem Vertrauensraumwechsel zu einem Fehler und in weiterer Folge zu einem inkonsistenten Systemzustand, in dem keine zuverlässigen Zertifikatsprüfungen mehr möglich sind, so wird der Konnektor in den abgesicherten Modus versetzt (siehe Abschnitt 4.7.4). Dieser Zustand kann durch einen Neustart des Konnektors behoben werden, dabei prüft der Konnektor während des Boot-Prozesses, ob ein unvollständiger Vertrauensraumwechsel vorliegt und setzt diesen gegebenenfalls fort.

6.3.5.3 Zertifikatsdienst Importierte CAs - CA hinzufügen

Die importierten CAs können im gleichnamigen Punkt des Zertifikatsdienstes eingesehen und weitere hinzugefügt werden, wie in Abbildung 122 dargestellt.

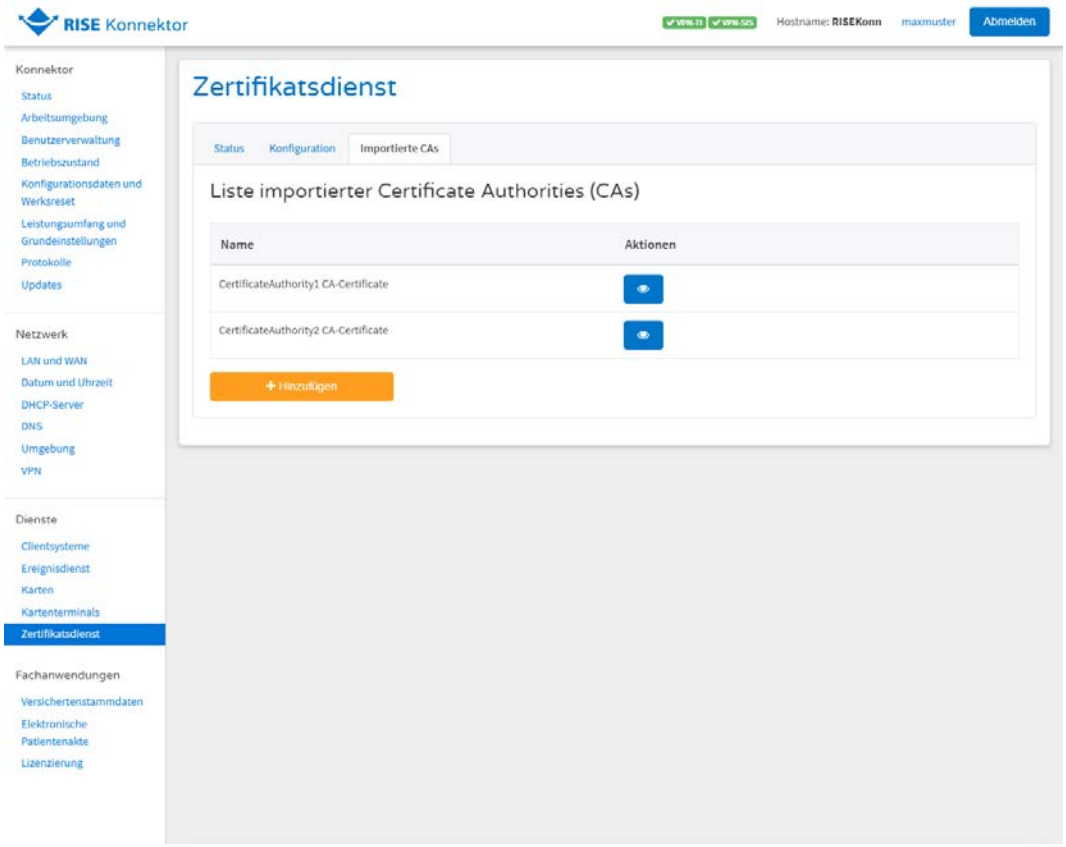


Abbildung 122: Zertifikate – Importierte CAs

Durch die Auswahl des Menüs “Hinzufügen” können Sie Zertifikate importieren.

Beim Starten des Zertifikatsdienstes wird automatisch eine interne Bereinigung der bestehenden Liste importierter CAs (siehe Tabelle 50) durchgeführt. Hierbei werden etwaig vorhandene QES-Zertifikate entfernt, da CA-Zertifikate zur Ableitung von QES-Zertifikaten nicht importiert werden können.

Sicherheitswarnung: Der Administrator übernimmt die Verantwortung für die Verlässlichkeit der importierten CA-Zertifikate. Der Administrator kann sich bei seiner Entscheidung für einen Import von CA-Zertifikaten auf die Informationen der gematik stützen. Die gematik veröffentlicht dazu Informationen über CA-Betreiber, welche die Erfüllung der Sicherheitsanforderungen der gematik nachgewiesen haben.

Abbildung 123: Zertifikate – Importierte CAs – Zertifikat anzeigen/löschen

ReferenzID	Belegung	Bedeutung
Liste importierter CAs (CERT_IMPORTED_CA_LIST)	Liste von manuell importierten Zertifikaten; Standard-Wert: leere Liste	Der Administrator kann Zertifikate importieren, anzeigen und löschen.

Tabelle 50: Konfigurationsparameter Zertifikatsdienst – Importierte CAs

6.3.5.4 Fehlercodes

Die in Tabelle 51 ersichtlichen Fehlercodes können im Rahmen des Zertifikatsdienstes auftreten.

Fehler-code	Fehlertyp	Severity	Fehlertext
1028	Technical	Warning	Die OCSP-Prüfung konnte nicht durchgeführt werden (1). TOLERATE_OCSP_FAILURE=true
1029	Technical	Error	Die OCSP-Prüfung konnte nicht durchgeführt werden (2). TOLERATE_OCSP_FAILURE=false
1001	Technical	Error	Es liegt keine gültige TSL vor.
1002	Technical	Error	Zertifikate lassen sich nicht extrahieren.
1003	Security	Error	Mehr als ein markierter V-Anker gefunden.

Fehler-code	Fehlertyp	Severity	Fehlertext
1004	Technical	Error	TSL-Signer-CA lässt sich nicht extrahieren.
1005	Technical	Error	Element "PointersToOtherTSL" nicht vorhanden.
1006	Technical	Error	TSL-Downloadadressen wiederholt nicht erreichbar.
1007	Security	Error	Vergleich der ID und SequenceNumber entspricht nicht der Vergleichsvariante 6a.
1008	Security	Warning	Die TSL ist nicht mehr aktuell.
1009	Security	Warning	Überschreitung des Elements NextUpdate um TSL-Grace-Period.
1011	Technical	Error	TSL-Datei nicht wellformed.
1012	Technical	Error	Schemata der TSL-Datei nicht korrekt.
1013	Security	Error	Signatur ist nicht gültig.
1016	Security	Error	KeyUsage ist nicht vorhanden bzw. entspricht nicht der vorgesehenen KeyUsage.
1017	Security	Error	ExtendedKeyUsage entspricht nicht der vorgesehenen ExtendedKeyUsage.
1018	Security	Error	Zertifikatstyp-OID stimmt nicht überein.
1019	Technical	Error	Zertifikat nicht lesbar.
1021	Security	Error	Zertifikat ist zeitlich nicht gültig.
1023	Security	Error	AuthorityKeyIdentifier des End-Entity-Zertifikats von SubjectKeyIdentifier des Zertifikats unterschiedlich.
1024	Security	Error	Zertifikats-Signatur ist mathematisch nicht gültig.
1026	Technical	Error	Das Element "ServiceSupplyPoint" konnte nicht gefunden werden.
1027	Technical	Error	CA kann nicht in den TSL-Informationen ermittelt werden.
1030	Security	Error	OCSP-Zertifikat nicht in TSL-Informationen enthalten.
1031	Security	Error	Signatur der Response ist nicht gültig.

Fehler-code	Fehlertyp	Severity	Fehlertext
1032	Technical	Error	OCSP-Responder nicht verfügbar.
1033	Security	Error	Kein Element PolicyInformation vorhanden.
1036	Security	Error	Das Zertifikat ist ungültig. Es wurde nach der Sperrung der ausgebenden CA ausgestellt.
1039	Security	Warning	Warnung, dass Offline-Modus aktiviert ist und keine OCSP-Statusabfrage durchgeführt wurde.
1040	Security	Error	Bei der Onlinestatusprüfung ist ENFORCE_CERTHASH_CHECK auf "true" gesetzt, die OCSP-Response enthält jedoch keine certHash-Erweiterung.
1041	Security	Error	Der certHash in der OCSP-Response stimmt nicht mit dem certHash des vorliegenden Zertifikats überein.
1042	Technical	Error	Das TSL-Signer-Zertifikat kann nicht aus dem sicheren Speicher des Systems geladen werden.
1043	Technical	Error	CRL kann aus technischen Gründen nicht ausgewertet werden.
1044	Technical	Warning	Warnungen, dass zum angefragten Zertifikat keine Statusinformationen verfügbar sind.
1047	Security	Warning	Das Zertifikat wurde vor oder zum Referenzzeitpunkt widerrufen.
1048	Technical	Error	Es ist ein Fehler bei der Prüfung des QCStatements aufgetreten (z.B. nicht vorhanden, obwohl gefordert).
1050	Technical	Warning	Die einem TUC zur Zertifikatsprüfung beigefügte OCSP-Response zu dem zu prüfenden Zertifikat kann nicht erfolgreich gegen das Zertifikat validiert werden.
1051	Security	Error	Die in einem OCSP-Response zurückgelieferte Nonce stimmt nicht mit den Nonce des OCSP-Requests überein.
1052	Security	Error	Attribut-Zertifikat kann dem übergebenen Basis-Zertifikat nicht zugeordnet werden.
1053	Technical	Error	Die CRL kann nicht heruntergeladen werden.
1054	Technical	Error	Eine verwendete CRL ist zum aktuellen Zeitpunkt nicht mehr gültig.

Fehler-code	Fehlertyp	Severity	Fehlertext
1055	Security	Error	CRL-Signer-Zertifikat nicht in TSL-Informationen enthalten.
1057	Security	Error	Signatur der CRL ist nicht gültig.
1058	Technical	Error	Die OCSP-Response enthält eine Exception-Meldung.
1059	Security	Error	Zertifikat für QES-Zertifikatsprüfung nicht qualifiziert.
1060	Technical	Error	Die VL kann nicht aktualisiert werden.
1061	Security	Error	CA (laut TSL) nicht autorisiert für die Herausgabe dieses Zertifikatstyps.
1062	Security	Error	Das QES-EE-Zertifikat ist ungültig. Es wurde nach der Sperrung der ausgebenden QES-CA ausgestellt.
4127	Security	Error	Import der TSL-Datei fehlgeschlagen
4128	Technical	Error	Der manuelle Import der TSL-Datei schlägt fehl
4129	Technical	Error	Der manuelle Import der BNetzA-Vertrauensliste schlägt fehl
4130	Security	Error	Signatur- oder Gültigkeitsprüfung der CRL fehlgeschlagen
4131	Technical	Error	Zum angegebenen CardHandle keine Karte gefunden.
4132	Security	Error	Extraktion des Ablaufsdatums fehlgeschlagen
4133	Security	Error	Import der BNetzA-Vertrauensliste fehlgeschlagen
4196	Technical	Error	Fehler bei der CV-Zertifikatsprüfung
4255	Security	Error	Fehler beim Import des TSL-Signer-CA Cross-Zertifikats
4260	Security	Error	Zertifikat nicht vorhanden in TSL

Tabelle 51: Fehlercodes des Zertifikatsdienstes

6.4 RISE Konnektor Fachanwendungen

Mit dem RISE Konnektor kann auch auf Fachanwendungen zugegriffen werden. Der RISE Konnektor ist so konzipiert, dass er Fachanwendungen als gesamte Module

unterstützt. Diese können je nach Firmwarestand variieren. Aktuell sind die folgenden Fachanwendungen verfügbar:

- Versichertenstammdaten-Dienst (VSD)
- Arzneimitteltherapiesicherheit (AMTS)
- Notfalldatenmanagement (NFDM)
- Elektronische Patientenakte (ePA)

Diese Anwendungen und das von ihnen verwendete einheitliche Protokollformat werden in den folgenden Kapiteln beschrieben.

6.4.1 Allgemeine Merkmale

Im Folgenden wird eine Übersicht über allgemeingültige Merkmale der Fachmodule gegeben.

6.4.1.1 Format der Protokolldateien

Details zum Herunterladen der Protokolle der Fachmodule befinden sich in Abschnitt 6.1.2.7.

Dieser Abschnitt beschreibt die Felder der Datensätze des Exports im JSON-Format. Die Daten werden als "Single-Line-JSON" ausgegeben. Durch das JSON Format ist eine automatisierte Auswertung möglich.

Tabelle 52 fasst die Felder zusammen, die mindestens pro JSON-Datensatz vorhanden sind.

Name	Beschreibung
corrid	Zeichenkette zur Korrelation zugehöriger Protokolleinträge
gematikSeverity	Siehe Abschnitt 4.7, "Schweregrad"
logtype	Siehe Abschnitt 4.7, "Typ"
msg	Log-Nachricht. Dieses Feld kann ebenfalls JSON-kodierte Datensätze enthalten.
timeReported	Zeitstempel der Meldung

Tabelle 52: Felder des JSON-Datensatzes der Systemprotokolldatei der Fachmodule

Hinweis: Der Datensatz kann auch mehr Felder enthalten. Diese müssen aber nicht immer vorhanden sein und sollten daher für eine automatische Auswertung nicht herangezogen werden.

6.4.2 Lizenzierung

Um die Fachmodule AMTS, NFDM und ePA nutzen zu können ist es notwendig, dass der Konnektor über gültige Lizenzen für diese verfügt. Dies wird beim Start eines der Fachmodule überprüft und nur wenn die Lizenz zum Startzeitpunkt gültig ist, startet das entsprechende Fachmodul vollständig und kann genutzt werden. Eine Lizenz ist dann gültig, wenn die Konnektor-Identität des Konnektors, auf dem die Fachmodule gestartet werden, in der Lizenz enthalten ist und der Startzeitpunkt im Gültigkeitszeitraum der Lizenz liegt. Abbildung 124 zeigt die Übersicht über die am Konnektor aktiven Lizenzen.

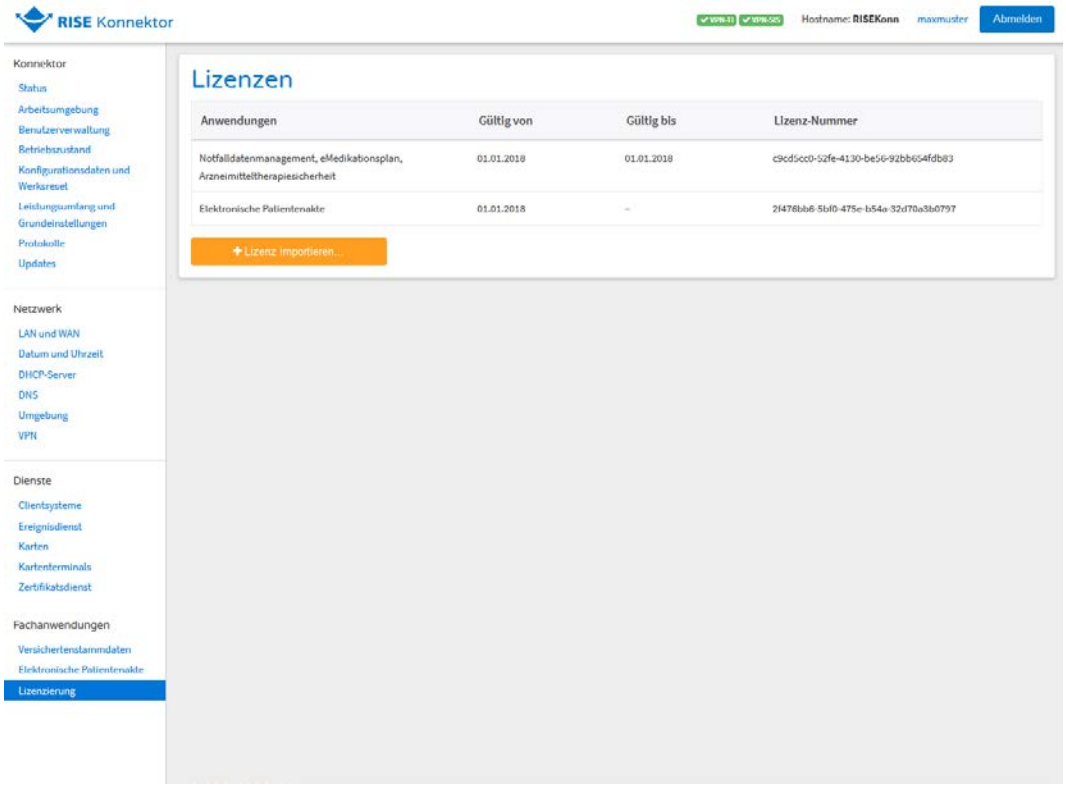


Abbildung 124: Aktive Lizenzen des Konnektors

Sie können als Leistungserbringer eine Lizenz für einen oder mehrere Konnektoren beim Vertriebspartner beantragen. Sie erhalten nach erfolgreicher Bearbeitung 2 Dateien, eine Lizenzdatei und eine Signaturdatei. Diese können durch einen Klick auf “Lizenz importieren…” auf den Konnektor importiert werden (siehe Abbildung Abbildung 125).

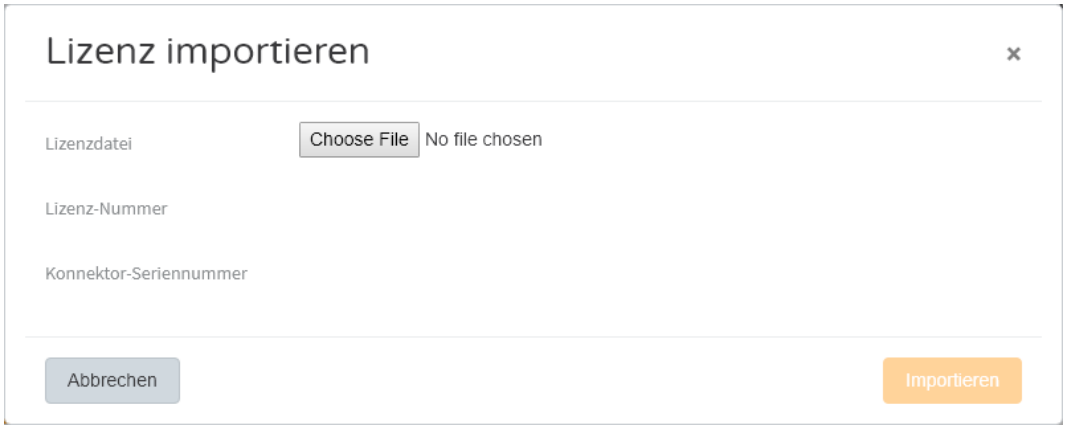


Abbildung 125: Dialog zum Hochladen einer Lizenzdatei

6.4.3 Versichertenstammdaten-Dienst (VSD)

Mit dem Versichertenstammdaten-Dienst (VSD) wird das sichere Auslesen von Gesundheitsdaten durch den RISE Konnektor unterstützt.

6.4.3.1 VSD-Konfiguration

Zur sicheren Kommunikation des Versichertenstammdaten-Dienst sind Konfigurationen vorzunehmen. Diese betreffen einerseits Einstellungen zur Auslesezeit und Aktualisierung der Versichertendaten, andererseits die Kommunikation des RISE Konnektors zu VSDM-Fachdiensten in der zentralen Telematikinfrastruktur.

Abbildung 126 zeigt die Benutzermaske und die Konfigurationsparameter des VSDM Fachmodules des RISE Konnektors. Die Einstellungen zum automatischen Aktualisieren von Gesundheitskarten sind nur dann ersichtlich, wenn das Kontrollkästchen "Online Aktualisierung gesteckter Gesundheitskarte automatisch starten" aktiviert ist.

Ein automatisches Aktualisieren gesteckter Gesundheitskarten bedeutet, dass das automatische Aktualisieren durchgeführt wird, als sei es von den in der Benutzeroberfläche eingestellten Mandanten, Clientsystem und Arbeitsplatz angestoßen worden.

Hinweis: Um das automatische Aktualisieren gesteckter Gesundheitskarten korrekt einstellen zu können, müssen unter dem Menüpunkt "Arbeitsumgebung" Informationen zum Mandanten, Clientsystem und Arbeitsplatz angegeben sein. Es muss zumindest je eine Angabe getroffen werden.

Hinweis: Wenn "AutoUpdate" aktiviert wird, muss immer auch der "Standalone-Betrieb" (siehe Abschnitt 6.1.8) analog dazu aktiv sein und umgekehrt, um dadurch einen spezifikationskonformen Einsatz zu gewährleisten.

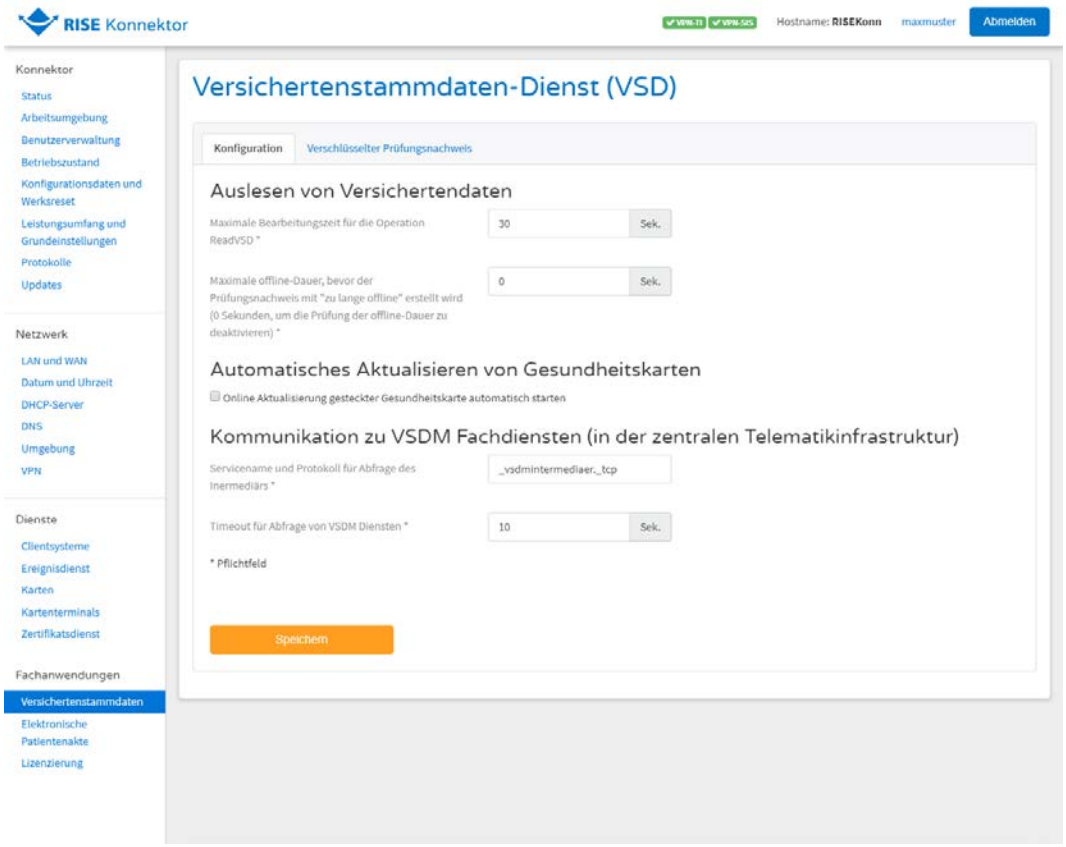


Abbildung 126: Konfiguration des Versichertenstammdaten-Dienst

Die Konfigurations-Parameter zum Versichertenstammdaten-Dienst sind in Tabelle 53 angeführt.

ReferenzID	Belegung	Bedeutung
Maximale Bearbeitungszeit für die Operation ReadVSD (MAXTIME_VSDM)	Sekunden; Standard-Wert: 30 Sek.	Der Wert gibt an, wie lange die Operation ReadVSD maximal dauern darf. Braucht die Anfrage länger als hier spezifiziert, kommt es zu einem Fehler.
Maximale Offline-Dauer bevor der Prüfungsnachweis mit "zu lange offline" erstellt wird (TIMEOUT_TI_OFFLINE)	Sekunden; Standard-Wert: keine Prüfung auf maximalen Offline-Zeitraum.	Maximaler Zeitraum, in der die Anbindung des Leistungserbringers an die Telematikinfrastruktur offline sein darf, bevor der Prüfungsnachweis mit dem Ergebnis "6" erstellt wird. Es ist auch möglich die Prüfung der Offline-Dauer auszuschalten: die Dauer wird dafür auf 0 Sekunden gesetzt. Die spezifischen Regelungen bezüglich des

ReferenzID	Belegung	Bedeutung
		maximalen Offline-Zeitraums müssen zwischen den Vertragspartnern vereinbart werden.
Online Aktualisierung gesteckter Gesundheitskarte automatisch starten (EGK_ALWAYS)	Boolean; Standard-Wert: False	Gibt an, ob beim Stecken einer eGK der Anwendungsfall "Automatische Onlineprüfung VSD" gestartet werden soll.
Servicename und Protokoll für Abfrage des Intermediärs (SRVNAME_INT_VSDM)	256 Zeichen; Standard-Wert: _vsdmintermediaer._tcp	Servicename und Protokoll für Abfrage der Resource Records des Intermediär beim DNS-SD.
Timeout für Abfrage von VSDM-Diensten (TIMEOUT_VSDM)	Sekunden; Standard-Wert: 10 Sek.	Timeout für VSDM-Dienste.

Tabelle 53: Versichertenstammdaten-Dienst – Parameter zur Konfiguration

6.4.3.2 VSD – Verschlüsselter Prüfungsnachweis

Der Prüfungsnachweis (PNW) dient der Abrechnung ärztlicher Leistungen. Der Leistungserbringer kann eine Onlineprüfung und Aktualisierung durchführen und Ergebnisse einsehen (siehe Abbildung 127). Prüfungsnachweise werden verschlüsselt auf Gesundheitskarten geschrieben und gelesen.

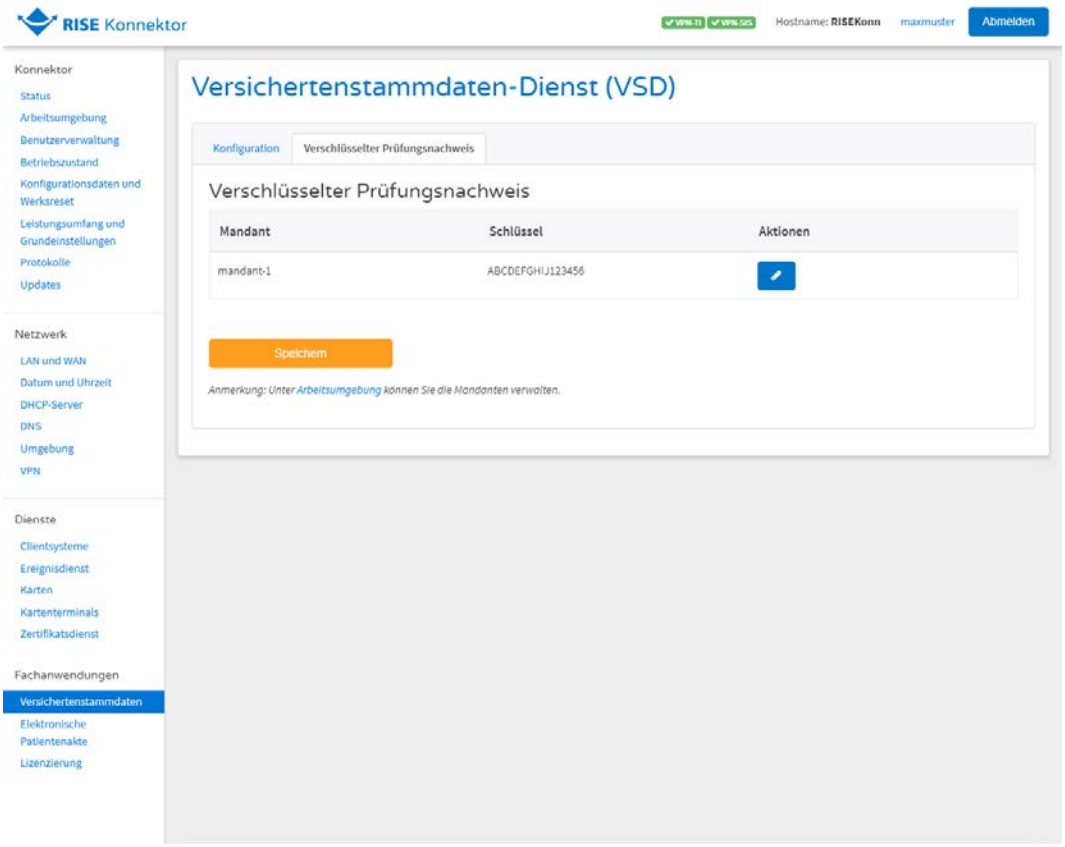


Abbildung 127: Verschlüsselter Prüfungsnachweis

Um den Schlüssel des Prüfungsnachweises (PNW-Key) zu ändern, klicken Sie auf das Aktionssymbol. Es erscheint eine Eingabemaske (siehe Abbildung 128).

Abbildung 128: Prüfungsnachweis Schlüssel bearbeiten

ReferenzID	Belegung	Bedeutung
Schlüssel (KEY_RECEIPT)	16 Zeichen	16 Zeichen lange Eingabe zur Generierung der Schlüssel für den Prüfungsnachweis
Mandant (MANDANT_SMB)	256 Zeichen	Gibt die Zuordnung zwischen einem Mandanten und einem SM-B. Um die Zuordnungen zwischen mehreren Mandanten und mehreren SM-B zu definieren, muss der

ReferenzID	Belegung	Bedeutung
		Parameter mehrere Male verwendet werden. Jedem Mandanten muss mindestens ein SM-B zugeordnet werden.

Tabelle 54: VSD - Parameter des verschlüsselten Prüfungsnachweises

Sicherheitshinweis: Der Administrator ist verpflichtet, unterschiedliche Zeichen zur Generierung des Schlüssels VSDM-PNW-Key zu verwenden, wenn mehrere Konnektor-Paare (Offline- und Online-Konnektor) administriert werden.

6.4.3.3 Fehlercodes

Die in Tabelle 55 ersichtlichen Fehlercodes können im Rahmen des Versichertenstammdaten-Dienstes auftreten.

Fehler-code	Fehlertyp	Severity	Fehlertext
3001	Technical	Error	VSD ungültig/nicht konsistent
3011	Technical	Error	Verarbeiten der Versichertendaten gescheitert
3020	Technical	Error	Lesen KVK gescheitert
3021	Technical	Error	KVK Prüfsumme falsch, Daten korrupt
3039	Technical	Error	Prüfungsnachweis nicht entschlüsselbar
3040	Technical	Error	Es ist kein Prüfungsnachweis auf der eGK vorhanden
3041	Technical	Error	SM-B nicht freigeschaltet
3042	Technical	Error	HBA nicht freigeschaltet

Tabelle 55: Versichertenstammdaten-Dienst – Fehlercodes

6.4.4 Arzneimitteltherapiesicherheit (AMTS)

Mit dem Fachmodul eMP/AMTS wird das sichere Auslesen und Schreiben des elektronischen Medikationsplans auf der Gesundheitskarte durch den RISE Konnektor unterstützt.

Sicherheitshinweis: Die Umgebung beim Leistungserbringer muss sicherstellen, dass nur spezifikationskonforme Zugriffe auf die Dienstschnittstellen des Fachmoduls erfolgen. Die Betriebsumgebung muss des Weiteren alle Forderungen des

Schutzprofils PP-0098,[13] Kapitel 3 erfüllen, u.a. den physischer Schutz und ein vertrauenswürdiges Clientsystem.

6.4.4.1 AMTS-Konfiguration

Für das Fachmodul AMTS ist keine separate Konfiguration notwendig. Im Zuge der Konfiguration der Protokollierung Abschnitt 6.1.2.8 können aber Einstellungen speziell für AMTS vorgenommen werden.

6.4.4.2 Fehlercodes

Die in Tabelle 56 ersichtlichen Fehlercodes können im Rahmen des Arzneimitteltherapiesicherheit-Fachmoduls auftreten.

Fehler-code	Fehlertyp	Severity	Fehlertext
6000	Technical	Fatal	Interner Fehler - Die Operation konnte nicht durchgeführt werden.
6010	Technical	Fatal	Einwilligung bereits vorhanden.
6049	Security	Error	Smartcard nicht freigeschaltet.
6051	Technical	Error	eGK-Generation 1 und 1+ nicht unterstützt.
6052	Security	Error	Verbindungsfehler zwischen Karten.
6054	Technical	Error	eMP/AMTS-Daten sind inkonsistent. Bitte Daten erneut schreiben.
6056	Technical	Error	Einverständnis nicht erteilt.
6057	Business	Error	Versicherten-ID von eGK und zu speichernden Daten unterscheiden sich.
6058	Technical	Error	eMP/AMTS-Daten konnten nicht validiert werden.
6059	Business	Error	Nicht genügend Speicherplatz auf der eGK.
6060	Technical	Error	Einwilligung konnte nicht validiert werden.
6061	Business	Error	Keine Einwilligung vorhanden.
6063	Security	Error	eGk gesperrt.

[13] BSI-CC-PP-0098, Schutzprofil 2: Anforderungen an den Konnektor, Version 1.5.4, Stand 17.03.2020

Fehler-code	Fehlertyp	Severity	Fehlertext
6064	Business	Error	Fachanwendungen verborgen.
6065	Business	Error	Löschung der eMP/AMTS-Daten nicht zugestimmt.
6068	Business	Error	Es sind keine eMP/AMTS-Daten auf der eGK gespeichert.

Tabelle 56: Arzneimitteltherapiesicherheit – Fehlercodes

6.4.5 Notfalldatenmanagement (NFDM)

Mit dem Fachmodul NFDM wird das sichere Auslesen, Schreiben und Löschen von Notfalldaten und persönlichen Erklärungen auf der Gesundheitskarte durch den RISE Konnektor unterstützt.

Sicherheitshinweis: Die Umgebung beim Leistungserbringer muss sicherstellen, dass nur spezifikationskonforme Zugriffe auf die Dienstschnittstellen des Fachmoduls erfolgen. Die Betriebsumgebung muss des Weiteren alle Forderungen des Schutzprofils PP-0098,[14] Kapitel 3 erfüllen, u.a. den physischer Schutz und ein vertrauenswürdiges Clientsystem.

6.4.5.1 NFDM-Konfiguration

Für das Fachmodul NFDM ist keine separate Konfiguration notwendig. Im Zuge der Konfiguration der Protokollierung Abschnitt 6.1.2.8 können aber Einstellungen speziell für NFDM vorgenommen werden.

6.4.5.2 Fehlercodes

Die in Tabelle 57 ersichtlichen Fehlercodes können im Rahmen des Notfalldatenmanagement-Fachmoduls auftreten.

Fehler-code	Fehlertyp	Severity	Fehlertext
5000	Technical	Fatal	Die eGK ist defekt.
5001	Technical	Error	HBA/SMC-B nicht freigeschaltet.
5002	Security	Error	Fachliche Rolle nicht berechtigt zur Ausführung.
5003	Technical	Error	Notfalldatensatz nicht konsistent.

[14] BSI-CC-PP-0098, Schutzprofil 2: Anforderungen an den Konnektor, Version 1.5.4, Stand 17.03.2020

Fehler-code	Fehlertyp	Severity	Fehlertext
5004	Technical	Fatal	Unbekannte Version der Speicherstruktur für den Notfalldatensatz auf der eGK.
5006	Technical	Error	Dekomprimierung des Notfalldatensatzes gescheitert.
5007	Technical	Error	Decodierung des Notfalldatensatzes gescheitert.
5008	Security	Error	Die Versicherten-ID des Notfalldatensatzes stimmt nicht mit der Versicherten-ID der eGK überein.
5009	Technical	Error	Die Kodierung (base64) des Notfalldatensatzes ist gescheitert.
5010	Technical	Error	Die Komprimierung des Notfalldatensatzes ist gescheitert.
5011	Security	Error	Es konnte keine Berechtigungsregel ermittelt werden.
5012	Technical	Error	Das Löschen des Notfalldatensatzes ist gescheitert.
5013	Business	Error	Der Notfalldatensatz überschreitet die maximal zulässige Größe.
5014	Security	Error	Das Primärsystem hat keine Zugriffsberechtigung auf die eGK.
5015	Security	Error	Das Primärsystem hat keine Zugriffsberechtigung auf den HBA/die SMC-B.
5016	Security	Error	Die gegenseitige Authentisierung von eGK und HBA/SMC-B (Card-to-Card-Authentisierung) ist gescheitert.
5017	Security	Error	Der Notfalldatensatz ist nicht valide.
5018	Security	Error	Die Signaturprüfung konnte nicht durchgeführt werden.
5019	Security	Error	PIN-Verifikation gescheitert.
5020	Business	Error	Der Notfalldatensatz ist verborgen.
5021	Business	Error	Es ist kein Notfalldatensatz auf der eGK gespeichert.
5103	Technical	Error	Datensatz „Persönliche Erklärungen“ nicht konsistent.
5104	Technical	Fatal	Unbekannte Version der Speicherstruktur für den Datensatz „Persönliche Erklärungen“ auf der eGK.

Fehler-code	Fehlertyp	Severity	Fehlertext
5106	Technical	Error	Dekomprimierung des Datensatz „Persönliche Erklärungen“ gescheitert.
5107	Technical	Error	Decodierung des Datensatz „Persönliche Erklärungen“ gescheitert.
5108	Security	Error	Die Versicherten-ID des Datensatz „Persönliche Erklärungen“ stimmt nicht mit der Versicherten-ID der eGK überein.
5110	Technical	Error	Die Komprimierung des Datensatz „Persönliche Erklärungen“ ist gescheitert.
5112	Technical	Error	Das Löschen des Datensatz „Persönliche Erklärungen“ ist gescheitert. <
5113	Business	Error	Der Datensatz „Persönliche Erklärungen“ überschreitet die maximal zulässige Größe. <
5114	Security	Error	Der Datensatz „Persönliche Erklärungen“ ist nicht valide.
5120	Business	Error	Der Datensatz „Persönliche Erklärungen“ ist verborgen.
5121	Business	Error	Es ist kein Datensatz „Persönliche Erklärungen“ auf der eGK gespeichert.
5501	Security	Warning	Prüfung der qualifizierten elektronischen Signatur unvollständig oder nicht durchführbar bzw. Signatur ungültig.
5504	Security	Error	Signatur des Notfalldatensatzes ungültig. Prüfung der Hashwertkette bzw. kryptographische Prüfung der Signatur fehlgeschlagen.
5505	Security	Error	Die Prüfung des Signaturzertifikats des Notfalldatensatzes auf Konformität zu einer qualifizierten elektronischen Signatur ist gescheitert.
5500	Technical	Fatal	Interner Fehler.

Tabelle 57: Notfalldatenmanagement – Fehlercodes

6.4.6 Elektronische Patientenakte (ePA)

Das Fachmodul elektronische Patientenakte bietet eine Schnittstelle für die Verwaltung der Dokumente einer Person in deren elektronischer Patientenakte,

einem Aktenkonto. Für den Zugriff auf Metadaten und Dokumente muss sich ein Nutzer, also eine Institution über das Fachmodul ePA authentisieren.

6.4.6.1 ePA-Konfiguration

Zur sicheren Kommunikation mit der ePA-Fachanwendung sind Konfigurationen vorzunehmen. Diese betreffen die Kommunikation des RISE Konnektors zur ePA-Fachanwendung in der zentralen Telematikinfrastruktur mittels TLS und TCP.

Abbildung 129 zeigt die Benutzermaske und die Konfigurationsparameter des ePA Fachmoduls des RISE Konnektors.

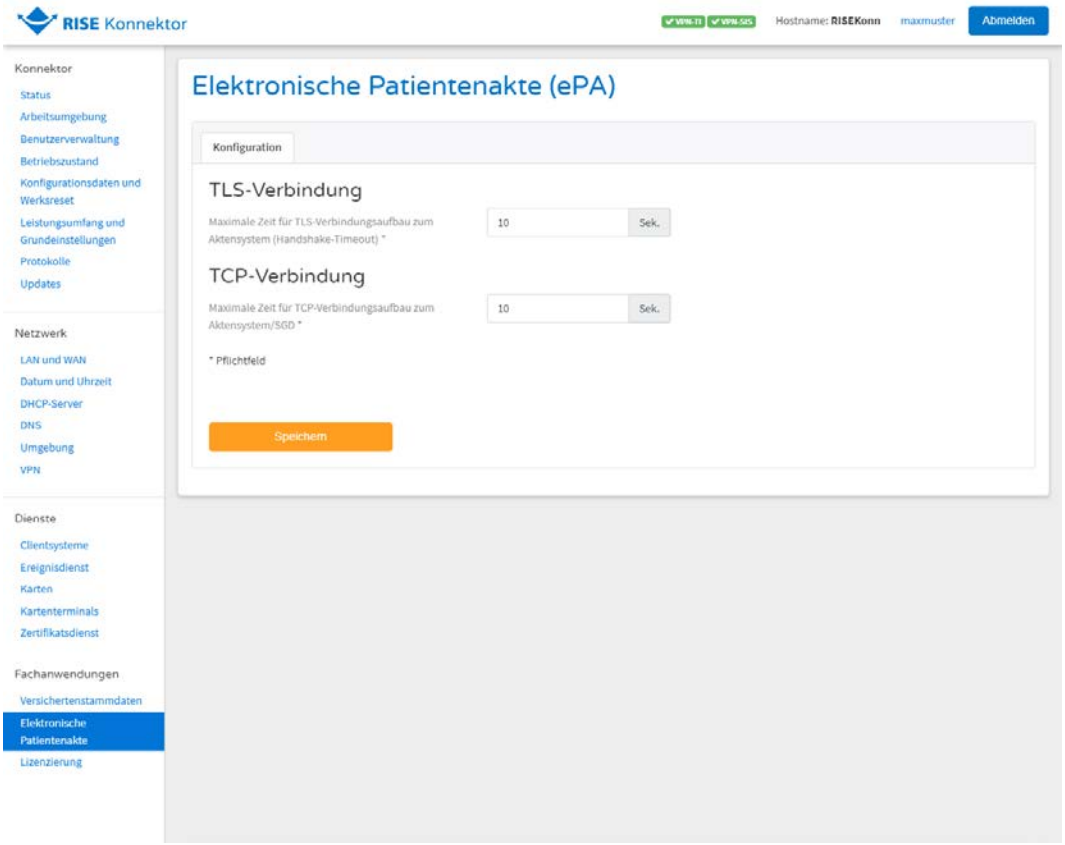


Abbildung 129: Konfiguration des Fachmoduls elektronische Patientenakte

Die Konfigurations-Parameter zum Fachmodul elektronische Patientenakte sind in Tabelle 58 angeführt.

ReferenzID	Belegung	Bedeutung
Maximale Zeit für TLS-Verbindungsaufbau zum Aktensystem (Handshake-Timeout) (EPA_TLS_HS_TIMEOUT)	Sekunden; Standard-Wert: 10 Sek.	Anzahl Sekunden die der Konnektor auf den TLS-Verbindungsaufbau zum Aktensystem wartet (Handshake-Timeout).
Maximale Zeit für TCP-Verbindungsaufbau	Sekunden;	Anzahl Sekunden, die der

ReferenzID	Belegung	Bedeutung
zum Aktensystem/SGD (EPA_SERVER_TIMEOUT)	Standard-Wert: 10 Sek.	Konnektor maximal auf den TCP-Verbindungsaufbau zum Aktensystem/SGD wartet.

Tabelle 58: Fachmodul elektronische Patientenakte – Parameter zur Konfiguration

6.4.6.2 Fehlercodes

Die in Tabelle 59 ersichtlichen Fehlercodes können im Rahmen des Fachmoduls elektronische Patientenakte auftreten.

Fehler-code	Fehlertyp	Severity	Fehlertext
7200	Technical	Error	Lokalisierung des Aktensystems fehlgeschlagen.
7202	Security	Error	Verbindung zum Aktensystem fehlgeschlagen.
7203	Security	Error	Die gegenseitige Authentisierung von eGK und SMC-B (Card-to-Card-Authentisierung) ist gescheitert.
7205	Technical	Error	Es konnte kein freigeschaltetes SM-B mit einem zulässigen Institutionstyp gefunden werden.
7206	Technical	Error	Prüfung der Zugriffsberechtigung fehlgeschlagen.
7209	Technical	Error	PIN-Verifikation gescheitert.
7211	Technical	Error	Keine Berechtigung für das Aktenkonto vorhanden.
7212	Technical	Error	Summe der Dokumente überschreitet maximal zulässige Größe von 250 MB.
7213	Technical	Error	Sperrstatus des Zertifikats der eGK nicht ermittelbar.
7214	Security	Error	Das Schlüsselmaterial der Akte entspricht nicht den Sicherheitsanforderungen.
7215	Technical	Error	Fehler im Aktensystem - Die Operation konnte nicht durchgeführt werden.
7217	Technical	Error	Die Operation wurde am Kartenterminal abgebrochen.
7220	Infrastructure	Error	Aktensystem nicht erreichbar.

Fehler-code	Fehlertyp	Severity	Fehlertext
7221	Security	Error	Zertifikat auf SMC-B ungültig.
7400	Technical	Error	Fehler - Die Operation konnte nicht durchgeführt werden.
7402	Technical	Warning	Das Aktenkonto ist bereits eingerichtet.
7403	Technical	Error	Das Aktenkonto kann noch nicht verwendet werden.
7404	Technical	Error	Das Aktenkonto existiert nicht (mehr) in diesem ePA-Aktensystem.
7405	Technical	Warning	Das Aktenkonto wurde bei diesem ePA-Aktensystem gekündigt, kann aber aktuell noch benutzt werden.
7406	Technical	Warning	Das Aktenkonto wurde bei diesem ePA-Aktensystem gekündigt und ist nur noch für einen Kontowechsel lesend zugreifbar.

Tabelle 59: Elektronische Patientenakte – Fehlercodes

6.4.6.3 Nutzung des Default-Aufrufkontexts

Das Fachmodul elektronische Patientenakte stellt für Aufrufe der IHE-Schnittstelle (dem PHRService) die Komfortfunktion eines Default-Aufrufkontexts zur Verfügung. Das heißt, werden bei einem solchen Aufruf keine SOAP-Header übergeben, so greift das Fachmodul auf den im Informationsmodell hinterlegten Aufrufkontext zurück und verwendet diesen zur Durchführung der jeweiligen Operation.

Um die Funktion des Default-Aufrufkontexts nutzen zu können, muss dieser einmalig durch den Administrator im Menüpunkt “Arbeitsumgebung” zusätzlich zur gegebenenfalls bereits bestehenden Arbeitsumgebung eingerichtet werden (siehe Abschnitt 6.1.4). In Tabelle 60 finden sich die benötigten Werte, welche für den Mandanten, das Clientsystem und den Arbeitsplatz des Default-Aufrufkontextes definiert und damit einer SMC-B, welche anschließend mit diesem neuen Kontext freigeschalten werden muss, zugewiesen werden müssen. Diese Werte sind exakt so zu übernehmen wie sie hier angegeben sind, andernfalls wird der Default-Aufrufkontext vom Fachmodul nicht erkannt.

Referenz	Belegung
Mandant	Mandant_ePA_Default

Referenz	Belegung
Clientsystem	Clientsystem_ePA_Default
Arbeitsplatz	Workplace_ePA_Default

Tabelle 60: Fachmodul elektronische Patientenakte - Belegung des Default-Aufrufkontextes

6.4.6.3.1 Fehlerfälle

Ist der Default-Aufrufkontext nicht oder nicht korrekt eingerichtet, so resultiert ein Aufruf der IHE-Schnittstelle ohne übergebene SOAP-Header in einem Syntaxfehler mit dem Fehlertext “epaFM Default-Aufrufkontext ist nicht korrekt konfiguriert in der Arbeitsumgebung”.

Wurde die SMC-B nicht mit dem neuen Default-Aufrufkontext freigeschalten, so liefert das Fachmodul bei dem Versuch, den Default-Aufrufkontext zu verwenden, den Fehler 7205 aus Tabelle 59.

7 Entsorgung des RISE Konnektors

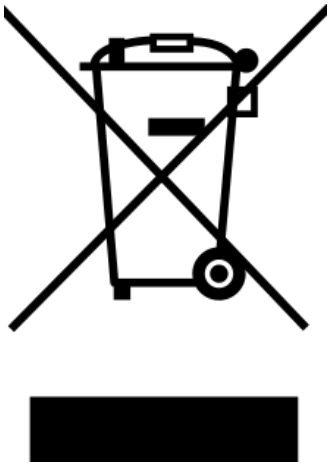


Abbildung 130: Entsorgung des RISE Konnektors

7.1 Entsorgung der Verpackung

Entsorgen Sie die Verpackung sortenrein.

Geben Sie Pappe und Karton zum Altpapier, Folien in die Wertstoff-Sammlung.

Bitte beachten Sie, dass die Originalverpackung des RISE Konnektors auch als Rücksendeverpackung verwendet werden kann, bevor Sie diese entsorgen.

7.2 Entsorgung des Altgerätes

Vor der Entsorgung des RISE Konnektors müssen die Sicherheitshinweise in Abschnitt 3.4 zur sicheren Außerbetriebnahme beachtet werden.

Altgeräte dürfen nicht über den Hausmüll entsorgt werden!

Batterien und Akkus gehören nicht in den Hausmüll!

Sollte der RISE Konnektor einmal nicht mehr benutzt werden können, ist jeder Verbraucher gesetzlich verpflichtet, Altgeräte getrennt vom Hausmüll zu entsorgen.

Der RISE Konnektor Hersteller bietet eine fachgerechte Entsorgung, welche durch den Verbraucher genutzt werden soll. Der RISE Konnektor ist bei der Stiftung Elektro-Altgeräte Register (ear) unter der WEEE-Reg.-Nr. DE 64684405 registriert; der Hersteller wird hierfür durch die MEDKONNEKT GmbH mit Sitz in München vertreten.

Dadurch wird sichergestellt, dass Altgeräte fachgerecht entsorgt und negative Auswirkungen auf die Umwelt vermieden werden. Daher sind elektrische Geräte mit dem Symbol gem. Abbildung 130 gekennzeichnet.

8 Anhang A - Signaturrichtlinien

8.1 SignDocument

8.1.1 Allgemein

- Max. Größe eines einzelnen SignDocument-Requests: 250 MB.
- Max. Anzahl SignRequests je SignDocument-Request: 50. Sind mehr als 50 SignRequests vorhanden wird die Operation mit Fehler 4000 “Syntaxfehler” abgebrochen.
- Die Dokumentgröße ist mit 26 MB beschränkt. Sind größere Dokumente in einem SignDocument-Request vorhanden wird die Operation mit Fehler 4000 “Syntaxfehler” abgebrochen.
- Es wird das Signaturzertifikat in die Signatur eingebettet. Weitere Zertifikate in der Zertifikatskette werden nicht eingebettet.
- Sperrinformationen werden ausschließlich für das Signaturzertifikat in Form von OCSP-Responses in die Signatur eingebettet (wenn durch IncludeRevocationInfo angefordert).

8.1.2 Parameterbelegung Außenschnittstelle

Tabelle 61 gilt für alle Signaturverfahren.

Parameter	Wert
CardHandle	CardHandle zu gesteckter Signaturkarte
Crypt	Crypt steuert die Auswahl der Schlüssel für die Signaturerstellung entsprechend **[gemSpec_Kon#TIP1-A_5010]**
Context	MandantId, ClientSystemId, WorkplaceId, UserId
JobNumber	Jobnummer nach den Vorgaben aus **[gemSpec_Kon#4.1.8.1.4]**[15]
TvMode	Keine Einschränkung. Der Parameter wird vom Konnektor nicht ausgewertet.
SignRequest.RequestID	$RequestId$ (verpflichtend)
SignRequest.Document.ID	$DocId$

[15] siehe https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/konzepte-und-spezifikationen/, letzter Zugriff: 20.10.2020

Parameter	Wert
SignRequest.Document.ShortText	$ShortText$ (für QES verpflichtend)

Tabelle 61: Parameterbelegung an der Außenschnittstelle

8.1.2.1 PAdES

Parameter	Wert
SignRequest.OptionalInputs.SignatureType	http://uri.etsi.org/02778/3
SignRequest.Document.Base64Data	base64-kodiertes PDF/A Dokument (max. 26 MB)
SignRequest.Document.Base64Data.MimeType	application/pdf-a
SignRequest.IncludeRevocationInfo	false

Tabelle 62: Parameterbelegung für PAdES

Wird gegen die Parameterbelegung verstoßen, wird die Operation mit Fehler 4000 "Syntaxfehler" abgebrochen.

Weitere Parameter werden nicht berücksichtigt.

8.1.2.2 CAdES

Parameter	Wert
SignRequest.OptionalInputs.SignatureType	urn:ietf:rfc:5652
SignRequest.OptionalInputs.IncludeEContent	true (enveloping) / false (detached)
SignRequest.OptionalInputs.ReturnUpdatedSignature	Optional, mögliche Werte sind: http://ws.gematik.de/conn/sig/sigupdate/parallel (Parallelsignatur), http://ws.gematik.de/conn/sig/sigupdate/counter/documentexcluding (Gegensignatur). Es muss bereits eine Signatur im Dokument enthalten sein. Für Parallelsignaturen muss IncludeEContent = true gesetzt sein. Für Gegensignaturen wird IncludeEContent ignoriert und immer eine enveloping Signatur erstellt. Parallel- und Gegensignaturen können ausschließlich als nonQES Signaturen erstellt werden.
SignRequest.OptionalInputs.Schemas	Wird SignRequest.Document.Base64Data

Parameter	Wert
	übergeben (kein XML) wird dieser Parameter ignoriert. Wird ein XML Dokument (Base64XML) übergeben, so werden die übergebenen Schemata gemäß TUC_KON_155 in die Signatur eingebettet. Es gelten die Vorgaben zu XML-Dokumenten gemäß Abschnitt "Einschränkungen für XML-Dokumente und Schemata" (siehe Abschnitt 8.3).
SignRequests.OptionalInputs.Properties	Es können zusätzliche CAdES-Attribute übermittelt werden, die in die Signatur eingebracht werden . Folgende Attribute werden im Request ignoriert und nicht in die Signatur eingebracht (sofern vorhanden): SigningCertificate, SigningCertificateV2, MessageDigest, ContentType, SigningTime und CMSAlgorithmProtect . Jedes Property darf maximal 500 kB groß sein. Requests mit größeren Properties beantwortet der Konnektor mit Fehler 4000 "Syntaxfehler" . Es dürfen maximal 10 Properties in einem Request enthalten sein. Sind mehr als 10 Properties enthalten reagiert der Konnektor mit Fehler 4000 "Syntaxfehler" .
SignRequest.Document.Base64Data	base64 kodiertes Dokument (max. 26 MB). Nicht in Verbindung mit SignRequest.Document.Base64XML zulässig.
SignRequest.Document.Base64Data.MimeType	QES: application/pdf-a, text/plain, text/plain; charset=iso-8859-15, text/plain; charset=utf-8, image/tiff. nonQES: zusätzlich weitere Dokumenttypen, welche als Binärdokument nach **[gemSpec_Kon]** behandelt werden.
SignRequest.Document.Base64XML	base64 kodiertes XML Dokument (max. 26 MB), es gelten die Vorgaben zu XML-Dokumenten gemäß Abschnitt "Einschränkungen für XML-Dokumente und Schemata" (siehe Abschnitt 8.3). Nicht in Verbindung mit SignRequest.Document.Base64Data zulässig.
SignRequest.IncludeRevocationInfo	QES: true / false, nonQES: false

Tabelle 63: Parameterbelegung für CAdES

Wird gegen die Parameterbelegung verstoßen, wird die Operation mit Fehler 4000 “Syntaxfehler” abgebrochen.

Weitere Parameter werden nicht berücksichtigt.

8.1.2.3 XAdES QES NFDM

Parameter	Wert
SignRequest.Document.RefURI	Der Wert muss übereinstimmen mit dem Wert des Attributs ID des Elements NFD:Notfalldaten.
SignRequest.Document.Base64XML	base64-kodiertes XML-Dokument (max. 26 MB), es gelten die Vorgaben zu XML-Dokumenten gemäß Abschnitt “Einschränkungen für XML-Dokumente und Schemata” (siehe Abschnitt 8.3). Das Dokument muss dem Schema für NFD Dokumente (NFD_Document.xsd[16]) entsprechen.
SignRequest.OptionalInputs.SignatureType	urn:ietf:rfc:3275
SignRequest.OptionalInputs.SignaturePlacement.WhichDocument	$DocId$
SignRequest.OptionalInputs.SignaturePlacement.CreateEnvelopedSignature	false
SignRequest.OptionalInputs.SignaturePlacement.XPathFirstChildOf	“/*[local-name()=‘NFD_Document’]/*[local-name()=‘SignatureArzt’]”
SignRequest.OptionalInputs.GenerateUnderSignaturePolicy.SignaturePolicyIdentifier	urn:gematik:fa:sak:nfdm:r1:v1
SignRequest.IncludeRevocationInfo	true

Tabelle 64: Parameterbelegung für XAdES QES

Weitere Parameter werden ignoriert.

Wird gegen die Profilierung der Schnittstelle verstoßen reagiert der Konnektor mit Fehler 4111 “ungültiger Signaturtyp oder Signaturvariante”.

16 https://fachportal.gematik.de/fileadmin/user_upload/fachportal/files/Spezifikationen/Produktivbetrieb/Schemata_WDSL/OPB3.1_Schemadateien_R3.1.1_ab01.10.2019.zip, /gematik_schema-R3.1.1_01.10.2019/fa/nfds/. Diese Schema-Datei ist ab 1.10.2019 gültig und enthält eine externe Referenz via “schemaLocation”. Letzter Zugriff: 04.09.2019

8.1.3 Beschaffenheit von XAdES-Signaturen, welche vom RISE Konnektor erstellt wurden

XAdES-Signaturen beinhalten drei Reference-Elemente, welche folgende Inhalte durch die Signatur schützen :

- das Dokument
- die SignedProperties
- das Manifest

Es wird Canonical XML 1.1 (http://www.w3.org/2006/12/xml-c14n11) zur Kanonikalisierung eingesetzt. Dies beugt XSW (XML Signature Wrapping) durch Ausnutzung von Namespace-Mappings vor.[17]

Es werden ID-basierte Referenzen verwendet. Hinweise zur Vermeidung von XSW sind unter Abschnitt 8.2.3 vermerkt.

8.2 VerifyDocument

8.2.1 Allgemein

- Max. Größe eines einzelnen VerifyDocument-Requests: 40 MB. Größere Requests werden mit Fehler 4000 “Syntaxfehler” abgebrochen.
- Max. Größe eines Dokuments: 26 MB. Sind größere Dokumente im Request vorhanden wird die Operation mit Fehler 4000 “Syntaxfehler” abgebrochen.
- Anzahl der Signaturen je Dokument
  - CAdES: Es dürfen max. 20 Signaturen je Dokument enthalten sein. Sind mehr als 20 Signaturen in einem Dokument enthalten wird die Operation mit Fehler 4112 “Dokument nicht konform zu Regeln für nonQES” abgebrochen.
  - PAdES: Es ist nur eine einzelne Signatur zulässig. Ansonsten wird die Operation mit Fehler 4001 “interner Fehler” abgebrochen.
  - XAdES (NFDM): Es ist nur eine einzelne Signatur zulässig. Sind zusätzliche Signaturen enthalten wird die Operation mit Fehler 4024 “Formatvalidierung fehlgeschlagen (XML)” abgebrochen.
- Qualifizierte Zeitstempel werden bei der Signaturprüfung nicht ausgewertet. Der für die Prüfung tatsächlich verwendete Zeitstempel wird im VerificationReport ausgewiesen.

Tabelle 65 gibt einen Überblick über die vom Konnektor unterstützen kryptographischen Algorithmen für die Signaturprüfung.

[17] Jensen, Meiko, Lijun Liao, and Jörg Schwenk. “The curse of namespaces in the domain of xml signature.” Proceedings of the 2009 ACM workshop on Secure web services. ACM, 2009.

Signaturverfahren	QES/nonQES	Signaturalgorithmus	Schlüssellänge	Hashalgorithmus
XAdES	QES	RSASSA-PKCS1-v1_5	1976 - 4096 Bit	SHA-256, SHA-384, SHA-512
XAdES	QES	RSASSA-PSS	1976 - 4096 Bit	SHA-256, SHA-384, SHA-512
XAdES	QES	ECDSA auf der Kurve brainpoolP256r1	256 Bit	SHA-256
CAdES und PAdES	QES	RSASSA-PKCS1-v1_5	1976 - 4096 Bit	SHA-256, SHA-384, SHA-512
CAdES und PAdES	QES	RSASSA-PSS	1976 - 4096 Bit	SHA-256, SHA-384, SHA-512
CAdES und PAdES	QES	ECDSA auf der Kurve brainpoolP256r1	256 Bit	SHA-256
CAdES und PAdES	nonQES	RSASSA-PSS	2048 Bit	SHA-256
CAdES und PAdES	nonQES	ECDSA auf der Kurve brainpoolP256r1	256 Bit	SHA-256
S/MIME	nonQES	RSASSA-PSS	2048 Bit	SHA-256
S/MIME	nonQES	ECDSA auf der Kurve brainpoolP256r1	256 Bit	SHA-256

Tabelle 65: Unterstützte kryptographische Algorithmen für die Signaturprüfung

Wird eine Signaturprüfung für eine Signatur angefordert, welche nicht mit einem der oben genannten Algorithmen erzeugt wurde, weist der Konnektor auf die fehlende Eignung dieses Algorithmus hin.

8.2.2 Schnittstelle VerifyDocument

Parameter	Wert
Context	MandantId, ClientSystemId, WorkplaceId, UserId.
TvMode	Keine Einschränkung. Der Parameter wird vom Konnektor nicht ausgewertet.

Parameter	Wert
OptionalInputs.UseVerificationTime	Referenzzeitpunkt für Signaturprüfung.
OptionalInputs.ReturnVerificationReport	Anfordern eines ausführlichen Prüfberichts.
Document	bei der Prüfung von detached oder enveloped Signaturen (siehe Abschnitt 8.3).
SignatureObject	Zu prüfende Signatur, sofern diese nicht im Dokument enthalten ist (nicht für PAdES).
IncludeRevocationInfo	QES: true / false (für PAdES: false). nonQES: false.

Tabelle 66: Parameterbelegung für VerifyDocument

Wird gegen die Parameterbelegung verstoßen, wird die Operation mit Fehler 4000 "Syntaxfehler" abgebrochen.

Für die Prüfung von XAdES Signaturen nach der Signaturrichtlinie NFDM gelten die Vorgaben aus **[gemRL_QES_NFDM]**.

Weitere Parameter werden ignoriert.

Wird gegen die Profilierung der Schnittstelle verstoßen reagiert der Konnektor mit Fehler 4111 "ungültiger Signaturtyp oder Signaturvariante".

8.2.3 Beschaffenheit von XAdES-Signaturen

- Zu Kanonikalisierung und Transformation werden folgende Algorithmen unterstützt :
  - Kanonikalisierung
    - Canonical XML 1.1 (omit comments) (http://www.w3.org/2006/12/xml-c14n11)
  - Transformation (zusätzlich)
    - base64 (http://www.w3.org/2000/09/xmldsig#base64)
- Es sind max. 10 Transformationen je Reference-Element zulässig. Sind mehr Transformationen vorhanden reagiert der Konnektor mit Fehler 4208 "Signatur nicht konform zur Profilierung der Signaturformate".
- Es sind max. 10 Reference-Elemente zulässig.
- Transformationen im SignedProperty SignaturePolicyIdentifier.SignaturePolicyId.Transforms sind nicht zulässig. Es wird nur ein Identifier übergeben. Sind Transformationen enthalten reagiert der Konnektor mit Fehler 4208 "Signatur nicht konform zur Profilierung der Signaturformate".
- Es werden nur dokument-interne Referenzen verarbeitet.

- KeyInfo.RetrievalMethod darf nicht vorhanden sein. Das Signaturzertifikat ist nach **[gemSpec_Kon]** in KeyInfo.X509Data vorhanden. Andernfalls reagiert der Konnektor mit Fehler 4208 "Signatur nicht konform zur Profilierung der Signaturformate".
- Zur Vermeidung von XSW dürfen Referenzen auf QualifyingProperties, KeyInfo und Manifest nur innerhalb des aktuellen ds:Signature-Elements liegen. Dies beugt XSW bei parallelen Signaturen vor. IDs zur Referenzierung von Objekten werden durch NFD_Document.xsd vorgegeben.
- Die verwendeten IDs müssen eindeutig sein. Kommen IDs mehrfach vor reagiert der Konnektor mit Fehlercode 4208 "Signatur nicht konform zur Profilierung der Signaturformate".
- Es muss genau ein Manifest-Element vorhanden sein. Andernfalls reagiert der Konnektor mit Fehlercode 4208 "Signatur nicht konform zur Profilierung der Signaturformate".
- Es muss genau ein QualifyingProperties-Element vorhanden sein.
- Eine QualifyingPropertiesReference ist nicht erlaubt.
- Durch die Einschränkung von XML-Schema-Elementen (xs:any u.ä. - siehe Abschnitt 8.3) sind folgende Einschränkungen auf XAdES Signaturen erforderlich:
  - Es sind nur zwei ds:Object-Elemente (ein Manifest und ein QualifyingProperties) zulässig.
  - Manifest und QualifyingProperties können auch in einem ds:Object liegen.
  - SignedSignatureProperty SignerRole: Da das Kindelement ClaimedRoles durch xs:any definiert ist kann es nicht befüllt werden, CertifiedRoles hingegen kann befüllt werden. Da nur ein Teil des Elements befüllt sein darf, wird das Element nicht verarbeitet sondern ignoriert.
  - SignedSignatureProperty CommitmentTypeIndication: Auch hier können durch die Verwendung von xs:any Teile nicht befüllt werden: Die definierten Kindelemente dürfen befüllt werden, CommitmentTypeIndication wird jedoch ignoriert.
  - SignedProperties AllDataObjectsTimeStamp und IndividualDataObjectsTimeStamp: Es ist das Kindelement EncapsulatedTimeStamp zu verwenden.
  - UnsignedSignatureProperty SignatureTimeStamp: Es ist das Kindelement EncapsulatedTimeStamp zu verwenden. SignatureTimeStamp wird jedenfalls ignoriert, da in der TI kein qualifizierter Zeitstempel erzeugt werden kann.
- Zusätzlich zu obigen Einschränkungen werden nur Signaturen, die nach **[gemSpec_Kon]** erstellt wurden, akzeptiert.

Sofern nicht anders angegeben reagiert der RISE Konnektor auf Verstöße gegen diese Einschränkungen mit Fehler 4124 "Dokument nicht konform zu Regeln für QES".

8.3 Einschränkungen für XML-Dokumente und Schemata

- Max. Größe eines Dokuments: 26 MB. Größere Dokumente werden mit Fehler 4000 “Syntaxfehler” abgelehnt.
- Max. Größe eines Schemas: 1 MB. Größere Schemata werden mit Fehler 4000 “Syntaxfehler” abgelehnt.
- Max. Anzahl an Schemata je Request: 10. Sind mehr Schemata enthalten reagiert der Konnektor mit Fehler 4000 “Syntaxfehler”.
- DTD ist deaktiviert.
- Sämtliche externe Referenzen sind deaktiviert: XInclude, schemaLocation, noNamespaceSchemaLocation.
- schemaLocation-Anweisungen sind in NFD_Document.xsd enthalten. Hier werden keine externen Schemata geladen sondern die im Konnektor hinterlegten Schemata. Unterstützt werden die Schemata zu XMLDSig und XAdES. Das Matching erfolgt anhand der Namespaces.
- Die max. Hierarchietiefe in XML Strukturen ist auf 30 limitiert.
- Es sind max. 20 Attribute je Element zulässig.
- Max. Länge von XML-Namen (z.B. Elementnamen, Attributnamen, Namespace-Prefixes, usw.): 100
- Max. Anzahl von Elementen im Dokument: 30000 .
- Eine Einschränkung für die maximale Breite eines XML-Zweiges existiert nicht. Die max. Breite ist nur durch die Gesamtelementzahl beschränkt.
- Zusätzlich werden in Schemadateien die folgenden Elemente ignoriert.
  - xs:any
  - processContents=“lax”
  - processContents=“skip”
  - namespace=“##any”
  - namespace=“##other”

Sofern nicht anders angegeben reagiert der Konnektor auf Verstöße gegen diese Einschränkungen mit

- Fehler 4024 “Formatvalidierung fehlgeschlagen (XML)” für XML Dokumente
- Fehler 4026 “XML-Schema nicht valide” für XML Schema

8.4 Beschaffenheit von PAdES Signaturen

Das Attribut signing-time darf in der Signatur enthalten sein, wird vom RISE Konnektor jedoch nicht verarbeitet.

8.5 Beschaffenheit von CAdES Signaturen

Folgende CAdES Attribute dürfen in Signaturen enthalten sein, werden jedoch vom RISE Konnektor nicht verarbeitet:

- 0.4.0.19122.1.1 (signer-attributes-v2)
- 1.2.840.113549.1.9.16.2.15 (id_aa_ets_sigPolicyId)

Zusätzliche Attribute, welche durch dss:Properties (im SignRequest) in die Signatur eingebracht werden können, werden bei der Signaturprüfung nicht berücksichtigt.