# Release Notes

**Einboxkonnektor**

# secunet konnektor 3.5.3:2.0.0

**Rechenzentrumskonnektor**

# secunet konnektor 3.5.3:2.1.0

**Stand 21.12.2020 (deutsch)**

Der Hersteller empfiehlt, sowohl Einbox- wie auch Rechenzentrumskonnektoren auf die Version 3.5.3 zu aktualisieren, sofern in der jeweiligen Einsatzumgebung die Konfiguration von mehr als 16 Intranet Routen erforderlich ist. In allen anderen Fällen ist ein Update nicht nötig.

Bitte beachten Sie die ggf. vorhandenen Hinweise des Herstellers zum Release unter https://www.secunet.com/konnektor/ sowie zur Installation im Bereich "Download" der produktspezifischen Unterseiten.

Die Version 3.5.3 des secunet Konnektors setzt den Produkttypsteckbrief Konnektor 3.6.0-2 (PTV3) der gematik um.

## Besondere Hinweise zu dieser Version

- **Verwendung einer größeren Anzahl von Intranet Routen**
  Die Version 3.5.3 unterstützt die Konfiguration von bis zu 256 Intranet Routen (siehe Abschnitt „Korrekturen gegenüber der Version 3.5.2“). Hierbei ist zu beachten, je mehr Intranet Routen konfiguriert werden, desto länger dauert die Anwendung des sich daraus ergebenden Regelwerks. Insbesondere bei Änderungen des Regelwerks, der Intranet Routen oder auch der IP-Adresse, einschließlich der Erneuerung des DHCP-Leases, der LAN-Schnittstelle kann es zu temporären Verzögerungen bei der Interaktion mit dem Gerät wie auch bei den, über den Konnektor, laufenden Kommunikationsverbindungen kommen.
- **Verpflichtende Angabe eines Next Hops je Intranet Route**
  Es muss bei der Konfiguration sichergestellt werden, dass bei sämtlichen Intranet Routen ein entsprechender Next Hop eingetragen ist. Falls das KMS für die Konfiguration der Konnektoren eingesetzt wird, ist darauf zu

achten, nicht die Option „Standard-Gateway“ bei der Übertragung von Intranet Routen zu verwenden.

## Allgemeine Hinweise zu dieser Version

- **Verwendung zugelassener Firmwareversionen**
  In der Telematikinfrastruktur dürfen nur zugelassene oder genehmigte Konnektoren eingesetzt werden. Konnektoren mit Firmwareversionen bei denen die Genehmigung oder die Zulassung abgelaufen ist, sind auf eine zugelassene bzw. genehmigte Firmware zu aktualisieren.

  Informieren Sie sich vor der Nutzung eines Modularen Konnektors von secunet zunächst auf der Webseite der gematik über zugelassene bzw. genehmigte secunet Konnektoren.

  Sie finden eine Auflistung unter:

  https://fachportal.gematik.de/zulassungen/online-produktivbetrieb/

  Weitere Informationen zu den zugelassenen oder genehmigten secunet Konnektoren finden Sie auf der Produktwebseite der secunet in der Rubrik „Hinweise und FAQs“ der jeweiligen Produktausprägung:

  https://www.secunet.com/konnektor/

- **Update PTV1 auf PTV3 (3.5.3)**
  Da es sich bei diesem Update um ein Major-Update von der Produkttypversion 1 (PTV1) auf Produkttypversion 3 (PTV3) handelt, empfiehlt der Hersteller, vor dem Update ein Backup der Konfiguration des Konnektors durchzuführen.

  Sollte der Update-Vorgang rückgängig gemacht werden müssen, so ist eine Rückkehr zur PTV1-Version 2.0.47 generell möglich. Nach diesem (etwaigen) Downgrade muss die Konfiguration des Konnektors einem Review unterzogen werden.

- **Änderung der Konnektor-Konfiguration**
  Der PTV3-Konnektor bedingt ein neues XML-Konfigurationsschema, was zur Folge hat, dass keine neuen Konfigurationsbackups (PTV3) in PTV1-Konnektoren eingespielt werden können.

  Wird ein Upgrade von PTV1 auf PTV3 bzw. ein Downgrade von PTV3 auf PTV1 durchgeführt, so sorgt der Konnektor automatisch dafür, dass die Konfiguration für den jeweiligen Konnektorprodukttyp umgeschrieben wird. Da dieses Umschreiben nicht vollends eindeutig umkehrbar ist, ist nach einem erfolgten Downgrade die Konfiguration generell zu begutachten und ggf. anzupassen.

- **Lizenz zur Nutzung der Fachmodule NFDM sowie eMP/AMTS**
  Die Lizenzierung von Funktionalitäten wurde mit dem PTV3 Konnektor eingeführt. Eine Lizenzierung erfolgt individuell für einen Konnektor, identifiziert anhand seiner Seriennummer.

  Um die Fachmodule NFDM und eMP/AMTS nutzen zu können, müssen diese lizenziert und freigeschaltet werden. Eine Freischaltung ist nur in Kombination möglich.

- **Prüfung von Zertifikaten für ECDSA Schlüssel**
  Vor dem Hintergrund, dass die Telematikinfrastruktur aktuell (PTV3) noch keine ECC-CA-Zertifikate bereitstellt und die TSL nur RSA Zertifikate enthält, ist eine Prüfung der Zertifikatskette für ECDSA Schlüssel nicht möglich und ein positives Prüfungsergebnis ausgeschlossen.

  Obwohl der Konnektor ECDSA-Signaturen grundsätzlich verarbeiten kann, lehnt der PTV3-Konnektor daher Zertifikate für ECDSA-Schlüssel ab.

- **Browser-Cache leeren nach Update**
  Nach einem Update des Konnektors ist der Browser-Cache zu leeren um sicherzustellen, dass das Management-UI der neu installierten Version und nicht die GUI der vorherigen Version aus dem Browser Cache aufgerufen wird.

- **TLS-Verbindungen (TLS 1.2)**
  Der PTV3 Konnektor unterstützt ausschließlich TLS 1.2.

  Die Verwendung von TLS 1.1 ist aufgrund der Abkündigung durch die gematik entfallen.

- **Signaturproxy**
  Um die lokale Anzeige auf den Primärsystemen (PVS, KIS, RIS, LIMS, WaWi etc.) für die Signaturerstellung und Signaturprüfung zu realisieren, kann ein Signaturproxy verwendet werden.

  Hierzu nutzt der Signaturproxy die Primärsystemschnittstelle des Konnektors zum Service Discovery, der Weiterleitung des Signaturauftrages an den Konnektor bzw. zum Abruf einer Signaturantwort für das Primärsystem sowie zur Signaturprüfung.

  Der Signaturproxy ist nicht Lieferbestandteil des Konnektors bzw. des Updates. Der Signaturproxy kann separat von der Produktwebseite des Konnektors abgerufen werden (https://www.secunet.com/konnektor/).

## Neuerungen seit secunet konnektor Firmware 3.5.2

- **Keine Neuerungen**

## Korrekturen gegenüber der Version 3.5.2

- **Erhöhung der Anzahl der Intranet Routen**
  Die Anzahl der konfigurierbaren Intranet Routen wurde auf 256 erhöht. Damit einher geht die Verpflichtung zur Konfiguration eines Next Hops je Intranet Route (siehe nächsten Spiegelpunkt).

## Bekannte Fehler der Version

- **Anzeige der URL zum Download des Firmware Updates**
  Die Internet-URL zum Download des Firmware Updates wird in der GUI nicht anzeigt.
- **Display Messages nach SICCT für Null-Pin Verfahren**
  Im Kommando SICCT MODIFY VERIFICATION DATA werden mehr Display Messages gesendet als nach SICCT-Spezifikation für Null-PIN-Verfahren gefordert.

## Sonstige Hinweise zur Version

- **Ausstattung mit ECC fähigen Gerätekarten (gSMC-K)**
  Zur Aufrechterhaltung des Sicherheitsniveaus werden zukünftig Gerätekarten verwendet, welche sowohl RSA- als auch ECC-Schlüssel beinhalten. In der Übergangsphase, welche bis Ende 2024 geht, können RSA-Schlüssel zur Authentisierung weiterverwendet werden.

  Welche Konnektoren bereits auf die Verwendung von ECC-Schlüsseln vorbereitet sind, ist anhand der ersten drei Stellen der Seriennummer (Beispiel für eine Seriennummer: <301/20/10-1234567>) zu erkennen.

  So beinhalten Einboxkonnektoren beginnend mit der Seriennummer <307> sowie Rechenzentrumskonnektoren beginnend mit der Seriennummer <315> die neuen Geräteidentitäten.

| Kryptographische Verfahren | Typ des Sicherheitsmoduls |
|---|---|
| RSA-Schlüssel | STARCOS 3.6 Health SMCK R1 v1.0.7<br>gematik zugelassene G2-Karten mit der Zulassungsnr. <gematik_gSMCK-G2_2017-04-10_001082> |
| RSA- und ECC-Schlüssel | TCOS Security Module Card - K Version 2.0 Release 1 v2.2.3<br>gematik zugelassene G2-Karten mit der Zulassungsnr. <gematik_SiGu_2018-02-22_001359> |

- **Basisdienst TBAuth**
  Der optionale Basisdienst zur tokenbasierten Authentisierung (TBAuth) wird nicht unterstützt.
- **Automatisches Softwareupdate von Konnektor und Kartenterminals**

  Die automatische Aktualisierung der Software des Konnektors sowie der angeschlossenen und vom Konnektor verwalteten Kartenterminals wird nicht unterstützt.

  Es wird der automatische Abruf neuer Software vom Konnektor unterstützt.
- **EC_No_Online_Connection nicht zurückgesetzt**

  Es kann in seltenen Fällen vorkommen, dass der Betriebszustand "EC_No_Online_Connection" nicht zurückgesetzt wird, obwohl die Ursache behoben ist.

Um den Betriebszustand in so einem Fall zurückzusetzen, muss der TI- oder SIS-Tunnel kurz abgebaut und anschließend wieder aufgebaut werden.

## Sonstige Hinweise zur Downgrade eines PTV3-Konnektors

- **Downgrade bei einem als PTV3 ausgelieferten Konnektor**
  Bei einem ab Werk als PTV3 ausgelieferten Konnektor mit der Firmwareversion 3.5.0 oder höher ist ein Downgrade auf PTV1 (VSDM Konnektor, Firmwareversion 2.0.47) zu vermeiden.

  Wenn trotzdem ein Downgrade durchgeführt wird, kann es bei Durchführung eines vollständigen Werksresets vorkommen, dass der Konnektor beim nächsten Neustart einen Fehlerzustand signalisiert.

  Wenn der Konnektor diesen Zustand anzeigt, kann durch die Durchführung eines Werksrests für FailSafe der Fehlerzustand aufgehoben werden. Es ist anschließend ein Neustart durchzuführen.

## Sonstige Hinweise zum Update von den Versionen PTV1 auf PTV3

**Die nachfolgenden Hinweise sind bei einem Update von den Versionen 2.0.36, 2.0.37 und 2.0.38 auf 3.5.3 zu beachten.**

**Bitte beachten Sie die eventuell vorhandenen Hinweise des Herstellers zum Release unter https://www.secunet.com/konnektor/ sowie zur Installation im Bereich "Download" der produktspezifischen Unterseiten.**

- **Online-Update des Konnektors über den KSR-Dienst**
  Die Aktualisierung der Konnektoren über den KSR-Dienst ist die empfohlene Methode, sofern der Konnektor den Fehlerzustand EC_Security_Log_Not_Writeable bisher nicht erreicht hat.
- **Update des Konnektors, bei Signalisierung des Fehlerzustandes EC_Security_Log_Not_Writeable**
  Zeigt der Konnektor den Fehlerzustand EC_Security_Log_Not_Writeable, so muss der Konnektor zunächst "aus dem Zustand gebracht" werden. Nur dann kann der Konnektor eine Verbindung zur Telematikinfrastruktur (TI) und zum KSR-Dienst aufbauen. Zusätzlich ist zu beachten, dass der Fehlerzustand während des Downloads vom KSR-Dienst erneut auftreten kann, so dass die Verbindung zur TI und damit auch der Download des Softwareupdates unterbrochen werden könnte.
- **Offline-Update des Konnektors via Datei-Upload**
  Ein Offline-Update wird für die Konnektoren mit dem Fehlerbild EC_Security_Log_Not_Writeable empfohlen.

  Weitergehende Informationen erhalten Sie von ihrem DVO bzw. PVS-Anbieter.
- **Prüfen des Sicherheitsprotokolls nach dem Softwareupdate**
  Es wird empfohlen, nach der Installation den Zustand des Sicherheitsprotokolls (im Bereich Diagnose) zu prüfen und im Falle des Zustandes "Protokollspeicher knapp", ältere Einträge zu löschen.
- **Neutrale Konfigurationswerte**
  Die Auslieferungskonfiguration des Konnektors wurde neutral ausgeprägt. Damit ergeben sich gleiche Voraussetzungen bei Konfigurationen unterschiedlicher VPN-Zugangsdienste.

- **Hinterlegung der in der Einsatzumgebung verwendeten Netzbereiche**
  Alle in der Einsatzumgebung verwendeten Netzbereiche müssen vor dem Update auf 2.0.47 oder eine neuere Version in der Konfiguration des Konnektor hinterlegt werden.

  Ansonsten sind Komponenten der Einsatzumgebung (wie z.B. Arbeitsplätze und Kartenterminals) in Netzbereichen, die dem Konnektors nicht explizit bekannt gemacht wurden, nach einem Update nicht mehr erreichbar.