Release Notes

Einboxkonnektor

secunet konnektor 3.5.0:2.0.0

Rechenzentrumskonnektor

secunet konnektor 3.5.0:2.1.0

Stand 31.07.2020 (deutsch)

Der Hersteller empfiehlt, sowohl Einbox- wie auch Rechenzentrumskonnektoren auf die Version 3.5.0 zu aktualisieren.

Diese Empfehlung gilt insbesondere für Konnektoren, die noch nicht auf die Version 2.0.47 umgestellt wurden.

Besondere 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:

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

- **Update PTV1 auf PTV3 (3.5.0)**
  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.

- **Lizenz zur Nutzung der Fachmodule NFDM sowie eMP/AMTS**
  Die Lizenzierung von Funktionalitäten wird 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.

- **Verwendung von eHBA G0 Vorläuferkarten**
  Bei Verwendung von eHBA G0 Vorläuferkarten gelten die folgenden Einschränkungen bzgl. Ver-/Entschlüsselung:

  > Lediglich die personenbezogene Ver-/Entschlüsselung von Daten über den Konnektor, z. B. im Rahmen von KIM, ist für Nutzer von eHBA G0 Ausweisen beeinträchtigt.

  Erst bei Verwendung von elektronischen Heilberufsausweisen der zweiten Generation (eHBA G2) kann die Ver-/Entschlüsselung vollumfänglich genutzt werden.

  Alle anderen Vorläuferkarten, sind von dieser Einschränkung nicht betroffen. Insbesondere mit ZOD 2.0 und eZA Karten ist die Signatur von NFDM Daten mit allen im Feld verfügbaren Heilberufsausweisen möglich.

  Die gematik empfiehlt die Verwendung von eHBA G2 Karten.

- **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.

Neuerungen seit secunet konnektor Firmware 2.0.47

- **Produkttypversion**
  Die Version 3.5.0 des secunet Konnektors setzt den Produkttypsteckbrief Konnektor 3.6.0-2 (PTV3) der gematik um.

  - **Fachmodule NFDM, eMP/AMTS**
    Der PTV3 Konnektor stellt den Primärsystemen die Fachmodule zur Umsetzung der Fachanwendungen Notfalldatenmanagement (NFDM) sowie elektronischer Medikationsplan (eMP/AMTS) zur Verfügung.

    Um die Fachanwendungen nutzen zu können, werden entsprechend angepasste Primärsysteme benötigt.

  - **Kommunikation im Medizinwesen (KIM)**
    Zur Nutzung des neuen Kommunikationsstandards in der Telematikinfrastruktur „Kommunikation im Medizinwesen (KIM)“ stellt der PTV3 Konnektor den Clientsystemen die erforderlichen Basisdienste, wie z.B. QES um Dokumente qualifiziert signieren zu können, zur Verfügung.

    Clientsysteme können somit unter Verwendung des LDAP-Proxies, des Verschlüsselungs- sowie des Signaturdienstes den sicheren E-Mail- und Datenaustausch realisieren.

  - **LDAP Proxy**
    Der PTV3 Konnektor ermöglicht es Clientsystemen und Fachmodulen durch Nutzung des LDAP-Proxies Daten aus dem Verzeichnisdienst der TI-Plattform (VZD) abzufragen.

  - **Neuer Basisdienst – Verschlüsselungsdienst**
    Der Verschlüsselungsdienst bietet Schnittstellen zum hybriden und symmetrischen Ver- und Entschlüsseln von Dokumenten an.

    Die unterstützten Verfahren sowie zusätzliche Informationen sind dem Abschnitt Verschlüsselungsdirektive des Handbuchs zum PTV3 Konnektor zu entnehmen.

    Hinweis zu XML-Verschlüsselung – Hybrid
    Der PTV3 Konnektor unterstützt bei der RSA-basierten hybriden Verschlüsselung von [XMLEnc-1.1] Dokumenten für den Schlüsseltransport ausschließlich den Algorithmus RSAES-OAEP gemäß [PKCS#1].

- **Neuer Basisdienst – Signaturdienst (QES und nonQES)**
  Der Signaturdienst bietet Clientsystemen und Fachmodulen eine Schnittstelle zum Signieren von Dokumenten und Prüfen von Dokumentensignaturen. Es werden qualifizierte elektronische Signaturen (QES) wie auch nicht qualifizierte elektronische Signaturen (nonQES) unterstützt.

  Die implementierten Signaturverfahren sowie zusätzliche Informationen sind den Abschnitten Dokumentensicherheit sowie Signaturdirektive des Handbuchs zum PTV3 Konnektor zu entnehmen.

  Hinweis zu nonQES-XAdES

  Die Erzeugung und Verifikation von nonQES-XAdES Signaturen wird nicht unterstützt.

  Der Konnektor beantwortet Aufrufe zu Signaturerstellung einer nonQES-XAdES-Signatur daher mit Fehler 4111 und alle Aufrufe zur Signaturprüfung einer nonQES-XAdES-Signatur mit Fehler 4112.

- **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/).

- **Lizenzmanagement**
  Die Lizenzierung von Funktionalitäten wird mit dem PTV3 Konnektor eingeführt. Eine Lizenzierung erfolgt individuell für einen Konnektor, identifiziert anhand seiner Seriennummer.

  Hierzu ist der PTV3-Konnektor mit einem Lizenzmanagement ausgestattet, über das neue Features des Konnektors freigeschaltet werden können, indem eine neue Lizenz über die Management-UI hochgeladen wird.

  Bis auf die Fachmodule NFDM und eMP/AMTS sind werksseitig alle Features lizenziert und freigeschaltet.

Die Freischaltung beinhaltet auch die Funktionalitäten zur Ver-/Entschlüsselung, Signaturerstellung/–prüfung sowie zum Abruf von Daten aus dem Verzeichnisdienst der TI-Plattform via LDAP Proxy:

- Signaturdienst (QES/nonQES)
- Verschlüsselungsdienst
- LDAP

Zusätzlich kann die nachfolgend angegebene Anzahl von SMC_Bs sowie Kartenterminals (KT) lizenzfrei angeschlossen und genutzt werden:

- bis zu 10 SMC-Bs
- bis zu 50 Kartenterminals (KT) pro Konnektoreinheit (dies entspricht insgesamt 50 KTs beim Einbox- und 100 KTs beim RZ-Konnektor).

- **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.

- **Erweiterung des Kartendienstes**
  Es wurden Methoden zur Aktivierung bzw. Deaktivierung von PINs integriert. Diese Methoden unterstützten auch die PINs für NFDM, AMTS und QES.

- **QES Zertifikatsprüfung**
  Umsetzung der QES-Zertifikatsprüfung inkl. BnetzA-VL Management.

- **Manueller Import von CA-Zertifikaten**
  Die Verwendung manuell importierter CA-Zertifikate wurde umgesetzt.

- **Abbruch TLS-Verbindungsaufbau bei Nichterreichbarkeit des OCSP Responders**
  Der TLS-Verbindungsaufbau wurde in PTV1 nicht abgebrochen, auch wenn der OCSP-Responder zur Zertifikatsprüfung technisch nicht erreichbar war. Mit der Änderung der Spezifikationen für PTV3 wird nun der TLS-Verbindungsaufbau abgebrochen, sofern der OCSP-Responder zum Zeitpunkt der Zertifikatsprüfung technisch nicht erreichbar ist.

- **Erweiterungen der Management-UI**
  Die GUI wurde um Einstellungen für die neuen Dienste erweitert. Auch wurden vereinzelt kleinere Verbesserungen in der GUI vorgenommen. So ist es z.B. nicht mehr notwendig, eine separate Liste der LEKTR-Netze zu pflegen. Es sind nur noch die Intranet-Routen zu definieren.

- **Änderung der Konnektor-Konfiguration**
  Der PTV3-Konnektor bedingt ein neues XML-Konfigurationsschema. Dieser Hinweis ist für den Benutzer wichtig, da 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.

- **Hardware-beschleunigte AES-Implementierung**
  Der PTV3-Konnektor kann auf die hardwarebeschleunige Ver- und Entschlüsselung der Intel CPU zugreifen (AES-NI). Zusätzlich implementierte Selbsttests mit ‚known answers' (Testvektoren) stellen sicher, dass die AES-Implementierung spezifikationskonform ist. Dieses Feature muss in der Management-UI explizit eingeschaltet werden (ist im Auslieferungszustand inaktiv). Zur abschließenden Aktivierung ist ein Neustart des Konnektors erforderlich.

  Bis zur nächsten Deaktivierung ist dieses Feature systemweit aktiv. Auch nach einer Deaktivierung muss der Konnektor neu gestartet werden, damit die reine Software-Implementierung vom System dann aktiviert werden kann.

- **Verhalten bei kritischen Updates**
  Die Überschreitung der Deadline bei kritischen Updates führt zu einer Sperrung des TI Zugangs.

- **Selbsttest**
  Der PTV3 Konnektor verfügt über einen Selbsttest, der die Integrität sicherheitsrelevanter Komponenten prüft. Dies geschieht bei jedem Start, während des Betriebs regelmäßig alle 24 Stunden und nach manuellem Anstoß über die Bedienoberfläche.

- **Intel Microcode-Updates**
  Der PTV3-Konnektor ist mit den neusten Microcode-Updates für die verbaute Intel-CPU ausgestattet. Diese werden automatisch bei jedem Start des Konnektor geprüft und eingespielt.

- **Neue DNS-Zone**
  Die DNS-Zone **konlan** wurde hinzugefügt und wird durch den Namensdienst beauskunftet.

- **Komponenten aktualisiert**
  Zusätzlich zur Aktualisierung von Komponenten aufgrund funktionaler Änderungen wurden aufgrund der kontinuierlichen Schwachstellenanalyse (CVEs) sowie der statischen Code-Analyse Versionsupdates von Komponenten durchgeführt.

Korrekturen gegenüber der Version 2.0.47

- **VSDM Prüfnachweis**

  Die Längen-Byte-Ermittlung beim Schreiben des Prüfungsnachweises wurde korrigiert.

- **Setzen der Systemzeit beim Start des Konnektors**
  Es wurde bei PTV1-Versionen beobachtet, dass die Systemzeit nicht immer korrekt gesetzt wurde. Die Zuverlässigkeit beim Setzen der Systemzeit beim Start des Konnektors wurde erhöht.

- **Aktualisierung der TSL**
  Der Umgang mit der „Trust-service Status List (TSL)“ wurde verbessert. Insbesondere wurden Beschränkungen bzgl. der Reihenfolge sowie der maximalen Anzahl von Cross-CV-Zertifikaten in einer TSL aufgehoben.

- **Korrektur für ti-wa-Zone (DNS)**
  Da die ti-wa-Zone bei der Gematik ohne DNSSEC betrieben wird, wurde dies im Konnektor angepasst.

- **DNS Abfrage für KSR-Dienst**
  Um einmalige Probleme beim Beziehen der DNS-SD Informationen im laufenden Betrieb automatisiert zu beheben, wird die DNS-SD Auflösung für den KSR nicht mehr nur initial sondern auch beim Ändern des TI Zustands durchgeführt.

- **Korrektur für Fehlercode 47709**
  Bessere Anzeige, wenn die DomainLEKTR nicht gesetzt ist.

- **Standardeinstellung für IKE-Reauthentifizierungszeit korrigiert**
  Die Standardeinstellung für die IKE-Reauthentifizierungszeit wurde korrigiert.

- **Standardwerte MTU-Size geändert**
  Die Standardwerte für die MTU-Size wurden auf 1418 Byte geändert.

- **Lokalisierung der GUI aktualisiert**
  Es wurden Aktualisierungen der Übersetzungsdatei für die GUI umgesetzt.

- **Aktivierung von Bestandsnetzen**
  Es wird sichergestellt, dass die Liste aller Bestandsnetzwerke jederzeit alle Elemente enthält.

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 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 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 3.5.0 zu beachten.

Bitte beachten Sie die Kundeninformation „Konnektor Update auf die Firmware Version 2.0.47“. Das Dokument steht auf der Produktwebseite (https://www.secunet.com/konnektor/) zur Verfügung und ist, analog zum Update auf die Version 2.0.47, auch für ein Update auf die Version 3.5.0 gültig.

- **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 2.0.46 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.