Release Notes

Einboxkonnektor

secunet konnektor 6.0.8:2.0.0

Rechenzentrumskonnektor

secunet konnektor 6.0.8:2.1.0

Stand 25.03.2026 (deutsch)

Der Hersteller empfiehlt, sowohl Einbox- wie auch Rechenzentrums-konnektoren auf das Release Version 6.0.8 zu aktualisieren.

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

Die Version 6.0.8 (PTV6) des secunet Konnektors setzt den Produkttypsteckbrief Konnektor 6.0.2-0 (PTV6) der gematik um.

Besondere Hinweise zu dieser Version

- **Downgrade von PTV6 auf niederwertige Versionen**
  Die Version 6.0.8 vollzieht nach den Vorgaben des BSI und der gematik den Übergang von RSA-basierter Kryptographie zu ECC-basierter Kryptographie. Insbesondere wurden in dieser Version die Updatemechanismen des Konnektors auf die Verwendung von ECDSA Algorithmen umgestellt. **Daher ist ein Downgrade auf Vorgängerversionen der 6.0.8 nicht mehr möglich.**
- **Einspielen von Backups älterer Firmware Versionen**
  Das BSI hat die Nutzung von RSA-2048-Schlüsseln zum 31.12.2025 abgekündigt. Aus diesem Grund können Backups, die mit Vorgängerversionen von PTV6 erstellt wurden, in PTV6 Firmware 6.0.8 nicht mehr eingespielt werden. In der Version 6.0.8 wurde das Schlüsselmaterial zur Backup-Verschlüsselung auf RSA-4096 umgestellt. Wir empfehlen daher, nach dem erfolgreichen Upgrade ein neues Backup mit der aktualisierten Schlüssellänge anzulegen.

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 „Fragen und Hinweise“ der jeweiligen Produktausprägung:

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

- **Automatisches Softwareupdate von Konnektor und Kartenterminals**
  Die automatische Aktualisierung der Software des Konnektors sowie der angeschlossenen und vom Konnektor verwalteten Kartenterminals wird unterstützt.

  Beginnend mit dem PTV4-Release (Version 4.1.3 oder neuer) werden bereitstehende Updates für den Modularen Konnektor automatisch heruntergeladen und automatisch installiert; zuvor werden auch die erreichbaren Kartenterminals aktualisiert, sofern für diese ein Update zur Verfügung steht.

  Entsprechend den Spezifikationen der gematik, wird diese Funktion standardmäßig mit dem Update aktiviert. Die Konfiguration sowie eine Deaktivierung des automatischen Softwareupdates können über die Management-Oberfläche oder unter Verwendung der REST-API erfolgen.

  Die Informationen zum automatischen Softwareupdate sind dem Handbuch Kapitel 11.12 zu entnehmen.

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

Das Leeren des Browser Caches nach der Durchführung eines Updates wird seit der Version 4.1.3 erzwungen, um sicherzustellen, dass die jeweils neueste Version der GUI verwendet wird.

Neuerungen seit secunet Konnektor-Firmware 5.70.6

- **Anpassungen aufgrund Änderungen der gematik Spezifikation**
  - Durch den RSA-Phase-Out wird es künftig auch Karten im Feld geben, die ausschließlich EC-Zertifikate besitzen und keine RSA-Zertifikate mehr. Daher wurde die Logik angepasst, um bei fehlendem RSA-Zertifikat automatisch auf das vorhandene EC-Zertifikat zurückzugreifen.
  - Das Pairing von Kartenterminals soll künftig automatisch im Rahmen eines Wartungspairings auf EC umgestellt werden – vorausgesetzt, das bestehende Pairing erfolgte bislang über RSA und sowohl das Kartenterminal als auch der Konnektor verfügen über ein EC-Zertifikat. Zu diesem Zweck wird der Konnektor beim Verbindungsaufbau künftig stets auch EC-CipherSuites anbieten. Bei ECC-fähigem Kartenterminal, wird automatisch ein Wartungspairing mit dem EC-Zertifikat initiiert. Voraussetzung ist, dass auch eine aktuelle KT-Firmware zum Einsatz kommt.
  - Zukünftige Kartengenerationen sollen unterstützt werden, während ältere Kartenversionen wegfallen. Dafür wird die Kartenerkennung so angepasst, dass auch Karten mit einer höheren Versionsnummer als G2.1 unterstützt werden. Gleichzeitig werden eGKs mit einer kleineren Versionsnummer als G2.1 nicht mehr unterstützt.
  - Die Auswertung des CryptType-Werts sowie der Angaben zum Signaturalgorithmus soll künftig nur noch eingeschränkt erfolgen. Ob RSA oder EC verwendet wird, leitet sich vorrangig aus der Generation der verwendeten Karte ab. Alle betroffenen Stellen – insbesondere die Mappings der Außenschnittstellen – werden entsprechend angepasst, sodass nicht mehr standardmäßig RSA verwendet wird, sondern die Entscheidung auf Basis der Kartengeneration getroffen wird.
  - Für TLS-Verbindungen zu Diensten in die TI sollen nur noch EC-Ciphersuiten verwendet werden. Dafür wurde ein Konfigurationsschalter („RSA-Ciphersuiten für die TLS-Verbindung zur TI “) eingeführt, über den die Möglichkeit zur Nutzung von RSA-Ciphersuiten aktiviert und deaktiviert werden kann. Per Default ist die Möglichkeit zur Nutzung von RSA aktiviert.

- Die gematik hat neue Rollen definiert, welche Operationen im Kontext NFDM durchführen dürfen. Daher wurden diese Rollen für die Auswertung im Fachmodul erweitert.
- Im Rahmen der PoPP-Spezifikation hat die gematik drei neue CardService-Operationen definiert, um Kartenkommandos, die vom PoPP-Server über das PVS übertragen werden, auf der eGK ausführen zu können. Diese werden im Konnektor umgesetzt.
- Die OCSP-Abfragen, die in Signaturen eingebettet werden, sollen nach dem Signaturzeitpunkt erstellt werden. Demnach wird im Ablauf der Signaturerstellung nun vor der OCSP-Abfrage der Signaturzeitpunkt bestimmt.
- Bereits beim Stecken einer HBA bzw. SMC-B erfolgt eine OCSP-Prüfung und das Ergebnis wird für weitere Operationen gecached.
- Es wurden neue Betriebszustände eingeführt, die Anzeigen, ob in der LE-Umgebung noch G2-Karten in Benutzung sind, um den Anwender darauf hinzuweisen, dass diese ausgetauscht werden müssen.
- Im Signatur-Report werden Algorithmen, die potenziell unsicher sind, entsprechend gekennzeichnet. Die entsprechenden Enddaten wurden korrekt implementiert.
- Die Aktualisierung der TSL wird immer beim Neustart angestoßen und nicht, wie bisher, wenn die letzte Aktualisierung länger als 24 Stunden her ist.
- Der Wertebereich für den Parameter PinCommandTimeout ist auf 150 Sekunden erhöht werden.
- Mit dem Change C_11840 fordert die gematik, dass eine HBA-Karte, die bereits eine Kartensitzung zu einer anderen User-ID mit erhöhtem Sicherheitszustand hat, zunächst gemäß TUC_KON_024 zurückgesetzt wird. Erst danach wird wie gewohnt mit der Aktivierung der Komfortsignatur fortgefahren. Zuvor wurde dieser Fall mit einem Fehler abgebrochen. Die Änderung optimiert den internen Ablauf dahingehend, dass anstelle eines Abbruchs nun automatisch die Rücksetzfunktion der betroffenen Karte aufgerufen wird.
- Für Konnektoren, die ein ECC-Zertifikat besitzen ist es nicht mehr möglich, sich mittels RSA beim VPN Zugangsdienst zu registrieren.
- Die Spezifikation und das Verhalten im Konnektor wurde angepasst, sodass beim Aufruf von StopSignature geprüft wird, ob der verwendete Aufrufkontext die Berechtigung besitzt auf die Karte zuzureifen, welche zum Signatur-Job gehört.

- Beim Hochladen von Zertifikaten war es bisher noch möglich RSA-2048-Zertifikate hochzuladen. Dies wird nun gemäß Spezifikation unterbunden.
- Der Schalter zur Unterstützung der ECC Ciphersuiten im Rahmen von TLS („ECC-Ciphersuiten verwenden“) ist nach Installation der 6.0.8 Firmware aktiviert und kann auch nicht mehr deaktiviert werden. Beim Versuch der Deaktivierung und anschließendem Speichern wird eine Fehlermeldung ausgegeben.

- **Aktualisierung und Erweiterung GUI**
  - Zukünftig sollen für die Verbindung auf Port 8500 auch EC-Ciphersuiten verwendet werden. Dafür kann ein EC-Zertifikat erzeugt und an der Schnittstelle verwendet werden.
  - Die gematik hat spezifiziert, dass dem Nutzer der Fingerprint der TLS-Server-Zertifikate des Konnektors angezeigt werden soll. Hierfür wurde die Anzeige der Zertifikate für Nutzer erweitert.
  - Passwörter für Administratoren müssen nicht mehr zwingend in einem gewissen Zeitintervall geändert werden. Dafür gelten stärkere Regeln für die Passwörter. Nach dem Update ist eine zwangsweise Änderung des Passworts nicht mehr nötig. Darüber wird der Benutzer mit einer Info nach dem Update in der UI zusätzlich informiert.
  - Für KeyStores gibt es in der GUI eine Möglichkeit, dass die Passwörter für KeyStores mit einem entsprechend starken Passwort generiert werden können.
  - Die automatische Re-Registrierung mit ECC-Zertifikaten war bisher per default deaktiviert. Nun wird der Konfigurationswert mit dem Update automatisch aktiviert.

- **Anpassungen ePA**
  - Das Fachmodul ePA und alle damit verbundenen Funktionen im Basis-Konnektor wie SGD und VAU-Protokoll wurden entfernt.
  - Da das ePA-Fachmodul im Konnektor nicht mehr enthalten ist, wurde die zugehörige Konfiguration beim Firmware-Update entfernt und die ePA-Unterstützung generell aus dem Konnektor entfernt.

- **Erweiterung und Optimierung der Protokollierung**
  - Zur besseren Auswertung des Protokolls in Fehlerfällen bei der Kommunikation mit Kartenterminals wird nun ein Protokolleintrag

erzeugt, wenn die Verbindung zum Kartenterminal aufgrund eines Timeouts abgebrochen wird.

- **Erweiterung und Optimierung von Software-Komponenten**
  - Die Bouncy Castle Bibliothek wurde angepasst, um alle gematik- und BSI-Anforderungen zu erfüllen. Nun wird der neuste Stand der Bouncy Castle Bibliothek verwendet, um die TLS-Implementierung unterstützen zu können.
  - Im Rahmen dieser Anpassung wurde der RFC 7627 ("Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension") umgesetzt, d.h. beim TLS-Verbindungsaufbau wird die Extended Master Secret Extension verwendet.
  - Andere im AK verwendete Bibliotheken wurden, wo es nötig war, auf den aktuellsten Stand gebracht werden.
  - Die folgenden Komponenten wurden auf ihre jeweils aktuellste Version aktualisiert:
    - Bind 9.20.7
    - CCID 1.5.5
    - curl 8.13.0
    - DHCP 4.4.3-P1
    - GnuPG 2.4.7
    - ntp 4.2.8p18
    - OpenSSL 3.4.0
    - PC/SC 2.0.1
    - SQLite 3.49.01

- **Andere Optimierungen**
  - Für die Kommunikation der Keep-Alive-Nachrichten wird nun ein eigener Threadpool verwendet. Dadurch wird nicht länger der gleiche Threadpool wie für die Verarbeitung fachlicher Nachrichten genutzt, was zuvor das Zeitverhalten beim Senden der Keep-Alive-Nachrichten beeinträchtigen konnte.
  - Implementierung von Stabilisierungsmaßnahmen bei unerwartetem Aufhängen des Anwendungskonnektors.

Korrekturen gegenüber der Version 5.70.6

- Bisher wurde vor der Signaturprüfung eine strukturelle Auswertung des Payloads durchgeführt. In der 6.0.8 erfolgt die Signaturprüfung zukünftig immer vor jeglicher fachlichen oder strukturellen Verarbeitung des signierten Inhalts.
- Bei allen Operationen, die eine PIN-Eingabe erfordern (z. B. VerifyPIN, ChangePIN) wurde der Namespace in den Antworten korrigiert. Der Konnektor liefert in den Responses nun den korrekten Namespace gemäß CardService-Version 8.2.
- Wie bereits bei manuellen Updates wird nun auch bei automatischen Updates geprüft, ob Administrator-Zugangsdaten für das jeweilige Terminal hinterlegt sind. Nur dann wird das automatische Update eingeplant.
- Konnektoren mit sowohl RSA- als auch ECC-Zertifikaten auf der gSMC-K können künftig auch LZV-Pakete verarbeiten, die keine RSA-Zertifikate enthalten. In diesen Fällen wird der Download trotzdem als vollständig angesehen. Zusätzlich wird für alle Prüfungen im Konnektor künftig die Laufzeit der ECC-Zertifikate verwendet. Zudem wird sichergestellt, dass auch die Registrierung ohne gültige RSA-Zertifikate funktioniert.
- Mehrere technische Anpassungen sollen Verbindungsabbrüche zwischen dem AK und NK verhindern:
  - *Automatische Wiederherstellung:* Bei PCSC-Kommunikationsfehlern wird die Verbindung automatisch neu aufgebaut.
  - *TCP-Stabilität:* Aktivierung von Keepalive-Nachrichten, um Verbindungsabbrüche bei längeren Leerlaufzeiten zu vermeiden.
  - *Netzwerktreiberwechsel:* Umstellung vom „virtIO“-Treiber auf den stabileren Intel-Netzwerktreiber.
  - *Firewall-Optimierung:* Bestimmte Kommunikationsregeln (z. B. für MQTT, REST, PC/SC) wurden in einen statischen Bereich verschoben, damit sie auch bei Konfigurationsänderungen aktiv bleiben und Verbindungen bestehen bleiben.
- Es kam im Feld zu Fehlern, da eine Laufzeitverlängerung erneut angestoßen wurde, obwohl bereits laufzeitverlängerte Zertifikate verwendet wurden. Nun wird verhindert, dass auch beim Ablauf laufzeitverlängerter Zertifikate eine erneute Laufzeitverlängerung erfolgt.
- Beim TLS-Verbindungsaufbau mit EC-Zertifikaten wurde unter bestimmten Bedingungen ein Signaturalgorithmus für die CertificateVerify-Nachricht gewählt, der von einer frühen Serie der im

Konnektor eingebauten SMC-Ks nicht unterstützt wurde. Dies konnte zu Verbindungsabbrüchen, u.A. beim Zugriff auf VSDM Services führen und den Zugriff auf Kartenterminals verhindern. Nun erfolgt eine adäquate Filterung der Signaturalgorithmen bereits in der ClientHello-Nachricht.

- Bei der Validierung der Signaturalgorithmen für die BNetzA-VL wurde der Algorithmus SHA384_RSA_MGF1 abgelehnt, obwohl dieser zulässig und technisch möglich ist. Der Algorithmus wurde nun in die Liste der erlaubten Algorithmen aufgenommen.
- In der Operation CheckCertificateExpiration wurde bisher nicht die spezifizierten Fehlercodes zurückgegeben, wenn die adressierte Karte das adressierte Zertifikat nicht besessen hat. Dies wurde in dem PTV6-Release behoben.
- Wenn eine TSL bei einem manuellen Update nicht übernommen wurde, weil die TSL (ID + Sequenznummer) bereits im System enthalten ist, wurde bisher der Statuscode 200 zurückgegeben. Um eine klare Trennung herzustellen, wird nun der Fall
  - „die TSL wurde übernommen" mit dem Statuscode 200 beantwortet
  - und "die TSL enthält die gleichen IDs und wird daher nicht übernommen" mit dem Statuscode 204 beantwortet.
- Für einen ChangePin über ein Remote-Kartenterminal, wurde die APDU-Erstellung für dieses Kommando angepasst, damit es fehlerfrei mit allen Kartenterminals am Markt durchgeführt werden kann.
- Beim Protokollieren von Fehlern wurde ein Detailfeld bisher nicht gefüllt. Dies hat teilweise die Fehleranalyse erschwert. Nun wird das vorgesehene Feld auch befüllt.
- Unter bestimmten Umständen konnte es passieren, dass das Label der Kartenterminals im Infomodel auf den Hostname zurückgesetzt wurde. Dieses Verhalten wurde behoben.
- Eine Deregistrierung mit einer abgelaufenen SMC-B war bisher nicht möglich. Dieses Verhalten wurde durch die Korrekturen im PTV6-Release beseitigt.
- Die Fehlermeldung beim Registrieren, wenn die SMC-B noch nicht beim OCSP freigeschaltet wurde, war für User nicht interpretierbar. Nun wird dem User eine aussagekräftige Fehlermeldung präsentiert.
- Beim Löschen oder Ändern der Intranetroute kam es zu einem Fehler. Es wurde ein Fix implementiert, der Konflikte zwischen der Schnittstellenadresse und den Netzwerken korrekt erkennt und behandelt.

- In manchen Fällen wurde keine Zeitsynchronisation durchgeführt, wodurch auch keine Warn- oder Fehlerzustände (EC_NTP_TIMESYNC_PENDING_WARNING, ...CRITICAL) gesetzt wurden. Die Erkennung des Zeitsynchronisationsstatus wurde angepasst. Auch ohne vorhandene Statusdatei wird nun über eine „First Boot“-Datei korrekt erkannt, ob eine Synchronisation aussteht.
- Für die Prüfung von XML-Signaturen im Zusammenhang mit NFDM-Usecases wurden Konfigurationsparameter der Signatur-Komponente so angepasst, dass die Hash-Algorithmen, die in der TI über das Jahr 2025 hinaus erlaubt sind, ohne Warnung als erlaubt gelten.

Bekannte Fehler der Version

Die Firmware-Version 6.0.8 enthält keine bekannten Fehler.