Release Notes

Einboxkonnektor

secunet konnektor 5.50.3:2.0.0

Rechenzentrumskonnektor

secunet konnektor 5.50.3:2.1.0

Stand 10.08.2023 (deutsch)

Der Hersteller empfiehlt, sowohl Einbox- wie auch Rechenzentrumskonnektoren auf das Wartungsrelease Version 5.50.3 zu aktualisieren.

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 5.50.3 (PTV5#WR3) des secunet Konnektors setzt den Produkttypsteckbrief Konnektor 5.54.1-0 (PTV5Plus) der gematik um.

Besondere Hinweise zu dieser Version

- **Fachmodul Laufzeitverlängerung umgesetzt**
  In der Version PTV5#WR3 wird das Fachmodul Laufzeitverlängerung eingeführt. Mit der Laufzeitverlängerung ist es möglich Zertifikate der gSMC-K's eines Konnektors, welche vor dem 31.12.2025 ablaufen, durch verlängerte Zertifikate zu ersetzen.
  Hierbei unterstützt Sie in der Konnektoroberfläche eine interaktive Schritt-für-Schritt Anleitung, welche Sie mit einem Upgrade auf die Version PTV5#WR3 im Menü „System -> Laufzeitverlängerung" finden.
  Beachten Sie zudem die Hinweise in Kapitel 11.5 im Handbuch.
- **Lizenz zur Nutzung des Fachmoduls Laufzeitverlängerung**
  Um den Leistungsumfang des Fachmoduls Laufzeitverlängerung nutzen zu können, muss dieses lizenziert und freigeschaltet werden.

  Sofern bereits vorher auf dem Konnektor eine PTV1, PTV3, PTV4 oder PTV5 Lizenz lizenziert und freigeschaltet ist, können dessen

Funktionalitäten auch nach dem Update auf die Lizenz zur Laufzeitverlängerung weiterhin genutzt werden.

- **Downgrade von PTV5#WR3 auf niederwertige Versionen**
  Sollte der Update-Vorgang auf die Version PTV5#WR3 rückgängig gemacht werden müssen, so ist eine Rückkehr zu vorherigen Versionen generell möglich. Nach diesem (etwaigen) Downgrade muss die Konfiguration des Konnektors einem Review unterzogen werden.

  Wenn nach der Laufzeitverlängerung der Zertifikate (siehe Handbuch Kapitel 11.5) bereits die Registrierung beim VPN-Zugangsdienst mit diesen Zertifikaten erfolgt ist, dann ist kein Downgrade des Modularen Konnektors möglich, da es sonst zu inkonsistenten Zuständen bezüglich der Registrierung des Modularen Konnektors beim VPN-Zugangsdienst kommen kann. Ein Downgrade ist erst nach einer Deregistrierung der verlängerten Zertifikate möglich. Zudem sollte darauf geachtet werden, dass die Zertifikate, mit denen der Konnektor ab Werk ausgestattet ist, weiterhin registriert und gültig sind. Ist dies nicht der Fall, sollte von einem Downgrade abgesehen werden, da der Konnektor sonst nicht mehr lauffähig ist.

- **Problemlösung beim TLS-Verbindungsaufbau mit Kartenterminals**
  In der Konnektoroberfläche kann für den TLS-Verbindungsaufbau (TLS Handshake) mit Kartenterminals ein Timeout bis zu 60 Sekunden eingestellt werden. Jedoch wurde dieser vom Konnektor spätestens nach 10 Sekunden abgebrochen, auch wenn das Timeout höher als 10 Sekunden eingestellt ist. Dieses Verhalten wird in diesem Release behoben.

  Möchten Sie eine Cherry eGK-Tastatur des Modells G87-1505 mit einer höheren Produktversion als der 3.0.1:1.1.1 nutzen, empfehlen wir dringend die Nutzung dieser eGK-Tastaturen nur in Verbindung mit dem Release PTV5#WR3 oder höherwertigen. Ansonsten kann es durch das oben beschriebene Verhalten des Konnektors zu Inkompatibilitäten führen.

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/

- **Update von PTV4 bzw. PTV4Plus auf PTV5#WR3**
  Bei dem Update von der Produkttypversion 4 (PTV4) bzw. der Produkttypversion 4 Plus (PTV4Plus) auf die Produkttypversion 5 Wartungsrelease 3 (PTV5#WR3), empfiehlt der Hersteller, vor dem Update ein Backup der Konfiguration des Konnektors durchzuführen.

- **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 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 sicher zu stellen, dass die jeweils neueste Version der GUI verwendet wird.

- **TLS-Verbindungen (TLS 1.2)**
  Seit PTV3 unterstützt der Konnektor ausschließlich TLS 1.2. Die Verwendung von TLS 1.1 ist aufgrund der Abkündigung durch die gematik entfallen.

Neuerungen seit secunet konnektor Firmware 5.1.3

- **Lizenzierung Laufzeitverlängerung**
  Ist eine Laufzeitverlängerungs-Lizenz vorhanden, ist nun automatisch die Funktionalität Laufzeitverlängerung mit lizensiert.
- **Lizenzierung ePA 2.5**
  Ist eine ePA 2.0 Lizenz vorhanden, ist nun automatisch die ePA 2.5 Funktionalität mit lizensiert.
- **Einführung neuer Backup Typ**
  Der neue Backup Typ "Gesamtexport ohne Benutzer" erstellt ein Backup der gesamten Konfiguration ausgenommen der User-Konfiguration.
- **Voraussetzung „RSA-Zertifikate“ für eGK‘s entfernt**
  In Zukunft sollen eGK‘s auch ohne RSA-Zertifikate hergestellt werden. Damit diese genutzt werden können, erwartet der Konnektor im Umgang mit eGK’s ab sofort nicht mehr zwingend RSA Zertifikate.
- **Neuer Fehlercode für zu große Dokumente**
  Es wird ein neuer Fehlercode 4283 für zu große Dokumente bei den Operationen der Services Signature-Service und Encryption-Service eingeführt.
- **Optimierungen bei der Kommunikation mit Clients**
  Für die, vom Konnektor generierten EC PrivateKeys wurden bisher in den PrivateKeys, die Kurvenparameter der Kurve BrainpoolP256r1 explizit angegeben. Damit konnte mindestens ein Client nicht umgehen. Um dies zu verbessern, werden die Kurvenparameter in den PrivateKeys nun als Named-Curved-Parameter hinterlegt.
- **Optimierung des Zusammenstellens der Betriebsdaten**
  In bestimmten Konstellationen konnte es dazu kommen, dass beim Zusammenstellen der Betriebsdaten es zu einer Exception beim Zugriff auf die Daten gekommen ist, da nicht alle Informationen vorlagen.

  Fehlende Informationen im Schema als optional definierte Felder führen jetzt nicht mehr zum Abbruch des Vorgangs.

- **Anpassung unterstütze Kurven für TLS-Verbindungen**
  Unterstützung der NIST Kurve P256 für Zertifikate für die TLS-Verbindungen.
- **Anpassung Prüfung Aufrufkontext StopSignature**
  Bei der Operation StopSignature wird nun geprüft, dass dessen Aufrufkontext dem Aufrufkontext aus dem Operationsaufruf von SignDocument für den jeweiligen Signaturauftrag entspricht.
- **Entfernung Ciphersuiten**
  Ciphersuiten TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA und TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA als erlaubte Ciphersuiten entfernt (für alle Verbindungen).
- **Verknüpfung Autoupdates zwischen KT und Konnektor**
  Die Ausführung von Autoupdates der Terminals und des Konnektors waren bisher miteinander verknüpft. Nun erfolgen die Terminal-Updates auch automatisch (sofern konfiguriert), wenn kein Konnektor-Update ansteht.
- **Anpassungen aufgrund Änderungen der gematik Spezifikation**
  - Die Betriebszustände EC_FW_Update_Available, EC_NK_Certificate_Expiring und EC_NK_Certificate_Expired wurden in der Spezifikation ergänzt und sind somit auch im Konnektor umgesetzt.
  - Gemäß Spezifikationsanpassungen soll es möglich sein, die ClientAuthentification für den TLS Verbindungsaufbau (aktiviert/deaktiviert) bei den LDAP Verbindungen separat zu konfigurieren. Dies ist nun möglich.
  - Gemäß Spezifikationsanpassungen, gilt für SignDocument und EncryptDocument nun eine harte Grenze von genau 25 MB. Der Grenzwert wurde entsprechend reduziert.
  - Gemäß Spezifikationsanpassungen, soll das Zertifikatsprofil C.ZD.SIG auch vom Konnektor unterstützt werden. Daher wurde das Profil bzw. die zugehörigen OIDs entsprechend mit aufgenommen.
  - Gemäß Spezifikationsanpassungen, soll bei der im Fehlerfall protokollierte ICCSN die letzten 10 Zeichen ausgeblendet (Ersatz durch 'X') werden. Die Anpassung der ICCSN erfolgt vor der Protokollierung.

- Im ePA EncryptedKeyContainer muss laut Spezifikation eine andere Algorithmus ID verwendet werden. Diese wird nun verwendet.
- Gemäß Spezifikationsanpassungen, gibt es den neuen IHE Fehler PolicyViolation, der nun entsprechend im Fachmodul ePA behandelt wird.

- **Optimierungen/Erweiterungen bei der Protokollierung**
  - Die Protokollierung bei IP-RenewRetry war unvollständig. Nun werden alle relevanten Informationen protokolliert.
  - Wenn in einer OCSP-Response die Signatur komplett gefehlt hat, wurde nicht der Fehlercode 1031 "Signatur der Response ist nicht gültig." protokolliert, sondern nur ein generischer Fehler, dass die OCSP-Response ungültig ist. Nun wird auch in diesem Fall der Fehlercode 1031 protokolliert.
  - Auftretende CardTerminalExceptions beim Auslesen der Terminalinformationen wurden im Vergleich zu anderen RuntimeExceptions anders behandelt. Dies hat dazu geführt, dass bei einer CardTerminalException der Fehlercode 4040 nicht protokolliert wurde. Um die Fehleranalyse zu verbessern, werden nun alle RuntimeExceptions gleichbehandelt.
  - Zusätzliche Protokollierung von fehlgeschlagenen Login-Versuchen.
- **Anpassungen/Erweiterungen Betriebszustände**
  - Einige Betriebszustände finden sich in der Spezifikation in unterschiedlichen Schreibweisen (mit enthaltenen Leerzeichen und auch ohne). Die gematik hat klargestellt, dass die Schreibweise mit Leerzeichen verwendet werden soll. Daher wird nun diese Schreibweise verwendet.
  - Zur Anzeige, dass erneuerte Zertifikate für die Verbindung zum Clientsystem bzw. zur TI vorhanden sind, wurden die Betriebszustände EC_OTHER_ERROR_STATE(4) und EC_OTHER_ERROR_STATE(5) definiert.
  - Betriebszustände mit der Severity FATAL, ERROR und WARNING führen nur noch zu einer Aktivierung der Service-LED

- **Optimierung bei der Kommunikation mit einem Aktensystem**
  Bei der Kommunikation mit den Aktensystemen kann es dazu kommen, dass diese nicht mit einem normalen SOAP-Fault antworten. Sie antworten dann mit einer HTTP-Antwort, die im Body zwar ein SOAP-Fault enthält, aber als HTTP-Responsecode etwas anderes als 200, 400 oder 500 zurückgibt. Diese Rückgabe wird normalerweise nicht als SOAP-Fault erkannt, sondern "nur" als HTTP-Fehlermeldung die dann zu einer anderen Exception führt, bei der der Body nicht weiter ausgewertet wird.

  Um diese Responses dennoch weiter verarbeiten zu können, wurde die Konfiguration des SOAP-Frameworks im Code entsprechend angepasst.

- **Optimierte Fehlermeldung beim Alternativen-Login**
  Wenn für den Alternativen-Login bzw. Werksreset die vom User eingegeben Response abgelaufen ist, hat sich die Fehlernachricht nicht von der Fehlermeldung unterschieden, wenn die Response falsch eingegeben wurde.

  Nun wird eine differenzierte Fehlermeldung zurückgegeben, um den User eine bessere Rückmeldung bzgl. der Fehlersituation anzeigen zu können.

- **Zugriff auf SDS bei deaktiviertem TLS-Mandatory**
  Wenn TLS-Mandatory nicht aktiviert war, musste dennoch explizit für den SDS-Zugriff TLS-Mandatory deaktiviert werden damit ein Zugriff über HTTP auf den SDS möglich war.

  Gewollt ist, dass bei deaktiviertem TLS-Mandatory ein Zugriff auf den SDS automatisch möglich ist. Dies ist nun der Fall, da beide Konfigurationen ausgewertet werden.

- **Rücknahme der Konnektorfreischaltung ohne Deregistrierung beim VPN-Zugangsdienst**
  Es kann Situationen geben, in denen der Konnektor sich nicht mehr beim VPN-Zugangsdienst deregistrieren konnte (keine Internetverbindung aus der Praxis vorhanden, keine gültige SMC-B mehr vorhanden, usw.). Auch in solchen Situationen soll es möglich sein, die Registrierung im Konnektor lokal zu entfernen, so dass der Konnektor keine TI-Verbindung mehr aufzubauen versucht.

  Dies ist nun möglich und wird als zusätzliche Option zur Freischaltung in der Oberfläche angeboten. Weitere Informationen finden Sie im Kapitel 9.6.2.3 des Handbuches.

- **Aktualisierung/Erweiterung GUI**
  - Die GUI wurde bzgl. der neuen Schnittstellen und Betriebszustände aktualisiert.
  - Für die Clientsystem-Zertifikate wird dem Benutzer bereits in der GUI direkt das Ablaufdatum dieser Zertifikate angezeigt
- **Optimierung VSDM**

  Bisher wurden die Vorgangsnummern nur aus einer UUID gebildet. Ebenso haben nur von extern angestoßene Prozesse eine eigenständige Vorgangsnummer bekommen. Intern getriggerte Prozesse (wie z.B. die tägliche Prüfung der TSL) haben immer die gleiche Vorgangsnummer gehabt.

  Dies wurde angepasst. Die Vorgangsnummer hat nun einen Präfix, über den sich ableiten lässt, wodurch der Vorgang getriggert wurde (SOAP, REST, etc.). Zusätzlich wird für die verschiedenen internen Prozesse nun auch eine eigene Vorgangsnummer vergeben. Somit können Vorgänge anhand der Protokollierung besser nachvollziehen werden.
- **Optimierung/Erweiterung ePA Funktionalitäten**
  - Bei Fehlerfällen bzgl. der Kommunikation mit ePA Aktensystemen (inkl. SGD) soll der Operationsname mit protokolliert werden, um die Fehlermeldungen besser den einzelnen Diensten bzw. den Operationen zuordnen zu können und somit die Fehleranalyse zu erleichtern. Daher wird im Fehlerfall der Operationsnamen nun mitprotokolliert.
  - Der Organisationsname sowie der Vor- und Nachname werden bei der Operation RequestFacilityAutorisation via SOAP übergeben um dann unter anderem am Kartenterminal Display genutzt zu werden. Da es sich dabei um extern bereitgestellte Daten handelt, werden diese vor der Verarbeitung auf nicht erlaubte Zeichen geprüft und die Anzeige verboten. Die Validierung wurde angepasst, so dass nun alle Zeichen, die am Terminal angezeigt werden können auch akzeptiert werden. Steuerzeichen werden weiterhin abgelehnt. Nicht darstellbare Zeichen werden, wie von der gematik gewünscht, ersetzt**.**
  - Bisher wurden Fehlerantworten von den Aktensystemen lediglich protokolliert, aber nicht dem eigentlichen Aufrufer bereitgestellt. Anstelle der Antwort wurde lediglich ein FM ePA spezifischer Fehlercode ausgegeben. Nun wird die empfangene Exception bzw. gematik Error-Information weitergeleitet, um diese Information

spezifikationskonform dem User auch im ErrorTrace anzeigen zu können.

- Durch die Vererbungshierarchie haben sich alle Aktensystem-Clients auf Events für das Update von Konfigurationen registriert. Dieses hat dazu geführt, dass auch die PhrDocumentService-Clients, welche pro Aufruf neu erzeugt werden, sich für die Events registriert haben. Somit gab es für diese Clients immer eine bestehende Referenz, weswegen sie nicht aus dem Speicher entfernt werden konnten.
  Die Implementierung im Fachmodul wurde so angepasst, dass die Clients, die nur einmalig erzeugt werden, nun explizit von einer Klasse erben die auf Konfigurationsänderungen reagiert. Die PhrDocumentService-Clients gehören nicht dazu, womit auch keine Referenz mehr auf diese, nach der eigentlichen Nutzung, besteht.

Korrekturen gegenüber der Version 5.1.3

- **Anpassung Konnektor-Selbsttest**
  Die Komponente ‚connector-selftest' wird sowohl beim initialen Start des Konnektors als auch alle 24 Stunden ausgeführt. In beiden Fällen führt ein fehlgeschlagener Test zum Herunterfahren des Konnektors. Der Test, welcher alle 24 Stunden periodisch ausgeführt wird, wird jeweils um 6:00 Uhr morgens ausgeführt.
  Aus dem Feld wurde gemeldet, dass einige Modulare Konnektoren sich um 6:00 morgens abschalten. Eine Analyse des Herstellers hat gezeigt, dass dieses Fehlverhalten an der Komponente ‚connector-selftest' ausgemacht werden konnte.
  Der Selbsttest wurde so angepasst, dass dieses Fehlverhalten behoben werden konnte.
- **Darstellung Terminal Versionsnummer**
  Die ManufacturerData der Terminals wurden bisher nicht korrekt ausgewertet, so dass die Versionsnummern ggf. falsch dargestellt wurden. Nun wird ManufacturerData korrekt interpretiert.
- **Problemlösung beim TLS-Verbindungsaufbau mit Kartenterminals**
  In der Konnektoroberfläche kann für den TLS-Verbindungsaufbau (TLS Handshake) mit Kartenterminals ein Timeout bis zu 60 Sekunden eingestellt werden. Jedoch wurde dieser vom Konnektor spätestens nach 10 Sekunden abgebrochen, auch wenn das Timeout höher als 10

Sekunden eingestellt ist. Dieses Verhalten wird in diesem Release behoben.

- **Status der QES-PIN**
  Der erwartete Status der QES-PIN nach dem Aktivieren der Komfort-Signatur ist VERIFIED. Der Status wurde bisher allerdings als VERIFIABLE ausgegeben, wenn vorher noch der Status der PIN.CH abgefragt wurde. Die internen Abläufe wurden angepasst, so dass nun der erwartete Status ausgegeben wird.

- **Automatisches Zurücksetzen vom Betriebszustand für Karten**
  Der Betriebszustand EC_CARD_PROTOCOL_ERROR_RESET (Unerwarteter Fehler bei der Kommunikation mit einer Karte, der zum Zurücksetzen der Karte führt) konnte nur durch einen Neustart des Konnektors wieder zurückgesetzt werden.

  Nun kann der Administrator dies zurücksetzen, bzw. wird der Betriebszustand automatisch zurückgesetzt, sobald wieder eine normale Kommunikation mit der zurückgesetzten Karte erfolgt.

- **Nutzung von eingebetteter OSCP Response**
  Die in der Signatur enthaltene OCSP-Response wurde immer verworfen und es wurde stattdessen immer eine eigene OCSP-Anfrage für das Signer-Zertifikat erstellt. Nun wird, wenn die vorgegeben Bedingungen eingehalten werden auch die eingebettete OCSP-Response verwendet.

- **Beibehaltung des Betriebszustandes bis gültige TSL eingespielt**
  Bei einer abgelaufenen TSL, können neuere aber dennoch abgelaufene TSLen eingespielt werden (um die TSLen für einen möglicherweise notwendigen Vertrauensankerwechsel trotzdem noch einspielen zu können). Dies hat dazu geführt, dass der Betriebszustand bzgl. der abgelaufenen TSL kurzfristig zurückgesetzt wurde, obwohl auch die neue TSL bereits abgelaufen war. Nun wird in dem Fall der Betriebszustand beibehalten, bis ein aktuell gültige TSL eingespielt wird.

- **Beibehaltung der ECC-Einstellung für TLS-Verbindungen**
  Gemäß Spezifikation wurde die Konfiguration EccUseForClientSystem-ConnectionEnabled eingeführt, dessen Defaultwert „false“ ist. Vorher gab es nur den Konfigurationsschalter EccCipherEnabled, der für alle TLS-Verbindungen galt.
  Wurde EccCipherEnabled vor dem Update auf die Firmware 5.1.0 (oder höher) auf true gesetzt, so wurden bereits ECC-Ciphersuiten gegenüber den Clientsystemen verwendet. Mit einem Update auf die Firmware 5.1.0 (oder höher) und der damit verbunden Einführung von EccUseForClientSystemConnectionEnabled, wurden dann für den User

unerwartet, die ECC-Ciphersuiten gegenüber den Clientsystemen nicht mehr verwendet.
Nun werden weiterhin ECC-Ciphersuiten nach einem Update verwendet, da die Konfiguration EccUseForClientSystemConnectionEnabled bei einem Firmwareupdate aktiviert wird, insofern EccCipherEnabled vorher aktiviert war.

Bekannte Fehler der Version

- Aktuell sind keine Fehler bekannt.

Sonstige Hinweise zum Update von den Versionen PTV1/3/4 auf PTV5#WR3

Der nachfolgende Hinweis ist bei einem Update von den Versionen 2.0.47 (PTV1) bzw. 3.5.0, 3.5.2, 3.5.3 (PTV3) bzw. 4.1.3 (PTV4) auf 5.50.3 (PTV5#WR3) zu beachten.

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

- **Elliptische Kurven-basierte SSD-Verschlüsselung**
  Nach erfolgtem Update von einer Version vor PTV4 auf die Version 5.50.3 (PTV5#WR3) des Konnektors findet eine für den Benutzer transparente, einmalige und automatische Umstellung der SSD-Verschlüsselung von RSA auf Elliptische Kurven statt. Für etwaige Downgrades des Konnektors wird der RSA-Schlüssel parallel zum Elliptischen Kurvenschlüssel auf der gSMC-K beibehalten. Alle gSMC-Ks aller Konnektor-Versionen partizipieren automatisch an diesem neuen Verfahren.
- **Einspielen eines Backups einer Firmwareversion vor PTV4Plus**

  Beim Einspielen eines mit der Version 4.1.3 oder älter erstellten Backups sind die Einstellungen bzgl. der automatischen Installation nicht enthalten.

  Die allgemeinen Werte für die automatische Installation werden daher beim Einspielen des Backups auf die Standardwerte der PTV5#WR3-Version eingestellt.

  Mit dem Backup könnten auch Terminalkonfigurationen hinzugefügt worden sein, die bisher nicht bekannt waren. Für diese Terminals wird gemäß den Vorgaben der gematik die Auto-Update Funktionalität aktiviert.