Konnektor DNSSEC-Workaround (secunet & RISE)

Oct 13, 2026 · @Skola

Hintergrund

secunet- und RISE-Konnektoren bauen nach einem Neustart keine VPN-Verbindung zur TI mehr auf. Abhilfe schafft der manuell hinterlegte Root-Trust-Anchor KSK-2024 (Key Tag 38696).

- **Ursache:** Am 11.10.2026 hat die DNS-Root-Zone auf den neuen Schlüssel KSK-2024 umgestellt. Im Konnektor ist nur der alte Anker hinterlegt, deshalb scheitert die DNSSEC-Prüfung (SERVFAIL).
- **Laufende Konnektoren:** Sie arbeiten mit bereits geprüften Daten weiter. Der Fehler tritt erst nach einem Neustart oder einer Zwangstrennung auf.
- **Betroffen:** Konnektoren von secunet und RISE.
- **Grundregel bis zur Herstellerlösung:** Nicht neu starten, das automatische Firmware-Update aktiviert lassen.
- **Erprobt:** Am 13.10.2026 bei einem RISE-Konnektor mit Firmware 6.1.3 erfolgreich umgesetzt.

Diagnose

Das Problem liegt vor, wenn im Konnektor-Log Fatal-Einträge 4180 mit SERVFAIL vom lokalen Resolver (127.0.0.1) auf TI-Namen stehen.

Code	Meldung (Beispiel)	Bedeutung
4180	`NoNameservers ... _isakmp._udp.ti-extern.<Zugangsdienst>.service-ti.de IN SRV: Server 127.0.0.1 UDP port 53 answered SERVFAIL`	Hauptfehler: VPN-Zugangsdienst nicht auflösbar
4180	`... _ldap._tcp.vzd.telematik. IN PTR ... SERVFAIL`	Folgefehler: Verzeichnisdienst nicht auflösbar
30059 / 30060	Keine Liste von LDAP-Servern / keine LDAP-Verbindung	Folgefehler ohne VPN-Tunnel

Vor jeder Änderung:

1. Firmware-Version notieren (Konnektor-Oberfläche oder `http://<Konnektor-IP>/connector.sds`).
2. Konfigurationssicherung erstellen.
3. Keinen Werksreset durchführen, dabei geht die Registrierung verloren.

Workaround secunet

Bei secunet wird der Anker als XML-Block in die Einstellungen des VPN-Zugangsdienstanbieters eingetragen (Vorgabe der gematik).

1. An der Administrationsoberfläche des Konnektors anmelden.
2. **VPN → VPN-Zugangsdienst → VPN-Zugangsdienstanbieter** öffnen.
3. Den Eintrag **„DNSSEC Trustanchor Internet“** bearbeiten und den Inhalt komplett durch das XML unten ersetzen.
4. Speichern.
5. Den Konnektor vollständig neu starten. Das ist zwingend.

Das XML aus diesem Codeblock kopieren und nicht aus dem gematik-PDF, dort entstehen beim Kopieren Leerzeilen und Umbrüche.

```
<?xml version="1.0" encoding="UTF-8"?>
<TrustAnchor id="0AF79DEA-A7CD-43DC-9EDD-AD241CA63AE2"
source="http://data.iana.org/root-anchors/root-anchors.xml">
<Zone>.</Zone>
<KeyDigest id="Kjqmt7v" validFrom="2010-07-15T00:00:00+00:00">
<KeyTag>19036</KeyTag>
<Algorithm>8</Algorithm>
<DigestType>2</DigestType>
<Digest>49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5</Dig
est>
</KeyDigest>
<KeyDigest id="Klajeyz" validFrom="2017-02-02T00:00:00+00:00">
<KeyTag>20326</KeyTag>
<Algorithm>8</Algorithm>
<DigestType>2</DigestType>
<Digest>E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D</Dig
est>
</KeyDigest>
<KeyDigest id="xHj5DzE" validFrom="2015-09-14T00:00:00+00:00">
<KeyTag>9239</KeyTag>
<Algorithm>8</Algorithm>
<DigestType>2</DigestType>
<Digest>2ab7a6a7baec0799040a5a95a50bdad685a2654300892c34854db0315a9d4042</Dig
est>
```

```
</KeyDigest>
<KeyDigest id="Kmyv6jo" validFrom="2024-07-18T00:00:00+00:00">
<KeyTag>38696</KeyTag>
<Algorithm>8</Algorithm>
<DigestType>2</DigestType>
<Digest>683D2D0ACB8C9B712A1948B27F741219298D0A450D612C483AF444A4C0FB2B16</Dig
est>
</KeyDigest>
</TrustAnchor>
```

Workaround RISE

Bei RISE werden die Root-Schlüssel als einzelne Felder unter den manuellen Trust-Anchors eingetragen. Eine offizielle RISE-Anleitung gab es bei Erstellung noch nicht. Der Weg ist übertragen vom secunet-Workaround und am 13.10.2026 mit Firmware 6.1.3 erprobt.

1. An der Konnektor-Oberfläche anmelden.
2. **Netzwerk → DNS → Reiter „Trust-Anchors“** öffnen.
3. Unter „Manuell konfigurierte Trust-Anchors“ mit **+** zwei Zeilen anlegen (Werte aus der Tabelle unten).
4. **Speichern**, dann den Konnektor neu starten.

Zone	Key Tag	Algorithmus	Digest Type	Digest
`.`	38696	8	2	`683d2d0acb8c9b712a1948b27f741219298d0a450d612c483af444a4c0fb2b16`
`.`	20326	8	2	`e06d44b80b8f1d39a95c0b0d7c65d08458e880409bbc683457104237c7f8ec8d`

- Die Zone ist nur ein Punkt, die Root-Zone.
- 38696 ist der neue Schlüssel (KSK-2024) und der entscheidende Eintrag. 20326 (KSK-2017) kommt nur zur Sicherheit dazu.
- Den Digest prüfen: Am Anfang und am Ende darf kein Leerzeichen stehen.
- **Nicht** „RFC5011-Aktualisierungen zurücksetzen“ drücken.
- Den Bereich „Trust-Anchors aus TSL“ (Zone `telematik.`) nicht anfassen.

Funktionsprüfung

Der Workaround hat gegriffen, wenn die VPN-Verbindung zur TI „Verbunden“ zeigt und das Einlesen einer Versichertenkarte in der Praxis klappt.

- [ ] VPN-Verbindung zur TI „Verbunden“. SIS „Getrennt“ ist normal, wenn die Praxis den Sicheren Internet Service nicht gebucht hat.
- [ ] Im Log stehen keine neuen 4180-Fehler (DNS) und keine 30059/30060-Fehler (LDAP).
- [ ] Betriebszustand ohne aktive Fehler, Kartenterminals verbunden, SMC-B freigeschaltet.
- [ ] Test in der Praxis: Versichertenkarte einlesen, Signatur bzw. E-Rezept mit Heilberufsausweis.

Diese Meldungen sind in den ersten Minuten nach dem Neustart normal und verschwinden von selbst:

Meldung	Bedeutung
Firewall-Regelset beim Aufbau der VPN-Verbindung geändert / Firewall neu geladen	Der Tunnel ist aufgebaut, die TI-Regeln werden gesetzt
`EC_FeatureOrTUC_Not_Available` (GetCards, GetPinStatus, VerifyPin)	Die Dienste fahren noch hoch, das Praxisverwaltungssystem fragt zu früh an
30014 Socket-Lesefehler	Die Kartenterminals verbinden sich neu
4257 RSA-Zertifikat nicht vorhanden auf Karte	Karte nur mit ECC-Zertifikat, harmlos

Treten diese Fehler nach 5–10 Minuten noch auf, Kartenterminals und SMC-B gezielt prüfen.

Vorbeugung und Nachgang

Konnektoren, die noch verbunden sind, bekommen den Anker vorbeugend. So ist ein späterer Neustart kein Risiko mehr.

- **Vorbeugend:** Den Anker eintragen und speichern, den Neustart danach in Absprache mit der Praxis außerhalb der Sprechzeiten.
- **Ticket:** Im Ticket als manuelle Abweichung dokumentieren, mit Einrichtung, Konnektortyp und Firmware-Version.
- **Nach dem Hersteller-Update:** Sobald secunet bzw. RISE eine offizielle Lösung ausliefert, prüfen, ob der manuelle Eintrag entfernt werden soll.
- **Auf dem Laufenden bleiben:** gematik Fachportal, Seite „Wartungen & Sonstige Informationen“, auf eine RISE-spezifische Anleitung prüfen.

Quellen

- gematik TI-Status, inkl. Workaround-PDF für secunet (12.10.2026)
- IANA root-anchors.xml, zum Gegenprüfen der Digests
- VonDoczuDoc: Analyse SERVFAIL / Trust Anchor
- KZV Sachsen-Anhalt: Aktuelle Störung TI
- Cloudflare: Root KSK-2024 Rollover