FAQ – Umstellung der Verschlüsselungsalgorithmen RSA/ECC

Version 1.00, Stand: 06.08.2025

Inhalt

1. Was ist RSA/ECC?

RSA und ECC sind zwei verschiedene Verschlüsselungsverfahren, die in der Telematikinfrastruktur (TI) eingesetzt werden, um Daten sicher zu übertragen und zu schützen. Diese Verfahren sind Teil der technischen Sicherheitsgrundlage der TI und kommen in verschiedenen Komponenten und Diensten des Gesundheitswesens zum Einsatz. Die Umstellung von RSA auf ECC ist Teil der Weiterentwicklung der TI hin zu noch höheren Sicherheitsstandards.

2. Muss der Wechsel von RSA auf ECC erfolgen, wenn ja warum?

Ja, der Umstieg vom Verschlüsselungsalgorithmus RSA2048 auf ECC256 ist eine zentrale Maßnahme, um sicherzustellen, dass die Komponenten und Dienste der TI auch künftig den höchsten Sicherheitsstandards entsprechen. Hintergrund ist eine Vorgabe des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der Bundesnetzagentur in Deutschland.

3. Wann läuft die Gültigkeit des aktuellen Verschlüsselungsalgorithmus ab?

Die Gültigkeit des aktuellen Verschlüsselungsalgorithmus RSA2048 läuft zum 31. Dezember 2025 aus und muss auf das neue Verfahren ECC256 umgestellt werden. Dieses gilt als sicherer und effizienter als RSA2048.

4. Kann meine Praxis einen Konnektor mit nur RSA-Identität nach dem 31.12.2025 noch nutzen?

Nein, das RSA-Gerätezertifikat läuft zum Jahresende nach einer zweijährigen Verlängerung aus und ist damit ungültig.

5. Welche Komponenten sind von der Umstellung betroffen?

- Konnektor
- Heilberufsausweis (eHBA)
- Praxisausweis SMC-B (Security Module Card Typ B)
- e-Health-Kartenterminal und (gSMC-KT)
- Praxisverwaltungssystem (PVS) und KIM

Für weitere Informationen verweisen wir auf die Seite der gematik. Sie sollten die oben genannten Komponenten von Ihrem zuständigen Dienstleister vor Ort zeitnah prüfen lassen.

6. Was passiert, wenn ich den Tausch bzw. Wechsel zum TI-Gateway nicht vornehmen lasse?

Der Austausch des Konnektors bzw. der Wechsel zum TI-Gateway ist zwingend erforderlich, da mit Ablauf des Zertifikates keine Anbindung mehr zur TI besteht und Anwendungen wie eRezept, eAU, KIM etc. nicht mehr genutzt werden könnten.

7. Wer übernimmt die anfallenden Kosten für den Wechsel/Tausch?

Der Austausch von Komponenten (Konnektor, Wechsel zu TI-Gateway, SMC-B Karten etc.) ist möglicherweise mit Kosten verbunden, die über die monatliche TI-Pauschale refinanziert werden. Einmalige Einrichtungs- und Hardwarekosten können von der KVB nicht erstattet werden.

8. Ist eine Zertifikatsverlängerung des Konnektors möglich?

Sofern die Laufzeit des Sicherheitszertifikates Ihres Konnektors bereits in der Vergangenheit bis 31.12.2025 verlängert wurde, ist keine weitere Laufzeitverlängerung mehr möglich. Perspektivisch ist der neue TI-Zugang über das TI-Gateway das Mittel der Wahl auf dem Weg in die TI 2.0.

Für Konnektoren, die in den Jahren 2020, 2021 und 2022 produziert wurden, wird ein **anwenderfreundliches Verfahren zur Verlängerung der ECC-Zertifikate** eingesetzt. Die Zertifikate werden um jeweils drei Jahre verlängert. Somit haben diese Konnektoren dann eine maximale Laufzeit von 8 Jahren. Dieses Verfahren bietet eine Alternative zur Anschaffung neuer Konnektoren.

Praxen sollten sich rechtzeitig bei den jeweiligen Anbietern/Servicepartnern über die möglichen Optionen informieren.

9. Bis wann kann der Einbox-Konnektor genutzt werden?

Die Nutzung von Einbox-Konnektoren ist maximal bis Ende 2030 möglich. Das haben die Gesellschafter der gematik am 26. Juni 2025 beschlossen. Hintergrund ist die Weiterentwicklung der Verschlüsselungstechnik für Gesundheitsdaten und eine entsprechende Begrenzung der aktuell verwendeten Zertifikate. Die Laufzeit der Konnektoren, die heute neu eingesetzt werden, enden demnach ohnehin bis spätestens 2030.

Was ist der TI-Gateway?

Mit dem TI-Gateway wird in den Praxen kein Konnektor mehr vor Ort für die TI-Anbindung benötigt. Die Nutzer verbinden sich per sicherem VPN-Zugang mit einem Rechenzentrum, dort steht in geschützter Umgebung ein Hochleistungskonnektor. Dieser wurde von der gematik geprüft und zugelassen und ersetzt mit seiner Leistungsfähigkeit eine Vielzahl an Konnektoren. Konfigurationen, Wartungsarbeiten und das Einspielen neuer Updates erfolgen zentral und werden durch den von der gematik zugelassenen Anbieter durchgeführt.

10. Was sind die Vorteile des Wechsels zum TI-Gateway?

Das TI-Gateway bietet eine leistungsstarke und benutzerfreundliche Möglichkeit, sich mit der TI zu verbinden – ganz ohne eigene Konnektoren vor Ort. Es zeigt, wie die TI in Zukunft einfacher und flexibler genutzt werden kann. Bereits zur Jahresmitte sind über das TI-Gateway mehr als 8.000 virtuelle Konnektoren im Einsatz. Diese verbinden nicht nur Arztpraxen und Apotheken, sondern auch größere Einrichtungen wie Krankenhäuser, Medizinische Versorgungszentren und neue Nutzergruppen wie Pflegeeinrichtungen sicher mit der TI. Die technische Prüfung der

Vertrauenswürdigkeit bleibt weiterhin bestehen, um den Schutz sensibler Gesundheitsdaten zu gewährleisten. Mit dem Übergang zur TI 2.0 entsteht eine digitale Infrastruktur, die sich besser an die Anforderungen der Versorgungspraxis anpasst. Aufwändiger IT-Support für die Installation oder Wartung physischer Konnektoren ist nicht mehr notwendig – ein Vorteil insbesondere für kleinere Einrichtungen, für die dies bisher eine Hürde darstellte.

11. Wo erhalte ich weitere Informationen?

Für weiterführende Informationen können Sie sich direkt an Ihren TI-Anbieter oder IT-Servicepartner wenden. Zusätzlich empfehlen wir folgende Informationsquellen der gematik:

- https://www.gematik.de/telematikinfrastruktur/rsa2ecc-migration
- Laufzeitverlängerung | gematik

Weitere Informationen finden Sie auch auf der Themenseite "Telematikinfrastruktur" der KVB-Website.