Auf einen Blick

gematik
Nationale Agentur für Digitale Medizin

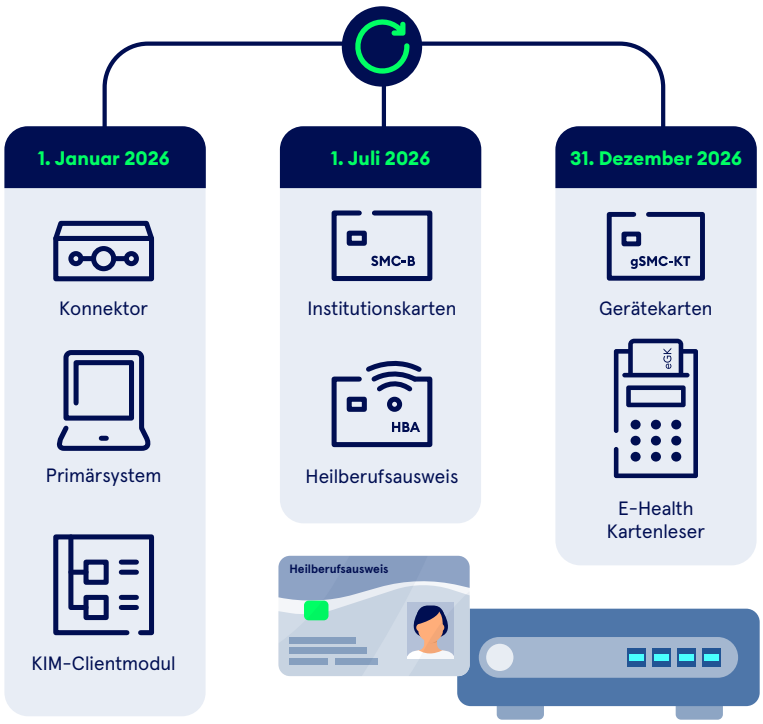
TI-Verschlüsselung: Umstellung von RSA auf ECC

Informationen für Praxen, Kliniken und Apotheken
seit 1. Januar 2026

Warum erfolgt die Umstellung?

Seit dem 1. Januar 2026 sollte RSA in der TI nicht mehr verwendet werden – ein sicherer TI-Zugang ist ausschließlich mit ECC-Verschlüsselung gewährleistet.

Hintergrund: Seit dem 1. Januar 2026 gilt für die Telematikinfrastruktur (TI) der moderne und kryptographisch sichere Elliptic-Curve-Cryptography-Verschlüsselungsalgorithmus (ECC), der den bisherigen Standard Rivest-Shamir-Adleman (RSA) ablöst. Grundlage sind Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der europäischen eIDAS-Verordnung.

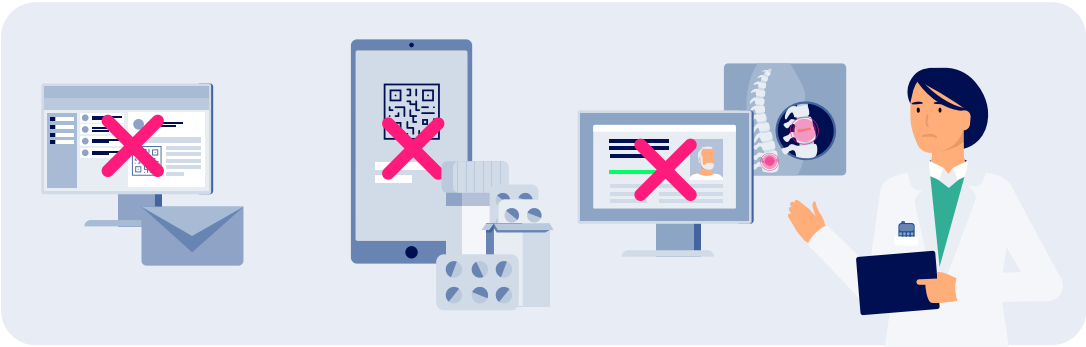


Was bedeutet das für Praxen, Kliniken & Apotheken?

TI-Komponenten, insbesondere **Konnektor, Primärsystem & KIM-Clientmodul,** sollten auf ECC umgestellt sein bzw. durch ECC-fähige Komponenten ersetzt worden sein. Für Einrichtungen, die noch Komponenten nutzen, die ausschließlich RSA-fähig sind, kann es seit dem 1. Januar 2026 zu Beeinträchtigungen im TI-Betrieb kommen.

Spätestens ab dem 1. Juli 2026 müssen **Heilberufsausweise (HBA) und Institutionskarten (SMC-B-Karten)** auf ECC umgestellt sein.

Gerätekarten für die Kartenterminals (gSMC-KT) müssen bis zum 31. Dezember 2026 ECC-fähig sein.



Was sind mögliche Folgen aufgrund nicht umgestellter Komponenten?

Betroffene Systeme können nicht mehr auf die TI zugreifen, z. B.:

- E-Rezept kann nicht erzeugt, signiert oder abgerufen werden.
- eAU kann nicht übertragen werden.
- KIM-Nachrichten können nicht abgerufen oder versendet werden.
- TI-basierte Authentifizierung schlägt fehl.
- Apotheke kann Verordnungen nicht beliefern.
- ePA kann nicht abgerufen werden.

Was ist im Problemfall zu tun?

Eine Überprüfung der ECC-Fähigkeit und der Konfiguration der Komponenten sollte umgehend eingeleitet werden. In der Zwischenzeit sollte auf bekannte Ersatzverfahren zurückgegriffen werden.

Schritt 1

IT-Dienstleister vor Ort kontaktieren

Schritt 2

Prüfen lassen:

- Ist der Konnektor bereits auf ECC umgestellt?
- Ist die Konnektor-Firmwareversion aktuell?
- Falls noch nicht, bietet sich ein Wechsel auf das TI-Gateway an?
- Ist das aktuelle Primärsystem-Update installiert?
- Ist das KIM-Clientmodul auf dem neuesten Stand?

Schritt 3

Austausch bzw. Updates beauftragen

Mehr erfahren auf:

www.gematik.de/telematikinfrastruktur/rsa2ecc-migration

 © gematik GmbH | Stand: 12/25