

## Austausch von Zertifikaten notwendig – jetzt Handlungsbedarf prüfen

Damit TI-Komponenten und Dienste auch weiterhin an angemessen hohen Sicherheitsstandards ausgerichtet sind, ist die Umstellung der Verschlüsselungsalgorithmen von RSA-2048 auf ECC-256 erforderlich. Dies erfolgt auf Empfehlung des BSI und der Europäischen eIDAS.

Da RSA-2048 nur noch befristet bis Ende 2025 zulässig ist, müssen eine Reihe von TI-Komponenten in den Praxen ausgetauscht werden, falls eine Komponente lediglich den sogenannten RSA- und nicht den aktuelleren ECC-Algorithmus bedienen kann.

Um Betriebsausfälle in Ihrer Praxis zu vermeiden, prüfen Sie bitte anhand der nachfolgenden Checkliste, ob Komponenten vom notwendigen Zertifikatswechsel betroffen sind.

### SMC-B (Praxisausweis) und eHBA (elektronischer Heilberufsausweis) der Generation G2.0

Mit den für den Austausch zuständigen Kartenanbietern ist abgestimmt, alle von der Umstellung betroffenen Ausweise bis zum Ende des Jahres 2025 zu tauschen. Der Anbieter **d-trust** hat bereits mit der Tauschaktion begonnen. Die Firma **medisign** ist in Vorbereitung und wird ihre Kunden per E-Mail informieren. **T-Systems** plant, entsprechende Informationen per E-Mail und per Post ab Mitte September zu versenden.

Sie können vorab bereits prüfen, ob Sie vom Austausch betroffen sind. Prüfen Sie bitte die Karten wie folgt auf ECC-Fähigkeit:



#### SMC-B

- über die Konnektor-Management-Oberfläche (Admin): Menüpunkt „Kartenverwaltung“ oder „Zertifikate“.

- über das Kartenterminal: bei bestimmten Modellen (z. B. CHERRY ST1506) navigieren Sie zu Menü → Einstellungen → Status → SMC-B Informationen

Sind ECC-Zertifikate vorhanden? → Es besteht kein Handlungsbedarf.

Sind KEINE ECC-Zertifikate vorhanden? → Benachrichtigung des Kartenanbieters beachten, ggf. Rücksprache bezüglich Beantragung halten.



#### eHBA

Prüfen Sie den Kartentyp anhand des Aufdrucks auf Ihrem eHBA, meist auf der Rückseite. Bei Ausweisen des Anbieters medisign steht zusätzlich eine Versionsnummer.

**G2 und/oder Version 3.20:** Nicht ECC-fähig → neuen eHBA über die Webseite der ZÄK S-H bestellen

**G2.1 und/oder Version 10.21:** ECC-fähig → Es besteht kein Handlungsbedarf.

Bei Fragen wenden Sie sich bitte an den Kartenhersteller!



#### Konnektor

Bei Konnektoren, deren Laufzeit bis Ende 2025 verlängert worden ist, handelt es sich in der Regel um sogenannte „RSA-only Konnektoren“. Diese müssen durch neue Konnektoren oder durch eine TI-Gateway-Anbindung abgelöst werden. Die TI-Gateway-Anbindung wird von der gematik empfohlen, da Inbox-Konnektoren nur noch bis Ende 2030 unterstützt werden.

Erkennen eines RSA-only Konnektors: Admin-Oberfläche des Konnektors, Suche nach „gSMC-K“.

Wird nur ein RSA-Zertifikat angezeigt? → Austausch gegen neuen Konnektor oder Anbindung an TI-Gateway. Kontaktieren Sie hierfür Ihren jeweiligen Anbieter!

Alternativ kann Ihr Konnektor-Anbieter mit Hilfe der Seriennummer erkennen, ob es sich um ein RSA- oder ECC-Zertifikat handelt.

Sollte Ihr Konnektor (RSA) betroffen sein, empfehlen wir, sich rechtzeitig um einen Umstieg zu kümmern und nicht bis Dezember 2025 zu warten, um DVO-Engpässe zu vermeiden.

## Austausch von Zertifikaten notwendig – jetzt Handlungsbedarf prüfen

### gSMC-KT (Gerätekarte Kartenterminal)

Identifikation einer gSMC-KT G2.0:

- über den Konnektor je nach Hersteller: „Praxis → Karten“ oder Kartenmanagement in der Admin-Oberfläche, Suche nach der gSMC-KT
- direkt am Kartenterminal je nach Hersteller:
  - Im Web-Interface: Menü „Info → gSMC-KT“ anzeigen  
Zeigt es nur RSA oder auch ECC? Wenn ECC fehlt → neue Karte bestellen
  - Im Terminal-Menü: Service → Test → Einzeltest → Slot 3 (oder 4)  
Anzeige „AUT“ + „AUT2“ → G2.1, es besteht kein Handlungsbedarf.  
Anzeige nur „AUT“ → G2.0 (RSA only), neue Karte bestellen.

Nach Abstimmung der gematik mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) wird die Nutzung älterer Karten (G2.0) über 2025 hinaus geduldet, sofern die Gültigkeit der Zertifikats-Laufzeit noch gegeben ist. Ein möglichst schneller Umstieg wird aber empfohlen.

Sollte bereits ein DVO-Termin geplant sein – z. B. wegen Austausch der SMC-B Karte – ist ggf. der gleichzeitige Austausch der gSMC-KT (Gen. 2.0) sinnvoll.

### eHealth-Kartenterminal

Prüfen Sie die Firmware auf Updates. Es sollte mindestens die aktuelle von den jeweiligen Kartenherstellern zur Verfügung gestellte KT-TSL geladen werden. Kontaktieren Sie hierzu die Hersteller oder Ihren Dienstleister vor Ort (DVO).

### KIM

Falls noch nicht geschehen, ist dringend der Umstieg von Version 1.0 auf Version 1.5 erforderlich. Beachten Sie, dass die Version KIM 1.5.2-9 (CM PTV >= 1.6.2-9) eingespielt sein muss. Zur Hilfestellung bei der Versionsermittlung kontaktieren Sie ggf. Ihren jeweiligen Anbieter!

### PVS (Praxisverwaltungssoftware)

E-Rezepte, eAU und EBZ dürfen ab 2026 nur noch mit "ECC-Signaturen" versehen werden. Ihr PVS-Anbieter wird Ihnen entsprechende Updates zur Verfügung stellen. Bitte spielen Sie grundsätzlich sämtliche Updates zeitnah ein. Bei Fragen wenden Sie sich an Ihren Anbieter!

Weitere Informationen und Verlinkungen finden Sie unter [www.kzv-sh.de/rsa-ecc](http://www.kzv-sh.de/rsa-ecc).