RSA-ECC-Migration

Die Telematikinfrastruktur (TI) stellt ihre Kryptografie von RSA (Rivest-Shamir-Adleman) auf die modernere ECC (Elliptic Curve Cryptography) um. Die Umstellung ist notwendig, da gemäß Technischer Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[1)] RSA (1900–3000 Bit) (im Folgenden als RSA-2048 betitelt) nur noch befristet bis Ende 2025 zulässig ist. Auch der europäische SOGIS-Katalog fordert diese Umstellung.[2)] Die Bundesnetzagentur (BNetzA) fordert daher „Vertrauensdiensteanbieter und Konformitätsbewertungsstellen, aber auch benannte Stellen für die Zertifizierung von qualifizierten Signatur- bzw. Siegelerstellungseinheiten“ auf, die verwendeten kryptographischen Algorithmen ihrer Produkte und Dienste zu überprüfen und ggf. rechtzeitig anzupassen.[3)]

Ziel der Migration ist, die Nutzung von RSA-2048 ab 2026 in der TI zu unterbinden. Anstelle von RSA-2048 soll dann ECC-256 als Standardverfahren genutzt werden. Dabei ist zu gewährleisten, dass alle Systeme weiterhin ohne Beeinträchtigungen oder Ausfälle funktionieren und die Versorgung gesichert bleibt.

Die Migration erfolgt in zwei Strängen:

- QES
- non-QES

Hintergrund sind die unterschiedlichen Regelungskreise bzw. -zuständigkeiten:

- **QES**: Die Regelung erfolgt auf europäischer Ebene über eIDAS. Die nationale Regulierungsbehörde ist die BNetzA. Seitens der gematik/dem BSI wird hier **kein Ermessensspielraum** gesehen. Auch wenn es keine offizielle Anweisung zur Sperrung aller QES-Zertifikate zum 31.12.2025 der BNetzA gibt, würde eine Nutzung über den Stichtag hinaus von der BNetzA wohl als Verletzung der Aufsichtspflicht gewertet werden und eine Anweisung nach sich ziehen, alle QES-Zertifikate umgehend zu sperren.
- **nonQES**: Hier liegt die Verantwortung bei der gematik in Abstimmung (im Benehmen) mit dem BSI. Die gematik sieht hier in Einzelfällen einen gewissen Handlungsspielraum, auch wenn das BSI (natürlich) von der Verwendung von RSA-2048 über den 31.12.2025 hinaus abrät. Somit wird es wohl darauf hinauslaufen, dass diese Anforderung kommuniziert und eingefordert wird, aber RSA-2048 in gewissen Einzelfällen bzw. für gewissen Komponenten und Dienste für (vermutlich unterschiedliche) Zeiträume toleriert wird.

Allgemein

Diverse Komponenten der TI müssen ECC-ready sein bzw. dahin migriert werden, insbesondere natürlich alle zentralen Dienst, aber auch die folgenden im Detail betrachteten Komponenten.

gematik-Seite zum Migrationsvorgehen:
https://wiki.gematik.de/spaces/RUAAS/pages/655759627/Planungs-+und+Umsetzungshorizont

Konnektor

- Konnektoren, deren gSMC-K noch RSA-only ist, müssen bis Ende 2026 ausgetauscht bzw. auf das TI-Gateway migriert werden. Dabei handelt es sich um 28.000 Secunet-Konnektoren und 4500 CGM/KoCo-Konnektoren.[4)]
- Ausgetauscht bzw. migriert werden müssten (voraussichtlich) auch alle Konnektoren, die ECC auf der gSMC-K haben, aber die bis Ende 2025, aber deren Zertifikate bis Ende 2025 auslaufen, da auf Basis von PTV5+ eine weitere Laufzeitverlängerung nicht möglich ist.
- Erst der Konnektor der Produkttypversion 6 (PTV6-Konnektor) erzwingt die Nutzung von ECC-Zertifikaten.
- Der flächendeckende Rollout des PTV-6-Konnektors ist also Voraussetzung für eine reibungslose Migration auch der anderen Komponenten hin zu ECC.
- Der Konnektor erzwingt die Nutzung von ECC bei den Smartcards der G2.1, die sowohl mit RSA als auch ECC-Zertifikaten umgehen können, ist aber auch in der Lage mit ECC-only-Smartcards umzugehen. Darüber hinaus kann er rein technisch auch mit Karten der G2.0 umgehen, die RSA-only personalisiert sind.
- Der PTV5-Konnektor kann ECC, nutzt aber standardmäßig RSA, hier muss das Primärsystem angepasst werden, um ECC nutzbar zu machen.
- Voraussichtlich kann der PTV5-Konnektor auch mit ECC-only-Karten umgehen, die ja beim HBA ab 1.1.2026 zu erwarten wären nach aktueller Planung. Da es ja noch keine ECC-only-Echtkarten gibt, konnte das noch nicht produktiv getestet werden.

Primärsysteme

- Die Primärsysteme müssen für die Nutzung von ECC über den PTV-6 Konnektor angepasst werden.
- Dies gilt auch für die Nutzung von ECC über den PTV-5-Konnektor, hier muss explizit ECC-Signatur aufgerufen werden, da der PTV-5 standardmäßig RSA nähme.
- Für KIM sind keine Anpassungen für die Migration der KIM-Clientmodule notwendig, da diese ja die Funktionalität zur Kryptographie kapseln.

KIM-Clientmodule

- Zur ECC-Fähigkeit ist ein KIM-Clientmodul der Version 1.5.2-9 notwendig. Der Rollout läuft seit Ende Juni 2025. Planung ist, diesen flächendeckend bis Ende Q3 abzuschließen.
- Ein PTV6-Konnektor ist keine Voraussetzung für die Migration.
- Ohne dieses Version des KIM-Clientmoduls fällt der KIM-Clientdienst aus, sobald ECC verpflichtend ist bzw. Signaturkomponenten oder Primärsysteme ECC zum Signieren/Verschlüsseln von Nachrichten anfordern. Dies betrifft dann auch indirekt QES-relevante Anwendungsfälle, die über KIM abgewickelt werden, wie eAU, eArztbrief und eEB.

Auch die KIM-Fachverfahren (Anwendungen) und Payloads müssen auf ECC migrieren. Die gematik stellt hierzu Handreichungen zur Verfügung.

QES-Migration

eHBA

- **Massentausch aller eHBA der Generation 2.0 (G2.0) in eHBA der Generation 2.1 (G2.1) bis 31.12.2025**
  - eHBA G2.0 sind nur mit RSA-Zertifikaten personalisiert
  - eHBA G2.1 sind sowohl mit RSA- als auch mit ECC-Zertifikaten personalisiert
  - **Ergebnis:**
    - Alle Leistungserbringenden besitzen einen eHBA, der es Ihnen ermöglicht, ECC-QES-Signaturen zu erstellen.
- **Massensperrung aller noch gültigen RSA-QES-Zertifikate** durch die VDA (über OSCP voraussichtlich) **zum Stichtag 31.12.2025**. Bei einem VDA sind die QES-HBA-Zertifikate sowieso nur mit der Gültigkeit bis 31.12.2025 ausgestellt worden.
  - **Ergebnis:**
    - eHBA G2.0 sind ab dem Stichtag nicht mehr für eine QES-Signatur nutzbar. Ärzt*innen, die bis dahin keinen eHBA G2.1 besitzen, können somit keine E-Rezepte und auch keine eAU mehr ausstellen, da der Konnektor sowohl das Endentitäts-Zertifikat (auch über OCSP) als auch das zugehörige QES-CA-Zertifikat bei der Erstellung prüft.[5)]
    - Die nonQES-RSA-Zertifikate der eHBA sind formal weiter zunächst gültig.

Ideal wäre natürlich die gleichzeitige Sperrung auch der nonQES-Zertifikate falls möglich. Eine Anforderung der gematik fordert dies zumindest. Eine weitere Variante wäre das Setzen von „unknown“ als Status im OCSP-Responder für die relevante RSA-CA, die damit nicht mehr unterstützt wird.

- **CA-Zertifikate der VDA** (eHBA-Anbieter) **für QES mit RSA** werden in der Vertrauensliste der BNetzA **auf „withdrawn“** gesetzt. Bei einem VDA laufen die QES-RSA-CA-Zertifikate sowieso zum 31.12.2025 aus.
  - **Ergebnis:**
    - Die eHBA-Anbieter können keine weiteren RSA-QES-Endentitäts-Zertifikate ausstellen (signieren).
    - Leistungserbringende können mittels RSA keine QES-Signatur mehr erstellen, da der Konnektor sowohl das Endentitäts-Zertifikat (auch über OCSP) als auch das zugehörige QES-CA-Zertifikat bei der Erstellung prüft.
- **eHBA wird geplant ab 1.1.2026 als ECC-only ausgegeben** (s. Release Smartcards 25-5, mit dem die Änderungen der freigegebenen Änderungsliste Smartcards_25-5 veröffentlicht werden, hier: HBA ohne personalisierte RSA-Objekte)

NFDM-Fachmodul

Über das Setzen des Parameters `Crypt` kann man in PTV5 angeben, dass man ECC nutzen möchte, auch wenn standardmäßig RSA genutzt wird (wenn man hier nix angibt). Bei alten PTV5-Konnektoren muss also das PS ermöglichen explizit ECC anzugeben, damit mit| ECC-only-Karten noch signiert werden kann. Bei NFDM kann man den Parameter aber nicht mitgeben.[6)] ⇒ NFDM kaputt ab 1.1.2026 für PTV5-Konnektoren

Einführung des `Crypt`-Parameters zur Steuerung welcher Schlüssel gewählt wird (RSA

oder ECC) für die QES-Signatur mit Version 5.6.0 der Konnektor-Spec (PTV4 bzw. 5) Mit Version 5.23.0 bleibt der Parameter zwar, aber wird nicht mehr ausgewertet (PTV6), sondern die Kartengeneration entscheidet, was genutzt wird.

nonQES-Migration

Die nonQES-Migration erfolgt sukzessive ab 2026.

Smartcards

- **Sperrung der nonQES-Zertifikate** auf den G2.1-Karten:
  - Für die nonQES-Zertifikate des **eHBA** ergäben sich die **folgenden Varianten** als Sperrmechanismus:
    - **Massensperrung**: Sperrung aller EE-Zertifikate für eine betreffende RSA CA zu einem Stichtag
    - **OCSP-Status** „unknown“: Konfiguration des OCSP-Responders, dass betreffende RSA CAs nicht mehr unterstützt werden
    - **Einzelsperrung** nur für die non-QES-Zertifikate vorsehen
    - Termin: 01.07.2025 (s. https://www.linkedin.com/posts/benny-geitner_ecc-rsa2ecc-ti-activity-7376140813925371904-IIVn/)
- **Ausgabe** der Karten nur noch als **ECC-only**
  - eHBA wird geplant ab 1.1.2026 als ECC-only ausgegeben (s. Release Smartcards 25-5, mit dem die Änderungen der freigegebenen Änderungsliste Smartcards_25-5 veröffentlicht werden, hier: HBA ohne personalisierte RSA-Objekte)
  - Andere TI-Smartcards (eGK, SMC-B, gSMC-K, gSMC-KT) werden weiterhin mit RSA und ECC personalisiert (benötigen PTV6-Konnektor)
  - gematik legt dann fest, wann für diese Karten ECC-only-Karten ausgegeben werden. Frühester Zeitpunkt: Rollout PTV-6-Konnektor abgeschlossen.

Übersignatur

Geregelt in § 15 Vertrauensdienstegesetz (VDG):

> Sofern hierfür Bedarf besteht, sind qualifiziert elektronisch signierte, gesiegelte oder zeitgestempelte Daten durch geeignete Maßnahmen neu zu schützen, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird.

Durch qualifizierter Bewahrungsdienste für qualifizierte elektronische Signaturen gemäß Artikel 34 eIDAS-VO kann die Vertrauenswürdigkeit der Signaturen durch Übersignaturen verlängert werden.

1)

BSI TR-02102-1 - Kryptographische Verfahren: Empfehlungen und Schlüssellängen.
2)

SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.3, February 2023.
3)

https://www.elektronische-vertrauensdienste.de/EVD/DE/Aktuelles/Meldungen/anbieter/RSA2048.html.
4)

https://www.hausaerztlichepraxis.digital/praxis/e-health-und-it/ti-komponenten-im-check-wer-muss-tauschen-167623.html.
5)

Vgl. dazu in der Konnektorspec den TUC_KON_150 "Dokumente signieren", der vom Primärsystem über die Operation SignDocument() aufgerufen wird. Dieser ruft u.a. den TUC_KON_159 "Signaturdatenelemente nachbereiten„ auf, der die Signatur prüft. Die Prüfung des Zertifikats erfolgt über TUC_KON_037 "Zertifikat prüfen". Dieser wiederum nutzt intern den TUC_PKI_030 "QES-Zertifikatsprüfung" zur Zertifikatsprüfung.
6)

s. https://gemspec.gematik.de/downloads/gemRL/gemRL_QES_NFDM/gemRL_QES_NFDM_V1.4.1.pdfSignaturrichtlinie NFDM