

## Signaturen der Abrechnungsinformationen von E-Rezepten

### Inhalt

Signaturen der Abrechnungsinformationen von E-Rezepten .....	1
Abrechnungsinformation.....	1
Prüfung der Abrechnungsinformationen .....	2
Mengengerüst .....	3
Signaturprüfung .....	3
Online-Prüfung des Signaturzertifikates gegenüber der TI.....	4
Anbindung für Apothekenrechenzentren .....	4
Anbindung für Rechenzentren der Krankenkassen .....	4
Interimslösungen .....	4
Cachen von Statusinformationen .....	5
Alterung von Signaturen.....	5

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0			Initiale Version	gematik
1.1.0	15.07.2021		Überarbeitung bzgl. eingebetteten OCSP-Response für Signaturen mit SMC-B	gematik
1.2.0	18.08.2021		Einschränkungen bei der Zertifikatsprüfung	gematik
1.3.0	30.06.2022		Überarbeitung der Einschränkungen gemäß dem aktuellen Status	gematik

### Abrechnungsinformation

Die **Abrechnungsinformation** für ein E-Rezept besteht aus drei signierten Datensätzen: Verordnungsdatensatz, Abgabedatensatz und der Quittung.

Der **Verordnungsdatensatz** wird im PVS/ZPVS/KIS erstellt und mit dem HBA des verordnenden (Zahn-)Arztes mit einer QES versehen. Hierfür wird der Konnektor der (Zahn-)Arztpraxis/des Krankenhauses verwendet.

Der **Abgabedatensatz** wird im AVS nach der Belieferung des E-Rezepts erstellt und mit dem HBA des Apothekers mit einer QES oder mit der SMC-B der Apotheke mit einer nonQES versehen. Hierfür wird der Konnektor der Apotheke verwendet.

Wenn der Workflow zum E-Rezept durch die Apotheke beendet wird, erstellt der E-Rezept-Fachdienst eine sogenannte **Quittung**, welche den ordnungsgemäßen Durchlauf des Workflows bestätigt. Sie wird mit einem Signaturzertifikat der Komponenten-PKI der TI mit einer nonQES versehen.

Hinweis: Es ist perspektivisch vorgesehen, dass die Quittung mit einem Zertifikat gemäß eIDAS-Siegel signiert wird. Dies soll die Prüfung der Signatur mit Standardbibliotheken außerhalb des zentralen Netzes der TI ermöglichen. Die gematik informiert, wenn die Umsetzung startet.

Alle drei signierten Datensätze beinhalten die Information der Rezept-ID. Diese ermöglicht die Datensätze einander zuzuordnen.

Während der Erstellung einer QES mit Konnektor wird der Status des Signaturzertifikates geprüft und im Fehlerfall, d.h. insbesondere wenn die Gültigkeit zu diesem Zeitpunkt negativ ist oder die Gültigkeit am OCSP-Responder nicht ermittelt werden kann, abgebrochen. Der OCSP-Response wird bei erfolgreicher Statusprüfung in die Signatur eingebettet. Für detaillierte Informationen siehe Spezifikation Konnektor [gemSpec\_KON].

Hinweis: Falls das PVS den OCSP-Response der Signaturprüfung nicht in den Verordnungsdatensatz einbettet, ändert das nichts daran, ob oder ob nicht die QES gültig ist. Die eingebettete OCSP-Response ermöglicht eine einfachere Prüfung der Gültigkeit des Signaturzertifikates zum Signaturzeitpunkt. Falls diese Information fehlt, kann das prüfende System den OCSP-Responder abfragen.

Hinweis: Es ist geplant, dass der E-Rezept-Fachdienst die OCSP-Response des Signaturzertifikates nachträglich einbettet, wenn das PVS diesen nicht bei der Erstellung der QES eingebettet hat.

Während der Erstellung einer nonQES mit Konnektor wird der Status des Signaturzertifikates geprüft. Ist das Zertifikat ungültig, wird der Signaturvorgang abgebrochen. Die Einbettung des OCSP-Response in eine nonQES-Signatur wird durch den Konnektor nicht unterstützt.

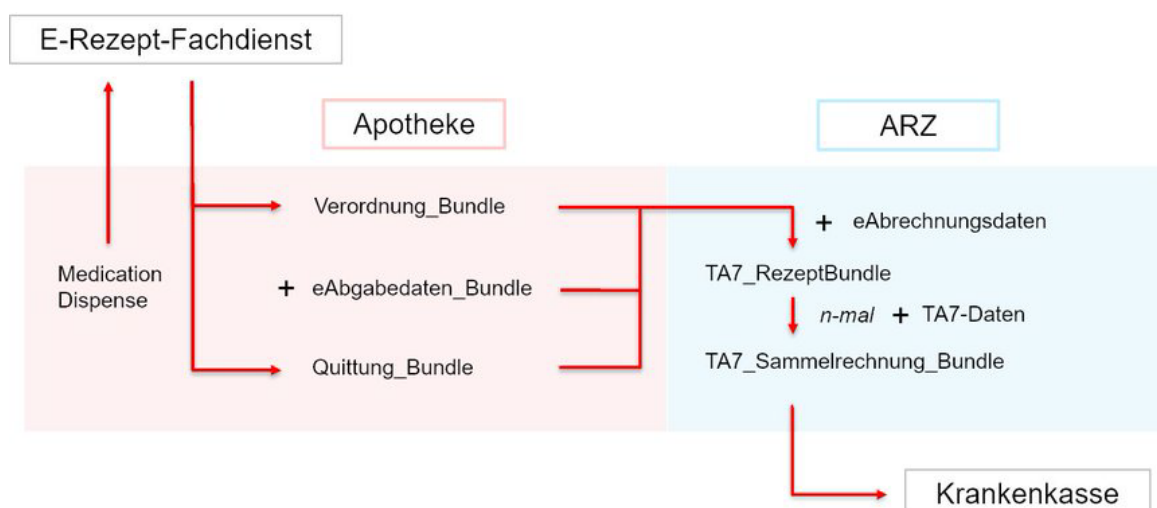
Der E-Rezept-Fachdienst prüft stündlich den Status des Signaturzertifikates für die Quittungen. Es werden nur Quittungen erstellt, wenn die Gültigkeitsprüfung innerhalb der vergangenen 24 h erfolgreich durchgeführt werden konnte und der Status OK ist.

Der E-Rezept-Fachdienst bettet den OCSP-Response des Signaturzertifikates in die Signatur ein.

## Prüfung der Abrechnungsinformationen

Die Abrechnungsinformationen werden von der Apotheke in den Abrechnungsprozess gegeben. In diesem Prozess werden die Abrechnungsinformationen durch unterschiedliche Institutionen geprüft:

- Apothekenrechenzentren
- Kopfstellen als Dienstleister der Kassen
- Prüfdienstleitern der Krankenkassen
- Krankenkassen



**Abbildung 1: Workflow Abrechnung E-Rezepte**  
Bildquelle: <https://github.com/DAV-ABDA/eRezept-Beispiele>

## Mengengerüst

Im systemspezifischen Konzept für die Anwendung E-Rezept [gemSysL\_eRp] ist ein Mengengerüst basierend auf dem Rezeptaufkommen von 2018 beschrieben. Das Gesamtaufkommen für abgegebene Rezepte lag bei 685 Mio. Verordnungszeilen, mit einem Maximalwert für einen einzelnen Tag bei 3,7 Mio. Verordnungszeilen.

## Signaturprüfung

Die Signaturprüfung kann mittels einer Komponente der TI (Konnektor, ggf. Basis-/KTR-Consumer) durchgeführt werden. Das erfordert bei der hohen Anzahl von Prüfungen einen umfangreichen Aufbau von Kapazitäten dieser Komponenten.

Alternativ - und durch die gematik empfohlen - können die Rechenzentren mit einer eigenen Implementierung die Signatur prüfen. Die Prüfung des Signaturzertifikates ist gemäß [gemSpec\_PKI] umzusetzen. Siehe auch <https://github.com/gematik/ref-GemLibPki>.

Für die Prüfung der QES-signierten Datensätze kann der in die Signatur eingebettete OCSP-Response genutzt werden. Zusätzlich muss geprüft werden, ob die CA des signierenden Zertifikates gemäß der Vertrauensliste der Bundesnetzagentur (BNetzA) zum Signaturzeitpunkt gültig war.

Für die Prüfung der nonQES-signierten Datensätze kann, sofern vorhanden, der in die Signatur eingebettete OCSP-Response genutzt werden. Zusätzlich muss geprüft werden, ob die CA des signierenden Zertifikates gemäß der TSL der TI zum Signaturzeitpunkt gültig war. Die CA wird aus dem signierenden Zertifikat bestimmt. Die TSL der TI stellt den Vertrauensanker der TI dar und ist unter <https://download.tsl.ti-dienste.de/> verfügbar. Für weitere Informationen zum Vertrauensraum der TI siehe [gemSpec\_PKI].

Wenn kein OCSP-Response in die Signatur eingebettet ist, bspw. bei nonQES-Signaturen durch den Konnektor, dann ist die Gültigkeit des Zertifikates online zu prüfen.

### Einschränkungen bei der Signaturprüfung:

(a) Konnektor prüft Quittung nicht

Gemäß der gematik-Spezifikation wird die Quittung durch den E-Rezept-Fachdienst mittels einem Zertifikat mit dem Zertifikatsprofil C.FD.OSIG (siehe [gemSpec\_PKI#5.9.3.6 C.FD.OSIG Signatur Fachdienst (OSIG, nonRepudiation)]) signiert. Da für dieses Zertifikatsprofil die Prüfvorschrift im Konnektor erst nachträglich spezifiziert wurde, kann die Signatur der Quittung nur mit neueren Konnektoren geprüft werden. Die Signaturprüfung ist alternativ durch eine eigene Implementation durchzuführen.

## Online-Prüfung des Signaturzertifikates gegenüber der TI

Die OCSP-Responder für die Statusprüfung der Zertifikate in der TI liefern für ein angefragtes Zertifikat die Gültigkeit zum Abfragezeitpunkt. Wenn das Zertifikat gesperrt ist, dann wird der Zeitpunkt der Sperrung mit übermittelt. Der OCSP-Response wird für die Lebensdauer des Zertifikates (Attribut validity), d.h. für 5 Jahre bereitgestellt.

Die OCSP-Responder der Trusted Service Provider (TSP), welche SMC-Bs herausgeben, sind im zentralen Netz der TI und im Internet erreichbar. Hierbei bestehen die folgenden Performanceanforderungen an die Spitzenlast:

- Zentrales Netz der TI: 1100 Aufrufe pro Sekunde
- Internet: 30 Aufrufe pro Sekunde

Aufgrund des Mengengerüsts besteht die Notwendigkeit, dass die prüfenden Institutionen über das zentrale Netz der TI auf die OCSP-Responder zugreifen.

### Anbindung für Apothekenrechenzentren

Apothekenrechenzentren (ARZ) sind Abrechnungsdienstleister im Gesundheitswesen und damit berechtigt, eine SMC-B ORG zu beantragen/benutzen, womit ein TI-Zugang und die KIM-Nutzung gewährleistet wird.

Hierfür wurde die oid\_abrechnungsdienstleister eingeführt. Herausgeberin der SMC-B ORG für Abrechnungsdienstleister ist die gematik und damit die D-TRUST der einzige Kartenanbieter.

Die ARZ haben die Möglichkeit, sich mittels Konnektor oder Basis-Consumer an das zentrale Netz der TI anzubinden. Mit der Operation VerifyCertificate des Konnektors bzw. Basis-Consumer kann die Gültigkeit von Zertifikaten der TI geprüft werden. Siehe auch [gemSpec\_Kon] bzw. [gemSpec\_Basis\_KTR\_Consumer].

### Anbindung für Rechenzentren der Krankenkassen

Die Rechenzentren der Krankenkassen können sich mittels Basis- oder KTR-Consumer an das zentrale Netz der TI anbinden.

Mit der Operation VerifyCertificate des Basis- / KTR-Consumer kann die Gültigkeit von Zertifikaten der TI geprüft werden. Siehe auch [gemSpec\_Basis\_KTR\_Consumer].

### Interimslösungen

Für eine Übergangszeit, in der das Volumen der zu prüfenden E-Rezepte noch nicht dem vollen Mengengerüst entspricht und die Institutionen noch nicht auf das zentrale Netz der TI zugreifen können, stehen zwei alternative Lösungen zu Verfügung.

### *OCSP-Responder im Internet*

Für SMC-Bs ist die im Internet erreichbare Adresse des OCSP-Responders aus dem Zertifikat ermittelbar (Attribut: AuthorityInfoAccess). OCSP-Requests müssen gemäß Vorgaben aus RFC6960 (s. Kap. 4.1) gebildet werden (gemSpec\_PKI#GS-A\_4674-01).

Es ist die verfügbare Spitzenlast der Schnittstelle des OCSP-Responders im Internet zu beachten.

Für das Signaturzertifikat des E-Rezept-Fachdienstes: Der OCSP-Responder der Komponenten-PKI der TI ist nicht im Internet erreichbar.

### *OCSP-Forwarder*

Es kann der durch den E-Rezept-Fachdienst bereitgestellten OCSP-Forwarder genutzt werden. (<https://erp.app.ti-dienste.de/ocspf>)

Die OCSP-Forwarder-Schnittstelle wird im Internet angeboten. Sie leitet OCSP-Requests an die OCSP-Responder im zentralen Netz der TI weiter.

Für die Schnittstelle wird ein API-Key genutzt. Der API-Key kann bei der gematik ([transition@gematik.de](mailto:transition@gematik.de)) beantragt werden.

## Cachen von Statusinformationen

Die Abrechnung gegenüber den Krankenkassen erfolgt mit zeitlichem Versatz zur Erstellung der Abrechnungsinformationen. D.h. wenn eine größere Anzahl an Abrechnungsinformationen geprüft werden soll, kann der Status jeder verwendeten SMC-B einer Apotheke bzw. des Signaturzertifikates des Fachdienstes gecached und für alle mit der Identität vor dem Prüfzeitpunkt signierten Daten genutzt werden. Dies senkt die Anzahl der notwendigen Online-Statusprüfungen signifikant.

## Alterung von Signaturen

Da der OCSP-Response nur für die Lebensdauer des Zertifikates zur Verfügung steht, muss die Prüfung ggf. während dieses Zeitraums stattfinden und dann revisionssicher gespeichert werden.

Zur allgemeinen Frage der Alterung der Signatur. Nach unserem Verständnis dienen die Signaturen (insbesondere die des E-Rezept-Fachdienstes) der Abrechnung. Um innerhalb einer Aufbewahrungsfrist von 10 Jahren der Signatur zu vertrauen, empfehlen wir ein revisionssicheres Archivieren, um Manipulationen und evtl. gefälschte Signaturen über die Revisionssicherung und Zeitstempel zu erkennen. Letzterer ist ein Indikator, ob das Signaturverfahren zum Zeitpunkt der Archivierung als sicher galt. Eine Alternative zur Langzeitaufbewahrung von signierten Dokumenten wäre die BSI-Richtlinie TR-ESOR ([https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI TR 03125 V1 2 1.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_V1_2_1.pdf)).