

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# Spezifikation Signaturdienst

Version: 1.9.0 CC  
Revision: 1131959  
Stand: 14.02.2025  
Status: zur Abstimmung  
freigegeben  
Klassifizierung: öffentlich\_Entwurf  
Referenzierung: gemSpec\_SigD

---

## Dokumentinformationen

---

### Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

### Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	30.04.2019		freigegeben	gematik
1.1.0	28.06.2019		Einarbeitung Änderungsliste P19.1	gematik
1.2.0	02.10.2019		Einarbeitung Änderungsliste P20.2	gematik
			Einarbeitung Änderungsliste P21.1	gematik
1.3.0	02.03.2020		freigegeben	gematik
1.4.0	12.10.2020		Einarbeitung Scope-Themen zu R4.0.1	gematik
1.5.0	06.02.2023		Einarbeitung IDP_Maintenance_22.2	gematik
1.6.0	30.01.2024		Einarbeitung ePA fuer alle	gematik
1.7.0	13.06.2024		Einarbeitung Änderungsliste IDP_24.3	gematik
1.8.0	12.07.2024		Einarbeitung C_11901 (ePA für alle - Release 3.0.2)	gematik
1.9.0 CC	14.02.2025		Einarbeitung C_12138 (ePA für alle - Release 3.0.5)	gematik

---

## Inhaltsverzeichnis

---

<b>1 Einordnung des Dokuments.....</b>	<b>4</b>
1.1 Zielsetzung.....	4
1.2 Zielgruppe.....	4
1.3 Geltungsbereich.....	4
1.4 Abgrenzungen.....	4
1.5 Methodik.....	5
<b>2 Systemüberblick.....</b>	<b>6</b>
<b>3 Systemkontext.....</b>	<b>7</b>
3.1 Akteure und Rollen.....	7
3.2 Nachbarsysteme.....	8
3.3 Sicherheitsanforderungen für den operativen Betrieb.....	8
<b>4 Zerlegung des Signaturdienstes.....</b>	<b>10</b>
<b>5 Übergreifende Festlegungen.....</b>	<b>11</b>
<b>6 Funktionsmerkmale.....</b>	<b>13</b>
<b>6.1 Schnittstellen I_Remote_Sign_Operations und I_Remote_Get_Certificate. 13</b>	
6.1.1 Operationsdefinition I_Remote_Sign_Operations::sign_Data.....	14
6.1.2 Operationsdefinition I_Remote_Get_Certificate.....	16
6.1.3 Umsetzung I_Remote_Sign_Operations::sign_Data und I_Remote_Get_Certificate	17
.....	17
<b>6.2 Schnittstelle P_Create_Identity.....</b>	<b>18</b>
<b>6.3 Schnittstelle P_Delete_Identity.....</b>	<b>18</b>
<b>7 Anhang - Verzeichnisse.....</b>	<b>19</b>
7.1 Abkürzungen.....	19
7.2 Glossar.....	19
7.3 Abbildungsverzeichnis.....	19
7.4 Tabellenverzeichnis.....	19
<b>7.5 Referenzierte Dokumente.....</b>	<b>20</b>
7.5.1 - Dokumente der gematik.....	20
7.5.2 - Weitere Dokumente.....	20

---

## 1 Einordnung des Dokuments

---

### 1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen an den Produkttyp Signaturdienst einschließlich der durch ihn bereitgestellten Schnittstellen.

### 1.2 Zielgruppe

Das Dokument richtet sich an Hersteller des Signaturdienstes und Anbieter von Signaturdiensten.

### 1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens für den Online-Produktivbetrieb. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z.B. gemPTV\_ATV\_Festlegungen, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

#### Wichtiger Schutzrechts-/Patentrechtshinweis

*Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.*

### 1.4 Abgrenzungen

Spezifiziert werden in diesem Dokument die vom Signaturdienst bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang, Kap. 7.5-Referenzierte Dokumente).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten. Diese sind in dem Produkttypsteckbrief des Signaturdienstes verzeichnet.

Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen zum Themenbereich Betrieb. Die betrieblichen Anforderungen sind im Anbietertypsteckbrief zum TSP X.509 nonQES eGK mit Option Signaturdienst verzeichnet.

## 1.5 Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Sie werden im Dokument wie folgt dargestellt:

**<AFO-ID> - <Titel der Afo>**

Text / Beschreibung

[<=]

Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und der Textmarke [<=] angeführten Inhalte.

---

## 2 Systemüberblick

---

Der Signaturdienst erzeugt elektronische Signaturen für Versicherte in der Umgebung des Anbieters des Signaturdienstes. Der Anbieter des Signaturdienstes wird hierbei nicht als Vertrauensdiensteanbieter gemäß Verordnung (EU) Nr. 910/2014 [eIDAS] behandelt, da er lediglich im Kontext von Anwendungen der Telematikinfrastruktur agiert und keine beliebigen und übergreifend validierbaren Signaturen erzeugt. Die vom Signaturdienst ausgestellten elektronischen Signaturen sind kryptographische Bestätigungen basierend auf asymmetrischer Kryptographie und Teil des Vertrauensraums für X.509 nonQES-Identitäten der Telematikinfrastruktur.

Die vom Signaturdienst erstellten elektronischen Signaturen nutzen Versicherte ( „Online-Nutzer“) für die nachweisbare Bestätigung von Befugnissen im Kontext der elektronischen Patientenakte. Bei Befugnis-Erteilung mittels eGK in der LEI ist der Signaturdienst hingegen nicht erforderlich.

Versicherte können elektronische Signaturen, mittels Authentisierung durch einen sektoralen Identity Provider, in der vom Anbieter des Signaturdienstes geführten Umgebung erstellen lassen. Die elektronischen Signaturen des Signaturdienstes werden mittels der Identität ID.CH.AUT\_ALT oder ID.CH.SIG eines Trust Service Provider X.509 nonQES-eGK erzeugt, welche nicht auf der elektronischen Gesundheitskarte verfügbar ist.

Der Signaturdienst erstellt elektronische Signaturen für Versicherte ausschließlich über korrespondierende Identitäten bzw. Personenidentifizierungsdaten eines sektoralen Identity Provider gemäß [gemSpec\_IDP\_Sek] im Auftrag des Kartenherausgebers der eGK des Versicherten. Die Ausstellung der Zertifikate im Signaturdienst kann asynchron zur Ausstellung der Zertifikate der eGK und bedarfsgerecht erfolgen. Die Laufzeit der Zertifikate C.CH.AUT\_ALT und C.CH.SIG des Signaturdienstes ist unabhängig von den Laufzeiten der Zertifikate der eGK, eine Synchronisation der Restlaufzeiten ist dabei nicht erforderlich. Gleiches gilt für die Zertifikatssperrung.

Personenidentifizierungsdaten sind ein Datensatz, der es ermöglicht, die Identität des Versicherten abzubilden. Die von einem sektoralen Identity Provider bereitgestellten Personenidentifizierungsdaten entsprechen den Personenidentifizierungsdaten im Zertifikat C.CH.AUT der eGK des Versicherten. Die Zertifikatsprofile C.CH.AUT\_ALT und C.CH.SIG für die vom Signaturdienst ausgestellten elektronischen Signaturen sind in [gemSpec\_PKI] festgelegt.

Der Betreiber des TSP X.509 eGK für die Zertifikate auf der eGK und der TSP nonQES-eGK für die C.CH.SIG des Signaturdienstes können unterschiedlich sein.

---

## 3 Systemkontext

---

### 3.1 Akteure und Rollen

Im Kontext des Signaturdienstes treten folgende Akteure auf:

**Anbieter** des Signaturdienstes:

Anbieter eines Signaturdienstes setzen die in dieser Spezifikation beschriebenen Aufgaben des Signaturdienstes um.

**Kartenherausgeber eGK**

Kartenherausgeber der eGK beauftragen den Anbieter eines Signaturdienstes, um für ihre Versicherten elektronische Signaturen ausstellen zu lassen. Dazu beauftragt der Kartenherausgeber eGK für jeden Versicherten beim Anbieter des Signaturdienstes das Signaturzertifikat. Der Kartenherausgeber eGK übermittelt hierzu die für das elektronische Identifizierungsmittel notwendigen Personenidentifikationsdaten des Versicherten (u.a. Name, KVNR) an den Anbieter des Signaturdienstes. Der Kartenherausgeber eGK veranlasst die Sperrung von Signaturzertifikaten bzgl. seiner Versicherten beim TSP X.509 nonQES-eGK, der das Zertifikat erstellt hat.

**Versicherte**

Versicherte nutzen mittels eigener Client-Systeme den Signaturdienst, um mittels der elektronischen Signatur anderen Diensten Aktivitäten, wie das Ausstellen von Befugnissen, nachweisbar zu bestätigen.

Versicherte richten sich an den Kartenherausgeber ihrer eGK, falls sie ihr Signaturzertifikat sperren lassen möchten.

**Sektoraler Identity Provider**

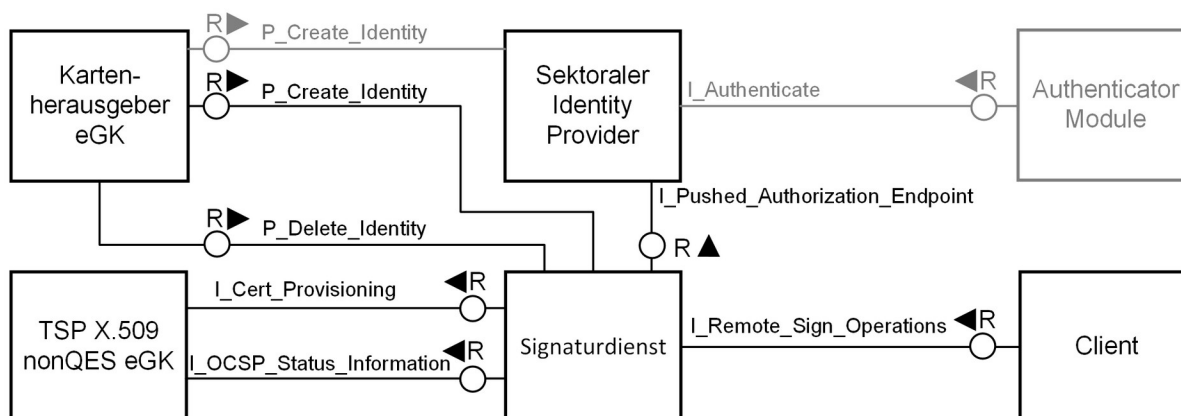
Ein sektoraler Identity Provider einer autoritativen Stelle (z. B. eine Krankenversicherung) gibt für ihre Versicherten eine digitale Identität aus. Diese Versicherten-ID wird über Standards der OpenID Foundation Anwendungen der TI zur Verfügung gestellt. Zu den Aufgaben einer autoritativen Stelle gehören:

- die Feststellung der Versichertenidentität auf geeigneter Basis (Identity Proofing),
- die Authentifizierung der Versicherten vor Zusicherung der Versicherten-ID,
- geben diese Versicherten-ID für digitale Anwendungen und Dienste heraus,
- und stellen die Verwaltung sicher.

Der sektorale Identity Provider übernimmt aus diesen Aufgaben die Identitätsfeststellung und Authentifizierung von Versicherten sowie die Bestätigung ihrer Attribute. Die verschiedenen Dienste und sektoralen Identity Provider sind über den Federation Master [gemSpec\_IDP\_FedMaster] in einem Vertrauensraum organisiert. Jedoch ist es aufgrund der direkten Beziehungen zwischen Karteherausgeber der eGK, sektoralen Identity Provider, Signaturdienst und ePA-FdV nicht notwendig, dass der Signaturdienst die Funktionen der Föderation verwendet. Es besteht im Fall einer Anmeldung für den Zugriff auf eine elektronische Patientenakte eine klare Verbindung zwischen ePA-FdV, Signaturdienst und sektoralen Identity Provider, sodass die Vertrauensbeziehungen hier nicht über die Mechanismen der Föderation aufgebaut werden müssen.

## 3.2 Nachbarsysteme

Die folgende Abbildung zeigt die Beziehung zu benachbarten Systemen mit den vom Signaturdienst bereitgestellten und genutzten Schnittstellen.



**Abbildung 1 Benachbarte Systeme des Signaturdienstes mit bereitgestellten und genutzten Schnittstellen**

Der Signaturdienst wird als Provider einer technischen Schnittstelle zum Erstellen elektronischer Signaturen für Clients und einer Prozessschnittstelle für Kartenherausgeber eGK zum Beauftragen und Löschen von Signaturzertifikaten aufgerufen.

Der Signaturdienst nutzt die Schnittstellen des TSP X.509 nonQES - eGK zum Erstellen von Zertifikaten.

## 3.3 Sicherheitsanforderungen für den operativen Betrieb

Der Anbieter Signaturdienst muss die folgenden Anforderungen erfüllen:

### A\_19033 - Schützenswerte Objekte

Der Anbieter Signaturdienst MUSS die folgenden kryptographischen Objekte als schützenswerte Objekte in seinem Sicherheitskonzept berücksichtigen: (a) Private Schlüssel, (b) Öffentlicher Schlüssel, (c) Öffentlicher Schlüssel von Antragstellern, (d) Anträge zur Ausstellung von X.509-Zertifikaten, (e) Authentisierungsinformationen von Sperrberechtigten, (f) Dokumentation über beauftragte und durchgeführte Sperrungen, (g) Statusinformationen, (h) Zulassungsdokumente, (i) Registrierungsdokumente, (j) Authentisierungsinformationen zur Authentisierung von internen Akteuren bzw. Rollen, (k) Protokolldaten, (l) Konfigurationsdaten.

[<=]

### A\_19037 - Gesicherte interne Schnittstellen des Anbieters Signaturdienst

Der Anbieter Signaturdienst MUSS für den internen Datenaustausch einen Mechanismus zur Sicherung der Datenintegrität, der Authentizität und zur Vertraulichkeit der Daten zur Verfügung stellen.[<=]

### A\_19038 - Datenaustausch zwischen gematik und Anbieter Signaturdienst

Der Anbieter Signaturdienst MUSS für den Datenaustausch zur gematik einen Mechanismus zur Sicherung der Datenintegrität, der Authentizität und zur Vertraulichkeit der Daten zur Verfügung stellen.[<=]



#### **A\_19039 - Gesicherte externe Schnittstellen des Anbieters Signaturdienst**

Der Anbieter Signaturdienst MUSS für den Datenaustausch mit anderen Rollen und Diensten einen Mechanismus zur Sicherung der Datenintegrität, der Authentizität und zur Vertraulichkeit der Daten zur Verfügung stellen. Hierzu gehören die Schnittstellen von

- a) Anbieter Signaturdienst zum berechtigten Zertifikatsantragsteller zur Beantragung und Ausstellung von Zertifikaten,
- b) Anbieter Signaturdienst zum Sperrantragsteller für die Sperrung von Zertifikaten. [≤]

#### **A\_19040 - Eindeutige Verbindung Zertifikatsnehmer und privater Schlüssel**

Der Anbieter Signaturdienst MUSS sicherstellen, dass der öffentliche Schlüssel, dem die Attribute des Zertifikatsnehmers in einem Zertifikat zugeordnet werden, und der private Schlüssel des Zertifikatsnehmers zusammengehören. [≤]

#### **A\_19041-01 - Umsetzung Signaturdienst für Zertifikate**

Der Anbieter Signaturdienst MUSS nach erfolgreicher erster Authentifizierung des Antragstellers die erforderlichen Angaben zur Zertifikatserstellung an den Erstellungsdiens des TSP X.509 nonQES - eGK weiterleiten. [≤]

#### **A\_19042 - Trennung der Signaturdienst-Betriebsumgebungen**

Der Anbieter Signaturdienst MUSS sicherstellen, dass das Testsystem von dem Produktivsystem technisch, organisatorisch und betrieblich so getrennt werden, dass keine gegenseitige Beeinflussung und keine Verwechslung möglich sind. [≤]

#### **A\_19043 - Datenschutzgerechte Antrags- und Sperrprozesse**

Der Anbieter Signaturdienst MUSS die Antrags- und Sperrprozesse datenschutzgerecht ausgestalten, d.h. insbesondere sind für die Verarbeitung der Antrags- und Sperrauftragsdaten die Datenschutzgrundsätze gemäß Art. 5 DSGVO zu berücksichtigen sowie die technischen und organisatorischen Maßnahmen nach Art. 25 und Art. 32 DSGVO zu treffen. [≤]

#### **A\_19044 - Löschung von Signaturdienst-Zertifikatsstatusinformationen, Zertifikats- und Sperranträgen**

Der Anbieter Signaturdienst MUSS die Zertifikatsanträge und die Sperraufträge zu einem X.509-Zertifikat unverzüglich löschen, sobald die gesetzlichen oder vertraglichen Aufbewahrungsfristen erreicht sind. [≤]

#### **A\_19045 - Fehlerprotokollierung**

Falls es erforderlich sein sollte, dass der Anbieter Signaturdienst eine Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung durchführt, MÜSSEN die Protokolldaten entsprechend des Datenschutzgrundsatzes der Datenminimierung gemäß Art. 5 Abs. 1 Satz 1 lit.c) DSGVO unter Berücksichtigung der Art. 25, 32 DSGVO derart gestaltet sein, dass nur personenbezogene Daten in der Art und dem Umfang enthalten sind, wie sie zur Behebung erforderlich sind. [≤]

#### **A\_26271 - Signaturdienst - Schutz vor DoS-Angriffen aus dem Internet**

Der Anbieter eines Signaturdienstes MUSS für alle vom Internet erreichbaren Schnittstellen Maßnahmen zum Schutz vor DoS-Angriffen treffen. [≤]

---

## 4 Zerlegung des Signaturdienstes

---

Eine Zerlegung des Produkttyps Signaturdienst wird nicht vorgegeben.

---

## 5 Übergreifende Festlegungen

---

Der Signaturdienst muss die folgenden übergreifenden Anforderungen erfüllen.

### **A\_17373-03 - Signaturdienst - Produkt erfordert Authentisierung auf dem Vertrauensniveau "hoch"**

Der Hersteller des Signaturdienstes MUSS sein Produkt so implementieren, dass dieses die Freischaltung nach einer Authentisierung des Nutzers über einen sektoralen Identity Provider auf dem Vertrauensniveau "gematik-ehealth-loa-high" vorsieht oder einer Authentisierung auf dem Vertrauensniveau "gematik-ehealth-loa-substantial" zu welcher eine Einwilligung des Anwenders zur Nutzung dieses Verfahrens zum Zugriff auf Daten mit hohem Schutzbedarf vorliegt. [≤]

### **A\_17336-03 - Signaturdienst - Sicherheitsniveau der Authentisierung auf dem Vertrauensniveau "hoch"**

Der Anbieter des Signaturdienstes MUSS für den angebotenen Signaturdienst sicherstellen, dass die Nutzung nur nach Authentisierung des Nutzers über einen zugelassenen sektoralen Identity Provider auf dem Vertrauensniveau "gematik-ehealth-loa-high" erfolgt oder nach einer Authentisierung auf dem Vertrauensniveau "gematik-ehealth-loa-substantial", zu welcher eine Einwilligung des Anwenders zur Nutzung dieses Verfahrens zum Zugriff auf Daten mit hohem Schutzbedarf vorliegt. [≤]

Die Anmeldung des Signaturzertifikates inklusive Identitätsnachweis und -überprüfung des Versicherten erfolgt durch den Kartenherausgeber eGK auf Grundlage der GKV-SV Richtlinie "Kontakt mit Versicherten" nach § 217f Abs. 4b SGB V.

Die Identifizierung der Versicherten im Rahmen der Einrichtung der Gesundheits-ID ist hinreichend. Ein zusätzliches Ident-Verfahren der Versicherten ist in diesem Fall nicht erforderlich.

Eine Notifizierung des Signaturdienstes, ist nicht gefordert. Ebenso ist nicht gefordert, dass der Anbieter ein qualifizierter oder nichtqualifizierter Vertrauensdiensteanbieter gemäß Verordnung (EU) Nr. 910/2014 ist.

Zur Erstellung der Signatur kann eine nach eIDAS zertifizierte qualifizierte Signatur/Siegelerstellungseinheit (QSEE) eingesetzt werden.

### **A\_17369 - Signaturdienst - Elektronische Identifizierungsmittel sind kryptographische Identitäten der TI (Befristet)**

Der Signaturdienst MUSS als elektronische Identifizierungsmittel kryptographische Identitäten ausstellen, die aus einem privaten und einem öffentlichen Schlüssel mit dazugehörigem Zertifikat des Typs C.CH.AUT\_ALT aus dem Vertrauensraum der TI bestehen. [≤]

### **A\_17369-01 - Signaturdienst - Signaturzertifikate sind kryptographische Identitäten der TI**

Der Signaturdienst MUSS elektronische Signaturen mittels kryptographischer Identitäten ausstellen, die aus einem privaten und einem öffentlichen Schlüssel mit dazugehörigem Zertifikat des Typs C.CH.SIG aus dem Vertrauensraum der TI bestehen. [≤]

### **A\_17370-01 - Signaturdienst - ECC-Verfahren für elektronische Signaturen**

Der Signaturdienst MUSS elektronische Signaturen auf der Grundlage von ECC-Schlüsseln erstellen. [≤]

Für die Erzeugung von ECC-Schlüsseln sind die Vorgaben in [gemSpec\_Krypt] einzuhalten.

### **A\_17371-01 - Signaturdienst - Keine RSA-Verfahren für elektronische Signaturen**

Der Signaturdienst DARF elektronische Signaturen NICHT auf der Grundlage von RSA-Schlüsseln erstellen.【<=】

### **A\_17339-01 - Signaturdienst - Speicherung privater Schlüssel mit einem HSM**

Der Anbieter des Signaturdienstes MUSS die privaten Schlüssel der Signaturzertifikate mit einem HSM speichern und sicherstellen, dass die Eignung des HSM durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als Evaluierungsschemata kommen dabei Federal Information Processing Standard (FIPS) oder Common Criteria mit mindestens folgender Prüftiefe in Frage:

1. FIPS 140-2 Level 3 oder
2. Common Criteria EAL 4.

【<=】

### **A\_17853-02 - Signaturdienst - Auskunft an Versicherten**

Der Anbieter des Signaturdienstes MUSS dem Versicherten, auf dessen Verlangen, Auskunft geben über erfolgte Zugriffe auf das Signaturzertifikat des Versicherten.【<=】

*Hinweis: Die Auskunft des Versicherten kann auch über den Kartenherausgeber erfolgen, der den Anbieter des Signaturdienstes mit der Erstellung des Signaturzertifikats beauftragt hat.*

### **A\_17864 - Signaturdienst - Anbieter des Signaturdienstes ist kein Anbieter eines ePA-Aktensystems**

Der Anbieter des Signaturdienstes MUSS unabhängig von Anbietern von ePA-Aktensystemen sein, d.h. es sind mindestens jeweils eigenständige Rechtspersonlichkeiten mit eigenständigen operativen Geschäfts- und Betriebsführungen und es ist eine strikte Vermeidung von Personenidentitäten bzw. Doppelrollen in den Funktionen Geschäftsführung, leitende Mitarbeiter und Zugangsberechtigte zum Betriebsort des Signaturdienstes bzw. ePA-Aktensystems gewährleistet.【<=】

*Hinweis: Die Anforderung schließt nicht aus, dass die Anbieter verbundene Unternehmen im Sinne des § 15 AktG sind.*

### **A\_18957 - Darstellen der Voraussetzungen für sicheren Betrieb des Produkts im Handbuch**

Der Hersteller des Signaturdienstes MUSS für sein Produkt im dazugehörigen Handbuch leicht ersichtlich darstellen, welche Voraussetzungen vom Betreiber und der Betriebsumgebung erfüllt werden müssen, damit ein sicherer Betrieb des Produktes gewährleistet werden kann.【<=】

### **A\_18958 - Sicherer Betrieb des Produkts nach Handbuch**

Der Anbieter eines Signaturdienstes MUSS die im Handbuch des eingesetzten Signaturdienstes beschriebenen Voraussetzungen für den sicheren Betrieb des Produktes gewährleisten.【<=】

---

## 6 Funktionsmerkmale

---

Der Signaturdienst realisiert die Funktionsmerkmale zur Erstellung elektronischer Signaturen. Das Funktionsmerkmal wird über die Implementierung der Schnittstellen `I_Remote_Sign_Operation`, `I_Remote_Get_Certificate`, `P_Create_Identity` und `P_Delete_Identity` realisiert.

### 6.1 Schnittstellen `I_Remote_Sign_Operations` und `I_Remote_Get_Certificate`

Die in diesem Abschnitt beschriebenen logischen Schnittstellen des Signaturdienstes werden durch das ePA Frontend des Versicherten und potentiell weitere Anwendungen verwendet, um Signaturen im Namen eines Versicherten zu erstellen ohne auf kryptographisches Material einer Smartcard zurückzugreifen. Die Freischaltung dieser Fernsignaturfunktion erfolgt nach Authentisierung gegenüber einem sektoralen Identity Provider.

#### **A\_17383-01 - Signaturdienst - Schnittstellen im Internet**

Der Signaturdienst MUSS die Schnittstellen `I_Remote_Sign_Operations` und `I_Remote_Get_Certificate` im Internet anbieten. [ $\leq$ ]

#### **A\_26272 - Signaturdienst - Erstellen einer Signaturidentität für Versicherte anderer Kostenträger bei Operationsaufruf**

Falls die Operationen der Schnittstellen `I_Remote_Sign_Operations` oder `I_Remote_Get_Certificate` aufgerufen werden, um eine Signatur für einen Nutzer zu erstellen,

- für den keine Signaturidentität `ID.CH.SIG` im Signaturdienst existiert und
- der nicht zu einem Kostenträger gehört, der den Anbieter des Signaturdienstes beauftragt hat

MUSS der Signaturdienst eine Signaturidentität `ID.CH.SIG` für diesen Nutzer erstellen und das dazugehörige Zertifikat `C.CH.SIG` an einem TSP X.509 nonQES eGK abrufen, wobei die für das Zertifikat benötigten Personenidentifikationsdaten des Nutzers aus dem Aufrufkontext der Operation (z.B. ID-Token oder Access Token) zu ermitteln sind. [ $\leq$ ]

Hinweis zu A\_26272: Das Erstellen von Signaturidentitäten bei der ersten Nutzung des Signaturdienstes durch einen Nutzer auf Basis des Operationsaufrufs kann auch für Nutzer erfolgen, die zu einem Kostenträger gehören, der den Anbieter des Signaturdienstes beauftragt hat.

#### **A\_26273 - Signaturdienst - Löschen von Signaturidentitäten für Versicherte anderer Kostenträger**

Der Signaturdienst MUSS Signaturidentitäten für Nutzer mit einer IK-Nummer,

- die nicht zu einem Kostenträger gehört, der den Anbieter des Signaturdienstes beauftragt hat und
- die ungleich der IK-Nummer 109500969 (="gematik-Kasse") ist und
- die ungleich der IK-Nummer 681100036 (="gematik Prüfkasse") ist

spätestens 2 Stunden nach ihrer Erzeugung löschen und das Zertifikat beim ausstellenden TSP X.509 nonQES eGK widerrufen. [ $\leq$ ]

**A\_17382-01 - Signaturdienst - Schutz gegen OWASP Top 10-Risiken**

Der Anbieter des Signaturdienstes MUSS sicherstellen, dass die Internet-Schnittstellen `I_Remote_Sign_Operations` und `I_Remote_Get_Certificate` resistent bezüglich der im aktuellen und den beiden vorherigen OWASP Top 10 Report(s) ausgewiesenen Risiken ist. [ $\leq$ ]

*Hinweis: Die Nichtanwendbarkeit eines OWASP Top 10-Risikos ist zu begründen. Für Informationen zum Umgang mit den OWASP Top 10-Risiken wird auf den aktuellen [OWASP Top 10 Report] und die darin enthaltenen Vorgehensweisen für z. B. Entwickler und Tester verwiesen.*

**A\_17528-01 - Signaturdienst - Schutz der Verbindung zum Signaturdienst**

Der Anbieter des Signaturdienstes MUSS sicherstellen, dass die Schnittstellen `I_Remote_Sign_Operations` und `I_Remote_Get_Certificate` von Klienten nur über eine gegen Abhören, Manipulation und Replay-Angriffe geschützte Verbindung genutzt werden kann. [ $\leq$ ]

**6.1.1 Operationsdefinition `I_Remote_Sign_Operations::sign_Data`****A\_17238-01 - Signaturdienst - Logische Schnittstelle `I_Remote_Sign_Operations` (Befristet)**

Der Signaturdienst MUSS die Schnittstelle `I_Remote_Sign_Operations::sign_Data` gemäß dem folgenden logischen Ablauf implementieren:

**Tabelle 1: Tab\_SigD\_01 - `I_Remote_Sign_Operations::sign_Data` - Definition**

Operation	I_Remote_Sign_Operations::sign_Data	
Beschreibung	Die Operation erzeugt eine ECDSA-Signatur unter Einhaltung der Vorgaben in [gemSpec_Krypt] des übergebenen Datum ( <i>Data</i> ) mittels des privaten Schlüssels des elektronischen Identifizierungsmittels ID.CH.AUT_ALT des aufrufenden Nutzers ( <i>Identifizier</i> ). Das signierte Datum ( <i>SignedData</i> ) und das Zertifikat des elektronischen Identifizierungsmittels C.CH.AUT_ALT der Identität, für die signiert wurde, werden als Ergebnis der Operation zurückgeliefert.	
Eingangsparameter		
Name	Beschreibung	Typ
Data	Die zu signierenden Daten.	Binary
Identifizier	Identifiziert, welches elektronisches Identifizierungsmittel ID.CH.AUT_ALT zur Signatur des Datums genutzt werden soll.  Der Identifizier ergibt sich aus den Attributen nach Authentisierung des Nutzers an einem sektoralen Identity Provider.	String
Ausgangsparameter		
Name	Beschreibung	Typ

<b>SignedData</b>	Das mit dem privaten Schlüssel des elektronischen Identifizierungsmittels ID.CH.AUT_ALT signierte Datum.	Binary
<b>Certificate</b>	Zertifikat C.CH.AUT_ALT des elektronischen Identifizierungsmittels, mit dessen zugehörigem privaten Schlüssel signiert wurde.	Certificate X.509

**[<=]**

*Hinweis: Wird die Schnittstelle ohne `privacy_mode` Parameter aufgerufen, wird eine Signatur mittels ID.CH.AUT\_ALT durchgeführt, analog zur bisherigen Implementierung.*

### A\_17238-03 - Signaturdienst - Logische Schnittstelle I\_Remote\_Sign\_Operations

Der Signaturdienst MUSS die Schnittstelle `I_Remote_Sign_Operations::sign_Data` gemäß dem folgenden logischen Ablauf implementieren:

**Tabelle 2: Tab\_SigD\_02 - I\_Remote\_Sign\_Operations::sign\_Data - Definition**

Operation	I_Remote_Sign_Operations::sign_Data	
Beschreibung	Die Operation erzeugt eine ECDSA-Signatur unter Einhaltung der Vorgaben in [gemSpec_Krypt] dem übergebenen Datum ( <i>Data</i> ) mittels des privaten Schlüssels des Signaturzertifikats ID.CH.SIG des aufrufenden Nutzers ( <i>Identifier</i> ). Das signierte Datum ( <i>SignedData</i> ) und das Signaturzertifikat C.CH.SIG mit dem signiert wurde, werden als Ergebnis der Operation zurück geliefert.	
Eingangsparameter		
Name	Beschreibung	Typ
Data	Die zu signierenden Daten bzw. im privacy_mode der zuvor durch den aufrufenden Client berechnete SHA256 Hashwert.	Binary
privacy_mode	Signalisierung, ob die zu signierenden Daten durch den Signaturdienst gehasht werden (false) oder ob bereits ein SHA256 Hashwert übermittelt wurde (true) - Default true	Boolean
guest_mode	Signalisierung, ob der Gast-Modus am sektoralen IDP genutzt werden soll.	Boolean
Identifier	Identifiziert, welches Signaturzertifikat ID.CH.SIG zur Signatur des Datums genutzt werden soll.  Der Identifier ergibt sich aus den Attributen nach Authentisierung des Nutzers an einem sektoralen Identity Provider. Falls guest_mode == true muss ein vom sektoralen IDP signiertes Token mit folgenden Attributen des Signaturinhabers ermittelt werden bzw. vorliegen:	variabel

	<ul style="list-style-type: none"> <li>urn:telematik:claims:display_name</li> <li>urn:telematik:claims:family_name</li> <li>urn:telematik:claims:given_name</li> <li>urn:telematik:claims:id</li> <li>urn:telematik:claims:organization.</li> </ul>	
<b>Ausgangsparameter</b>		
Name	Beschreibung	Typ
<b>SignedData</b>	Das mit dem privaten Schlüssel des Signaturzertifikat C.CH.SIG signierte Datum.	Binary
<b>Certificate</b>	Zertifikat C.CH.SIG mit dessen zugehörigem privaten Schlüssel signiert wurde.	Certificate X.509

**[<=]**

*Hinweis 1: Für die Signatur eines Datensatzes mit C.CH.SIG wurde keine neue Schnittstelle eingeführt. Es wird die Schnittstelle wiederverwendet, welche in Vorgängerversionen zur Signatur eines Datensatzes mit C.CH.AUT\_ALT (al.vi) verwendet wurde. Der Signaturdienst wird innerhalb eines ePA-FdV angesprochen, die ePA-FdVs sind in der Lage die unterschiedlichen Signaturdienst Versionen zu erkennen und damit die richtige Ausführung von sign\_data sicherzustellen.*

*Hinweis 2: Zur Anzahl der hinterlegten Zertifikate für Versicherte gibt es keine normativen Vorgaben. Die Anbieter von Signaturdiensten können das Management der Identitätsverwaltung frei im Rahmen der Spezifikation gestalten.*

## 6.1.2 Operationsdefinition I\_Remote\_Get\_Certificate

### A\_24682-01 - Signaturdienst - Logische Schnittstelle I\_Remote\_Get\_Certificate

Der Signaturdienst MUSS die Operation I\_Remote\_Get\_Certificate::get\_Certificate gemäß dem folgenden logischen Ablauf implementieren:

**Tabelle 3 Tab\_SigD\_01 - I\_Remote\_Get\_Certificate::get\_Certificate - Definition**

Operation	I_Remote_Get_Certificate	
<b>Beschreibung</b>	Die Operation liefert das Signaturzertifikat C.CH.SIG des aufrufenden Nutzers (Identifizier) zurück. Dieses wird verwendet, wenn nicht der Klartext eines zu signierenden Datensatzes an den Signaturdienst gesendet werden soll, aber das Signaturzertifikat selbst als Teil der zu signierenden Daten (wie etwa im Header eines JSON_Token) in die Signatur einfließt und daher bei der aufrufenden Anwendung bekannt sein muss, um den Hashwert zu erzeugen.	
<b>Eingangsparameter</b>		
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>
<b>guest_mode</b>	Signalisierung, ob der Gast-Modus am sektoralen IDP	Boolean



	genutzt werden soll.	
<b>Identifizier</b>	identifiziert, welches Signaturzertifikat zurückgegeben werden soll.  Der Identifizier ergibt sich aus den Attributen nach Authentisierung des Nutzers an einem sektoralen Identity Provider. Falls <code>guest_mode == true</code> muss ein vom sektoralen IDP signiertes Token mit folgenden Attributen des Signaturinhabers ermittelt werden bzw. vorliegen: <ul style="list-style-type: none"> <li>• <code>urn:telematik:claims:display_name</code></li> <li>• <code>urn:telematik:claims:family_name</code></li> <li>• <code>urn:telematik:claims:given_name</code></li> <li>• <code>urn:telematik:claims:id</code></li> <li>• <code>urn:telematik:claims:organization</code>.</li> </ul>	variabel
<b>Ausgangsparameter</b>		
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>
<b>Certificate</b>	Zertifikat C.CH.SIG, welches zum Identifizier beim Signaturdienst vorliegt.	Certificate X.509

[&lt;=]

### 6.1.3 Umsetzung I\_Remote\_Sign\_Operations::sign\_Data und I\_Remote\_Get\_Certificate

Die folgenden Anforderungen beschreiben die Umsetzung der Operation `I_Remote_Sign_Operations::sign_Data`.

#### A\_17527-01 - Signaturdienst - Aufruf der Remote Operationen nur über geschützte Verbindung

Der Signaturdienst MUSS sicherstellen, dass die Operation `I_Remote_Sign_Operations::sign_Data` und `I_Remote_Get_Certificate::get_Certificate` von Klienten nur über eine gegen Abhören, Manipulation und Replay-Angriffe geschützte Verbindung aufgerufen werden kann. [≤]

#### A\_17741-01 - Signaturdienst - Freischaltung vorzeitig beenden

Der Signaturdienst MUSS sicherstellen, dass der Client die Freischaltung der Operationen `I_Remote_Sign_Operations::sign_Data` und `I_Remote_Get_Certificate::get_Certificate` bzgl. eines Nutzers explizit beenden kann und somit beim nächsten Aufruf der Operationen durch diesen Nutzer eine erneute Authentifizierung erforderlich ist. [≤]

#### A\_18710-01 - Maximale Gültigkeit einer Authentifizierung

Der Signaturdienst und der Anbieter des Signaturdienstes MÜSSEN sicherstellen, dass eine erfolgreiche Authentifizierung des Nutzers für maximal 1 Stunde gültig ist, um die Operationen `I_Remote_Sign_Operations::sign_Data` und

I\_Remote\_Get\_Certificate::get\_Certificate von dem Client, von dem sich der Nutzer authentisiert hat, aufzurufen.【<=】

## 6.2 Schnittstelle P\_Create\_Identity

### A\_17375-02 - Signaturdienst - P\_Create\_Identity

Der Anbieter des Signaturdienstes MUSS eine Prozess-Schnittstelle umsetzen, mittels derer Kartenherausgeber dem Signaturdienst einen Auftrag zur Ausstellung eines Signaturzertifikats für einen Versicherten erteilen können. Der Auftrag MUSS die für das Signaturzertifikat notwendigen Personenidentifikationsdaten für die Zertifikate C.CH.AUT\_ALT und C.CH.SIG enthalten.

Die Zuordnung des Signaturzertifikats zu einem Nutzer erfolgt über die Identifikationsdaten des sektoralen Identity Provider.【<=】

*Hinweis: Für jeden Versicherten, der eine elektronische Patientenakte besitzt, muss auch ein entsprechendes Signaturzertifikat beim Signaturdienst beantragt werden.*

### A\_17372 - Signaturdienst - Schutz des Auftrags der Krankenkasse während des Transports

Der Anbieter des Signaturdienstes MUSS sicherstellen, dass die im Auftrag der Krankenkasse enthaltenen personenbezogenen oder sensiblen Daten während des Transports von der Krankenkasse zum Signaturdienst gegen Abhören, Manipulation und Replay-Angriffe geschützt werden.

【<=】

### A\_17379-01 - Signaturdienst - Zertifikatsabruf beim TSP X.509 nonQES eGK

Der Signaturdienst MUSS die Zertifikate des Typs C.CH.AUT\_ALT und C.CH.SIG über die Schnittstelle I\_Cert\_Provisioning zum Zertifikatabruf beim TSP X.509 nonQES eGK mit den vom Kartenherausgeber übermittelten Personenidentifikationsdaten aus dem Auftrag anfordern.【<=】

## 6.3 Schnittstelle P\_Delete\_Identity

### A\_17808-01 - Signaturdienst - P\_Delete\_Identity

Der Anbieter des Signaturdienstes MUSS eine Prozess-Schnittstelle umsetzen, mittels derer Kartenherausgeber die Löschung genau derjenigen Signaturzertifikate beim Signaturdienst veranlassen können, deren Ausstellung sie zuvor beauftragt haben.【<=】

---

## 7 Anhang - Verzeichnisse

---

### 7.1 Abkürzungen

Kürzel	Erläuterung
eGK	elektronische Gesundheitskarte
ePA	elektronische Patientenakte
HSM	Hardware Security Module
QES	Qualifizierte Elektronische Signatur
RSA	kryptographischer Algorithmus (nach Rivest, Shamir, Adleman)
TSP	Trust Service Provider

### 7.2 Glossar

Das Glossar wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt.

### 7.3 Abbildungsverzeichnis

Abbildung 1 Benachbarte Systeme des Signaturdienstes mit bereitgestellten und genutzten Schnittstellen.....8

### 7.4 Tabellenverzeichnis

Tabelle 1: Tab\_SigD\_01 - I\_Remote\_Sign\_Operations::sign\_Data - Definition.....14  
Tabelle 2: Tab\_SigD\_02 - I\_Remote\_Sign\_Operations::sign\_Data - Definition.....15  
Tabelle 3 Tab\_SigD\_01 - I\_Remote\_Get\_Certificate::get\_Certificate - Definition.....16

## 7.5 Referenzierte Dokumente

### 7.5.1 - Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte - Glossar
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemSpec_PKI]	gematik: Spezifikation PKI
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_X.509_TSP]	gematik: PKI für X.509-Zertifikate: Spezifikation Trust Service Provider X.509
[GVO_IOPVZ]	gematik: Geschäfts- und Verfahrensordnung für das Interoperabilitätsverzeichnis vesta: (Verzeichnis elektronischer Standards und Anwendungen im Gesundheitswesen)

### 7.5.2 - Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI-TR-03111]	Technical Guideline BSI TR-03111 Elliptic Curve Cryptography, Version 2.10, Date: 2018-06-01 <a href="https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_pdf.pdf?__blob=publicationFile&amp;v=2">https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_pdf.pdf?__blob=publicationFile&amp;v=2</a>
[eIDAS 910/2014]	Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
[eIDAS 2015/1502]	DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1502 DER KOMMISSION vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

[OWASP Top 10 Report]	OWASP Foundation, OWASP Top Ten Project: "OWASP Top 10 The Ten Most Critical Web Application Security Risks", <a href="https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project">https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project</a>
[RFC2119]	IETF (1997): Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, <a href="http://tools.ietf.org/html/rfc2119">http://tools.ietf.org/html/rfc2119</a>