

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# Spezifikation Signaturdienst

Version: 1.1.0  
Revision: 127092  
Stand: 28.06.2019  
Status: freigegeben  
Klassifizierung: öffentlich  
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	30.04.19		freigegeben	gematik
			Einarbeitung Änderungsliste P19.1	gematik
1.1.0	28.06.19		freigegeben	gematik

---

## Inhaltsverzeichnis

---

<b>1</b>	<b>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</b>	<b>Systemüberblick</b> .....	<b>6</b>
<b>3</b>	<b>Systemkontext</b> .....	<b>7</b>
3.1	Akteure und Rollen.....	7
3.2	Nachbarsysteme .....	7
<b>4</b>	<b>Zerlegung des Signaturdienstes</b> .....	<b>9</b>
<b>5</b>	<b>Übergreifende Festlegungen</b> .....	<b>10</b>
<b>6</b>	<b>Funktionsmerkmale</b> .....	<b>12</b>
6.1	<b>Schnittstelle I_Remote_Sign_Operations</b> .....	<b>12</b>
6.1.1	Operationsdefinition I_Remote_Sign_Operations::sign_Data .....	12
6.1.2	Umsetzung I_Remote_Sign_Operations::sign_Data .....	13
6.2	<b>Schnittstelle P_Create_Identity</b> .....	<b>14</b>
6.3	<b>Schnittstelle P_Delete_Identity</b> .....	<b>15</b>
<b>7</b>	<b>Anhang – Verzeichnisse</b> .....	<b>16</b>
7.1	<b>Abkürzungen</b> .....	<b>16</b>
7.2	<b>Glossar</b> .....	<b>16</b>
7.3	<b>Abbildungsverzeichnis</b> .....	<b>16</b>
7.4	<b>Tabellenverzeichnis</b> .....	<b>16</b>
7.5	<b>Referenzierte Dokumente</b> .....	<b>17</b>
7.5.1	– Dokumente der gematik.....	17
7.5.2	– Weitere Dokumente .....	17

---

# 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. Dokumentenlandkarte, 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 Identifizierungsmittel für Versicherte in der Umgebung des Anbieters des Signaturdienstes. Ein elektronisches Identifizierungsmittel ist gemäß Verordnung (EU) Nr. 910/2014 [eIDAS] eine materielle und/oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten verwendet wird. Die vom Signaturdienst ausgestellten elektronischen ~~Identifikationsmittel~~ **Identifizierungsmittel** sind kryptographische Identitäten basierend auf asymmetrischer Kryptographie und Teil des Vertrauensraums für X.509 nonQES-Identitäten der Telematikinfrastruktur. Die vom Signaturdienst erstellten elektronischen Identifizierungsmittel nutzen Versicherte zur Authentisierung an Diensten in der TI.

Versicherte können elektronische Signaturen mittels der vom Signaturdienst ausgestellten Identifizierungsmittel in der vom Anbieter des Signaturdienstes geführten Umgebung erstellen lassen. Die elektronischen Signaturen des Signaturdienstes sind eine Alternative zur elektronischen Signatur mittels der Identität ID.CH.AUT der eGK.

Der Signaturdienst erstellt elektronische Identifizierungsmittel für Versicherte ausschließlich im Auftrag des Kartenherausgebers der eGK des Versicherten. Vom Kartenherausgeber der eGK des Versicherten erhält der Anbieter des Signaturdienstes die Personenidentifizierungsdaten für das auszustellende elektronische Identifizierungsmittel. Personenidentifizierungsdaten sind ein Datensatz, der es ermöglicht, die Identität des Versicherten festzustellen. Die Personenidentifizierungsdaten für die vom Signaturdienst ausgestellten elektronischen Identifizierungsmittel entsprechen den Personenidentifizierungsdaten im Zertifikat C.CH.AUT der eGK des Versicherten. Das Zertifikatsprofil C.CH.AUT\_ALT für die vom Signaturdienst ausgestellten elektronischen ~~Identifikationsmittel~~ **Identifizierungsmittel** ist in [gemSpec\_PKI] festgelegt.

## 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 auf deren Wunsch hin elektronische **Identifikationsmittel** **Identifizierungsmittel** ausstellen zu lassen, die alternativ zur Identität ID.CH.AUT der eGK genutzt werden können. Falls sich ein Versicherter gegenüber dem Kartenherausgeber seiner eGK für ein elektronisches Identifizierungsmittel entscheidet, beauftragt der Kartenherausgeber eGK für diesen Versicherten beim Anbieter des Signaturdienstes das elektronische **Identifikationsmittel** **Identifizierungsmittel**. Der Kartenherausgeber eGK übermittelt hierzu die für das elektronische **Identifikationsmittel** **Identifizierungsmittel** notwendigen Personenidentifikationsdaten des Versicherten (u.a. Name, KVNR) an den Anbieter des Signaturdienstes.

Der Kartenherausgeber eGK veranlasst die Sperrung von elektronischen **Identifikationsmitteln** **Identifizierungsmitteln** bzgl. seiner Versicherten beim TSP X.509 nonQES eGK, der das Zertifikat für das elektronische **Identifikationsmittel** **Identifizierungsmittel** erstellt hat.

#### Versicherte

Versicherte nutzen mittels eigener Client-Systeme (z.B. mit einem ePA-Frontend des Versicherten) den Signaturdienst, um mittels der elektronischen **Identifikationsmittel** **Identifizierungsmittel** anderen Diensten ihre Identität zu bestätigen.

Versicherte richten sich an den Kartenherausgeber ihrer eGK, falls sie ihr elektronisches **Identifikationsmittel** **Identifizierungsmittel** sperren lassen möchten.

### 3.2 Nachbarsysteme

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

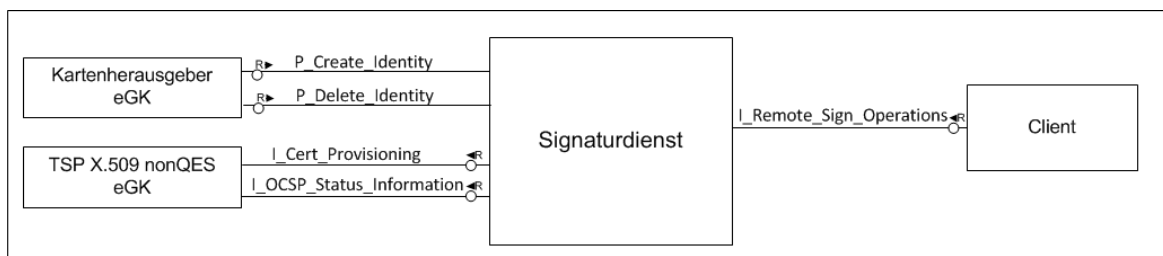


Abbildung 1: benachbarte Systeme des Signaturdienstes mit bereitgestellten und genutzten Schnittstellen

Der Signaturdienst wird als Provider einer technischen Schnittstelle zum Erstellen elektronischer Signaturen für Clienten und einer Prozessschnittstelle für Kartenherausgeber eGK zum Beauftragen und Löschen von elektronischen Identifizierungsmitteln für Versicherte aufgerufen.

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



---

## 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 - Signaturdienst - Produkt ist geeignet für Sicherheitsniveau "substanziell" gemäß eIDAS-Verordnung**

Der Hersteller des Signaturdienstes MUSS sein Produkt so implementieren, dass ein Anbieter des Signaturdienstes die Anforderungen der Verordnung (EU) Nr. 910/2014 an elektronische Identifizierungsmittel mit einem Sicherheitsniveau von mindestens "substanziell" erfüllen kann. [≤]

### **A\_17336 - Signaturdienst - Sicherheitsniveau "substanziell" gemäß eIDAS-Verordnung**

Der Anbieter des Signaturdienstes MUSS für den angebotenen Signaturdienst die Anforderungen der Verordnung (EU) Nr. 910/2014 an elektronische Identifizierungsmittel mit einem Sicherheitsniveau von mindestens "substanziell" erfüllen. Davon ausgenommen ist die Anmeldung gemäß Anhang 2.1 der Durchführungsverordnung (EU) 2015/1502. [≤]

Die Durchführungsverordnung (EU) 2015/1502 [eIDAS 2015/1502] gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 [eIDAS 910/2014] legt die Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel fest.

Die Anmeldung des elektronischen Identifizierungsmittels 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.

Im Rahmen der Anbieterzulassung prüft der unabhängige Sicherheitsgutachter, dass die vom Anbieter ausgestellten elektronischen Identifizierungsmittel die Mindestanforderungen des Sicherheitsniveaus "substanziell" erfüllen.

Eine Notifizierung des elektronischen Identifizierungssystems, welches die elektronischen Identifizierungsmittel ausstellt, 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**

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\_17370 - Signaturdienst - ECC-Verfahren für elektronische Identifizierungsmittel**

Der Signaturdienst MUSS elektronische Identifizierungsmittel auf der Grundlage von ECC-Verfahren erstellen. [≤]

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

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

Der Signaturdienst DARF elektronische Identifizierungsmittel NICHT auf der Grundlage von RSA-Verfahren erstellen.[<=]

#### **A\_17339 - Signaturdienst - Speicherung privater Schlüssel im HSM**

Der Anbieter des Signaturdienstes MUSS die privaten Schlüssel der elektronischen Identifizierungsmittel in 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\_17852 - Signaturdienst - Information des Versicherten über Änderungen an Authentifizierungsfaktoren**

Der Anbieter des Signaturdienstes MUSS den Versicherten über Änderungen an Authentifizierungsfaktoren informieren.

Die Information des Versicherten kann dabei auch über den Kartenherausgeber erfolgen, der den Anbieter des Signaturdienstes mit der Erstellung des elektronischen Identifizierungsmittels beauftragt hat.

[<=]

Hinweis: Dies könnten z. B. Änderungen von E-Mail-Adressen, Mobilfunknummern, registrierten Geräten oder Kennwörtern sein.

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

Der Anbieter des Signaturdienstes MUSS dem Versicherten auf dessen Verlangen Auskunft geben über

- erfolgte Zugriffe auf das elektronische Identifizierungsmittel des Versicherten und
- Änderungen der Authentifizierungsfaktoren des Versicherten.

Die Auskunft des Versicherten kann auch über den Kartenherausgeber erfolgen, der den Anbieter des Signaturdienstes mit der Erstellung des elektronischen Identifizierungsmittels beauftragt hat.

[<=]

Hinweis: Die Auskunft des Versicherten kann auch über den Kartenherausgeber erfolgen, der den Anbieter des Signaturdienstes mit der Erstellung des elektronischen Identifizierungsmittels 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.

---

## 6 Funktionsmerkmale

---

Der Signaturdienst realisiert die Funktionsmerkmale zur Erstellung elektronischer **Identifikationsmittel** **Identifizierungsmittel** und deren Nutzung für elektronische Signaturen. Das Funktionsmerkmal wird über die Implementierung der Schnittstellen `I_Remote_Sign_Operation`, `P_Create_Identity` und `P_Delete_Identity` realisiert.

### 6.1 Schnittstelle `I_Remote_Sign_Operations`

Die in diesem Abschnitt beschriebene logische Schnittstelle `I_Remote_Sign_Operations` setzt die gleichnamige Schnittstelle aus [gemKPT\_Arch\_TIP] um.

#### **A\_17383 - Signaturdienst - `I_Remote_Sign_Operations` im Internet**

Der Signaturdienst MUSS die Schnittstelle `I_Remote_Sign_Operations` im Internet anbieten. [<=]

#### **A\_17583 - Signaturdienst - Eintrag in das Interoperabilitätsverzeichnis vesta**

Der Hersteller des Signaturdienstes MUSS die Spezifikation seiner Implementierung der Schnittstelle `I_Remote_Sign_Operations::sign_Data` in das Interoperabilitätsverzeichnis vesta der gematik aufnehmen zu lassen. [<=]

Die Regeln zur Aufnahme in das Interoperabilitätsverzeichnis vesta sind in der Geschäfts- und Verfahrensordnung [GVO\_IOPVZ] beschrieben. **Regelungen zur Information der Hersteller von Clients des Signaturdienstes bei Änderungen der Implementierung der Schnittstelle werden in einer Folgeversion ergänzt.**

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

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

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 - Signaturdienst - Schutz der Verbindung zum Signaturdienst**

Der Anbieter des Signaturdienstes MUSS sicherstellen, dass die Schnittstelle `I_Remote_Sign_Operations` von Clienten nur über eine gegen Abhören, Manipulation und Replay-Angriffe geschützte Verbindung genutzt werden kann. [<=]

#### 6.1.1 Operationsdefinition `I_Remote_Sign_Operations::sign_Data`

##### **A\_17238 - Signaturdienst - Logische Schnittstelle `I_Remote_Sign_Operations`**

Der Signaturdienst MUSS die Schnittstelle `I_Remote_Sign_Operations::sign_Data` gemäß der folgenden logischen Signatur implementieren:

Tabelle 1: Tab\_SigD\_01 - I\_Remote\_Sign\_Operations::sign\_Data - Definition

Operation	I_Remote_Sign_Operations::sign_Data		
<b>Beschreibung</b>	Die Operation erzeugt eine ECDSA-Signatur unter Einhaltung der Vorgaben in [gemSpec_Krypt] an dem übergebenen Datum ( <i>Data</i> ) mittels des privaten Schlüssels des elektronischen Identifikationsmittels Identifizierungsmittels ID.CH.AUT_ALT des aufrufenden Nutzers ( <i>Identifizier</i> ). Das signierte Datum ( <i>SignedData</i> ) und das Zertifikat des elektronischen Identifikationsmittels Identifizierungsmittels C.CH.AUT_ALT der Identität, für die signiert wurde, werden als Ergebnis der Operation zurückgeliefert.		
<b>Eingangsparameter</b>			
Name	Beschreibung	Typ	opt.
<b>Data</b>	Die zu signierenden Daten.	Binary	-
<b>Identifizier</b>	Identifiziert, welches elektronisches Identifikationsmittel Identifizierungsmittel ID.CH.AUT_ALT zur Signatur des Datums genutzt werden soll.	String	-
<b>Ausgangsparameter</b>			
Name	Beschreibung	Typ	opt.
<b>signedData</b>	Das mit dem privaten Schlüssel des elektronischen Identifikationsmittels Identifizierungsmittels ID.CH.AUT_ALT signierte Datum.	Binary	-
<b>Certificate</b>	Zertifikat C.CH.AUT_ALT des elektronischen Identifikationsmittels Identifizierungsmittels, mit dessen zugehörigem privaten Schlüssel signiert wurde.	<b>Certificate X.509</b>	-

[&lt;=]

### 6.1.2 Umsetzung I\_Remote\_Sign\_Operations::sign\_Data

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

#### A\_17384 - Signaturdienst - Operationsaufruf erfordert erfolgreiche Authentifizierung

Der Signaturdienst MUSS sicherstellen, dass die Operation `I_Remote_Sign_Operations::sign_Data` nur nach vorheriger erfolgreicher Authentifikation des Nutzers mit einem Sicherheitsniveau von mindestens "substanziell" (gemäß genutzt wird, die die Anforderungen der Verordnung (EU) Nr. 910/2014 an elektronische Identifizierungssysteme) genutzt wird, mit einem Sicherheitsniveau von mindestens "substanziell" erfüllt. [≤]

**A\_18172 - Signaturdienst - Authentifizierungsverfahren erfüllen TR-03107-1 für substanzuell**

Der Anbieter des Signaturdienstes MUSS sicherstellen, dass nur Authentifizierungsverfahren genutzt werden, die vom BSI in der TR-03107-1 für ein Vertrauensniveau von mindestens "substanzuell" als geeignet eingestuft werden. [<=]

**A\_18173 - Signaturdienst - Anpassung Authentifizierungsverfahren bei Änderung TR-03107-1**

Der Anbieter des Signaturdienstes MUSS von ihm eingesetzte Authentifizierungsverfahren, die nach einer Aktualisierung der TR-03107-1 des BSI nicht mehr für das Vertrauensniveau "substanzuell" geeignet sind, unverzüglich zu einem nach der TR-03107-1 des BSI für "substanzuell" geeigneten Authentifizierungsverfahren migrieren. [<=]

**A\_17527 - Signaturdienst - Aufruf der Operation nur über geschützte Verbindung**

Der Signaturdienst MUSS sicherstellen, dass die Operation I\_Remote\_Sign\_Operations::sign\_Data von Clienten nur über eine gegen Abhören, Manipulation und Replay-Angriffe geschützte Verbindung aufgerufen werden kann. [<=]

**A\_17740 - Signaturdienst - Zeitlich begrenzte Freischaltung**

Der Signaturdienst MUSS sicherstellen, dass die Operation I\_Remote\_Sign\_Operations::sign\_Data bis 5 Minuten nach dem Zeitpunkt der Authentifizierung des Nutzers bzgl. seines elektronischen Identifizierungsmittels freigeschaltet ist und durch diesen Nutzer ohne erneute Authentifizierung aufgerufen werden kann. [<=]

**A\_17741 - Signaturdienst - Freischaltung vorzeitig beenden**

Der Signaturdienst MUSS sicherstellen, dass der Client die Freischaltung der Operation I\_Remote\_Sign\_Operations::sign\_Data bzgl. eines Nutzers explizit beenden kann und somit beim nächsten Aufruf der Operation durch diesen Nutzer eine erneute Authentifizierung erforderlich ist. [<=]

**A\_17742 - Signaturdienst - Anbieter stellt begrenzte Freischaltung sicher**

Der Anbieter des Signaturdienstes MUSS sicherstellen, dass nur derjenige Nutzer die Operation I\_Remote\_Sign\_Operations::sign\_Data für ein elektronisches Identifizierungsmittel ohne explizite Authentifizierung aufrufen kann, wenn sich der Nutzer für dieses elektronische Identifizierungsmittel vor weniger als 5 Minuten bereits erfolgreich an der Operation I\_Remote\_Sign\_Operations::sign\_Data authentisiert hat und seitdem der Client die Freischaltung nicht beendet hat. [<=]

## 6.2 Schnittstelle P\_Create\_Identity

**A\_17375 - Signaturdienst - P\_Create\_Identity**

Der Anbieter des Signaturdienstes MUSS eine Prozess-Schnittstelle umsetzen, mittels derer Kartenherausgeber dem Signaturdienst einen Auftrag zur Ausstellung eines elektronischen Identifizierungsmittels für einen Versicherten erteilen können. Der Auftrag MUSS die für das elektronische Identifizierungsmittel notwendigen Personenidentifikationsdaten für das Zertifikat C.CH.AUT\_ALT sowie die erforderlichen Verifikationsdaten, die der Signaturdienstanbieter zur Verifikation des Versicherten bei der Aktivierung des elektronischen Identifizierungsmerkmals benötigt, enthalten. [<=]

**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 - Signaturdienst - Zertifikatsabruf beim TSP X.509 nonQES eGK**

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

#### **A\_17381 - Signaturdienst - Verifikation des Versicherten vor erster Nutzung**

Der Anbieter des Signaturdienstes MUSS den Versicherten, für den das elektronische **Identifikationsmittel** **Identifizierungsmittel** ausgestellt wurde, mittels der vom Kartenherausgeber im Auftrag übermittelten Verifikationsdaten vor der ersten Nutzung des elektronischen **Identifikationsmittels** **Identifizierungsmittels** authentifizieren, um das elektronische **Identifikationsmittel** **Identifizierungsmittel** zu aktivieren. [<=]

### **6.3 Schnittstelle P\_Delete\_Identity**

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

Der Anbieter des Signaturdienstes MUSS eine Prozess-Schnittstelle umsetzen, mittels derer Kartenherausgeber die Löschung genau derjenigen elektronischen **Identifikationsmittel** **Identifizierungsmittel** 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.....7  
 |

### 7.4 Tabellenverzeichnis

|  
 Tabelle 1: Tab\_SigD\_01 - I\_Remote\_Sign\_Operations::sign\_Data - Definition.....13  
 |



## 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. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[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 2015/15]	DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1502 DER KOMMISSION vom 8. September 2015

02]	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>