

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# **Produkttypsteckbrief**

## ***Prüfvorschrift***

# **Signaturdienst**

Produkttyp Version: 1.1.3-0  
Produkttyp Status: freigegeben

Version: 1.0.0  
Revision: 245844  
Stand: 26.06.2020  
Status: freigegeben  
Klassifizierung: öffentlich  
Referenzierung: gemProdT\_SigD\_PTV\_1.1.3-0

---

## Historie Produkttypversion und Produkttypsteckbrief

---

### Historie Produkttypversion

Die Produkttypversion ändert sich, wenn sich die Anforderungslage für den Produkttyp ändert und die Umsetzung durch Produktentwicklungen ebenfalls betroffen ist.

| Produkttypversion | Beschreibung der Änderung               | Referenz                  |
|-------------------|-----------------------------------------|---------------------------|
| 1.0.0-0           | Initiale Version auf Dokumentenebene    | gemProdT_SigD_PTV_1.0.0-0 |
| 1.1.0-0           | Anpassung auf Release 3.1.1             | gemProdT_SigD_PTV_1.1.0-0 |
| 1.1.1-0           | Anpassung auf Release 3.1.2             | gemProdT_SigD_PTV_1.1.1-0 |
| 1.1.2-0           | Anpassung auf Release 3.1.3             | gemProdT_SigD_PTV_1.1.2-0 |
| 1.1.2-1           | Anpassung auf Release 3.1.3<br>Hotfix 2 | gemProdT_SigD_PTV_1.1.2-1 |

### Historie Produkttypsteckbrief

Die Dokumentenversion des Produkttypsteckbriefs ändert sich mit jeder inhaltlichen oder redaktionellen Änderung des Produkttypsteckbriefs und seinen referenzierten Dokumenten. Redaktionelle Änderungen haben keine Auswirkung auf die Produkttypversion.

| Version | Stand    | Kap. | Grund der Änderung, besondere Hinweise | Bearbeiter |
|---------|----------|------|----------------------------------------|------------|
| 1.0.0   | 26.06.20 |      | freigegeben                            | gematik    |

---

## Inhaltsverzeichnis

---

|                                                              |           |
|--------------------------------------------------------------|-----------|
| <b>1 Einführung .....</b>                                    | <b>4</b>  |
| 1.1 Zielsetzung und Einordnung des Dokumentes .....          | 4         |
| 1.2 Zielgruppe .....                                         | 4         |
| 1.3 Geltungsbereich .....                                    | 4         |
| 1.4 Abgrenzung des Dokumentes .....                          | 4         |
| 1.5 Methodik .....                                           | 5         |
| <b>2 Dokumente .....</b>                                     | <b>6</b>  |
| <b>3 Blattanforderungen.....</b>                             | <b>7</b>  |
| 3.1 Anforderungen zur funktionalen Eignung .....             | 7         |
| 3.1.1 Produkttest/Produktübergreifender Test .....           | 7         |
| 3.1.2 Herstellererklärung funktionale Eignung .....          | 10        |
| 3.2 Anforderungen zur sicherheitstechnischen Eignung .....   | 14        |
| 3.2.1 Herstellererklärung sicherheitstechnische Eignung..... | 14        |
| <b>4 Produktypspezifische Merkmale .....</b>                 | <b>16</b> |
| <b>5 Anhang – Verzeichnisse .....</b>                        | <b>17</b> |
| 5.1 Abkürzungen .....                                        | 17        |
| 5.2 Tabellenverzeichnis .....                                | 17        |
| 5.3 Referenzierte Dokumente .....                            | 17        |

---

## **1 Einführung**

---

### **1.1 Zielsetzung und Einordnung des Dokumentes**

Dieser Produkttypsteckbrief verzeichnet verbindlich die Anforderungen der gematik an Herstellung und Betrieb von Produkten des Produkttyps oder verweist auf Dokumente, in denen verbindliche Anforderungen mit ggf. anderer Notation zu finden sind. Die Anforderungen bilden die Grundlage für die Erteilung von Zulassungen, Zertifizierungen bzw. Bestätigungen durch die gematik. (Wenn im weiteren Dokument vereinfachend der Begriff „Zulassung“ verwendet wird, so ist dies der besseren Lesbarkeit geschuldet und umfasst übergreifend neben dem Verfahren der Zulassung auch Zertifizierungen und Bestätigungen der gematik-Zulassungsstelle.)

Die Anforderungen werden über ihren Identifier, ihren Titel sowie die Dokumentenquelle referenziert. Die Anforderungen mit ihrem vollständigen, normativen Inhalt sind dem jeweils referenzierten Dokument zu entnehmen.

### **1.2 Zielgruppe**

Der Produkttypsteckbrief richtet sich an Hersteller und Anbieter des Produkttyps Signaturdienst sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

Das Dokument ist außerdem zu verwenden von:

- der gematik im Rahmen des Zulassungsverfahrens
- Auditoren

Bei zentralen Diensten der TI-Plattform und fachanwendungsspezifischen Diensten beziehen sich Anforderungen, die sowohl an Anbieter als auch Hersteller gerichtet sind, jeweils auf den Anbieter als Zulassungsnehmer, bei dezentralen Produkten auf den Hersteller.

### **1.3 Geltungsbereich**

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Leistungsbeschreibung) festgelegt und bekannt gegeben.

### **1.4 Abgrenzung des Dokumentes**

Dieses Dokument macht keine Aussagen zur Aufteilung der Produktentwicklung bzw. Produktherstellung auf verschiedene Hersteller und Anbieter.

Dokumente zu den Zulassungsverfahren für den Produkttyp sind nicht aufgeführt. Die geltenden Verfahren und Regelungen zur Beantragung und Durchführung von Zulassungsverfahren können der Homepage der gematik entnommen werden.

## **1.5 Methodik**

Die im Dokument verzeichneten Anforderungen werden tabellarisch dargestellt. Die Tabellenspalten haben die folgende Bedeutung:

**Afo-ID:** Identifiziert die Anforderung eindeutig im Gesamtbestand aller Festlegungen der gematik.

**Afo-Bezeichnung:** Gibt den Titel einer Anforderung informativ wieder, um die thematische Einordnung zu erleichtern. Der vollständige Inhalt der Anforderung ist dem Dokument zu entnehmen, auf das die Quellenangabe verweist.

**Quelle (Referenz):** Verweist auf das Dokument, das die Anforderung definiert.

---

## 2 Dokumente

---

Die nachfolgenden Dokumente enthalten alle für den Produkttyp normativen Anforderungen.

**Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion**

| Dokumenten Kürzel     | Bezeichnung des Dokumentes                                                                         | Version |
|-----------------------|----------------------------------------------------------------------------------------------------|---------|
| gemSpec_TSL           | Spezifikation TSL-Dienst                                                                           | 1.17.0  |
| gemSpec_SigD          | Spezifikation Signaturdienst                                                                       | 1.3.0   |
| gemSpec_Perf          | Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform                              | 2.10.0  |
| gemKPT_Test           | Testkonzept der TI                                                                                 | 2.6.1   |
| gemSpec_DS_Hersteller | Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller                       | 1.1.0   |
| gemSpec_Krypt         | Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur | 2.16.0  |
| gemSpec_SST_LD_BD     | Spezifikation Logdaten und Betriebsdatenerfassung                                                  | 1.1.1   |
| gemSpec_Net           | Übergreifende Spezifikation Netzwerk                                                               | 1.17.1  |
| gemSpec_OM            | Übergreifende Spezifikation Operations und Maintenance                                             | 1.14.0  |
| gemSpec_PKI           | Übergreifende Spezifikation – Spezifikation PKI                                                    | 2.8.1   |

### Errata

Neben den vorgenannten Dokumenten werden auf der Internetseite der gematik bei Bedarf Errata-Dokumente mit normativen Ergänzungen bzw. Korrekturen zu den Spezifikationsdokumenten veröffentlicht. Sofern in den Errata der vorliegende Produkttyp benannt wird, sind diese bei der Umsetzung des Produkttyps entsprechend der Vorgabe in der Dokumentenlandkarte zu berücksichtigen. Dabei kann eine abweichende Produkttypversion festgelegt werden.

## 3 Blattanforderungen

Die folgenden Abschnitte verzeichnen alle für den Produkttypen normativen Anforderungen, die für die Herstellung und den Betrieb von Produkten des Produkttyps notwendig sind (Blattanforderungen). Die Anforderungen sind gruppiert nach der Art der Nachweisführung ihrer Erfüllung als Grundlage der Zulassung, Zertifizierung bzw. Bestätigung.

### 3.1 Anforderungen zur funktionalen Eignung

#### 3.1.1 Produkttest/Produktübergreifender Test

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Anforderungen an den technischen Teil des Produkttyps verzeichnet, deren Umsetzung im Zuge von Zulassungstests durch die gematik geprüft wird.

**Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"**

| Afo-ID      | Afo-Bezeichnung                                                                                | Quelle (Referenz) |
|-------------|------------------------------------------------------------------------------------------------|-------------------|
| TIP1-A_5120 | Clients des TSL-Dienstes: HTTP-Komprimierung unterstützen                                      | gemSpec_TSL       |
| A_17369     | Signaturdienst - Elektronische Identifizierungsmittel sind kryptographische Identitäten der TI | gemSpec_SigD      |
| A_17370     | Signaturdienst - ECC-Verfahren für elektronische Identifizierungsmittel                        | gemSpec_SigD      |
| A_17371     | Signaturdienst - Keine RSA-Verfahren für elektronische Identifizierungsmittel                  | gemSpec_SigD      |
| A_17383     | Signaturdienst - I_Remote_Sign_Operations im Internet                                          | gemSpec_SigD      |
| A_17238     | Signaturdienst - Logische Schnittstelle I_Remote_Sign_Operations                               | gemSpec_SigD      |
| A_17384     | Signaturdienst - Operationsaufruf erfordert erfolgreiche Authentifizierung                     | gemSpec_SigD      |
| A_17527     | Signaturdienst - Aufruf der Operation nur über geschützte Verbindung                           | gemSpec_SigD      |
| A_17741     | Signaturdienst - Freischaltung vorzeitig beenden                                               | gemSpec_SigD      |
| A_18710     | Maximale Gültigkeit einer Authentifizierung                                                    | gemSpec_SigD      |

|            |                                                                                                                              |                   |
|------------|------------------------------------------------------------------------------------------------------------------------------|-------------------|
| A_18711    | Signaturdienst – Nutzung einer erfolgreichen Authentifizierung                                                               | gemSpec_SigD      |
| A_17379    | Signaturdienst - Zertifikatsabruf beim TSP X.509 nonQES eGK                                                                  | gemSpec_SigD      |
| A_17678    | Performance - Rohdaten-Performance-Berichte - Übermittlung                                                                   | gemSpec_Perf      |
| GS-A_4145  | Performance – zentrale Dienste – Robustheit gegenüber Lastspitzen                                                            | gemSpec_Perf      |
| A_18018    | Performance - Signaturdienst - Spitzenlastvorgaben                                                                           | gemSpec_Perf      |
| A_17802    | Performance – Signaturdienst – Bearbeitungszeit unter Last                                                                   | gemSpec_Perf      |
| A_18178    | Performance - Signaturdienst - Erfassung von Rohdaten                                                                        | gemSpec_Perf      |
| GS-A_4384  | TLS-Verbindungen                                                                                                             | gemSpec_Krypt     |
| A_17416-01 | Schnittstelle Betriebsdatenerfassung Prüfung des TLS-Server-Zertifikats durch Fach- und zentrale Dienste                     | gemSpec_SST_LD_BD |
| A_17733-01 | Schnittstelle Betriebsdatenerfassung Datei-Upload                                                                            | gemSpec_SST_LD_BD |
| GS-A_4832  | Path MTU Discovery und ICMP Response                                                                                         | gemSpec_Net       |
| GS-A_4036  | Möglichkeit des Einsatzes von Hochverfügbarkeitsprotokollen                                                                  | gemSpec_Net       |
| GS-A_4763  | Einsatz von Hochverfügbarkeitsprotokollen                                                                                    | gemSpec_Net       |
| GS-A_3932  | Abfrage der in der Topologie am nächsten stehenden Nameservers                                                               | gemSpec_Net       |
| GS-A_3834  | DNS-Protokoll, Nameserver-Implementierungen                                                                                  | gemSpec_Net       |
| GS-A_3842  | DNS, Verwendung von iterativen queries zwischen Nameservern                                                                  | gemSpec_Net       |
| GS-A_4879  | DNSSEC, Zonen im Namensraum Internet mittels DNSSEC sichern                                                                  | gemSpec_Net       |
| GS-A_3832  | DNS-Protokoll, Resolver-Implementierungen                                                                                    | gemSpec_Net       |
| GS-A_4817  | Produkttypen der Fachanwendungen sowie der zentralen TI-Plattform, Einbringung des DNSSEC Trust Anchor für den Namensraum TI | gemSpec_Net       |
| GS-A_3934  | NTP-Client-Implementierungen, Protokoll NTPv4                                                                                | gemSpec_Net       |

|           |                                                                                                                                                           |             |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| GS-A_3937 | NTP-Client-Implementierungen, Association Mode und Polling Intervall                                                                                      | gemSpec_Net |
| GS-A_5025 | Versionierung von Produkten auf Basis von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten durch die Produktidentifikation | gemSpec_OM  |
| GS-A_3702 | Inhalt der Selbstauskunft von Produkten außer Karten                                                                                                      | gemSpec_OM  |
| GS-A_4543 | Rückgabe der Selbstauskunft von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten                                           | gemSpec_OM  |
| GS-A_5252 | Generische Fehlermeldungen außerhalb von WebServices                                                                                                      | gemSpec_OM  |
| GS-A_4637 | TUCs, Durchführung Fehlerüberprüfung                                                                                                                      | gemSpec_PKI |
| GS-A_4829 | TUCs, Fehlerbehandlung                                                                                                                                    | gemSpec_PKI |
| A_17688   | Nutzung des ECC-RSA-Vertrauensraumes (ECC-Migration)                                                                                                      | gemSpec_PKI |
| A_17689   | Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach ECC-RSA (ECC-Migration)                                                                    | gemSpec_PKI |
| A_17820   | Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach RSA (ECC-Migration)                                                                        | gemSpec_PKI |
| A_17821   | Wechsel des Vertrauensraumes mittels Cross-Zertifikaten (ECC-Migration)                                                                                   | gemSpec_PKI |
| GS-A_4642 | TUC_PKI_001: Periodische Aktualisierung TI-Vertrauensraum                                                                                                 | gemSpec_PKI |
| GS-A_4643 | TUC_PKI_013: Import TI-Vertrauensanker aus TSL                                                                                                            | gemSpec_PKI |
| GS-A_4646 | TUC_PKI_017: Lokalisierung TSL Download-Adressen                                                                                                          | gemSpec_PKI |
| GS-A_4647 | TUC_PKI_016: Download der TSL-Datei                                                                                                                       | gemSpec_PKI |
| GS-A_5336 | Zertifikatsprüfung nach Ablauf TSL-Graceperiod                                                                                                            | gemSpec_PKI |
| A_17690   | Nutzung der Hash-Datei für TSL (ECC-Migration)                                                                                                            | gemSpec_PKI |
| GS-A_4648 | TUC_PKI_019: Prüfung der Aktualität der TSL                                                                                                               | gemSpec_PKI |
| GS-A_4649 | TUC_PKI_020: XML-Dokument validieren                                                                                                                      | gemSpec_PKI |

|           |                                                             |             |
|-----------|-------------------------------------------------------------|-------------|
| GS-A_4650 | TUC_PKI_011: Prüfung des TSL-Signer-Zertifikates            | gemSpec_PKI |
| GS-A_4651 | TUC_PKI_012: XML-Signatur-Prüfung                           | gemSpec_PKI |
| GS-A_4898 | TSL-Grace-Period einer TSL                                  | gemSpec_PKI |
| GS-A_4899 | TSL Update-Prüfintervall                                    | gemSpec_PKI |
| A_17700   | TSL-Auswertung ServiceTypeIdentifier "unspecified"          | gemSpec_PKI |
| GS-A_4652 | TUC_PKI_018: Zertifikatsprüfung in der TI                   | gemSpec_PKI |
| GS-A_4653 | TUC_PKI_002: Gültigkeitsprüfung des Zertifikats             | gemSpec_PKI |
| GS-A_4654 | TUC_PKI_003: CA-Zertifikat finden                           | gemSpec_PKI |
| GS-A_4655 | TUC_PKI_004: Mathematische Prüfung der Zertifikatssignatur  | gemSpec_PKI |
| GS-A_4656 | TUC_PKI_005: Adresse für Status- und Sperrprüfung ermitteln | gemSpec_PKI |
| GS-A_4657 | TUC_PKI_006: OCSP-Abfrage                                   | gemSpec_PKI |
| GS-A_4660 | TUC_PKI_009: Rollenermittlung                               | gemSpec_PKI |
| GS-A_4749 | TUC_PKI_007: Prüfung Zertifikatstyp                         | gemSpec_PKI |
| GS-A_4661 | kritische Erweiterungen in Zertifikaten                     | gemSpec_PKI |
| GS-A_4662 | Bedingungen für TLS-Handshake                               | gemSpec_PKI |
| GS-A_4663 | Zertifikats-Prüfparameter für den TLS-Handshake             | gemSpec_PKI |
| GS-A_5077 | FQDN-Prüfung beim TLS-Handshake                             | gemSpec_PKI |
| GS-A_4751 | Fehlercodes bei TSL- und Zertifikatsprüfung                 | gemSpec_PKI |
| GS-A_4957 | Beschränkungen OCSP-Request                                 | gemSpec_PKI |
| GS-A_5215 | Festlegung der zeitlichen Toleranzen in einer OCSP-Response | gemSpec_PKI |

### 3.1.2 Herstellererklärung funktionale Eignung

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Anforderungen an den technischen Teil des Produkttyps verzeichnet, deren durchgeführte bzw. geplante Umsetzung und Beachtung der Hersteller bzw. der Anbieter durch eine Herstellererklärung bestätigt bzw. zusagt.

**Tabelle 3: Anforderungen zur funktionalen Eignung "Herstellererklärung"**

| <b>Afo-ID</b> | <b>Afo-Bezeichnung</b>                                              | <b>Quelle<br/>(Referenz)</b> |
|---------------|---------------------------------------------------------------------|------------------------------|
| A_17583       | Signaturdienst - Eintrag in das Interoperabilitätsverzeichnis vesta | gemSpec_SigD                 |
| GS-A_4155     | Performance – zentrale Dienste – Verfügbarkeit                      | gemSpec_Perf                 |
| GS-A_5028     | Performance – zentrale Dienste – Verfügbarkeit Produktivbetrieb     | gemSpec_Perf                 |
| GS-A_3055     | Performance – zentrale Dienste – Skalierbarkeit (Anbieter)          | gemSpec_Perf                 |
| GS-A_3058     | Performance – zentrale Dienste – lineare Skalierbarkeit             | gemSpec_Perf                 |
| TIP1-A_6517   | Eigenverantwortlicher Test: TBV                                     | gemKPT_Test                  |
| TIP1-A_6518   | Eigenverantwortlicher Test: TDI                                     | gemKPT_Test                  |
| TIP1-A_6519   | Eigenverantwortlicher Test: Hersteller und Anbieter                 | gemKPT_Test                  |
| TIP1-A_7358   | Qualität des Produktmusters                                         | gemKPT_Test                  |
| TIP1-A_6523   | Zulassungstest: Hersteller und Anbieter                             | gemKPT_Test                  |
| TIP1-A_6526   | Produkttypen: Bereitstellung                                        | gemKPT_Test                  |
| TIP1-A_6527   | Testkarten                                                          | gemKPT_Test                  |
| TIP1-A_4191   | Keine Echtdaten in RU und TU                                        | gemKPT_Test                  |
| GS-A_2162     | Kryptographisches Material in Entwicklungs- und Testumgebungen      | gemKPT_Test                  |
| TIP1-A_7330   | Tracedaten von echten Außenschnittstellen                           | gemKPT_Test                  |
| TIP1-A_7331   | Bereitstellung von Tracedaten an Außenschnittstelle                 | gemKPT_Test                  |
| TIP1-A_6079   | Updates von Referenzobjekten                                        | gemKPT_Test                  |
| TIP1-A_6080   | Softwarestand von Referenzobjekten                                  | gemKPT_Test                  |
| TIP1-A_6081   | Bereitstellung der Referenzobjekte                                  | gemKPT_Test                  |
| TIP1-A_6093   | Ausprägung der Referenzobjekte                                      | gemKPT_Test                  |
| TIP1-A_6082   | Versionen der Referenzobjekte                                       | gemKPT_Test                  |
| TIP1-A_6088   | Unterstützung bei Fehlernachstellung                                | gemKPT_Test                  |
| TIP1-A_5052   | Dauerhafte Verfügbarkeit in der RU                                  | gemKPT_Test                  |

|             |                                                                               |               |
|-------------|-------------------------------------------------------------------------------|---------------|
| TIP1-A_2775 | Performance in RU                                                             | gemKPT_Test   |
| TIP1-A_6085 | Referenzobjekte eines Produkts                                                | gemKPT_Test   |
| TIP1-A_2805 | Zeitnahe Anpassung von Produktkonfigurationen                                 | gemKPT_Test   |
| TIP1-A_6532 | Zulassung eines neuen Produkts: Aufgaben der TDI                              | gemKPT_Test   |
| TIP1-A_6533 | Zulassung eines neuen Produkts: Aufgaben der Hersteller und Anbieter          | gemKPT_Test   |
| TIP1-A_6536 | Zulassung eines geänderten Produkts: Aufgaben der TDI                         | gemKPT_Test   |
| TIP1-A_7333 | Parallelbetrieb von Release oder Produkttypversion                            | gemKPT_Test   |
| TIP1-A_7334 | Risikoabschätzung bezüglich der Interoperabilität                             | gemKPT_Test   |
| TIP1-A_6772 | Partnerprodukte bei Interoperabilitätstests                                   | gemKPT_Test   |
| TIP1-A_6529 | Produkttypen: Mindestumfang der Interoperabilitätsprüfung                     | gemKPT_Test   |
| TIP1-A_7335 | Bereitstellung der Testdokumentation                                          | gemKPT_Test   |
| TIP1-A_6524 | Testdokumentation gemäß Vorlagen                                              | gemKPT_Test   |
| A_17809     | Bereitstellung weiterer ePA-Produkttypen für Zulassungstest                   | gemKPT_Test   |
| A_17539     | Zuweisung alternativer Versicherten-Identitäten                               | gemKPT_Test   |
| GS-A_4385   | TLS-Verbindungen, Version 1.2                                                 | gemSpec_Krypt |
| A_18467     | TLS-Verbindungen, Version 1.3                                                 | gemSpec_Krypt |
| A_18464     | TLS-Verbindungen, nicht Version 1.1                                           | gemSpec_Krypt |
| A_17205     | Signatur der TSL: Signieren und Prüfen (ECC-Migration)                        | gemSpec_Krypt |
| A_17775     | TLS-Verbindungen Reihenfolge Ciphersuiten (ECC-Migration)                     | gemSpec_Krypt |
| A_17322     | TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration) | gemSpec_Krypt |
| A_17206     | XML-Signaturen (ECC-Migration)                                                | gemSpec_Krypt |
| GS-A_4009   | Übertragungstechnologie auf OSI-Schicht LAN                                   | gemSpec_Net   |
| GS-A_4831   | Standards für IPv4                                                            | gemSpec_Net   |
| GS-A_4010   | Standards für IPv6                                                            | gemSpec_Net   |

|           |                                                                                        |             |
|-----------|----------------------------------------------------------------------------------------|-------------|
| GS-A_4011 | Unterstützung des Dual-Stack Mode                                                      | gemSpec_Net |
| GS-A_4012 | Leistungsanforderungen an den Dual-Stack Mode                                          | gemSpec_Net |
| GS-A_4013 | Nutzung von UDP/TCP-Portbereichen                                                      | gemSpec_Net |
| GS-A_4018 | Dokumentation UDP/TCP-Portbereiche Anbieter                                            | gemSpec_Net |
| GS-A_4024 | Nutzung IP-Adressbereiche                                                              | gemSpec_Net |
| GS-A_4027 | Reporting IP-Adressbereiche                                                            | gemSpec_Net |
| GS-A_4759 | IPv4-Adressen Produkttyp zum SZSP                                                      | gemSpec_Net |
| GS-A_4033 | Statisches Routing TI-Übergabepunkte                                                   | gemSpec_Net |
| GS-A_4054 | Paketfilter Default Deny                                                               | gemSpec_Net |
| GS-A_4805 | Abstimmung angeschlossener Produkttyp mit dem Anbieter Zentrales Netz                  | gemSpec_Net |
| GS-A_3824 | FQDN von Produkttypen der Fachanwendungen sowie der zentralen TI-Plattform             | gemSpec_Net |
| GS-A_4810 | DNS-SD, Format von TXT Resource Records                                                | gemSpec_Net |
| GS-A_4820 | Schnittstelle I_NTP_Time_Information, Nutzung durch Zentrale Dienste der TI-Plattform  | gemSpec_Net |
| GS-A_3695 | Grundlegender Aufbau Versionsnummern                                                   | gemSpec_OM  |
| GS-A_3696 | Zeitpunkt der Erzeugung neuer Versionsnummern                                          | gemSpec_OM  |
| GS-A_3697 | Anlass der Erhöhung von Versionsnummern                                                | gemSpec_OM  |
| GS-A_4541 | Nutzung der Produkttypversion zur Kompatibilitätsprüfung                               | gemSpec_OM  |
| GS-A_4542 | Spezifikationsgrundlage für Produkte                                                   | gemSpec_OM  |
| GS-A_5054 | Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen | gemSpec_OM  |
| GS-A_5038 | Festlegungen zur Vergabe einer Produktversion                                          | gemSpec_OM  |
| GS-A_5039 | Änderung der Produktversion bei Änderungen der Produkttypversion                       | gemSpec_OM  |
| GS-A_3813 | Datenschutzvorgaben Fehlermeldungen                                                    | gemSpec_OM  |
| GS-A_5018 | Sicherheitsrelevanter Fehler an organisatorischen Schnittstellen                       | gemSpec_OM  |
| GS-A_3804 | Eigenschaften eines FehlerLog-Eintrags                                                 | gemSpec_OM  |

|           |                                                                                                   |             |
|-----------|---------------------------------------------------------------------------------------------------|-------------|
| GS-A_3807 | Fehlerspeicherung ereignisgesteuerter Nachrichtenverarbeitung                                     | gemSpec_OM  |
| GS-A_3805 | Loglevel zur Bezeichnung der Granularität FehlerLog                                               | gemSpec_OM  |
| GS-A_3806 | Loglevel in der Referenz- und Testumgebung                                                        | gemSpec_OM  |
| GS-A_4864 | Logging-Vorgaben nach dem Übergang zum Produktivbetrieb                                           | gemSpec_OM  |
| GS-A_5033 | Betriebsdokumentation der zentralen Produkte der TI-Plattform und anwendungsspezifischen Diensten | gemSpec_OM  |
| GS-A_4640 | Identifizierung/Validierung des TI-Vertrauensankers bei der initialen Einbringung                 | gemSpec_PKI |

## 3.2 Anforderungen zur sicherheitstechnischen Eignung

### 3.2.1 Herstellererklärung sicherheitstechnische Eignung

Sofern in diesem Abschnitt Anforderungen verzeichnet sind, muss der Hersteller deren Umsetzung und Beachtung zum Nachweis der sicherheitstechnischen Eignung durch eine Herstellererklärung bestätigen bzw. zusagen.

**Tabelle 4: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"**

| Afo-ID       | Afo-Bezeichnung                                                                                   | Quelle (Referenz)     |
|--------------|---------------------------------------------------------------------------------------------------|-----------------------|
| A_17373      | Signaturdienst - Produkt ist geeignet für Sicherheitsniveau "substanziell" gemäß eIDAS-Verordnung | gemSpec_SigD          |
| A_18957      | Darstellen der Voraussetzungen für sicheren Betrieb des Produkts im Handbuch                      | gemSpec_SigD          |
| GS-A_2524-01 | Produktunterstützung: Nutzung des Problem-Management-Prozesses                                    | gemSpec_DS_Hersteller |
| GS-A_2330-02 | Hersteller: Schwachstellen-Management                                                             | gemSpec_DS_Hersteller |
| GS-A_2525-01 | Hersteller: Schließen von Schwachstellen                                                          | gemSpec_DS_Hersteller |
| GS-A_2354-01 | Produktunterstützung mit geeigneten Sicherheitstechnologien                                       | gemSpec_DS_Hersteller |
| GS-A_2350-01 | Produktunterstützung der Hersteller                                                               | gemSpec_DS_Hersteller |
| GS-A_4944-01 | Produktentwicklung: Behebung von Sicherheitsmängeln                                               | gemSpec_DS_Hersteller |
| GS-A_4945-01 | Produktentwicklung: Qualitätssicherung                                                            | gemSpec_DS_Hersteller |

|              |                                                                               |                       |
|--------------|-------------------------------------------------------------------------------|-----------------------|
| GS-A_4946-01 | Produktentwicklung: sichere Programmierung                                    | gemSpec_DS_Hersteller |
| GS-A_4947-01 | Produktentwicklung: Schutz der Vertraulichkeit und Integrität                 | gemSpec_DS_Hersteller |
| A_17178      | Produktentwicklung: Basisschutz gegen OWASP Top 10 Risiken                    | gemSpec_DS_Hersteller |
| A_17179      | Auslieferung aktueller zusätzlicher Softwarekomponenten                       | gemSpec_DS_Hersteller |
| A_17205      | Signatur der TSL: Signieren und Prüfen (ECC-Migration)                        | gemSpec_Krypt         |
| A_17322      | TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration) | gemSpec_Krypt         |
| A_17206      | XML-Signaturen (ECC-Migration)                                                | gemSpec_Krypt         |
| GS-A_4641    | Initiale Einbringung TI-Vertrauensanker                                       | gemSpec_PKI           |
| GS-A_4748    | Initiale Einbringung TSL-Datei                                                | gemSpec_PKI           |

---

## **4 Produktypspezifische Merkmale**

---

Es liegen keine optionalen Ausprägungen des Produktyps vor.

---

## 5 Anhang – Verzeichnisse

---

### 5.1 Abkürzungen

| Kürzel | Erläuterung                 |
|--------|-----------------------------|
| Afo-ID | Anforderungs-Identifikation |
|        |                             |

### 5.2 Tabellenverzeichnis

|                                                                                                  |    |
|--------------------------------------------------------------------------------------------------|----|
| Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion .....                            | 6  |
| Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test" ..... | 7  |
| Tabelle 3: Anforderungen zur funktionalen Eignung "Herstellererklärung" .....                    | 10 |
| Tabelle 4: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung" .....          | 14 |
|                                                                                                  |    |

### 5.3 Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

| [Quelle] | Herausgeber: Titel, Version |
|----------|-----------------------------|
|          |                             |