

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# **Produkttypsteckbrief**

*Prüfvorschrift*

## **Zulassungsobjekt COS**

Produkttyp Version: 4.4.1-0  
Produkttyp Status: freigegeben

Version: 1.0.0  
Revision: 111375  
Stand: 15.05.2019  
Status: freigegeben  
Klassifizierung: öffentlich  
Referenzierung: gemProdT\_COS\_PTV\_4.4.1-0

---

## 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                       |
|-------------------|---|--------------------------------|
| 2.0.0             | Initiale Version G2-Karten für Vergabeverfahren                               | [gemProdT_Anhang_COS_PTV2.0.0] |
| 2.0.1             | Anpassung Produkttypversion auf Stand ORS1 vom 22.04.13                       | [gemProdT_Anhang_COS_PTV2.0.1] |
| 4.0.0             | Änderungen COS-Spezifikation aus Iteration 1 und Iteration 2 des G2-Projektes | [gemProdT_COS_PTV4.0.0]        |
| 4.0.1             | Änderungen COS-Spezifikation aus Iteration 2b des G2-Projektes                | [gemProdT_COS_PTV4.0.1]        |
| 4.1.0             | Änderungen COS-Spezifikation aus Iteration 3 des G2-Projektes                 | [gemProdT_COS_PTV4.1.0]        |
| 4.2.0             | Änderungen COS-Spezifikation aus Iteration 4 des G2-Projektes                 | [gemProdT_COS_PTV4.2.0]        |
| 4.3.0             | Einarbeitung der Errata R1.4.1 bis R1.4.6                                     | [gemProdT_COS_PTV4.3.0]        |
| 4.3.0-1           | Anpassung auf Releasestand 1.6.3  | [gemProdT_COS_PTV4.3.0-1]      |
| 4.3.1-0           | Anpassung auf Releasestand 1.6.4  | [gemProdT_COS_PTV4.3.1-0]      |
| 4.4.0-0           | Anpassung auf Releasestand 2.1.2  | [gemProdT_COS_PTV4.4.0-0]      |
| 4.4.1-0           | Anpassung auf Releasestand 3.1.0  | [gemProdT_COS_PTV4.4.1-0]      |

### 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   | 15.05.2019 |      | freigegeben                            | gematik    |

---

## Inhaltsverzeichnis

---

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Einführung.....</b>   | <b>5</b>  |
| 1.1      | Zielsetzung und Einordnung des Dokumentes .....                              | 5         |
| 1.2      | Zielgruppe .....   | 5         |
| 1.3      | Geltungsbereich .....  | 5         |
| 1.4      | Abgrenzung des Dokumentes .....  | 5         |
| 1.5      | Methodik.....  | 5         |
| <b>2</b> | <b>Dokumente .....</b>   | <b>7</b>  |
| <b>3</b> | <b>Blattanforderungen .....</b>  | <b>8</b>  |
| 3.1      | Anforderungen zur funktionalen Eignung .....                                 | 8         |
| 3.1.1    | Produkttest/Produktübergreifender Test .....                                 | 8         |
| 3.1.2    | Herstellererklärung funktionale Eignung .....                                | 9         |
| 3.2      | Anforderungen zur sicherheitstechnischen Eignung .....                       | 9         |
| 3.2.1    | CC-Evaluierung .....   | 9         |
| 3.2.2    | Herstellererklärung sicherheitstechnische Eignung.....                       | 10        |
| 3.2.3    | Zertifizierung nach Technischer Richtlinie.....                              | 10        |
| 3.3      | Anforderungen zur elektrischen, mechanischen und physikalischen Eignung..... | 11        |
| <b>4</b> | <b>spezifische Merkmale des Zulassungsobjektes .....</b>                     | <b>12</b> |
| <b>5</b> | <b>Anhang A – Verzeichnisse .....</b>  | <b>13</b> |
| 5.1      | Abkürzungen.....   | 13        |
| 5.2      | Tabellenverzeichnis.....   | 13        |
| 5.3      | Referenzierte Dokumente.....   | 13        |

---

## 1 Einführung

---

### 1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die Anforderungen der gematik an Herstellung und Betrieb des Zulassungsobjekts COS 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 COS-Hersteller und -Anbieter sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

### 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 das Zulassungsobjekt COS 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

Für das Betriebssystem (COS) definiert [gemSpec\_COS] die Anforderungen an die Funktionalität einer Betriebssystemplattform (COS/COS-Plattform) für elektronische Karten im Gesundheitswesen (eGK, HBA, ...), die internationalen Standards entsprechen und die internationale sowie europäische Interoperabilität sicherstellen.

Die nachfolgenden Dokumente enthalten alle für das COS normativen Anforderungen der gematik, die für eine Zulassung des Betriebssystems berücksichtigt werden müssen.

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

| Dokumenten Kürzel     | Bezeichnung des Dokumentes   | Version |
|-----------------------|--|---------|
| gemSpec_DS_Hersteller | Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller                       | 1.1.0   |
| gemSpec_Krypt         | Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur | 2.13.0  |
| gemKPT_Test           | Testkonzept der TI   | 2.3.0   |
| gemSpec_PKI           | Übergreifende Spezifikation – Spezifikation PKI  | 2.5.0   |
| gemSpec_OM            | Übergreifende Spezifikation Operations und Maintenance   | 1.12.0  |
| gemSpec_COS           | Spezifikation des Card Operating System (COS)  | 3.12.1  |

**Tabelle 2: Mitgeltende Dokumente**

| Dokumenten Kürzel  | Bezeichnung des Dokuments                    | Version |
|--------------------|--|---------|
| gemSpec_TLK_COS_G2 | gematik: Spezifikation COS/Objektsysteme     | 2.0.0   |
| BSI-CC-PP-0082     | BSI: Protection Profile – COS BSI-CC-PP-0082 | 2.0     |

### 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 die für das Zulassungsobjekt COS normativen Anforderungen, die für die Herstellung des Zulassungsobjektes COS 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

Die normativen Anforderungen an das COS sind in [gemSpec\_COS] festgelegt

Nachfolgend sind weitere funktionale Anforderungen an den technischen Teil des Zulassungsobjektes COS verzeichnet, deren Umsetzung im Zuge von Zulassungstests durch die gematik geprüft wird.

**Tabelle 3: Anforderungen zur funktionalen Eignung  
"Produkttest/Produktübergreifender Test"**

| Afo-ID      | Afo-Bezeichnung   | Quelle<br>(Referenz) |
|-------------|---|----------------------|
| G2_N000.300 | (N000.300) K_COS  | gemSpec_COS          |
| GS-A_4362   | X.509-Identitäten für Verschlüsselungszertifikate   | gemSpec_Krypt        |
| GS-A_4365   | CV-Zertifikate G2   | gemSpec_Krypt        |
| GS-A_4366   | CV-CA-Zertifikate G2  | gemSpec_Krypt        |
| GS-A_4379   | Card-to-Card-Authentisierung G2   | gemSpec_Krypt        |
| GS-A_4380   | Card-to-Server (C2S) Authentisierung und Trusted Channel G2   | gemSpec_Krypt        |
| GS-A_4381   | Schlüssellängen Algorithmus AES   | gemSpec_Krypt        |
| GS-A_3695   | Grundlegender Aufbau Versionsnummern  | gemSpec_OM           |
| GS-A_3700   | Versionierung von Produkten auf Basis von dezentralen Produkttypen der TI-Plattform durch die Produktidentifikation | gemSpec_OM           |
| GS-A_5026   | Versionierung von Karten durch die Produktidentifikation  | gemSpec_OM           |
| GS-A_5140   | Inhalt der Selbstauskunft von Karten  | gemSpec_OM           |
| GS-A_5009   | Prüfung der mathematischen Korrektheit von CV-Zertifikate der Generation 2  | gemSpec_PKI          |
| GS-A_5010   | Prüfung der Signatur eines CV-Zertifikats der Generation 2 mit Hilfe des CV-Zertifikats des Herausgebers            | gemSpec_PKI          |



|           |  |             |
|-----------|--|-------------|
| GS-A_5011 | Prüfung der Gültigkeit von CV-Zertifikaten der Generation G2 | gemSpec_PKI |
| GS-A_5012 | Prüfung von CV-Zertifikaten der Generation 2                 | gemSpec_PKI |

### 3.1.2 Herstellererklärung funktionale Eignung

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

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

| Afo-ID      | Afo-Bezeichnung  | Quelle (Referenz) |
|-------------|--|-------------------|
| GS-A_2162   | Kryptographisches Material in Entwicklungs- und Testumgebungen   | gemKPT_Test       |
| TIP1-A_4191 | Keine Echtdaten in RU und TU                                     | gemKPT_Test       |
| GS-A_3696   | Zeitpunkt der Erzeugung neuer Versionsnummern                    | gemSpec_OM        |
| GS-A_3697   | Anlass der Erhöhung von Versionsnummern                          | gemSpec_OM        |
| GS-A_4542   | Spezifikationsgrundlage für Produkte                             | gemSpec_OM        |
| GS-A_5038   | Festlegungen zur Vergabe einer Produktversion                    | gemSpec_OM        |
| GS-A_5039   | Änderung der Produktversion bei Änderungen der Produkttypversion | gemSpec_OM        |

## 3.2 Anforderungen zur sicherheitstechnischen Eignung

### 3.2.1 CC-Evaluierung

Der Produkttyp erfordert eine Zertifizierung nach Common Criteria [CC] auf der Grundlage des Protection Profiles [CC-PP-0082].

Für die Evaluierung sind die Inhalte der Schutzprofile normativ führend. Der Nachweis der im Folgenden aufgeführten Anforderungen erfolgt implizit durch die Vorlage des IT-Sicherheitszertifikats bei der gematik.

**Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "CC-Evaluierung"**

| Afo-ID    | Afo-Bezeichnung        | Quelle (Referenz) |
|-----------|------------------------|-------------------|
| GS-A_4367 | Zufallszahlengenerator | gemSpec_Krypt     |

|           |                    |               |
|-----------|--------------------|---------------|
| GS-A_4368 | Schlüsselerzeugung | gemSpec_Krypt |
|-----------|--------------------|---------------|

### 3.2.2 Herstellererklärung sicherheitstechnische Eignung

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

**Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"**

| Afo-ID       | Afo-Bezeichnung  | Quelle (Referenz)     |
|--------------|--|-----------------------|
| GS-A_2330-02 | Hersteller: Schwachstellen-Management                          | gemSpec_DS_Hersteller |
| GS-A_2350-01 | Produktunterstützung der Hersteller                            | gemSpec_DS_Hersteller |
| GS-A_2354-01 | Produktunterstützung mit geeigneten Sicherheitstechnologien    | gemSpec_DS_Hersteller |
| GS-A_2524-01 | Produktunterstützung: Nutzung des Problem-Management-Prozesses | gemSpec_DS_Hersteller |
| GS-A_2525-01 | Hersteller: Schließen von Schwachstellen                       | 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 |

### 3.2.3 Zertifizierung nach Technischer Richtlinie

**Tabelle 7: Anforderungen zur sicherheitstechnischen Eignung "Zertifizierung nach Technischer Richtlinie"**

| Afo-ID    | Afo-Bezeichnung                      | Quelle (Referenz) |
|-----------|--------------------------------------|-------------------|
| GS-A_5140 | Inhalt der Selbstauskunft von Karten | gemSpec_OM        |

### 3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung

Der Nachweis der elektrischen, mechanischen und physikalischen Eignung ist nur dann notwendig, wenn ein COS in einem Kartenkörper zugelassen werden soll. Sofern dabei spezifische Anforderungen der gematik zu beachten sind, werden diese nachfolgend aufgeführt. Der Nachweis erfolgt durch die Vorlage des Prüfberichts.

**Tabelle 8: Anforderungen zur elektrischen, mechanischen und physikalischen Eignung**

| Afo-ID | Afo-Bezeichnung                   | Quelle (Referenz) |
|--------|-----------------------------------|-------------------|
|        | Es liegen keine Anforderungen vor |                   |

---

## 4 spezifische Merkmale des Zulassungsobjektes

---

Die Spezifikation COS [gemSpec\_COS] lässt folgende Optionen zu:

- Bereitstellung logischer Kanäle gemäß [gemSpec\_COS#2]
- Bereitstellung der Funktion Kryptobox gemäß [gemSpec\_COS#2]
- Bereitstellung einer kontaktlosen Schnittstelle gemäß [gemSpec\_COS#2]
- Bereitstellung der Option\_PACE\_PCD gemäß [gemSpec\_COS#2]
- Bereitstellung einer USB-Schnittstelle gemäß [gemSpec\_COS#2]

---

## 5 Anhang A – Verzeichnisse

---

### 5.1 Abkürzungen

| Kürzel | Erläuterung                 |
|--------|-----------------------------|
| Afo-ID | Anforderungs-Identifikation |
| CC     | Common Criteria             |

### 5.2 Tabellenverzeichnis

|  |    |
|--|----|
| Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion .....  | 7  |
| Tabelle 2: Mitgeltende Dokumente.....  | 7  |
| Tabelle 3: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test" .....               | 8  |
| Tabelle 4: Anforderungen zur funktionalen Eignung "Herstellererklärung" .....                                  | 9  |
| Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "CC-Evaluierung" .....                             | 9  |
| Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung" .....                        | 10 |
| Tabelle 7: Anforderungen zur sicherheitstechnischen Eignung "Zertifizierung nach Technischer Richtlinie" ..... | 10 |
| Tabelle 8: Anforderungen zur elektrischen, mechanischen und physikalischen Eignung                             | 11 |

### 5.3 Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

| [Quelle]      | Herausgeber: Titel, Version   |
|---------------|---|
| [CC-PP-0082]  | BSI (21.11.2014): Common Criteria Protection Profile Card Operating System Generation 2 (COS), Version 3.1 R4, BSI-CC-PP-0082   |
| [CC]          | Internationaler Standard: Common Criteria for Information Technology Security Evaluation<br><a href="https://www.commoncriteriaportal.org/cc/">https://www.commoncriteriaportal.org/cc/</a> |
| [gemSpec_COS] | gematik: Spezifikation des Card Operating System  |

|                      |  |
|----------------------|--|
|                      | (COS) Elektrische Schnittstelle                        |
| [gemRL_PruefSichEig] | gematik: Richtlinie zur Prüfung der Sicherheitseignung |