

Verfahrensbeschreibung

Zulassung Produkte der Telematikinfrastruktur hier: Card Operating System (COS) G2

Version:	2.7.0
Revision:	\main\rel_ors1\rel_opb1\7
Stand:	04.12.2023
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemZul_Prod_COS_G2]

Dokumentinformationen

Änderungen zur Vorversion

In diesem Dokument wurde die Beschreibung der Möglichkeit aufgenommen, das BSI und die beauftragte Prüfstelle für das Zertifizierungsverfahren von der Geheimhaltungspflicht zu entbinden.

Dokumentenhistorie

Version	Stand	Kapitel	Grund der Änderung, besondere Hinweise	Bearbeiter
2.4.0	30.03.16		Anpassungen an Online-Produktivbetrieb	Zulassung
2.4.1	02.03.18		Link zur gematik-Website aktualisiert	gematik
	06.03.20	Kap 5.3	Ergänzung Möglichkeit der Entbindung der Geheimhaltungspflicht des BSI/der Prüfstelle	gematik
2.5.0	09.04.20		freigegeben	gematik
2.6.0	14.04.21	Kap 5.3	Ergänzung zum PP-COS	gematik
2.7.0	16.11.23	Kap 2.1 Kap. 4.2	Option DES und RSA-CVC entfernt gemSpec_TLK COS_G2 durch gemSpec_TLK G2 geändert, Verschiedene redaktionelle Anpassungen	gematik

Inhaltsverzeichnis

1	Einleitung	4
2	Zulassungsobjekt COS G2.....	5
2.1	Ausprägungsvarianten des Zulassungsobjekts.....	5
2.2	Zulassungen von Teilen des Zulassungsobjekts	5
3	Prüfbereiche und Rollen	6
3.1	Prüfbereiche.....	6
3.2	Rollen.....	6
4	Zulassungsverfahren	7
4.1	Verfahrensübersicht.....	8
4.2	Beibringung der Elemente des Zulassungsobjekts.....	8
5	Nachweise	10
5.1	Beibringung der Nachweise.....	10
5.1.1	Für ein vollständiges Zulassungsobjekt	10
5.1.2	Für Teile des Zulassungsobjekts.....	10
5.2	Nachweis der funktionalen Eignung	11
5.3	Nachweis der sicherheitstechnischen Eignung	11
5.3.1	Evaluierungsbeauftragung	11
5.3.2	Zertifizierungsbeauftragung.....	12
5.4	Nachweis der elektrischen, mechanischen und physikalischen Eignung	12
5.5	Wiederholung von Zertifizierungen	12
A1	– Abkürzungen	13
A2	– Abbildungsverzeichnis.....	13
A3	– Tabellenverzeichnis	13
A4	– Referenzierte Dokumente.....	14
A4.1	– Dokumente der gematik.....	14
A4.2	– Weitere Dokumente.....	14
A5	– Antragsformular und Mustervorlagen	14
A6	– Checkliste zur Antragstellung.....	15

1 Einleitung

Dieses Dokument beschreibt das Zulassungsobjekt mit seinen Ausprägungen und regelt die besonderen Prüfbereiche und Nachweispflichten des Antragstellers in diesem Verfahren. Es ist der übergeordneten Verfahrensbeschreibung für Zulassungs- und Bestätigungsverfahren [gemZul_übergrVerf] in der jeweils geltenden Fassung nachgeordnet. Die dort enthaltenen Regelungen gelten vollumfänglich für dieses Zulassungsverfahren. Die übergeordnete Verfahrensbeschreibung [gemZul_übergrVerf] kann der Internetpräsenz der gematik entnommen werden (siehe <https://fachportal.gematik.de/downloadcenter/zulassungs-bestaetigungsantraege-verfahrensbeschreibungen>).

2 Zulassungsobjekt COS G2

Das Zulassungsobjekt COS G2 (COS) ist ein Betriebssystem in einem Chipkartenmodul (als Träger des COS) mit Implementierung in einem Kartenkörper. Das Zulassungsobjekt COS ist ein Produkttyp, der der Zulassungsstelle vom Antragsteller beizubringen ist.

Der Antragsteller hat sicherzustellen, dass sich das Zulassungsobjekt eindeutig identifizieren lässt. Dazu gehören insbesondere

- die detaillierte und vollständige Bezeichnung des Zulassungsobjekts sowie
- die Abbildung sämtlicher Versionsnummern gemäß [gemSpec_OM].

Ferner hat der Antragsteller sicherzustellen, dass allen Prüfinstanzen dieselbe Version des Zulassungsobjekts vorliegt.

2.1 Ausprägungsvarianten des Zulassungsobjekts

Das COS kann folgende Ausprägungsvarianten haben, die entsprechend im Antrag anzugeben sind:

- kontaktlose Schnittstelle
- logische Kanäle
- Kryptobox
- USB-Schnittstelle
- PACE PCD

2.2 Zulassungen von Teilen des Zulassungsobjekts

Hersteller von Prozessorchipkarten können eine Zulassung erhalten für:

- COS im Chipkartenmodul (als Träger des COS) ohne Implementierung in einem Kartenkörper.

3 Prüfbereiche und Rollen

3.1 Prüfbereiche

Im Rahmen des Zulassungsverfahrens, sind folgende drei Prüfbereiche gemäß [gemProdT_COS zu durchlaufen:

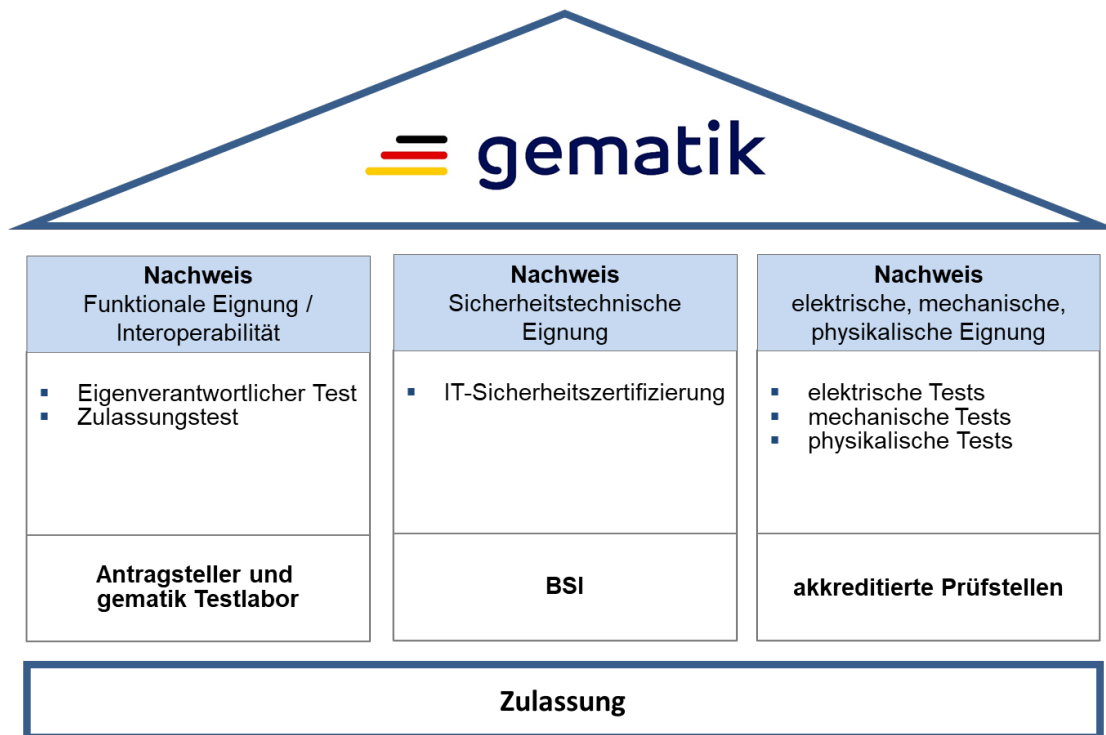


Abbildung 1: Prüfbereiche

3.2 Rollen

Folgende Rollen gemäß [gemZul_übergrVerf] werden in diesem Zulassungsverfahren benötigt:

- Antragsteller (Hersteller)
- Zulassungsstelle
- Testlabor der gematik
- Testmanager
- Zertifizierungsstelle (BSI) und
- akkreditierte Prüfstelle.

4 Zulassungsverfahren

Die folgende Verfahrensübersicht umfasst die Antragstellung, das Zulassungsobjekt, notwendige Nachweise sowie die Zulassungserteilung.

Das Zulassungsverfahren COS (Betriebssystem) steht in Abhängigkeit weiterer Zulassungsverfahren: Die zwingende Reihenfolge bei der Durchführung ist:

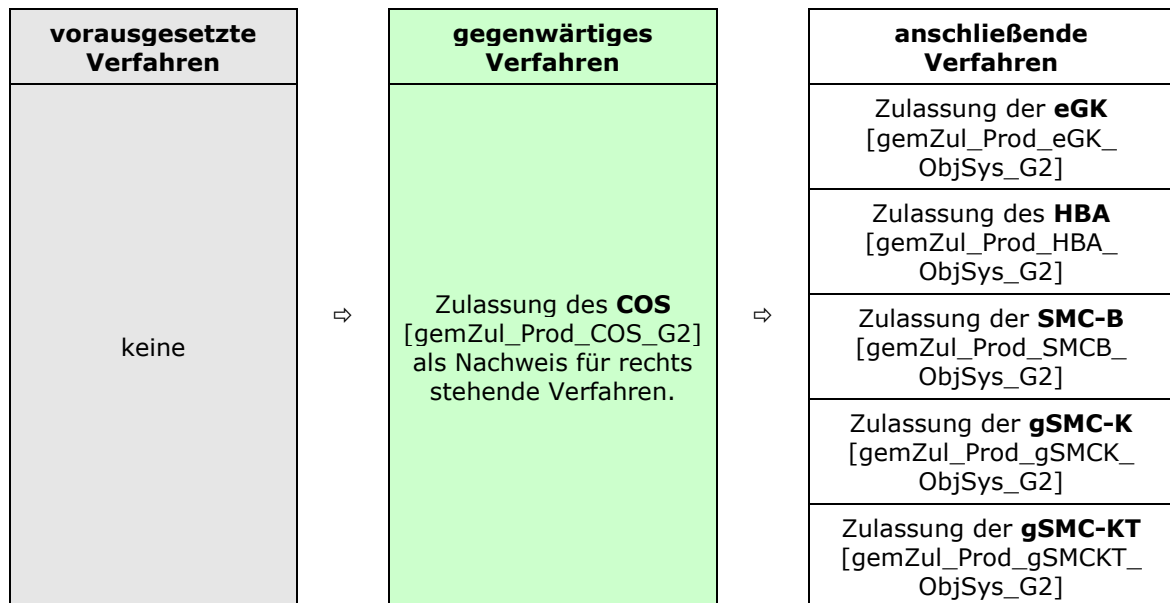


Abbildung 2: Reihenfolge Zulassungsverfahren

4.1 Verfahrensübersicht

Nachfolgend der schematische Ablauf des Zulassungsverfahrens:

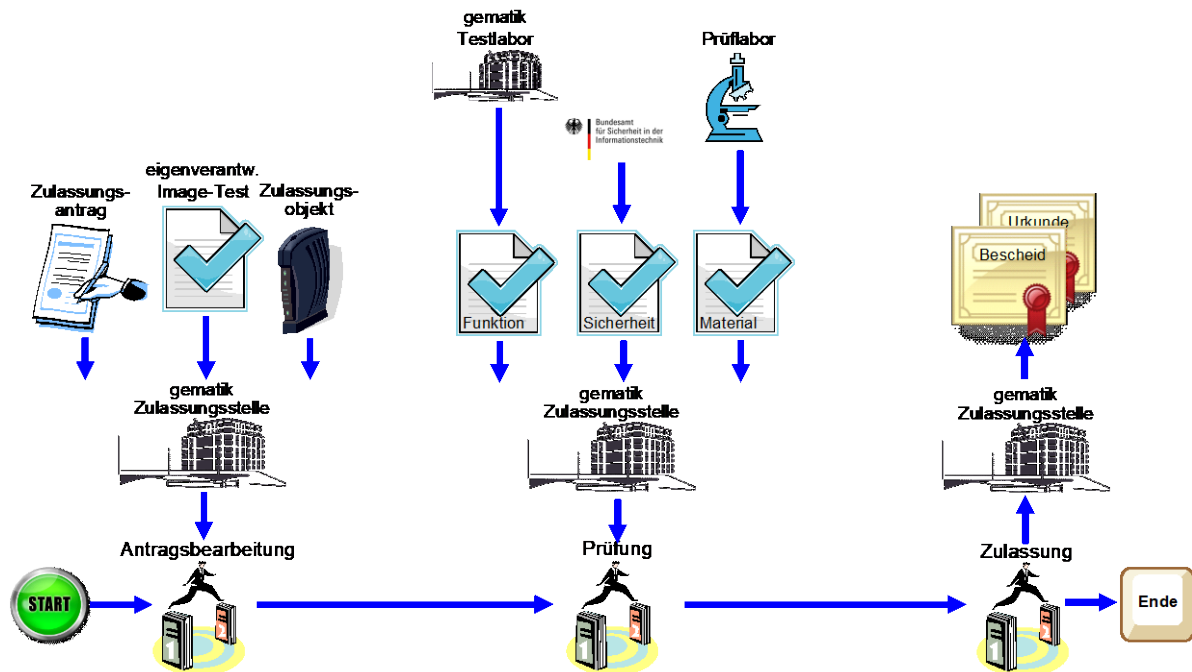


Abbildung 3: Schema Verfahrensablauf

Das Zulassungsverfahren beginnt mit der Antragstellung bei der Zulassungsstelle. Die Zulassungsstelle prüft den Zulassungsantrag auf Vollständigkeit und Korrektheit der Angaben. Im Positivfall beauftragt die Zulassungsstelle den funktionalen Zulassungstest im Testlabor der gematik.

Die Zulassungsstelle prüft die erforderlichen Nachweise gemäß Kapitel 5.1 auf Gültigkeit, Vollständigkeit und Korrektheit.

Ist das Prüfergebnis positiv, erteilt die Zulassungsstelle per Bescheid die Zulassung und stellt die Zulassungsurkunde aus. Bei negativem Prüfergebnis kann der Zulassungsantrag gegenüber dem Antragsteller abgelehnt werden.

4.2 Beibringung der Elemente des Zulassungsobjekts

Für die Durchführung des funktionalen Zulassungstests sind die zum Zulassungsobjekt gehörenden Dateien sowie das Zubehör durch den Antragsteller bereitzustellen.

- 20 Stück Prozessorchipkarten (COS im Chipkartenmodul als Träger des COS, implementiert in einem Kartenkörper). Herstellerspezifisch kann im Abstimmung mit dem Antragsteller eine höhere Stückzahl dieser Chipkarten notwendig sein.
- Software (d3-Images) gemäß [gemSpec_TLK G2].
- Zwei leere Karten, die mit einem Testlaborkartenimage geladen werden können und keine Reinitialisierungsmöglichkeit haben. Diese Karten benötigt die gematik vor der Testbeendigung und ruft diese dann beim Antragsteller ab.
- Wrapper (Werkzeug zum Auslesen von Zugriffsregeln).

- Dokumentation (Assurance Guide Documentation (AGD)).
- Lieferung der Beschreibung des Caching-Mechanismus beim Import von Public Keys.
- Werden vom Antragsteller Soll-/Soll-Nicht-Anforderungen gemäß Produkttypsteckbrief, aus dem Kapitel "Blattanforderungen, Anforderungen zur funktionalen Eignung, Produkttest / Produktübergreifender Test" an das Zulassungsobjekt nicht erfüllt, so hat der Antragsteller dies für jede Anforderung plausibel zu begründen und zu dokumentieren.
- Liste der umgesetzten Kann-Anforderungen gemäß Produkttypsteckbrief aus dem Kapitel "Blattanforderungen, Anforderungen zur funktionalen Eignung, Produkttest / Produktübergreifender Test".
- Nach Übermittlung der Informationen gemäß [gemZul_überggrVerf] für den Test der Karten-Images hat der Antragsteller eigenverantwortlich zu testen und das Ergebnis der Zulassungsstelle beizubringen.

Alle Dokumente können als PDF-Datei geliefert werden.

5 Nachweise

Mit der Unterschrift auf dem Zulassungsantrag erklärt der Antragsteller die durchgeführte bzw. geplante Umsetzung und Beachtung der im Produkttypsteckbrief in den Kapiteln der Herstellererklärungen (funktionale und sicherheitstechnische Eignung) gelisteten Anforderungen an das Produkt und die Prozesse des Antragstellers.

5.1 Beibringung der Nachweise

Die u. a. Tabelle zeigt die erforderlichen Nachweise für eine Zulassung des Betriebssystems COS.

Tabelle 1: erforderliche Nachweise der Zulassung für das Betriebssystem COS

Variante	Zulassungs- (teil)objekt	Funktional	Sicherheit (BSI)	elektrisch	mechanisch	physikalisch	zu lieferndes Objekt
1	COS	X	X	X	X	X	COS mit Kartenkörper
2	COS als Chipkartenmodul	X	X				COS ohne Kartenkörper

5.1.1 Für ein vollständiges Zulassungsobjekt

Die Zulassung als Betriebssystem inkl. Implementierung in einem Kartenkörper im Gesundheitswesen erfordert einen Nachweis

- der funktionalen Eignung,
- der sicherheitstechnischen Eignung sowie
- der elektrischen, mechanischen und physikalischen Eignung.

5.1.2 Für Teile des Zulassungsobjekts

Als Voraussetzung für die Zulassung des COS im Chipkartenmodul (als Träger des COS) ohne Implementierung in einem Kartenkörper sind folgende Nachweise zu erbringen:

- der funktionalen Eignung sowie
- der sicherheitstechnischen Eignung.

Für den konkreten Einzelfall gibt die Zulassungsstelle Auskunft.

5.2 Nachweis der funktionalen Eignung

Das Zulassungsverfahren erfordert einen Zulassungstest auf funktionale Eignung durch das Testlabor der gematik. Hierbei werden die Funktionalität und Interoperabilität geprüft.

Zur Testung des Zulassungsobjekts hat das Testlabor auf Basis der geltenden technischen Spezifikationen des [gemProdT_COS#3.1] die Testfälle erstellt. Der [gemProdT_COS] wird über die Internetpräsenz der gematik veröffentlicht (siehe <https://fachportal.gematik.de/hersteller-anbieter/komponenten-dienste/cos>).

Die Zulassungsstelle beauftragt das Testlabor der gematik mit der Prüfung der Ergebnisse aus den Eigenverantwortlichen Tests sowie der Durchführung des Zulassungstests zur funktionalen Eignung. Das Testlabor führt die Zulassungstests einmal durch und fasst die Ergebnisse unabhängig von ihrem Erfolg in einem Testbericht zusammen. Dieser Testbericht dient als Nachweis des durchgeführten funktionalen Tests.

5.3 Nachweis der sicherheitstechnischen Eignung

Die sicherheitstechnische Eignung eines Zulassungsobjekts ist durch eine vom BSI für das Prüfgebiet IT-Sicherheit anerkannte [Prüfst] zu evaluieren. Die Sicherheitsleistung wird durch das BSI in Form eines IT-Sicherheitszertifikats zertifiziert. Eine Übersicht über anerkannte [Prüfst] ist auf der Internetpräsenz des BSI veröffentlicht (siehe www.bsi.bund.de).

IT-Sicherheitszertifikate in diesem Sinne sind solche, die für die IT-Sicherheitszertifizierung durch das BSI ausgestellt wurden.

Für die Prüfung der IT-sicherheitstechnischen Eignung werden grundsätzlich die Anforderungen aus [gemProdT_COS#3.2] zu Grunde gelegt, wobei die Zertifizierung entsprechend des [PP_COS] stattfinden muss. Die Zertifizierung erfolgt auf Basis der allgemein anerkannten Sicherheitskriterien Common Criteria [CC] in der jeweils aktuellsten Fassung.

Zertifikate von ausländischen Zertifizierungsstellen können im Rahmen internationaler Abkommen anerkannt werden. Näheres hierzu ist in den internationalen CCRA-Abkommen sowie in den europäischen SOGIS-Abkommen geregelt.

Der Antragsteller kann das BSI und die von ihm beauftragte Prüfstelle von Ihrer Geheimhaltungspflicht gegenüber der gematik entbinden. Dies führt zu einem noch transparenteren Austausch zwischen Antragsteller, BSI, Prüfstelle und gematik und trägt zu einer Optimierung des Verfahrens bei. Die Vorlage der Verpflichtungserklärung über die Entbindung der Geheimhaltungspflicht im Zertifizierungsverfahren ist als letzte Seite im Zulassungsantrag beigefügt.

5.3.1 Evaluierungsbeauftragung

Zur Durchführung der Evaluierung beauftragt der Antragsteller eine von ihm ausgewählte, durch das BSI anerkannte [Prüfst]. Diese führt die sicherheitstechnische Prüfung (Evaluierung) gemäß [CC] durch.

5.3.2 Zertifizierungsbeauftragung

Zur Durchführung der Zertifizierung stellt der Antragsteller (i. a. R. der Hersteller) einen Antrag beim BSI ("Bescheid-Verfahren"). Das BSI begleitet und überwacht im Rahmen der Zertifizierung den Evaluierungsprozess. Für die IT-Sicherheitszertifizierung sind vom Antragsteller die Sicherheitsleistungen des Zulassungsobjekts zu formulieren. Nach Abschluss der Evaluierung und Abnahme des Evaluierungsberichts (auch Evaluation Technical Report bzw. ETR) stellt das BSI ein Zertifikat und einen Zertifizierungsreport aus. Das Zertifikat ist auf die von der gematik vergebene ZLS zu referenzieren.

5.4 Nachweis der 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.

Die elektrischen, mechanischen und physikalischen Anforderungen an das Zulassungsobjekt sind in [gemProdT_COS#3.3] geregelt.

Die Prüfungen der elektrischen, mechanischen und physikalischen Eignung sind von einer von der Deutschen Akkreditierungsstelle (DAkkS) akkreditierten [Prüfst] durchzuführen.

Die akkreditierte [Prüfst] ist durch den Antragsteller zu beauftragen. Der Nachweis der Eignung hat auf die von der gematik vergebene ZLS zu referenzieren.

Auskünfte hierüber erteilt die Zulassungsstelle.

5.5 Wiederholung von Zertifizierungen

Eine periodische Wiederholung der Zertifizierung ist notwendig, da die Gültigkeitsdauer eines BSI-Zertifikats auf fünf Jahre begrenzt ist. Deshalb ist ein erneutes Zertifikat noch vor Ablauf der Gültigkeitsdauer bei der Zulassungsstelle einzureichen. Nach positivem Prüfungsergebnis durch die Zulassungsstelle wird der neue Gültigkeitszeitraum von fünf Jahren intern vermerkt. Die bestehende Zulassung gilt dann fort, d. h. die Beibringung eines Zertifikats wegen periodischer Wiederholung erfordert keinen neuen Zulassungsantrag.

Anhang A

A1 – Abkürzungen

Kürzel	Erläuterung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CCRA	Common Criteria Recognition Agreement Zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten werden internationale Abkommen in Arbeitsgruppen ausgehandelt und von den entsprechenden Staaten unterzeichnet. Durch diese Abkommen wird die Mehrfachzertifizierung des gleichen Produktes in verschiedenen Staaten vermieden.
COS	Card Operating System - Betriebssystem
eGK	elektronische Gesundheitskarte
HBA	Heilberufsausweis
SGB	Sozialgesetzbuch
SMC	Security Module Card
SOGIS	Senior Officials Group Information System Security siehe CCRA
TI	Telematikinfrastruktur (der elektronischen Gesundheitskarte)
ZLS	Zulassungsschlüssel

Das **übergreifende Glossar** der gematik [gemGlossar] wird als eigenständiges Dokument zu Verfügung gestellt.

Begriff	Erläuterung
Produkttest	Das Produkt soll, als konkrete Ausprägung eines Produkttyps, die geforderten Funktionen und Schnittstellen spezifikationskonform realisieren und die Leistungsanforderungen erfüllen. Es wird das Verhalten eines Produkts an der Außenschnittstelle geprüft
Produktübergreifender Produkttest	Ergänzend zum Produkttest, der sich jeweils auf ein einzelnes Produkt bezieht, müssen Produkte auch integriert getestet werden.

A2 – Abbildungsverzeichnis

Abbildung 1: Prüfbereiche.....	6
Abbildung 2: Reihenfolge Zulassungsverfahren.....	7
Abbildung 3: Schema Verfahrensablauf	8

A3 – Tabellenverzeichnis

Tabelle 1: erforderliche Nachweise der Zulassung für das Betriebssystem COS.....	10
--	----

A4 – Referenzierte Dokumente

A4.1 – Dokumente der gematik

Der mit der vorliegenden Version korrelierende Entwicklungsstand der Konzepte und Spezifikationen wird je Produkttyp in Produkttypsteckbriefen konfiguriert. Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur TI, die nicht bereits in den Produkttypsteckbriefen referenziert sind. Version und Stand der referenzierten Dokumente sind dabei in der Tabelle nicht aufgeführt. Die gültigen Versionen der Produkttypsteckbriefe und ihre Zulassungsrelevanz werden in einer Dokumentenlandkarte definiert. Die zu dem vorliegenden Dokument passende(n) gültige(n) Versionsnummer(n) sind den Produkttypsteckbriefen zu entnehmen, in denen diese Dokumentenversion aufgeführt wird (siehe <https://fachportal.gematik.de/downloadcenter/>).

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemProdT_COS]	gematik: Produkttypsteckbrief – COS G2
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_TLK G2]	gematik: Spezifikation der Testlaborkarten COS und Objektsystem
[gemZul_übergrVerf]	gematik: übergeordnete Verfahrensbeschreibung für Zulassungs- und Bestätigungsverfahren

A4.2 – Weitere Dokumente

[Quelle]	Herausgeber: Titel
[CC]	Bundesanzeiger und DIN (ISO/IEC 15408 ff): Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation; siehe www.bsi.bund.de , Menüpunkt „Zertifizierung und Akkreditierung“)
[PP_COS]	BSI: Common Criteria Protection Profile - Card Operating System Generation 2 (PP COS G2), BSI-CC-PP-0082, Bundesamt für Sicherheit in der Informationstechnik
[Prüfst]	Verzeichnisse von anerkannten Prüfstellen siehe: - www.bsi.bund.de (Menüpunkt „Zertifizierung und Akkreditierung“) und von Bestätigungsstellen - www.bundesnetzagentur.de (Sachgebiet „qualifizierte elektronische Signatur“) und - www.dar.bam.de (Menüpunkt "Akkreditierte Stellen")

A5 – Antragsformular und Mustervorlagen

Bei der Antragstellung sind die Formulare und Muster der gematik im Zusammenhang mit dem hier beschriebenen Zulassungsverfahren in der jeweils geltenden Version zu verwenden (siehe <https://fachportal.gematik.de/zulassungen/zulassungsantraege>):

- „Antrag auf Zulassung eines Produktes der TI – COS-G2“

A6 – Checkliste zur Antragstellung

Die folgende Checkliste soll als Hilfestellung für die Beantragung einer Zulassung dienen. Sie erhebt keinen Anspruch auf Vollständigkeit.

lfd. Nr.	Aktion	erledigt
1	Verfahrensbeschreibung vom Fachportal der gematik downloaden	
2	Zulassungsantrag vom Fachportal der gematik laden und ausfüllen	
3	ggf. offene Fragen mit Zulassungsstelle klären (030/40041-200)	
4	Zulassungsantrag vorab an die Zulassungsstelle per E-Mail [zulassung@gematik.de] versenden und drucken	
5	Zulassungsantrag rechtsgültig unterschreiben und an Zulassungsstelle per Post versenden	
6	Produktidentifikation in das Zulassungsobjekt einarbeiten	
7	Durchführung der eigenverantwortlichen Image-Tests und Erstellen des Testergebnisses	
8	Zulassungsobjekt gemäß Definition im Zulassungsverfahren zusammenstellen und zusammen mit der Bestätigung an Zulassungsstelle versenden	
9	Nachweis der funktionalen Eignung gemäß Definition im Zulassungsverfahren klären und überwachen	
10	Nachweis zur Sicherheit gemäß Definition im Zulassungsverfahren beauftragen und an Zulassungsstelle versenden	
11	ggf. Nachweis der elektrischen, physikalischen und ggf. mechanischen Eignung gemäß Definition im Zulassungsverfahren beauftragen und an Zulassungsstelle versenden	