Elektronische Gesundheitskarte und Telematikinfrastruktur

Verfahrensbeschreibung

Zulassung Produkte der Telematikinfrastruktur hier: Konnektor

Version:	1.12.0
Revision:	75
Stand:	07.09.2021
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemZul_Prod_Kon]

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kapitel	Grund der Änderung, besondere Hinweise	Bearbeiter
1.2.0	30.06.16		Anpassungen an Online-Produktivbetrieb, Kommentierung durch Gesellschafter	gematik
1.4.0	14.06.17	3.1; 4.2; 5.3.; 5.6; A3.2	Anpassungen an eIDAS und Anzahl Testobjekte, Beibringung Sicherheitsgutachten	gematik
1.5.0	18.12.17	Kap. 2.1, Anhang B	Einarbeitung Feldtest für Konnektor Produkttypversion 3	gematik
1.5.1	27.02.18		Link zur gematik-Website aktualisiert	gematik
1.6.0	14.06.18	Kap. 5.3	Anpassung der IT-Sicherheitsprüfung und Einarbeitung Prüfung der Security Targets.	gematik
1.7.0	18.12.18		Anpassung Produkttypversion 4	gematik
1.8.0	17.12.19	Kap. 6/ Anhang B	Möglichkeit der Durchführung von Testmaßnahmen in der Produktivumgebung/ Besonderheiten für eine Zulassung zum Feldtest zur Beibringung der IT-Sicherheitsprüfung und -zertifizierung im Zusammenhang mit den Testmaßnahmen	gematik
1.9.0	08.01.20	Kap 5.2	Ergänzung Möglichkeit Nutzung ePA-Aktensystemsimulator	gematik
1.10.0	09.04.20	Kap 5.3	Ergänzung Möglichkeit der Entbindung der Geheimhaltungspflicht des BSI/der Prüfstelle	gematik
1.11.0	10.12.20	Anh. C	Sicherheitsnachweis bei Minor Releases	gematik
1.12.0	06.09.21		Einarbeitung kontrollierte Inbetriebnahme PTV 5 und Löschung Feldtest für PTV 4 und 5 (Anhang B)	gematik

Inhaltsverzeichnis

Dokumentinformationen 2
Änderungen zur Vorversion 2
Dokumentenhistorie 2
Inhaltsverzeichnis 3
1 Einleitung 5
2 Zulassungsobjekt Konnektor 6
2.1 Ausprägungsvarianten des Zulassungsobjekts 6
2.2 Zulassungen von Teilen des Zulassungsobjekts 6
3 Prüfbereiche und Rollen 7
3.1 Prüfbereiche 7
3.2 Rollen 8
4 Zulassungsverfahren 9
4.1 Verfahrensübersicht 9
4.2 Beibringung der Elemente des Zulassungsobjekts 11
5 Nachweise 12
5.1 Beibringung der Nachweise 12
5.2 Nachweis der funktionalen Eignung 12
5.3 Nachweis der sicherheitstechnischen Eignung 13
5.4 Nachweis der elektrischen, mechanischen und physikalischen Eignung 14
5.5 Wiederholung von Zertifizierungen 14
5.6 Auslieferung des Konnektors 14
5.7 Updates für installierte Konnektoren 14
6 Möglichkeit der Durchführung von Testmaßnahmen in der Produktivumgebung 16
Anhang A 18
A1 – Abkürzungen 18
A2 – Abbildungsverzeichnis 18
A3 – Referenzierte Dokumente 18
A3.1 – Dokumente der gematik 18
A3.2 – Weitere Dokumente 19
A4 – Antragsformular und Mustervorlagen 19
A5 – Checkliste zur Antragstellung 20

Anhang B – Besonderheiten für die Zulassung Konnektor Produkttypversion 5 21

Beibringung der Nachweise zur funktionalen Eignung im Rahmen der Kontrollierte Inbetriebnahme 21

Prüfbericht Umsetzungsbeschreibung der Kontrollierte Inbetriebnahme 21

Prüfbericht Abschlussbericht zur Kontrollierte Inbetriebnahme 21

Besonderheiten für eine Zulassung zur Kontrollierte Inbetriebnahme zur Beibringung der IT-Sicherheitsprüfung und -zertifizierung 22

Vorlagen: ..... Fehler! Textmarke nicht definiert.

Anhang C - Von Common Criteria abweichender Sicherheitsnachweis bei Minor-Releases des Konnektors 24

Grundlegender Ablauf 24

Beteiligte Prüfstelle und Evaluator 25

Fristen 25

Antragsteller-Dokumente 25

CVE-Analyse 26

Berücksichtigung des Update-Mechanismus 26

Antragsteller 27
Prüfstelle 27
gematik 27

Vertraulichkeit von Unterlagen 27

Handbuchinformationen 28

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/zulassungen/zulassungsantraege).

2 Zulassungsobjekt Konnektor

Der Konnektor ist eine dezentrale Komponente zur sicheren Anbindung von Clientsystemen der Leistungserbringer/der Kostenträgergeschäftsstellen an die Telematikinfrastruktur. Der Konnektor ist einerseits verantwortlich für den Zugriff auf die beim Leistungserbringer/der Kostenträgergeschäftsstelle befindlichen Kartenterminals sowie Karten und andererseits für die Kommunikation mit den zentralen Diensten der TI-Plattform und fachanwendungsspezifischen Diensten.

Das Zulassungsobjekt Konnektor 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, ggf. differenziert nach Hard- und Software gemäß [gemSpec_OM].

Ferner hat der Antragsteller sicherzustellen, dass allen Prüfinstanzen dieselben Versionen des Zulassungsobjekts vorliegen.

2.1 Ausprägungsvarianten des Zulassungsobjekts

Je nach Ausprägung des Zulassungsobjekts handelt es sich um andere/erweiterte Funktionalitäten mit unterschiedlichen Prüfanforderungen.

- Konnektor Produkttypversion 1 beinhaltet die Anwendung VSDM inklusive der Basisdienste „Sicheres Internet", „KV-Safenet-Anbindung".
- Konnektor Produkttypversion 2 beinhaltet zusätzlich zum Konnektor VSDM den Basisdienst QES.
- Konnektor Produkttypversion 3 beinhaltet zusätzlich zum Konnektor VSDM den Basisdienst QES und die Fachmodule Notfalldatenmanagement (NFDM), elektronischer Medikationsplan/Arzneimitteltherapiesicherheit (eMP/AMTS).
- Konnektor Produkttypversion 4 beinhaltet zusätzlich zum Konnektor Produkttypversion 3 das Fachmodul elektronische Patientenakte (ePA)
- Konnektor Produkttypversion 5 beinhaltet zusätzlich zum Konnektor Produkttypversion 4 die Erweiterungen für die elektronische Patientenakte Stufe 2.0 (ePA 2.0)

Ausprägungsvarianten, produkttypspezifische Merkmale und Prüfanforderungen werden durch den bei Antragstellung anzugebenden laut Übersicht Festlegung der zulassungsfähigen Versionsstände Produkttypen, Anbietertypen und weitere Anwendungen [1] der gematik gültigen Produkttypsteckbrief [gemProdT_Kon] sowie beim Konnektor Produkttypversion 5 das zusätzlich geltende Konzept für die Kontrollierte Inbetriebnahme Konnektor PTV 5 [gemKPT_Inbetriebnahme_Kon_PTV5] festgelegt.

2.2 Zulassungen von Teilen des Zulassungsobjekts

Für dieses Zulassungsobjekt gibt es nur die Gesamtzulassung und keine Teilzulassung.

[1] Die gültige Übersicht der Festlegung der zulassungsfähigen Versionsstände Produkttypen, Anbietertypen und weitere Anwendungen ist einzusehen im Fachportal der gematik (https://fachportal.gematik.de/downloadcenter/releases/release-von-uebergreifenden-normativen-dokumenten).

3 Prüfbereiche und Rollen

3.1 Prüfbereiche

Im Rahmen des Zulassungsverfahrens sind folgende drei Prüfbereiche gemäß [gemProdT_Kon] zu durchlaufen:

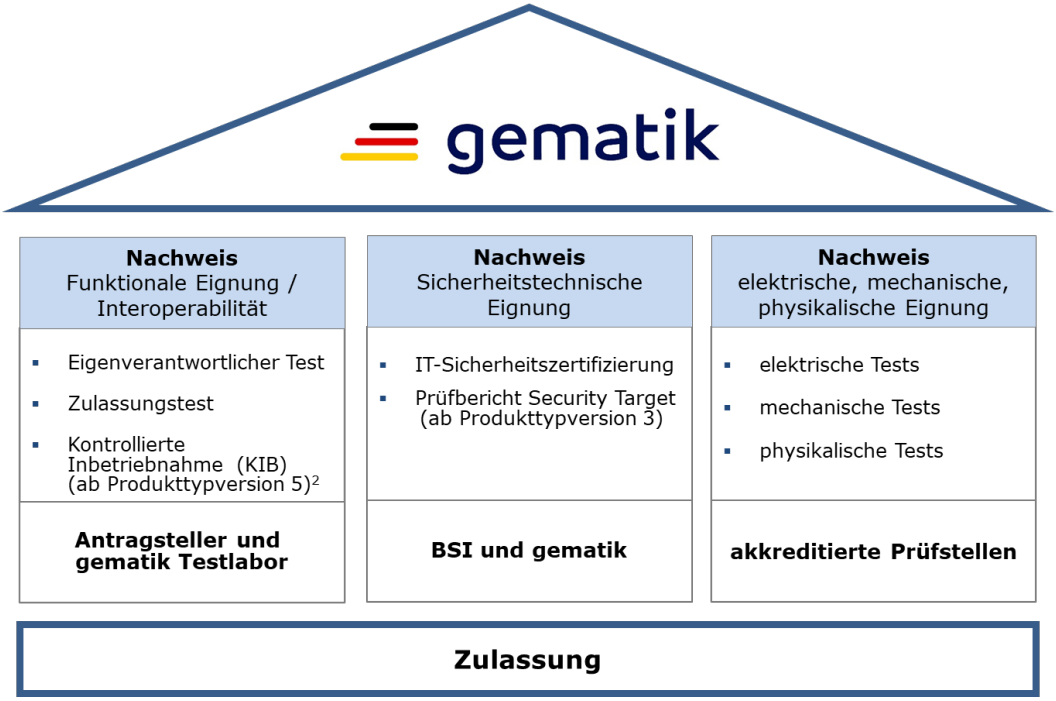

Abbildung 1: Prüfbereiche[2]

[2] Die Besonderheiten für die Zulassung des Konnektors Produkttypversion 5 sind im Anhang B beschrieben.

3.2 Rollen

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

- Antragsteller (Hersteller),
- Zulassungsstelle,
- Testmanager,
- Testlabor,
- Zertifizierungsstelle (BSI),
- akkreditierte Prüfstelle und
- Sicherheitsgutachter.

4 Zulassungsverfahren

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

Das Zulassungsverfahren Konnektor steht in Abhängigkeit keiner weiteren Zulassungsverfahren.

4.1 Verfahrensübersicht

Nachfolgend ist die schematische Darstellung des Zulassungsverfahrens für die Konnektoren mit den Produkttypen 3 und 4 zu sehen. (Für die Konnektoren Produkttyp 3 und 4 wurden von allen Antragstellern bereits Feldtests bei der Erstzulassung durchgeführt, deshalb wird dieser hier nachfolgend nicht mehr abgebildet. Für die Produkttypversionen 1 und 2 ist keine Neuzulassung mehr möglich.)

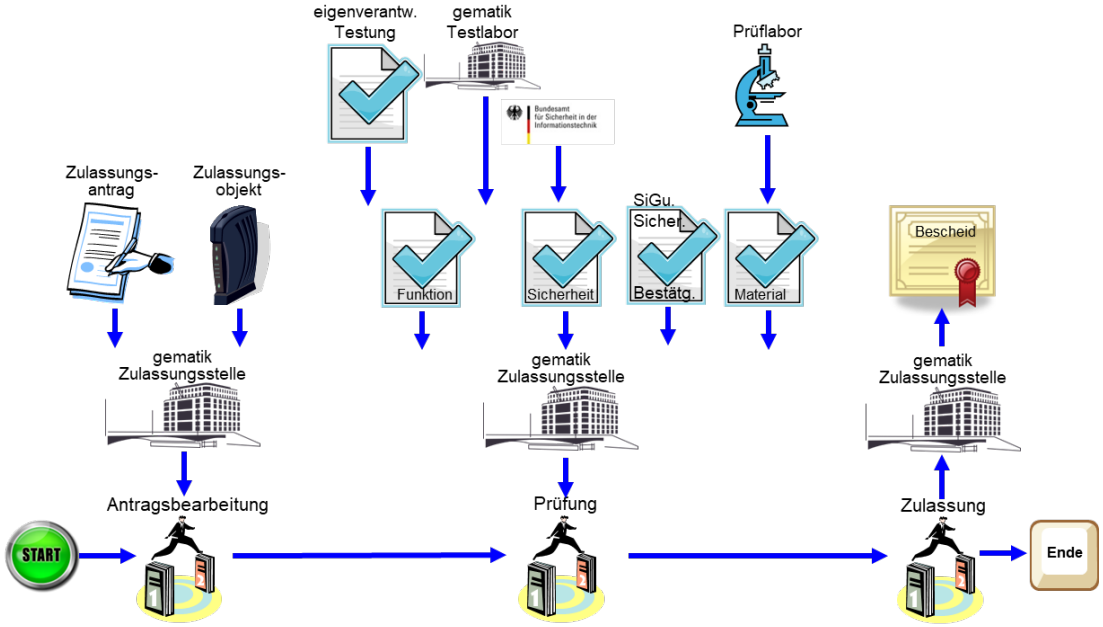

Abbildung 2: Schema Zulassungsverfahren

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.

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.

Der Ablauf des Zulassungsverfahrens für den Konnektor Produkttypversion 5 ist in Abbildung 3 beschrieben.

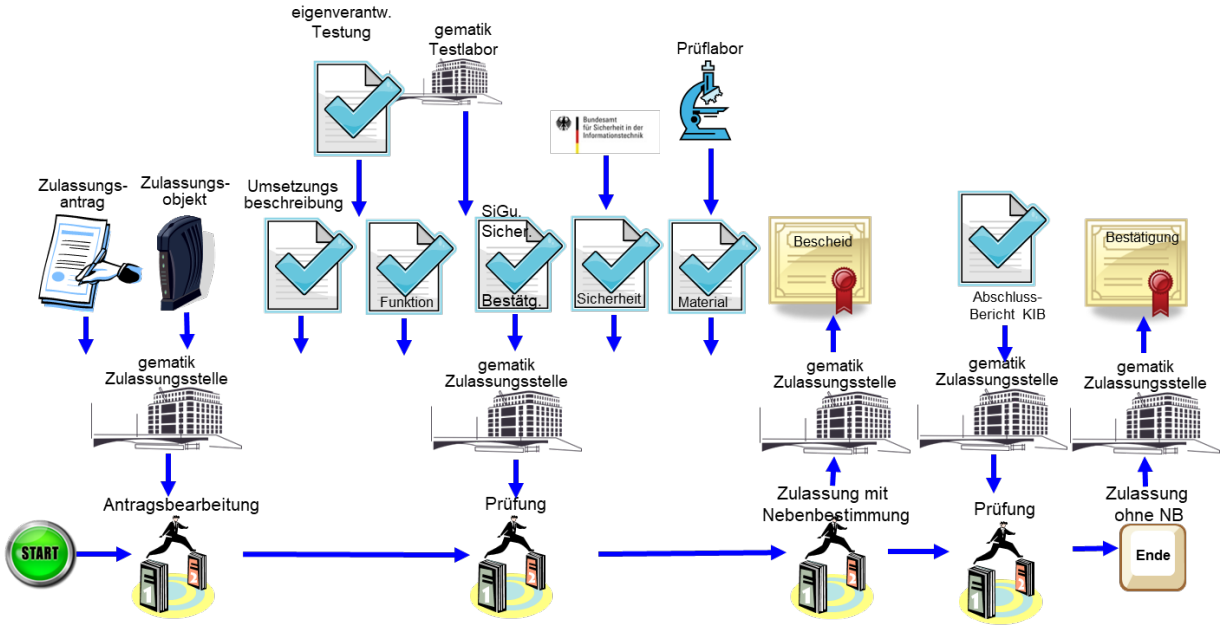

Abbildung 3: Schema Zulassungsverfahren Konnektor Produkttypversion 5

Das Zulassungsverfahren für den Konnektor Produkttypversion 5 beginnt mit der Antragstellung bei der Zulassungsstelle. Die Zulassungsstelle prüft den Zulassungsantrag auf Vollständigkeit, Nachvollziehbarkeit und Korrektheit. Im Positivfall beauftragt die Zulassungsstelle den funktionalen Zulassungstest im Testlabor.

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 mit Nebenbestimmungen[3]. Bei negativem Prüfergebnis kann der Zulassungsantrag gegenüber dem Antragsteller abgelehnt werden.

Nach Prüfung des Abschlussberichts der kontrollierten Inbetriebnahme mit positivem Ergebnis erfolgt die Bestätigung der gematik. Mit der Bestätigung der gematik hat der Antragsteller eine uneingeschränkte Zulassung für den Produktivbetrieb, sofern nicht weitere Nebenbestimmungen erlassen wurden.

[3] Die Zulassung mit Nebenbestimmungen erlaubt es dem Antragsteller, im Rahmen der Durchführung der kontrollierten Inbetriebnahme (siehe Anhang B) seinen Konnektor im Produktivbetrieb, befristet auf maximal sechs Monate, einzusetzen. Nach Prüfung der vom Antragsteller eingereichten, für die Durchführung der kontrollierten Inbetriebnahme geforderten Dokumentation, erteilt die gematik bei positivem Prüfergebnis die Bestätigung, dass der Konnektor ohne Einschränkungen für den Produktivbetrieb zugelassen ist, sofern nicht weitere Nebenbestimmungen erlassen wurden.

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:

- Hardware (wird im Kickoff vereinbart, mindestens aber 2 Geräte fabrikneu[4])
- sämtliche für den Betrieb notwendigen Anschlusskabel und Zubehör
- Software (Betriebssystem/Firmware)
- Client Software (z.B. Signaturproxy, Managementsoftware), die Notwendigkeit zur Beibringung ist dem [gemProdT_Kon] zu entnehmen
- notwendige Hilfsprogramme
  (z.B. um ein Firmware-Update einzuspielen, inkl. Anleitung)
- Bedienungsanleitung für den Konnektor
- 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".
- Der unterschriebene Testbericht EvT aus der eigenverantwortlichen Testung ist der Zulassungsstelle beizubringen.

Alle Dokumente können als PDF-Datei geliefert werden.

[4] Die Zulassungstests werden parallel in mehreren Testteams durchgeführt. Daher verkürzt sich die Testdauer bei der Bereitstellung mehrerer (derzeit ideal 20 Konnektoren) signifikant.

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 Zulassung des Produkts für die TI erfordert einen Nachweis

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

5.2 Nachweis der funktionalen Eignung

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

Zur Testung des Zulassungsobjekts hat das Testlabor auf Basis der geltenden technischen Spezifikationen des [gemProdT_Kon] Kap. 3.1 die Testfälle erstellt. Der [gemProdT_Kon] wird über die Internetpräsenz der gematik veröffentlicht (siehe https://fachportal.gematik.de/spezifikationen).

Der Antragsteller führt die Produkttests und nach Übermittlung der Zugangsinformationen gemäß [gemZul_übergrVerf] die produktübergreifenden Tests eigenverantwortlich durch. Der Antragsteller hat eigenverantwortlich zu testen, bis sein entwickeltes Zulassungsobjekt die 100%ige Testabdeckung gemäß [gemProdT_Kon] erfüllt. Die erfolgreiche Testung fasst der Antragsteller in dem unterschriebenen Testbericht EvT zusammen, der dem Testmanager beizubringen ist.

Der Antragsteller hat die Möglichkeit, für die Erstellung der EvTs den ePA-Aktensystemsimulator der gematik zu nutzen. Der ePA-Aktensystemsimulator wird von der gematik bereitgestellt.

Die Zulassungsstelle beauftragt das Testlabor mit der Prüfung der 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 wird festgestellt durch:

5.3.1 IT-Sicherheitsprüfung und -zertifizierung[5]

Die sicherheitstechnische Eignung eines Zulassungsobjekts ist durch eine vom BSI für das Prüfgebiet IT-Sicherheit anerkannte [Prüfst] gemäß [gemProdT_Kon], Kap. 3.2, zu evaluieren. Die Sicherheitsleistung wird durch das BSI zertifiziert. Eine Übersicht über anerkannte [Prüfst] ist auf der Internetpräsenz des BSI veröffentlicht (siehe www.bsi.bund.de).

Common Criteria Zertifikate (gemäß [gemProdT_Kon], Kap. 3.2.1) 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.

5.3.1.1 Prüfbeauftragung

Zur Durchführung der IT-Sicherheitsprüfung beauftragt der Antragsteller eine von ihm ausgewählte, durch das BSI anerkannte [Prüfst]. Diese führt die Prüfung durch.

5.3.1.2 Zertifizierungsbeauftragung

Zur Durchführung der Zertifizierung stellt der Antragsteller einen Antrag beim BSI. Das BSI begleitet und überwacht im Rahmen der Zertifizierung den Prüfprozess. Nach erfolgreicher Prüfung stellt das BSI ein Zertifikat, einen Bescheid und einen Report aus, die der Zulassungsstelle beizubringen sind. Das Zertifikat ist auf den von der gematik vergebenen ZLS zu referenzieren.

5.3.2 Prüfbericht Security Target[6]

Der Antragsteller beschreibt sein Security Target gemäß [gemProdT_Kon], Kap. 3.2, und reicht diese bei der Zulassungsstelle ein.

Die gematik prüft das Security Target und fasst das Ergebnis in einem Prüfbericht zusammen.

5.3.3 Sicherheitsgutachten

Die Erfüllung der Anforderungen zur sicherheitstechnischen Eignung hat der Antragsteller nachzuweisen. Die Bestätigungsbescheinigung der diesem Zulassungsverfahren vorangehenden Bestätigung „Sicherheitsgutachten" [gemZul_Best_SiGu] ist der Zulassungsstelle als Kopie einzureichen.

Die Bestätigung wird auf Gültigkeit geprüft.

Nachfristen bzw. Ausnahmen bedürfen der Schriftform durch die Zulassungsstelle.

---

[5]Ein von Common Criteria abweichender Sicherheitsnachweis bei Minor-Releases des Konnektors ist im Anhang C beschrieben.
[6] Dieser Nachweis ist für Konnektor ab Produkttypversion 3 zusätzlich beizubringen.

5.4 Nachweis der elektrischen, mechanischen und physikalischen Eignung

Die elektrischen, mechanischen und physikalischen Anforderungen an das Zulassungsobjekt sind in [gemProdT_Kon], Kap. 3.3, gelistet.

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 den von der gematik vergebenen Verfahrensschlüssel (ZLS) zu referenzieren.

Auskünfte hierüber erteilt die Zulassungsstelle.

5.5 Wiederholung von Zertifizierungen

Eine periodische Wiederholung der Zertifizierung des BSI (siehe Kap. 5.3.2) 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.

5.6 Auslieferung des Konnektors

Die Auslieferung des Konnektors muss immer mit einer eingebauten und zugelassenen Gerätekarte (gSMC-K) erfolgen.

5.7 Updates für installierte Konnektoren

Soll für eine installierte Produktivversion eine aktualisierte Firmware zur Verfügung gestellt werden, darf dies ausschließlich mit der Firmware aus einer zugelassenen Produktversion erfolgen.

Zusätzliche Anforderungen bzw. weitere Nachweise werden durch dieses Kapitel nicht abgeleitet.

Das Update über den Konfigurationsdienst wird gemäß folgender Grafik durchgeführt:

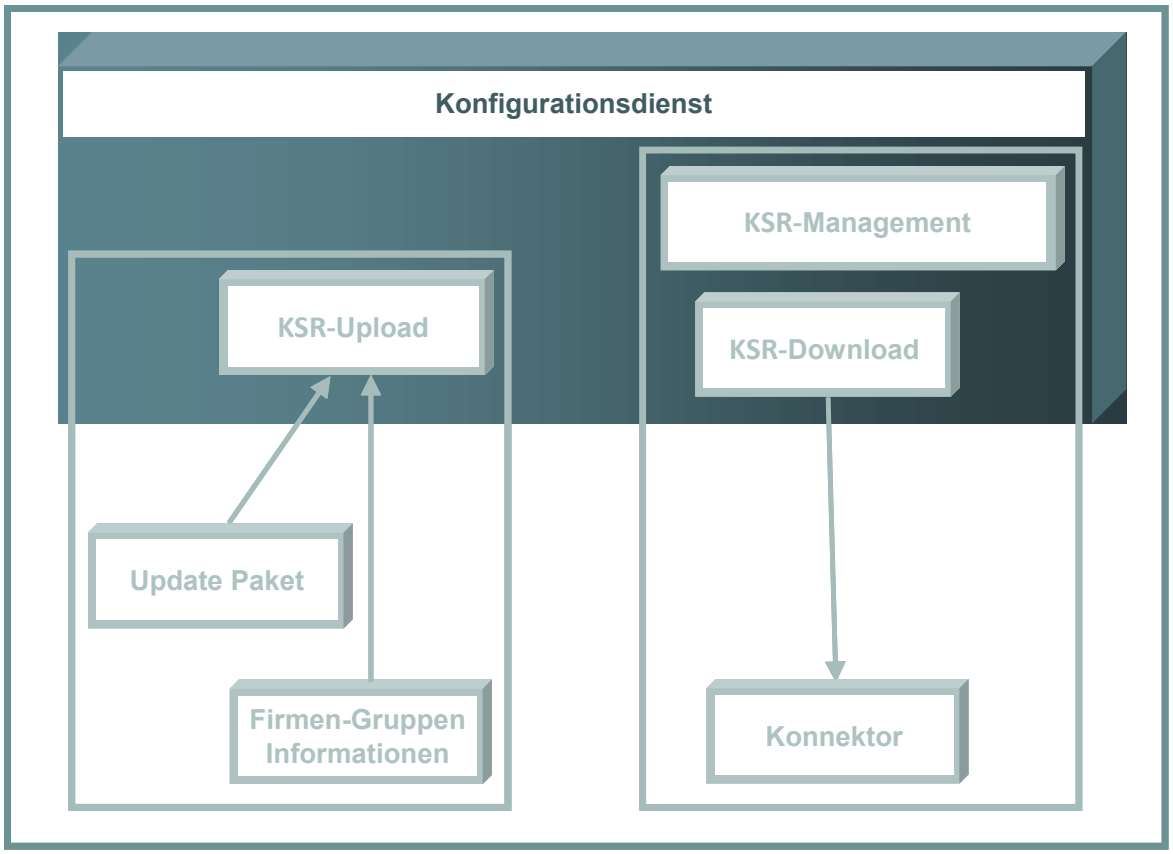

Abbildung 4: Update-Vorgang (schematisch)

Der Update-Vorgang wird entweder über den Konfigurationsdienst gemäß [gemSpec_KSR] oder über einen herstellerspezifischen Mechanismus von einer lokalen Datenquelle durchgeführt. Beide Varianten müssen die Anforderungen der [gemProdT_Kon] erfüllen. Die Firmware aus einer zugelassenen Produktversion ist vom Zulassungsinhaber zur Verfügung zu stellen.

6 Möglichkeit der Durchführung von Testmaßnahmen in der Produktivumgebung

Um ein effizientes Vorgehen für die Verfügbarkeit von neuen medizinischen Anwendungen auf Basis von sicheren Komponenten der Telematikinfrastruktur zu gewährleisten, bietet die gematik für die Antragsteller die freiwillige Möglichkeit, bereits vor durchzuführende kontrollierte Inbetriebnahmen bzw. vor der finalen Zulassung des Produkts für den Produktivbetrieb, mit einer eingeschränkten Zulassung, Testmaßnahmen in der Produktivumgebung durchzuführen.

Die Zulassung für solche Testmaßnahmen beruht immer auf einer Einzelfallentscheidung und basiert auf den aktuellen Erkenntnissen aus dem laufenden Zertifizierungs- und Zulassungsverfahren. Sofern diese Verfahren die notwendige Produktreife erkennen lassen, kann die gematik nach entsprechender Risikoabwägung und mit Einverständnis des BSI den Eintritt in Testmaßnahmen in der Produktivumgebung durch eine Zulassung, begrenzt auf die Durchführung der Testmaßnahmen, gestatten.

Sollten zum Zeitpunkt der Erteilung der eingeschränkten Zulassung noch nicht die erforderlichen Nachweise zur Sicherheit des Produkts vorliegen, ist der Startzeitpunkt und Zeitrahmen für die Testmaßnahmen so zu wählen, dass spätestens zum Ende der Testphase die Abnahme aller Prüfstellenberichte durch das BSI erfolgen kann.

Diese Testmaßnahmen in der Produktivumgebung ermöglichen dem Antragsteller, sein Produkt in einer frühen Entwicklungsphase unter realen Bedingungen zu testen.

Voraussetzungen:

- Laufendes Zulassungsverfahren bei der gematik.
- Notwendige Produktreife für die Durchführung der Testmaßnahme:
  - Zulassungstests der gematik und der Nachweis der eigenverantwortlichen Tests (EvT) müssen die vorläufige, positive Aussage über Funktionalität, Interoperabilität und Sicherheit ermöglichen sowie
  - Fortschritt im Zertifizierungsverfahren beim BSI, der eine positive Aussage über die Sicherheit für die Durchführung der Testmaßnahme ermöglichen muss.
- Der Antragsteller entbindet das BSI sowie die beauftragte Prüfstelle gegenüber der gematik von ihrer gesetzlichen und/oder vertraglichen Geheimhaltungspflicht, um Auskunft über den jeweiligen Stand des Zertifizierungsverfahrens sowie sicherheitsrelevante Sachverhalte zu erhalten.
- Einreichung der aktuellen, vom BSI bestätigten Meilensteinplanung zur Zertifizierung des Produkts.

- Einreichung einer Umsetzungsbeschreibung mit folgendem Mindestinhalt:
  - Liste mit den teilnehmenden Leistungserbringern inklusive Namen, Anschrift, Telefonnummer, E-Mail und Betriebsstättennummer,
  - Name der Primärsysteme sowie der Clientsysteme und Clientsystemhersteller, die an der Durchführung der Testmaßnahme beteiligt sind sowie
  - Zeitplan für die Durchführung der Testmaßnahme (angestrebtes Start- und Endedatum).
- Einwilligung des Antragstellers in die Durchführung von Penetrations-Tests für die Produktversionen, die in der Testmaßnahme eingesetzt werden.
- Der Antragsteller stellt der gematik auf Anfrage bis zu drei zusätzliche Testobjekte zur Durchführung von begleitenden Penetrations-Tests zur Verfügung (zusätzlich zu den für den funktionalen Test eingereichten Testobjekten).

Diese Zulassung ist befristet und mit Nebenbestimmungen verbunden, welche sich aus den Erkenntnissen des laufenden Zulassungsverfahrens ergeben, der Überwachung der Testmaßnahme dienen und, falls notwendig, einen unverzüglichen Rückbau, Austausch oder das ordnungsgemäße Unbrauchbarmachen ermöglichen.

Ein Widerruf der Zulassung ist jederzeit möglich. Dies gilt insbesondere dann, wenn während des laufenden Zertifizierungsverfahrens oder der Penetrations-Tests Erkenntnisse gewonnen werden, die einer sicheren Weiterführung der Testmaßnahmen im Produktivbetrieb entgegenstehen.

Die Zulassung ist begrenzt auf die Durchführung der Testmaßnahmen im Produktivbetrieb.

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 Mehrfach-Zertifizierung des gleichen Produktes in verschiedenen Staaten vermieden.
HBA	Heilberufsausweis
SMC	Security Module Card
SOGIS	Senior Officials Group Information System Security siehe CCRA
TI	Telematikinfrastruktur (der elektronischen Gesundheitskarte)
ZLS	Verfahrensschlüssel
gSMC-K	gematik: Produkte der Telematikinfrastruktur, hier: Sicherheitsmodul-karte Typ K

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

Kürzel	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.
produktüber-greifender Produkttest	Ergänzend zum Produkttest, der sich jeweils auf ein einzelnes Produkt bezieht, müssen Produkte auch integriert getestet werden.

A2 – Abbildungsverzeichnis

Abbildung 1: Prüfbereiche..... 7
Abbildung 2: Schema Zulassungsverfahren..... 9
Abbildung 3: Schema Zulassungsverfahren Konnektor Produkttypversion 5 10
Abbildung 4: Update-Vorgang (schematisch) 15

A3 – Referenzierte Dokumente

A3.1 – 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 der Übersicht Festlegung der zulassungsfähigen Versionsstände Produkttypen, Anbietertypen und weitere Anwendungen 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_Kon]	gematik: Produkttypsteckbrief Konnektor
[gemSpec_KSR]	gematik: Spezifikation Konfigurationsdienst
[gemSpec_OM]	gematik: Spezifikation Operations und Maintenance (Fehlermanagement, Versionierung, Monitoring)
[gemZul_übergrVerf]	gematik: übergeordnete Verfahrensbeschreibung für Zulassungs- und Bestätigungsverfahren
[gemZul_Best_SiGu]	gematik: Einführung der Gesundheitskarte – Bestätigung "Sicherheitsgutachten"
[gemKPT_Inbetriebnahme_Kon_PTV5]	gematik: Konzept für die Kontrollierte Inbetriebnahme Konnektor PTV 5
[gemZUL_Umsb_KON]	gematik: Vorlage Umsetzungsbeschreibung des kontrollierte Inbetriebnahme
[gemZUL_Abschl_KON]	gematik: Vorlage Abschlussbericht

A3.2 – Weitere Dokumente

[Quelle]	Herausgeber: Titel
[Prüfst]	Verzeichnisse von anerkannten Prüfstellen siehe: - www.bsi.bund.de (Menüpunkt „Zertifizierung und Akkreditierung“) und - www.dar.bam.de (Menüpunkt „Akkreditierte Stellen“)

A4 – 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 – Konnektor“

A5 – 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 der Zulassungsstelle klären [zulassung@gematik.de]	
4	Zulassungsantrag rechtsgültig unterschreiben und an die Zulassungsstelle per E-Mail [zulassung@gematik.de] versenden	
5	Produktidentifikation in das Zulassungsobjekt einarbeiten	
6	Durchführung der eigenverantwortlichen Tests und Erstellen des unterschriebenen Testberichts	
7	Zulassungsobjekt gemäß Definition im Zulassungsverfahren zusammenstellen und zusammen mit dem unterschriebenen Testbericht an den Testmanager versenden	
8	Nachweis der funktionalen Eignung gemäß Definition im Zulassungsverfahren klären und überwachen	
9	Nachweis der sicherheitstechnischen Eignung gemäß Definition im Zulassungsverfahren beauftragen und an Zulassungsstelle versenden	
10	Nachweis der elektrischen, mechanischen und physikalischen Eignung gemäß Definition im Zulassungsverfahren beauftragen und an Zulassungsstelle versenden	
11	Erstellung der Umsetzungsbeschreibung für die kontrollierte Inbetriebnahme (PTV 5)	
12	Durchführung der kontrollierten Inbetriebnahme und Erstellung des Abschlussberichtes (PTV 5)	

Anhang B – Besonderheiten für die Zulassung Konnektor Produkttypversion 5

Für die Zulassung eines Konnektors Produkttypversion 5 müssen weitere Nachweise erbracht werden, die belegen, dass die technische Funktionsfähigkeit und die technische Interoperabilität mit weiteren Komponenten der TI gegeben sind.

Für die uneingeschränkte Zulassung eines Konnektors Produkttypversion 5 müssen neben den Anforderungen aus [gemProdT_Kon] ebenfalls die Anforderungen aus dem [gemKPT_Inbetriebnahme_Kon_PTV5] erfüllt werden.

Für die Produktzulassung mit Nebenbestimmungen für die kontrollierte Inbetriebnahme müssen die Nachweise gemäß [gemZul_Prod_KON#5] beigebracht werden und zusätzlich eine Umsetzungsbeschreibung gemäß [gemKPT_Inbetriebnahme_Kon_PTV5]. Es wird dann die Produktzulassung mit Nebenbestimmungen erteilt. Die Produktzulassung mit Nebenbestimmungen erlaubt es dem Zulassungsnehmer, eine kontrollierte Inbetriebnahme gemäß den in der Umsetzungsbeschreibung beschriebenen Angaben durchzuführen. Der Rollout des Konnektors ist beschränkt auf die an der kontrollierten Inbetriebnahme teilnehmenden Leistungserbringer.

Die Zeitpunkte zur Übermittlung des Umsetzungskonzeptes und zur Anzeige des Starts der kontrollierten Inbetriebnahme sind dem [gemKPT_Inbetriebnahme_Kon_PTV5] zu entnehmen.

Wurde die kontrollierte Inbetriebnahme in der Produktivumgebung abgeschlossen und wurde dies von der gematik positiv bestätigt, sind die Nebenbestimmungen erfüllt. Der Zulassungsnehmer darf das Produkt dann bundesweit ausrollen.

B1 - Beibringung der Nachweise zur funktionalen Eignung im Rahmen der kontrollierten Inbetriebnahme

Zusätzlich zu den Nachweisen aus Kapitel 5.2 sind folgende Nachweise zu erbringen

- Prüfbericht Umsetzungsbeschreibung der kontrollierten Inbetriebnahme
- Prüfbericht Abschlussbericht zur kontrollierten Inbetriebnahme.

B1.1 - Prüfbericht Umsetzungsbeschreibung der kontrollierten Inbetriebnahme

Das Zulassungsverfahren erfordert eine Umsetzungsbeschreibung der kontrollierten Inbetriebnahme, welches durch den Antragsteller beizubringen ist.

Der Antragsteller beschreibt in der Umsetzungsbeschreibung die geplante Umsetzung der kontrollierten Inbetriebnahme gemäß [gemKPT_Inbetriebnahme_Kon_PTV5#4.2].

Die gematik prüft die Umsetzungsbeschreibung und dokumentiert das Ergebnis in einem Prüfbericht.

B1.2 - Prüfbericht Abschlussbericht zur kontrollierte Inbetriebnahme

Die Anforderungen der kontrollierten Inbetriebnahme sind in [gemKPT_Inbetriebnahme_Kon_PTV5] beschrieben.

Der Antragsteller führt die kontrollierte Inbetriebnahme laut [gemKPT_Inbetriebnahme_Kon_PTV5] durch, fasst die Ergebnisse in einem Abschlussbericht gemäß [gemKPT_Inbetriebnahme_Kon_PTV5#4.4] zusammen und übermittelt diesen an die Zulassungsstelle.

Die gematik prüft den Abschlussbericht und dokumentiert das Ergebnis in einem Prüfbericht.

Weist der Prüfbericht zum Abschlussbericht ein positives Ergebnis aus, dient dieser als weiterer Nachweis des durchgeführten funktionalen Tests und es wird die uneingeschränkte Zulassung von der Zulassungsstelle bestätigt.

B1.3 - Besonderheiten für eine Zulassung zur kontrollierten Inbetriebnahme zur Beibringung der IT-Sicherheitsprüfung und -zertifizierung

Die gematik kann eine auf die kontrollierte Inbetriebnahme beschränkte Zulassung ohne den Nachweis der Sicherheitsprüfung und -zertifizierung erteilen, wenn folgende Voraussetzungen erfüllt sind:

- Einwilligung des Antragstellers in die Durchführung von Penetrations-Tests für die Produktversionen, die in der Testmaßnahme eingesetzt werden.
- Der Antragsteller stellt der gematik auf Anfrage dafür bis zu drei zusätzliche Testobjekte zur Durchführung von begleitenden Penetrations-Tests zur Verfügung (zusätzlich zu den für den funktionalen Test eingereichten Testobjekten).
- Die von der gematik durchgeführten Penetrations-Tests zeigen keine zulassungsverhindernden Fehler.
- Notwendige Produktreife für die Durchführung die kontrollierte Inbetriebnahme:
    - Zulassungstests der gematik und der Nachweis der EvT müssen die vorläufige, positive Aussage über Funktionalität, Interoperabilität und Sicherheit ermöglichen sowie
    - Die Prüfstelle hat bis zum Zeitpunkt unmittelbar vor der Zulassung zur kontrollierten Inbetriebnahme im laufenden CC-Verfahren keine zulassungsverhindernden Fehler gefunden.
- Der Antragsteller entbindet das BSI sowie die beauftragte Prüfstelle gegenüber der gematik von ihrer gesetzlichen und/oder vertraglichen Geheimhaltungspflicht, um Auskunft über den jeweiligen Stand des Zertifizierungsverfahrens sowie sicherheitsrelevante Sachverhalte zu erhalten.
- Einreichung der aktuellen, vom BSI bestätigten Meilensteinplanung zur Zertifizierung des Produkts.

Der Nachweis der IT-Sicherheitsprüfung und -zertifizierung ist spätestens zum Ende der kontrollierten Inbetriebnahme notwendig, bevor die finale Freigabe für den Produktivbetrieb für den Flächenrollout ausgesprochen wird. Der Startzeitpunkt und Zeitrahmen für die Durchführung der kontrollierten Inbetriebnahme ist daher so zu wählen, dass spätestens zum Ende der kontrollierten Inbetriebnahme die Abnahme aller Prüfstellenberichte durch das BSI erfolgen kann.

Die auf die kontrollierte Inbetriebnahme beschränkte Zulassung ohne Beibringung der notwendigen Sicherheitsprüfung und -zertifizierung beruht immer auf einer Einzelfallentscheidung und basiert auf den aktuellen Erkenntnissen aus dem laufenden Zertifizierungs- und Zulassungsverfahren.

Diese Zulassung ist befristet und mit Nebenbestimmungen verbunden, welche sich aus den Erkenntnissen des laufenden Zulassungsverfahrens ergeben, der Überwachung der kontrollierten Inbetriebnahme dienen und, falls notwendig, einen unverzüglichen Rückbau, Austausch oder das ordnungsgemäße Unbrauchbarmachen ermöglichen.

Ein Widerruf ist insbesondere dann möglich, wenn während des laufenden Zertifizierungsverfahrens Erkenntnisse gewonnen werden, die einer sicheren Weiterführung der kontrollierten Inbetriebnahme entgegenstehen.

Anhang C - Von Common Criteria abweichender Sicherheitsnachweis bei Minor-Releases des Konnektors

Minor-Releases des Konnektors – also Releases mit klar abgestecktem Feature-Zuwachs (z.B. Komfortsignatur) oder mit einer klar abgesteckten Fehlerkorrektur, deren Gesamt-Änderungen aber sehr überschaubar und eindeutig abgegrenzt sind – müssen nicht mehr vollständig nach Common Criteria (CC) zertifiziert werden. Es ist ausreichend, wenn solche Minor-Releases den relevanten technischen Prüfungen durch die CC-Prüfstelle unterzogen werden – ohne formale Zertifizierung durch das BSI. Bei einem positiven Prüfergebnis der Prüfstelle und der Abnahme des Prüfberichts durch die gematik ist ein angemessener Sicherheitsnachweis für die Zulassung eines Minor-Release des Konnektors gegeben. Ein späteres Major-Release wird dann wieder vollständig durch das BSI CC-zertifiziert.

C1 - Grundlegender Ablauf

Für den Sicherheitsnachweis für ein Minor-Release ergeben sich folgende durchzuführende Tätigkeiten:

- Meilensteinplan
  - Der Antragsteller und die Prüfstelle erstellen einen Meilensteinplan für die Prüfung (dieser umfasst mindestens die für die gematik relevanten Termine: Lieferung von Sicherheitsvorgaben, Impact Analysis Report (IAR), ggf. Liste relevanter Common Vulnerabilities and Exposures (CVEs), Prüfbericht sowie den Kick-Off-Termin).
  - Der Meilensteinplan wird fortlaufend aktualisiert.
  - Die gematik erhält stets den aktuellen Meilensteinplan.
- Prüfvorgaben im Falle eines neuen Features
  - Der Antragsteller erstellt Prüfvorgaben in Form eines erweiterten Security Targets (wie es für nachfolgende Major-Releases sowieso erweitert werden muss).
  - Die gematik prüft die Prüfvorgaben und nimmt sie im Positivfall ab.
- Antragsteller-Dokumente
  - Der Antragsteller erstellt einen IAR.
  - Der Antragsteller erweitert die ADV Dokumente FSP, TDS, ARC und Mapping auf den Source Code.
  - Der Antragsteller erweitert die Testdokumentation.
  - Die Dokumente werden an die Prüfstelle gegeben.
  - Die Prüfstelle bewertet anhand der Dokumente, dass es sich um einen Minor-Change mit klar abgesteckten Änderungen handelt (Bewertung mit kurzer Begründung).
  - Die gematik prüft den IAR und die Prüfstellenbewertung bzgl. Minior-Change und nimmt diese im Positivfall ab.
  - Die Prüfstelle bildet sich anhand der Dokumente ein grundsätzliches Verständnis der Änderungen für die folgenden Tests / Schwachstellenanalysen, jedoch findet keine Evaluierung der Dokumente statt.
- (kurze) Kick-Off-Telefonkonferenz
  - Die Prüfstelle stellt der gematik das Prüfvorgehen / die Prüfschwerpunkte vor.
  - Klärung ggf. offener Punkte.
- CVE-Analyse

  - CVE-Analyse erfolgt durch den Antragsteller.
  - Die Bewertung der CVE-Analyse erfolgt durch die Prüfstelle.
  - Die Bewertung und Entscheidung über ggf. zusätzlich notwendige Maßnahmen aufgrund CVE-Analyse erfolgt durch die gematik.
- Eigentliche Prüfung
  - Die Tests erfolgen durch den Antragsteller, wie im CC-Verfahren auch.
  - Funktionale Tests, Penetrations-Tests und Schwachstellenanalyse (analog ATE_IND.2 und AVA_VAN.3 im CC-Verfahren) erfolgt durch die Prüfstelle anhand des TOE und dessen Quellcode gezielt für die vorgenommenen Änderungen (im Falle neuer Features entsprechend den Sicherheitsvorgaben).
- Prüfbericht
  - Die Prüfstelle liefert den Prüfbericht an die gematik.
  - Die gematik prüft den Prüfbericht und nimmt ihn im Positivfall ab (Erfüllung der Säule Sicherheit im Zulassungsverfahren).
  - Im Negativfall können Nachbesserungen am Bericht oder auch Nachprüfungen durch die Prüfstelle möglich sein.

Zu jeder Zeit können die gematik und die Prüfstelle über das Verfahren miteinander kommunizieren. Das Ziel ist ein schnelles Ausräumen etwaiger Unklarheiten / Missverständnisse um ein effizientes Verfahren zu ermöglichen und Nachforderungen am Ende des Verfahrens möglichst zu verhindern. Insbesondere bei identifizierten Problemen im Verfahren ist die gematik daher zeitnah einzubinden.

C2 - Beteiligte Prüfstelle und Evaluator

Für den Sicherheitsnachweis für ein Minor-Release des Konnektors muss der Antragsteller dieselbe vom BSI akkreditierte CC-Prüfstelle und dabei mindestens einen der CC-Evaluatoren beauftragen, die bei der vorherigen CC-Evaluierung des Konnektors involviert waren. Eine Kontinuität des Knowhows der Evaluatoren über den Konnektor muss sichergestellt werden. Die Erfüllung der Forderung zur Knowhow-Kontinuität ist im Rahmen des Sicherheitsnachweises zu dokumentieren.

C3 - Fristen

Ein Votum der Prüfstelle für ein Minor-Release darf nur auf Basis einer CC-zertifizierten Vorversion folgen, deren ETR-Abnahme nicht älter als 1 Jahr ist. Innerhalb dieser Zeit ist die Prüfung und Zulassung mehrere Minor-Releases möglich.

Das Votum der Prüfstelle im Rahmen des Sicherheitsnachweises für das Minor-Release darf nicht älter als drei Monate sein, um von der gematik abgenommen zu werden.

C4 - Antragsteller-Dokumente

Der Antragsteller erstellt für die Minor-Release Version der Firmware einen IAR bezogen auf die letzte CC-zertifizierte Vorversion der Firmware. Werden mehrere Minor-Releases nacheinander zur Zulassung gebracht, wird der vorhergehende IAR erweitert und die zusätzlichen Änderungen der neuen Minor-Version im IAR eindeutig kenntlich gemacht. Bezugspunkt des IAR bleibt die letzte CC-zertifizierte Vorversion.

Die detaillierte Dokumentation durch den Hersteller muss zu den neuen oder ggf. geänderten Funktionen diejenige Information enthalten, die man in einem CC-Verfahren in den entsprechenden Dokumenten der Klasse ADV erwarten würde – also FSP, TDS, ARC und das Mapping auf den Source Code. Da der Umfang der Änderungen übersichtlich sein soll,

kann die der Übersicht halber auch in einem einzigen Dokument erfolgen. Alternativ kann der Hersteller auch die vorhandenen CC-Herstellerdokumente erweitern (mit Änderungsmarkierungen). Die Detailtiefe muss den genannten CC-Aspekten entsprechen, damit der Evaluator die Verfeinerung des Designs von grober Änderungsbeschreibung bis hinunter zum Source-Code verstehen kann.

Gleiches gilt für die Testdokumentation, aus der ersichtlich werden muss, welcher Test welche Sicherheitseigenschaft der neuen oder geänderten Funktionalität abdeckt, und dass das Testen vollständig ist. Auch hier ist eine kompakte Darstellung in einem kurzen Dokument möglich oder ein Update der entsprechenden CC-Dokumente mit Änderungsmarkierungen.

Für das nachfolgende CC-Verfahren für die nächste Major-Version sind die genannten Dokumentationen ebenso gefordert und können entsprechend dort nachgenutzt werden. Es sollen also explizit nicht zusätzliche Dokumente/Inhalte nur für den Sicherheitsnachweis zum Minor-Release erstellt werden.

Ein Minor-Release ist stets fokussiert auf ein konkretes, abgegrenztes, neues Feature oder auf eine konkrete, abgegrenzte Korrektur eines Fehlers. Der IAR dient daher auch dazu, zu prüfen, dass es sich tatsächlich um ein Minor-Release handelt. Entsprechend prüft die Prüfstelle, dass der vom Antragsteller geplante Änderungsumfang als Minor-Release gewertet werden kann und übergibt ihre Bewertung an die gematik.

Unter Berücksichtigung der Einschätzung der Prüfstelle prüft die gematik auch den IAR und nimmt diesen im Positivfall ab.

Die Evaluierung der Dokumente durch die Prüfstelle ist im Rahmen des Sicherheitsnachweises für den Minor-Release nicht notwendig.

C5 - CVE-Analyse

Auch wenn Minor-Releases einen kleinen, klar abgesteckten Änderungsumfang haben müssen, ist im Rahmen des Sicherheitsnachweises eine CVE-Analyse vom Antragsteller durchzuführen. Nur so kann ein vollständiges Bild erhalten werden, anhand dessen entschieden werden kann, ob ggf. für den Konnektor relevante Schwachstellen bereits im Minor-Release geschlossen werden müssen.

Wie auch im CC-Verfahren üblich, bewertet die Prüfstelle die CVE-Analyse.

Die gematik erhält die für den Konnektor ggf. als relevant identifizierten CVEs inklusive der Bewertung der Prüfstelle. Unter Berücksichtigung dieser Bewertung und ggf. nach weiterer Rücksprache mit der Prüfstelle entscheidet die gematik, ob ggf. relevante CVEs bereits im Minor-Release behandelt werden müssen.

C6 - Berücksichtigung des Update-Mechanismus

Für einen Minor-Release ist immer auch ein Nachweis darüber zu erbringen, dass der Update-Mechanismus unverändert ist bzw. dieser weiterhin sicher ist, falls Änderungen zwingend erforderlich waren. So kann trotz eines formal nicht zertifizierten Update-Mechanismus weiterhin eine gültige Sicherheitsaussage für neue, auf eine nicht-zertifizierte Firmware-Version folgende Firmware-Versionen erhalten werden.

Dafür sind die im Folgenden beschriebenen Maßnahmen notwendig.

C6.1 - Antragsteller

Es ist eine Grundvoraussetzung für den Sicherheitsnachweis für Minor-Releases, dass der Antragsteller dieselbe Prüfstelle mit mindestens einem bei der vorherigen CC-Evaluierung des Konnektors involvierten Evaluatoren beauftragt. Insbesondere kennt der Prüfer somit auch den Update-Prozess und kann eventuelle Änderungen an diesem erkennen und beurteilen. Änderungen am Update-Prozess dürfen vom Antragsteller bei einem Minor-Release grundsätzlich nicht vorgenommen werden. Sollten an dieser Stelle dennoch Änderungen geplant sein (z.B. wegen sinnvoller Fixes wegen CVE Meldungen) müssen diese zuvor mit der gematik besprochen und von der gematik akzeptiert werden.

Sollten Änderungen am Update-Mechanismus vorgenommen worden sein, sind diese vom Antragsteller im IAR besonders hervorzuheben und verständlich zu beschreiben.

Der Antragsteller bestätigt im IAR, dass die Entwicklungs- und Produktionsstandorte sich seit der letzten CC-Evaluierung nicht geändert haben.

Der Antragsteller bestätigt im IAR, dass der Auslieferungsprozess der nicht-zertifizierten Firmware-Version die Auflagen aus der zertifizierten Version erfüllt.

Der Antragsteller muss für die nachfolgende CC-Zertifizierung des nächsten Major-Release den beim BSI eingereichten IAR auch der gematik vorlegen. Die gematik prüft, dass die Änderungen aus dem Minor-Release hier auch entsprechend aufgeführt sind.

C6.2 - Prüfstelle

Die Prüfstelle bewertet den IAR. Dabei prüft sie insbesondere, ob Änderungen enthalten sind, die den Update-Mechanismus betreffen. Sollten Änderungen am Update-Mechanismus enthalten sein (eben bspw. durch CVE-Analyse hervorgerufen), sind sie besonders kritisch von der Prüfstelle zu analysieren und zu hinterfragen.

Die Prüfstelle bezieht den Update-Mechanismus in die Prüfungen des Produkts mit ein. Sie begründet und bestätigt der gematik schriftlich im Rahmen des Prüfberichts unter Berücksichtigung des IAR und der ihr vorliegenden Dokumente, wie Handbücher und Source Code, dass der Update-Prozess entweder unverändert ist oder im Falle zwingend notwendiger Anpassungen (bspw. durch CVEs) weiterhin sicherheitstechnisch ohne Beanstandung ist.

Die Prüfstelle bestätigt auf Dokumentenlage der gematik schriftlich im Rahmen des Prüfberichts, dass die Entwicklungs- und Produktionsstandorte sich seit der letzten CC-Evaluierung nicht geändert haben.

Die Prüfstelle bestätigt der gematik schriftlich im Rahmen des Prüfberichts, dass der Auslieferungsprozess der nicht-zertifizierten Firmware-Version die Auflagen aus der zertifizierten Version erfüllt.

C6.3 - gematik

Die gematik spricht auf Grund der ihr vorliegenden Erklärungen und Dokumente von Antragsteller und der Prüfstelle einen Sicherheitsnachweis aus, der die Sicherheit des Update-Mechanismus/Firmware-Auslieferungsweges explizit umfasst.

C7 - Vertraulichkeit von Unterlagen

Der Antragsteller trifft Regelungen mit seiner Prüfstelle, damit die Vorgaben der Vertraulichkeit zur Weitergabe von Dokumenten an die gematik berücksichtigt und erfüllt werden.

C8 - Handbuchinformationen

Der Anwender muss geeignet informiert werden, dass es sich beim vorliegenden zugelassenen Produkt nicht um ein CC-zertifiziertes Produkt handelt.

Für den Anwender muss ebenso deutlich werden, dass es sich weiterhin um ein sicheres, zugelassenes Produkt handelt.

Die aus der CC-Zertifizierung erforderlichen Hinweise an den Anwender müssen in der Guidance verbleiben. Auch ein Konnektor mit einer nicht-zertifizierten Firmware-Version eines Minor-Release muss vom Nutzer so betrieben und verwaltet werden, als wäre dieser CC-zertifiziert.

Der Antragsteller hat im IAR zu erläutern, wie er die genannten Punkte sicherstellt und die Prüfstelle begründet und bewertet auf Dokumentenlage im Prüfbericht, ob die Antragstellermaßnahmen ausreichend sind.