gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Verfahrensbeschreibung

Bestätigung Sicherheitsgutachten

Version:	1.3.0
Revision:	\main\rel_opb1\6
Stand:	14.06.2017
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemZul_Best_SiGu]

Dokumentinformationen

Änderungen zur Vorversion

Anpassungen an die eIDAS-Verordnung.

Dokumentenhistorie

Version	Stand	Kapitel	Grund der Änderung, besondere Hinweise	Bearbeiter
0.0.1	14.12.12		Erst-Erstellung	Zulassung
1.0.0	15.05.14		Anpassung an EV0064, Änderung Ziele der Bestätigung, Kommentierung durch die Gesellschafter	Zulassung
1.1.0	19.08.15	2.1, 3.1, 4, A3.1	Ergänzung Verzeichnisdienst und Fachdienst KOM-LE	Zulassung
1.2.0	30.03.16		Anpassung an Online-Produktivbetrieb	Zulassung
1.2.1	03.03.17	5.1;2 A 3.2	Anpassung an eIDAS	Zulassung
1.3.0	14.06.17		freigegeben	gematik

Inhaltsverzeichnis

1 Einleitung

Dieses Dokument beschreibt das Bestätigungsobjekt 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 Bestätigungsverfahren. Die übergeordnete Verfahrensbeschreibung [gemZul_übergrVerf] kann der Internetpräsenz der gematik entnommen werden (siehe https://www.gematik.de).

2 Bestätigungsobjekt Sicherheitsgutachten

Für die Herstellung von dezentralen oder den Betrieb von zentralen Produkten werden ggf. gemäß dem jeweiligen Produkttypsteckbrief (siehe auch Kapitel 4) Anforderungen an die Sicherheit gestellt. Im Kapitel "Anforderungen zur sicherheitstechnischen Eignung | Sicherheitsgutachten" jedes Produkttypsteckbriefs sind diese zusammengefasst. Die zu auditierenden Prozesse werden unter dem Gesichtspunkt der sicheren Herstellung von Produkten bzw. Verarbeitung von sicherheitsrelevanten Daten im Sicherheitsgutachten (SiGu) bewertet.

Um Sicherheitsgutachten wiederverwenden zu können, ist eine Modularisierung umgesetzt worden. Somit wurde eine Mehrfacherbringung von gleichen Sicherheitsgutachten für verschiedene Verfahren vermieden.

Die Prozesse werden gemäß dem/den jeweiligen Produkttypsteckbrief(en) (siehe auch Kapitel 4) auditiert.

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

- die detaillierte und vollständige Bezeichnung des auditierten Prozesses sowie
- die Versionsnummer des Sicherheitsgutachtens gemäß [gemSpec_OM].

Ferner hat der Antragsteller sicherzustellen, dass allen Beteiligten dieselbe Version des Sicherheitsgutachtens vorliegt.

Werden in dem Sicherheitsgutachten gleich mehrere Prozesse/Produkttypen (z. B. für mehrere Produkte der zentralen TI) auditiert, so sind diese alle zu benennen. Wenn nötig, sind bei den Kriterien die Zugehörigkeiten zum jeweiligen Produkttyp sicherzustellen.

Werden in dem Sicherheitsgutachten gleich mehrere Standorte für einen Produkttyp auditiert, so sind diese alle zu benennen. Wenn nötig, sind bei den Kriterien die Zugehörigkeiten zum jeweiligen Standort sicherzustellen.

2.1 Ausprägungsvarianten des Sicherheitsgutachtens

Sicherheitsgutachten sind besonders dort notwendig, wo kryptographische oder personenbezogene Daten erzeugt, gespeichert, verarbeitet oder weitergeleitet werden. Für folgende Prozesse zum Betrieb eines Produktes bzw. zum Herstellungsprozess von Produkten müssen Sicherheitsgutachten vorgelegt werden:

- eGK-Kartenherausgeber bzw. beauftragte Dienstleister (siehe Abbildung 1) und/oder
- Trust-Center bzw. Zertifikatsdiensteanbieter (siehe Abbildungen 1 und 2) und/oder

- Kartenhersteller bzw. Kartenpersonalisierer (siehe Abbildungen 1 und 2) und/oder
- Betreiber eines Produktes
- Betreiber eines Fachdienstes.

Die Einhaltung der Sicherheitsanforderungen wird über den gesamten Lebenszyklus gefordert, d. h. von der Erzeugung über den Versand bis hin zur Nutzung. Bei verteilten Prozessen hat die Begutachtung jeden Teilprozess, die Schnittstellen zur Übertragung sicherheitskritischer Daten zwischen den Teilprozessen, die Speicherung der Daten in Produkten der TI sowie die Speicherung in verteilten Systemen, zu berücksichtigen.

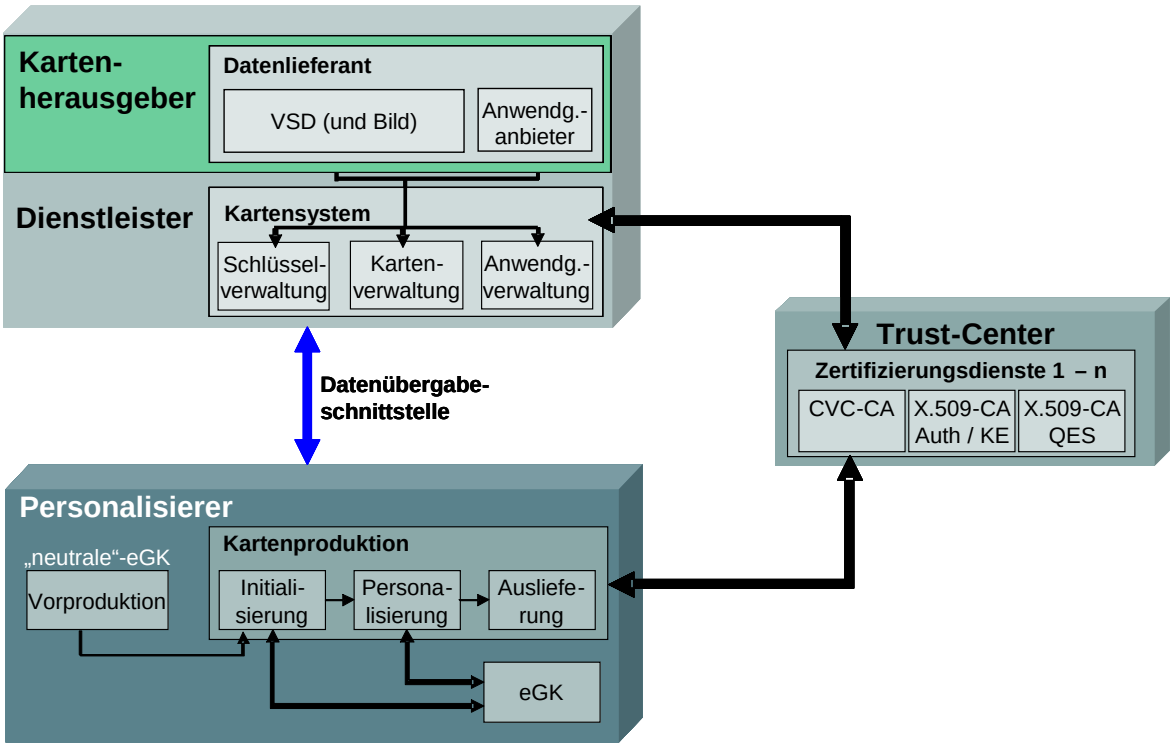

Abbildung 1: Herausgabe eGK (grün = kein Auditbericht)

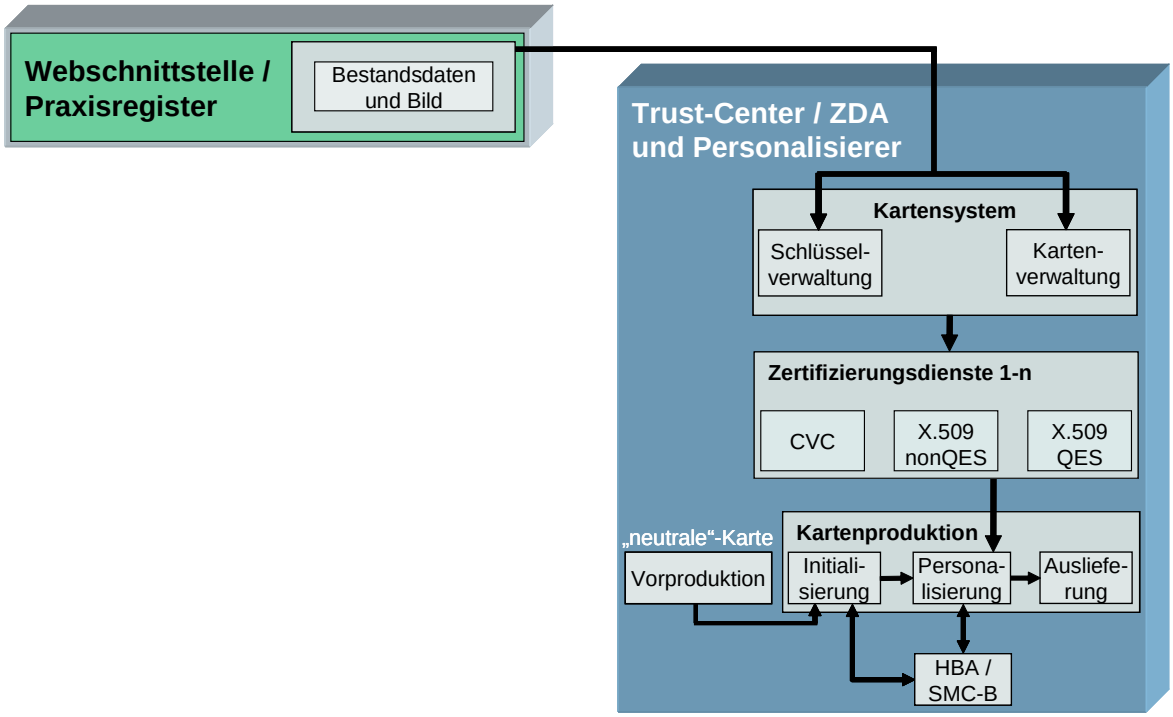

Abbildung 2: Herausgabe HBA und SMC-B (grün = kein Auditbericht)

2.2 Bestätigungen von Teilen des Sicherheitsgutachtens

Für die Prozesse gibt es nur die Gesamtbestätigung und keine Teilbestätigung.

3 Prüfbereiche und Rollen

3.1 Prüfbereiche

Im Bestätigungsverfahren ist lediglich der Prüfbereich Sicherheit zu durchlaufen:

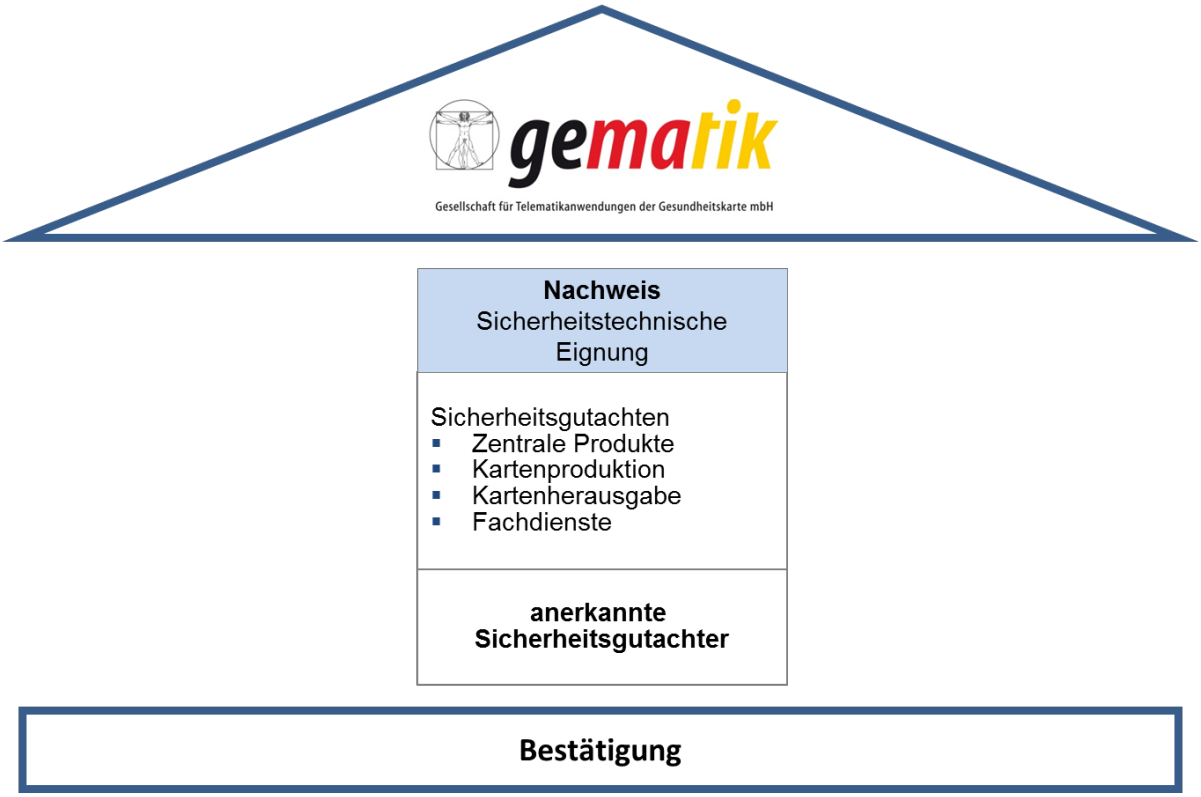

Abbildung 3: Prüfbereiche

***** Abhängig vom auditierten Prozess des Antragstellers können unterschiedliche Kriterien für die Sicherheitsgutachten gültig sein - siehe auch Tabelle im Kapitel 4.

3.2 Rollen

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

- Antragsteller
- Zulassungsstelle
- Datenschutz und Informationssicherheit
- anerkannter Sicherheitsgutachter

4 Bestätigungsverfahren

Der folgende Verfahrensablauf umfasst die Antragstellung, das Bestätigungsobjekt, notwendige Nachweise sowie die Bestätigungserteilung.

Das Bestätigungsverfahren Sicherheitsgutachten steht in Abhängigkeit zu weiteren Verfahren. Die zwingende Reihenfolge bei der Durchführung ist (siehe Folgeseite):

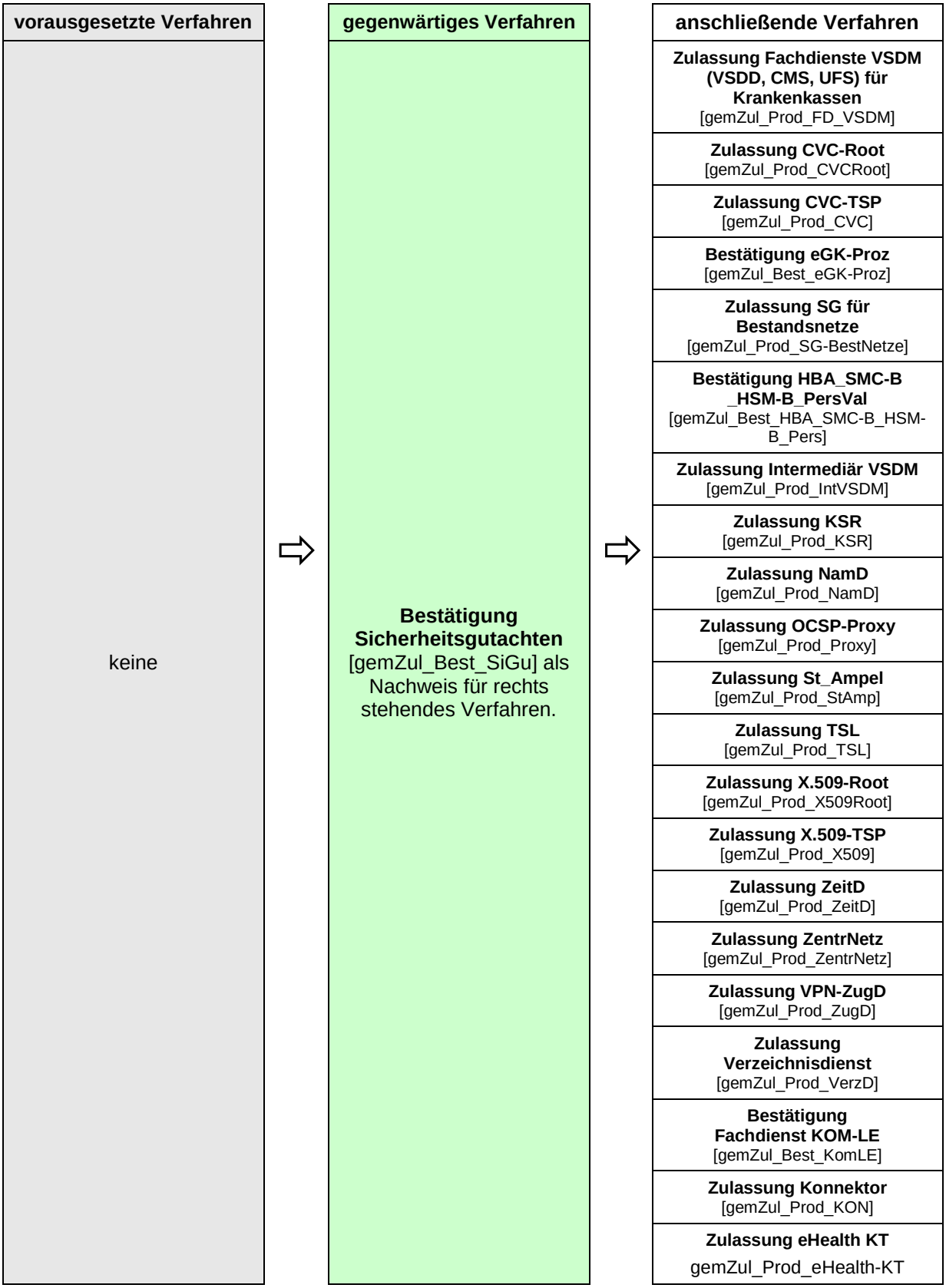

Abbildung 4: Reihenfolge Bestätigungsverfahren

4.1 Verfahrensübersicht

Nachfolgend die schematische Darstellung des Bestätigungsverfahrens.

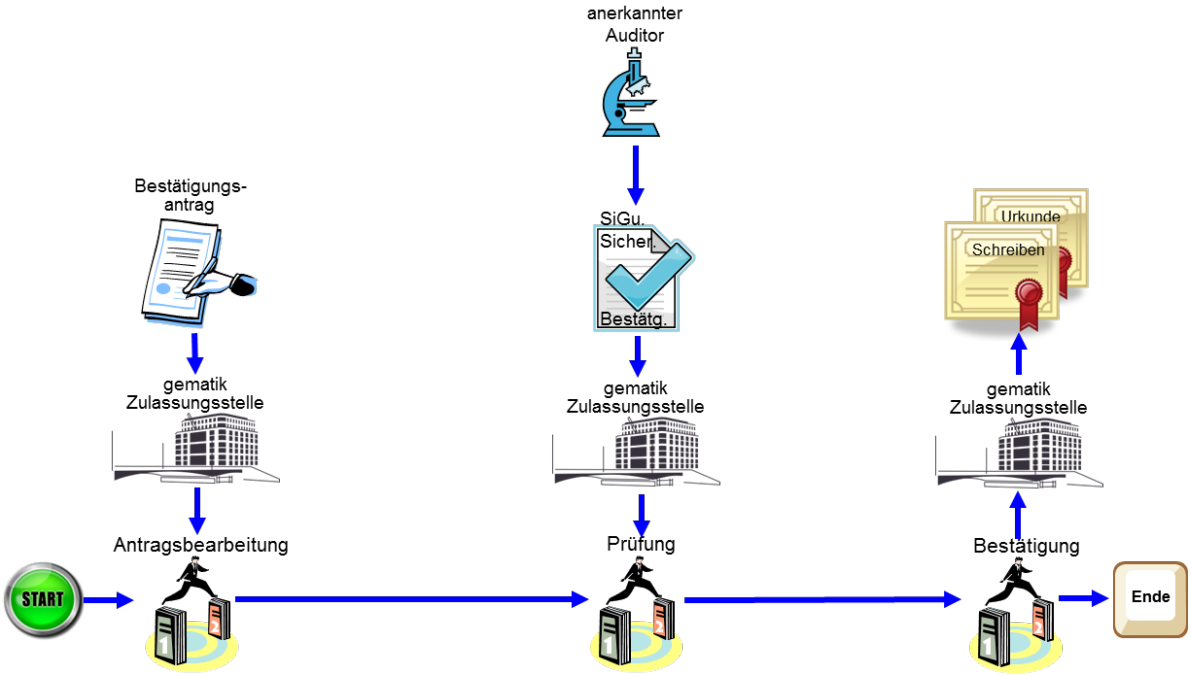

Abbildung 5: Schema Bestätigungsverfahren

Das Bestätigungsverfahren beginnt mit der Antragstellung bei der Zulassungsstelle. Die Zulassungsstelle prüft den Bestätigungsantrag auf Vollständigkeit und Korrektheit der Angaben. Im Positivfall beauftragt die Zulassungsstelle die Prüfung des Sicherheitsgutachtens bei der gematik Abteilung Datenschutz & Informationssicherheit.

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

Ist das Prüfergebnis positiv, erteilt die Zulassungsstelle die schriftliche Bestätigung. Bei negativem Prüfergebnis wird der Bestätigungsantrag gegenüber dem Antragsteller abgelehnt.

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 (sicherheitstechnische Eignung) gelisteten Anforderungen an das Produkt und die Prozesse des Antragstellers.

5.1 Beibringung der Nachweise

Die Bestätigung zur sicherheitstechnischen Eignung für die TI erfordert je nach Produkttyp ein Sicherheitsgutachten.

5.2 Nachweis der sicherheitstechnischen Eignung

Für den Betrieb eines Produktes bzw. für den Herstellungsprozess von Produkten sind jeweils im Kapitel 3.2 in den Produkttypsteckbriefen (siehe Anhang A3.1) Sicherheitsanforderungen gelistet, die durch ein Audit begutachtet werden müssen. Hierbei werden die Sicherheitsanforderungen gemäß den Anforderungen aus den jeweiligen Produkttypsteckbriefen auf Einhaltung bzw. Umsetzung geprüft und bewertet. Das Sicherheitsgutachten ist gemäß [gemRL_PruefSichEig_DS] zu erstellen. Er gilt als Nachweis und hat die Aussage zur sicherheitstechnischen Eignung entsprechend der Prüfgrundlage zu enthalten.

Zum Sicherheitsgutachten hat die gematik auf Basis der geltenden Produktspezifikationen die Produkttypsteckbriefe erstellt und wendet diese zur Prüfung einheitlich an. Die Produkttypsteckbriefe werden über die Internetpräsenz der gematik veröffentlicht (siehe https://www.gematik.de, Menüpunkt „Spezifikation“).

Der jeweilige Produkttypsteckbrief in der jeweils geltenden Version ist maßgebend für die Feststellung der sicherheitstechnischen Eignung.

Die Zulassungsstelle prüft das Sicherheitsgutachten auf Anwendbarkeit und die korrekte Versionsnummer.

Die Zulassungsstelle beauftragt die Beurteilung des Sicherheitsgutachtens bei der gematik Abteilung Datenschutz & Informationssicherheit, ob es vollständig, sorgfältig, objektiv und nachvollziehbar ist. Sie führt die Prüfung einmal auf Basis des jeweiligen Produkttypsteckbriefes komplett durch und fasst die Ergebnisse in einem Prüfbericht zusammen. Dieser Prüfbericht wird der Zulassungsstelle beigebracht.

5.3 Wiederholungsaudit für Sicherheitsgutachten / Änderungen an den Prozessen

Eine Wiederholung von Audits für Sicherheitsgutachten wird aus zwei Gründen notwendig:

- **periodische Wiederholung**
  Die Gültigkeitsdauer eines Sicherheitsgutachtens ist auf drei Jahre begrenzt. Deshalb ist ein erneutes Sicherheitsgutachten noch vor Ablauf der Gültigkeitsdauer einzureichen. Nach positivem Prüfungsergebnis durch die Zulassungsstelle wird der neue Gültigkeitszeitraum von drei Jahren intern vermerkt. Die bestehende Bestätigung gilt dann fort, d. h. die Beibringung eines Auditberichts wegen periodischer Wiederholung erfordert keinen neuen Bestätigungsantrag.

- **Wiederholung aufgrund erheblicher Änderungen**
  Beabsichtigt der Bestätigungsinhaber wesentliche technische, organisatorische oder bauliche Änderungen in der Herstellung oder dem Betrieb des Dienstes oder des Produkts, welche die Erfüllung der Anforderungen des jeweiligen Produkttyps betreffen, ist ein neuer Nachweis Sicherheitsgutachten vorzulegen. In diesem Fall ist ein neuer Antrag auf Bestätigung zu stellen und den Maßgaben des Kapitels 4 zu entsprechen.

Beim wiederholten Audit für Sicherheitsgutachten werden – wie beim Erstaudit – alle relevanten Bereiche geprüft. Der aktualisierte Auditbericht für die Produkte der TI ist an die Zulassungsstelle zu senden. Änderungen an einem Auditbericht für die Produkte der TI sind eindeutig über Versionsnummern kenntlich zu machen.

Anhang A

A1 – Abkürzungen

Kürzel	Erläuterung
CA	Certificate Authority. Zertifizierungsstelle, die CV's erstellt
CVC	Card Verifiable Certificate - Zertifikat für ein asymmetrisches Verfahren zur gegenseitigen Echtheitsprüfung von systemzugehörigen Chipkarten
eGK	elektronische Gesundheitskarte
HBA	Heilberufsausweis (englisch HPC)
Root	Oberste Zertifikat in einer Hierarchie einer PKI
SGB	Sozialgesetzbuch
TI	Telematikinfrastruktur (der elektronischen Gesundheitskarte)
X.509	Rahmenwerk der ITU-T für standardisierte Zertifikatsformate und die Zertifikatsprüfung in Authentisierungsdiensten
ZLS	Zulassungsschlüssel

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

A2 – Abbildungsverzeichnis

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 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://www.gematik.de).

[Quelle]	Herausgeber: Titel
[gemZul_übergrVerf]	gematik: übergeordnete Verfahrensbeschreibung für Zulassungs- und Bestätigungsverfahren
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemRL_PruefSichEig_DS]	gematik: Richtlinie zur Prüfung der Sicherheitseignung
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemProdT_CVC_TSP]	gematik: Produkttypsteckbrief Trust Service Provider CVC
[gemProdT_CVC_Root_ECC]	gematik: Produkttypsteckbrief CVC-Root ECC
[gemProdT_eGK_Sich]	gematik: Produkttypsteckbrief Bestätigungsgegenstand Sicherheit für die Herausgabe- und Nutzungsprozesse der eGK G2
[gemProdT_gematik-Root-CA]	gematik: Produkttypsteckbrief gematik Root-CA
[gemProdT_HBA_SMC-B_HSM-B_Pers]	gematik: Produkttypsteckbrief Personalisierung HBA / SMC-B / HSM-B G2
[gemProdT_FD_VSDM]	gematik: Produkttypsteckbrief Fachdienste VSDM
[gemProdT_Intermediär_VSDM]	gematik: Produkttypsteckbrief Intermediär VSDM
[gemProdT_Kon]	gematik: Produkttypsteckbrief Konnektor
[gemProdT_KSR]	gematik: Produkttypsteckbrief Konfigurationsdienst
[gemProdT_KT]	gematik: Produkttypsteckbrief eHealth Kartenterminal
[gemProdT_KV-SNet]	gematik: Produkttypsteckbrief Sicherheitsgateway für Bestandsnetze
[gemProdT_NamD]	gematik: Produkttypsteckbrief Namensdienst
[gemProdT_OCSP_Proxy]	gematik: Produkttypsteckbrief OCSP-Responder-Proxy
[gemProdT_St_Ampel]	gematik: Zulassung zentrale Produkte der Telematikinfrastruktur hier: Störungsampel
[gemProdT_TSL]	gematik: Produkttypsteckbrief TSL-Dienst
[gemProdT_X.509_TSP_QES]	gematik: Produkttypsteckbrief Trust Service Provider X.509 QES
[gemProdT_X509_TSP_nonQES_eGK]	gematik: Produkttypsteckbrief Trust Service Provider X.509 nonQES - eGK

[Quelle]	Herausgeber: Titel
[gemProdT_X.509_TSP_nonQES_HBA]	gematik: Produkttypsteckbrief Trust Service Provider X.509 nonQES - HBA
[gemProdT_X.509_TSP_nonQES_Komp]	gematik: Produkttypsteckbrief Trust Service Provider X.509 nonQES - Komponentenzertifikate
[gemProdT_X.509_TSP_nonQES_SMC-B]	gematik: Produkttypsteckbrief Trust Service Provider X.509 nonQES - SMC-B
[gemProdT_ZeitD]	gematik: Produkttypsteckbrief Zeitdienst
[gemProdT_ZentrNetz]	gematik: Produkttypsteckbrief Zentrales Netz der TI
[gemProdT_VPN_ZugD]	gematik: Produkttypsteckbrief VPN-Zugangsdienst
[gemProdT_VZD]	gematik: Produkttypsteckbrief Verzeichnisdienst
[gemProdT_FD_KOMLE]	gematik: Produkttypsteckbrief Fachdienst KOM-LE
[gemZul_Best_eGK-Proz]	gematik: Bestätigung zur Sicherheit für die Herausgabe- und Nutzungsprozesse der eGK
[gemLeit_Best_HBA_SMC-B_HSM-B_Pers]	gematik: Leitfaden Bestätigung der Validierung der Personalisierungsdaten HBA / SMC-B / HSM-B
[gemZul_Prod_CVC]	gematik: Zulassung dezentraler Produkte der Telematikinfrastruktur hier: CVC
[gemZUL_Prod_CVCRoot]	gematik: Zulassung dezentraler Produkte der Telematikinfrastruktur hier: CVC-Root
[gemZul_Prod_FD_VSDM]	gematik: Zulassung zentrale Produkte der Telematikinfrastruktur hier: Fachdienste VSDM (VSDD, CMS, UFS) für Krankenkassen
[gemZul_Prod_IntVSDM]	gematik: Zulassung zentrale Produkte der Telematikinfrastruktur hier: Intermediär VSDM
[gemZul_Prod_SG-BestNetze]	gematik: Zulassung zentrale Produkte der Telematikinfrastruktur hier: SG für Bestandsnetze
[gemZul_Prod_KON]	gematik: Zulassung dezentraler Produkte der Telematikinfrastruktur hier: Konnektor
[gemZul_Prod_KSR]	gematik: Zulassung zentrale Produkte der Telematikinfrastruktur hier: Konfigurationsdienst
[gemZul_Prod_eHealth-KT]	gematik: Zulassung dezentraler Produkte der Telematikinfrastruktur hier: eHealth-Kartenterminal
[gemZul_Prod_NamD]	gematik: Zulassung zentrale Produkte der Telematikinfrastruktur hier: Namensdienst
[gemZul_Prod_Proxy]	gematik: Zulassung zentrale Produkte der Telematikinfrastruktur hier: OCSP-Proxy
[gemZul_Prod_StAmp]	gematik: Zulassung zentrale Produkte der Telematikinfrastruktur hier: Störungsampel
[gemZul_Prod_TSL]	gematik: Zulassung zentrale Produkte der Telematikinfrastruktur hier: TSL-Dienst
[gemZul_Prod_X509Root]	gematik: Zulassung dezentraler Produkte der Telematikinfrastruktur hier: Root-X.509

[Quelle]	Herausgeber: Titel
[gemZul_Prod_X509]	gematik: Zulassung dezentraler Produkte der Telematikinfrastruktur hier: X.509
[gemZul_Prod_ZeitD]	gematik: Zulassung zentrale Produkte der Telematikinfrastruktur hier: Zeitdienst
[gemZul_Prod_ZentrNetz]	gematik: Zulassung zentrale Produkte der Telematikinfrastruktur hier: Zentrales Netz
[gemZul_Prod_ZugD]	gematik: Zulassung zentrale Produkte der Telematikinfrastruktur hier: VPN-Zugangsdienst
[gemZul_Prod_VerzD]	gematik: Zulassung zentrale Produkte der Telematikinfrastruktur hier: Verzeichnisdienst
[gemZul_Best_KomLE]	gematik: Bestätigung Fachdienst KOM-LE

A3.2 – Weitere Dokumente

[Quelle]	Herausgeber: Titel
[Prüfst]	Verzeichnisse von anerkannten Prüfstellen siehe: - www.bsi.bund.de (Menüpunkt „Zertifizierung und Akkreditierung“) und von Zulassungsstellen 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 Bestätigungsverfahren in der jeweils geltenden Version zu verwenden (siehe https://www.gematik.de, Menüpunkt „Zulassung“):

- „Antrag auf Bestätigung Sicherheitsgutachten“

A5 – Checkliste zur Antragstellung

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

lfd. Nr.	Aktion	erledigt
1	Verfahrensbeschreibung von der gematik-Website downloaden	
2	Bestätigungsantrag von der gematik-Website laden und ausfüllen	
3	ggf. offene Fragen mit der Zulassungsstelle klären (030/40041-200)	
4	Bestätigungsantrag vorab an die Zulassungsstelle per E-Mail [zulassung@gematik.de] versenden und drucken	
5	Bestätigungsantrag rechtsgültig unterschreiben und an Zulassungsstelle per Post versenden	
6	In das Sicherheitsgutachten die von der Zulassungsstelle vergebene ZLS einarbeiten	
7	Das Sicherheitsgutachten gemäß Definition im Bestätigungsverfahren zusammenstellen und an Zulassungsstelle versenden	