Verfahrensbeschreibung

Bestätigung Sicherheitsgutachten

Version:	1.12.1
Revision:	5
Stand:	27.03.2024
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemZul_Best_SiGu]

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	30.03.16		Anpassung an Online-Produktivbetrieb	Zulassung
1.3.0	14.06.17	5.1;2 A 3.2	Anpassung an eIDAS	Zulassung
1.3.1	27.02.18		Link zur gematik-Website aktualisiert	gematik
1.4.0	15.05.19		Ergänzung Anbieter Basis-Consumer, KTR-Consumer, Erweiterung Anbieter TSP X.509 eGK um ggf. Signaturdienst, Abbildungen angepasst	gematik
1.5.0	04.11.19		Betreiber Aktensystem ePA	gematik
1.6.0	27.04.20	2.1	ePA-Frontend des Versicherten hinzugefügt	gematik
1.7.0	08.02.21		IDP-Dienst hinzugefügt	gematik
1.8.0	12.11.21		Änderung KOM-LE in KIM und Umbenennung folgender Begriffe: aus "aAdG-NetG" wird "WANDA Basic", aus "aAdG" und "aAdG-NetG-TI" wird "WANDA Smart" (nähere Informationen finden Sie unter https://fachportal.gematik.de/)	gematik
1.9.0	09.02.22	4	Ergänzung IDP_Sek	gematik
1.10.0	23.06.22	4	Ergänzung Highspeed-Konnektor	gematik
1.11.0	13.01.23	4	Ergänzung TI-Gateway, IDP-FedMaster, Verzeichnisdienst FHIR, TI-Messenger	gematik
1.12.0	16.05.23	5.3	Überarbeitung	gematik
1.12.1	27.03.24	4	Ergänzung Anbieter eHealth-CardLink	gematik

© gematik – öffentlich

Inhaltsverzeichnis

Dokumentinformationen 2

Inhaltsverzeichnis 3

1 Einleitung 4

2 Bestätigungsobjekt Sicherheitsgutachten 5

2.1 Bestätigungen von Teilen des Sicherheitsgutachtens 5

3 Prüfbereiche und Rollen 6

3.1 Prüfbereiche 6

3.2 Rollen 6

4 Bestätigungsverfahren 7

4.1 Verfahrensübersicht 11

5 Nachweise 12

5.1 Beibringung der Nachweise 12

5.2 Nachweis der sicherheitstechnischen Eignung 12

5.3 Wiederholungsaudit für Sicherheitsgutachten/Änderungen an den Prozessen 13

Anhang A – Verzeichnisse 14

A1 – Abkürzungen 14

A2 – Abbildungsverzeichnis 14

A3 – Referenzierte Dokumente 14

A3.1 – Dokumente der gematik 14

A4 – Antragsformular und Mustervorlagen 16

A5 – Checkliste zur Antragstellung 17

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://fachportal.gematik.de/downloadcenter/zulassungs-bestaetigungsantraege-verfahrensbeschreibungen.

 © gematik – öffentlich

2 Bestätigungsobjekt Sicherheitsgutachten

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

Festlegungen zu Sicherheitsgutachten finden sich auch in der „Richtlinie zur Prüfung der Sicherheitseignung" [gemRL_PruefSichEig_DS].

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 Produkt-/Anbietertypsteckbrief(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 Produkt-/Anbietertyp sicherzustellen.

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

2.1 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 1: 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 auch Folgeseiten):

Produkte

Bei nachfolgenden Produkten kann der Anbieter (sofern eine Anbieterzulassung für das Anbieten des Produktes vorgesehen ist) das Sicherheitsgutachten aus der Produktzulassung in der Anbieterzulassung nachnutzen – sofern das vorhandene Sicherheitsgutachten den Nachweis aller Anforderungen zur betrieblichen Sicherheit aus dem Anbietertypsteckbrief des Anbieters mit abdeckt:

gegenwärtiges Verfahren	anschließendes Verfahren **Zulassung des Produktes**
Bestätigung Sicherheitsgutachten [gemZul_Best_SiGu] als Nachweis für rechts stehendes Verfahren	**CVC-Root** [gemZUL_Prod_CVCRoot]
	X.509-Root [gemZul_Prod_X509Root]
	TSP CVC [gemZul_Prod_CVC]
	TSP X.509 [gemZul_Prod_X509]
	TSL [gemZul_Prod_TSL]
	OCSP-Proxy [gemZul_Prod_Proxy]
	SG Bestandsnetze [gemZul_Prod_SG-BestNetze]
	Intermediär VSDM [gemZul_Prod_IntVSDM]
	KSR [gemZul_Prod_KSR]
	NamD [gemZul_Prod_NamD]
	St_Ampel [gemZul_Prod_StAmp]
	ZeitD [gemZul_Prod_ZeitD]
	ZentrNetz [gemZul_Prod_ZentrNetz]
	VPN-ZugD [gemZul_Prod_ZugD]

Fortführung der Tabelle **Produkte**

gegenwärtiges Verfahren	anschließendes Verfahren **Zulassung des Produktes**
Bestätigung Sicherheitsgutachten [gemZul_Best_SiGu] als Nachweis für rechts stehendes Verfahren	**sicheres Übermittlungsverfahren Fachdienst KOM-LE (KIM)** [gemZul_Prod_FD_KOM-LE]
	Konnektor [gemZul_Prod_KON]
	eHealth KT [gemZul_Prod_eHealth-KT]
	ePA-Frontend des Versicherten [gemZul_Prod_ePA_FdV]
	E-Rezept-Fachdienst [gemZul_Prod_FD_eRp]
	IDP-Dienst [gemZul_Prod_IDP-Dienst]
	Verzeichnisdienst [gemZul_Prod_VerzD]
	Highspeed-Konnektor [gemZul_Prod_Kon_Highspeed]
	IDP-Sek [gemZul_Prod_IDP_Sek]
	IDP_FedMaster [gemZul_Prod_IDP_FedMaster]
	TI-Messenger [gemZul_Prod_TI-M]
	Verzeichnisdienst FHIR [gemZul_Prod_VZD_FHIR]

Abbildung 2: Reihenfolge Bestätigungsverfahren Produkte

Anbieter

Für die nachfolgenden Anbieterzulassungen bzw. Betreiberbestätigungen benötigt der Antragsteller die Bestätigung seines Sicherheitsgutachtens:

gegenwärtiges Verfahren	anschließendes Verfahren **Zulassung des Anbieters**
Bestätigung Sicherheitsgutachten [gemZul_Best_SiGu] als Nachweis für rechts stehendes Verfahren	**Basis-Consumer** [gemZul_Anbieter]
	KTR-Consumer [gemZul_Anbieter]
	Signaturdienst [gemZul_Anbieter]
	Aktensystem ePA [gemZul_Anbieter]
	Aktensystem ePA gemZul_Best_Betreiber_Aktensystem_ ePA
	sicheres Übermittlungsverfahren Fachdienst KOM-LE (KIM) [gemZUL_Anbieter]
	IDP_Sek [gemZul_Anbieter]
	Highspeed Konnektor [gemZul_Anbieter]
	TI-Messenger Fachdienst [gemZul_Anbieter]
	TI-Gateway [gemZul_Anbieter]
	eHealth-CardLink [gemZul_Anbieter]

Abbildung 3: Reihenfolge Bestätigungsverfahren Anbieter

Fachdienste VSDM – Kartenproduktion – Kartenherausgabe – weitere Anwendungen

Für nachfolgende Verfahren benötigt der Antragsteller die Bestätigung seines Sicherheitsgutachtens:

gegenwärtiges Verfahren	anschließendes Verfahren
Bestätigung Sicherheitsgutachten [gemZul_Best_SiGu] als Nachweis für rechts stehendes Verfahren	**Zulassung Fachdienste VSDM (VSDD, CMS, UFS) für Krankenkassen** [gemZul_Prod_FD_VSDM]
	Bestätigung HBA_SMC-B _HSM-B_PersVal [gemLeit_Best_HBA_SMC-B_HSM-B_Pers]
	Bestätigung eGK-Proz [gemZul_Best_eGK-Proz]
	Bestätigung Weitere Anwendungen [gemZul_Best_Anwendungen_WANDA]

Abbildung 4: Reihenfolge Bestätigungsverfahren Fachdienste VSDM – Kartenproduktion – Kartenherausgabe – weitere Anwendungen

4.1 Verfahrensübersicht

Nachfolgend die schematische Darstellung des Bestätigungsverfahrens:

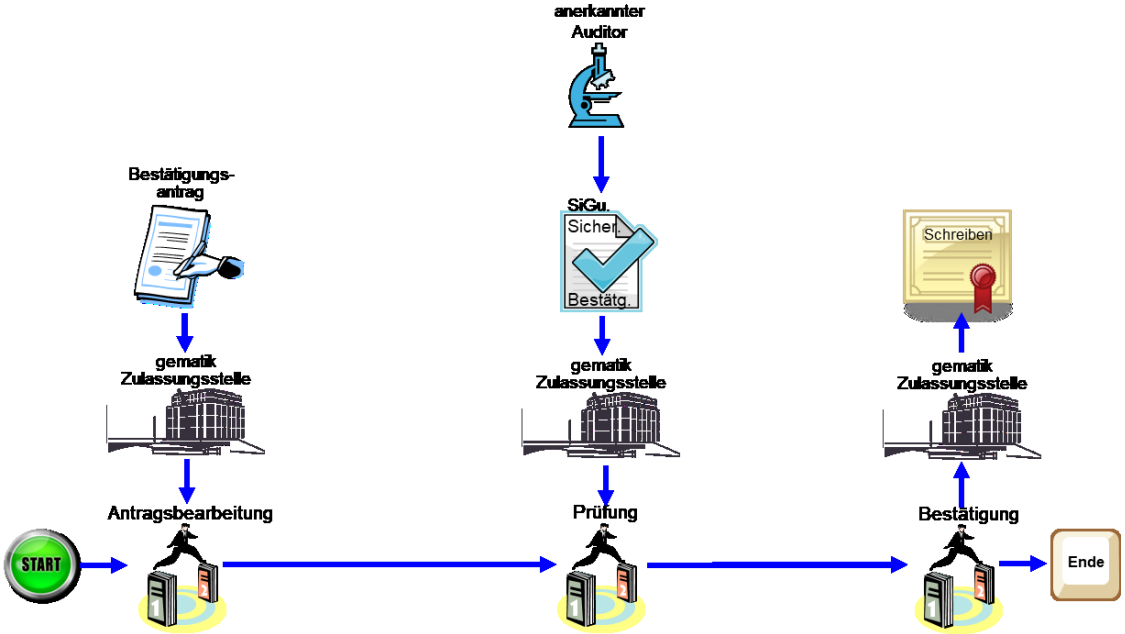

Abbildung 5: Schema Bestätigungsverfahren

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 & Informations-sicherheit.

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 sowie für Prozesse bei der Softwareentwicklung oder der Personalisierung sind jeweils im Kapitel 3.2 in den Produkt-/Anbietertypsteckbriefen (siehe Anhang A3.1) im Absatz „Sicherheitsgutachten" Anforderungen gelistet, deren Umsetzung durch ein Audit begutachtet werden muss. Das Sicherheitsgutachten ist gemäß [gemRL_PruefSichEig_DS] zu erstellen. Es gilt als Nachweis und hat die Aussage zur sicherheitstechnischen Eignung entsprechend der Prüfgrundlage zu enthalten.

Zum Sicherheitsgutachten hat die gematik auf Basis der geltenden Spezifikationen die Produkt-/Anbietertypsteckbriefe erstellt und wendet diese zur Prüfung einheitlich an. Die Produkt-/Anbietertypsteckbriefe werden über die Internetpräsenz der gematik veröffentlicht (siehe https://fachportal.gematik.de/dokumentensuche/#c2849).

Der jeweilige Produkt-/Anbietertypsteckbrief 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 sind ein erneuter Antrag auf Bestätigung und ein erneutes Sicherheitsgutachten noch vor Ablauf der Gültigkeitsdauer einzureichen.
- **Wiederholung aufgrund erheblicher Änderungen**
  Beabsichtigt der Bestätigungsinhaber wesentliche technische, organisatorische oder bauliche Änderungen in der Herstellung oder dem Betrieb des Dienstes oder des Produkts bzw. bei seinen Prozessen, welche die Erfüllung der Anforderungen des jeweiligen Produkt-/Anbietertyps betreffen, ist ein neuer Nachweis Sicherheitsgutachten vorzulegen. In diesem Fall ist ebenfalls ein neuer Antrag auf Bestätigung zu stellen.

Beim wiederholten Audit für Sicherheitsgutachten durch den Sicherheitsgutachter werden – wie beim Erstaudit – alle relevanten Bereiche geprüft. Das Sicherheitsgutachten ist an die Zulassungsstelle zu senden. Änderungen am Sicherheitsgutachten sind eindeutig über Versionsnummern kenntlich zu machen.

 © gematik – öffentlich

Anhang A – Verzeichnisse

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	Oberstes 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
VFS	Verfahrensschlüssel

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

A2 – Abbildungsverzeichnis

Abbildung 1: Prüfbereiche 6
Abbildung 2: Reihenfolge Bestätigungsverfahren Produkte 8
Abbildung 3: Reihenfolge Bestätigungsverfahren Anbieter 9
Abbildung 4: Reihenfolge Bestätigungsverfahren Fachdienste VSDM – Kartenproduktion – Kartenherausgabe – weitere Anwendungen 10
Abbildung 5: Schema Bestätigungsverfahren 11

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://fachportal.gematik.de/dokumentensuche/#c2849).

[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
[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_Anbieter]	gematik: Zulassung Anbieter
[gemZul_Prod_CVC]	gematik: Zulassung TSP CVC
[gemZUL_Prod_CVCRoot]	gematik: Zulassung CVC-Root
[gemZul_Prod_FD_VSDM]	gematik: Zulassung Fachdienste VSDM (VSDD, CMS, UFS) für Krankenkassen
[gemZul_Prod_IntVSDM]	gematik: Zulassung Intermediär VSDM
[gemZul_Prod_SG-BestNetze]	gematik: Zulassung SG für Bestandsnetze
[gemZul_Prod_KON]	gematik: Zulassung Konnektor
[gemZul_Prod_KSR]	gematik: Zulassung Konfigurationsdienst
[gemZul_Prod_eHealth-KT]	gematik: Zulassung eHealth-Kartenterminal
[gemZul_Prod_NamD]	gematik: Zulassung Namensdienst
[gemZul_Prod_Proxy]	gematik: Zulassung OCSP-Proxy
[gemZul_Prod_StAmp]	gematik: Zulassung Störungsampel
[gemZul_Prod_TSL]	gematik: Zulassung TSL-Dienst
[gemZul_Prod_X509Root]	gematik: Zulassung Root-X.509
[gemZul_Prod_X509]	gematik: Zulassung X.509
[gemZul_Prod_ZeitD]	gematik: Zulassung Zeitdienst
[gemZul_Prod_ZentrNetz]	gematik: Zulassung Zentrales Netz
[gemZul_Prod_ZugD]	gematik: Zulassung VPN-Zugangsdienst
[gemZul_Prod_VerzD]	gematik: Zulassung Verzeichnisdienst
[gemZul_Best_Anwendungen]	gematik: Bestätigung weiterer elektronischer Anwendungen des Gesundheitswesens sowie der Gesundheitsfoschung
[gemZul_Prod_FD_KOM-LE]	gematik: Zulassung Fachdienst KIM
[gemZul_Prod_FD_eRp]	gematik: Zulassung E-Rezept-Fachdienst
[gemZul_Prod_IDP-Dienst]	gematik: Zulassung IDP-Dienst

[Quelle]	Herausgeber: Titel
[gemZul_Prod_ePA_FdV]	gematik: Zulassung Frontend des Versicherten
[gemZul_Best_Betreiber_Aktensystem_ePA]	gematik: Bestätigung für Betreiber ePA-Aktensysteme
[gemZul_Prod_Kon_Highspeed]	gematik: Zulassung Highspeed-Konnektor
[gemZul_Prod_IDP_Sek]	gematik: Zulassung Sektoraler Identity Provider
[gemZul_Prod_IDP_FedMaster]	gematik: Zulassung Identity Provider Federation Master
[gemZul_Prod_TI-M]	gematik: Zulassung TI-Messenger
[gemZul_Prod_VZD_FHIR]	gematik: Zulassung Verzeichnisdienst FHIR

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://fachportal.gematik.de/downloadcenter/zulassungs-bestaetigungsantraege-verfahrensbeschreibungen

und den „Antrag auf Bestätigung Sicherheitsgutachten" auswählen.

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 vom gematik-Fachportal downloaden.	
2	Bestätigungsantrag vom gematik-Fachportal laden und ausfüllen.	
3	Ggf. offene Fragen mit der Zulassungsstelle klären (zulassung@gematik.de).	
4	Bestätigungsantrag rechtsgültig unterschreiben und an Zulassungsstelle per PDF versenden.	
5	In das Sicherheitsgutachten den von der Zulassungsstelle vergebenen Verfahrensschlüssel einarbeiten.	
6	Das Sicherheitsgutachten gemäß Definition im Bestätigungsverfahren zusammenstellen und an Zulassungsstelle versenden.	

© gematik – öffentlich