gematik

Verfahrensbeschreibung

Zulassung Produkte der Telematikinfrastruktur hier: Sektoraler Identity Provider

Version:	2.0.0
Revision:	4
Stand:	13.02.2023
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemZul_Prod_IDP_Sek]

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
1.0.0	08.02.2022		Ersterstellung	gematik
2.0.0	13.02.2023		Aufgrund der Erweiterung der Funktionalität des Produktes wurde das gesamte Dokument überarbeitet, besonders hinsichtlich der Prüfsäulen	gematik

Inhaltsverzeichnis

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 Sektoraler Identity Provider

Der Produkttyp Sektoraler Identity Provider stellt durch gesicherte JSON Web Token (JWT) attestierte Identitäten aus. Der sektorale Identity Provider übernimmt für Fachdienste die Aufgabe der Identifikation und Authentifizierung des Nutzers. Fachdienste müssen somit selbst keine Überprüfung des Nutzers implementieren, sondern können sich darauf verlassen, dass der Besitzer des bei ihnen vorgelegten ID_TOKEN sicher identifiziert und authentisiert wurde. Des Weiteren stellt der sektorale Identity Provider sicher, dass übertragene Attribute gültig sind.

Die Vertrauensbeziehungen zwischen Fachdiensten und Sektoralen Identity Providern werden dabei durch den Federation Master sichergestellt. Dieser verwaltet alle Anwendungen, welche die Anmeldung des Nutzers über die verschiedenen Sektoralen Identity Provider unterstützen.

Das Zulassungsobjekt ist ein Produkt, das der Zulassungsstelle vom Antragsteller beizustellen ist.

Der Antragsteller muss sicherstellen, 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 muss der Antragsteller sicherstellen, dass allen Prüfinstanzen dieselben Versionen des Zulassungsobjekts vorliegen.

2.1 Zulassungen von Teilen des Zulassungsobjekts

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

3 Prüfbereiche und Rollen

3.1 Prüfbereiche

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

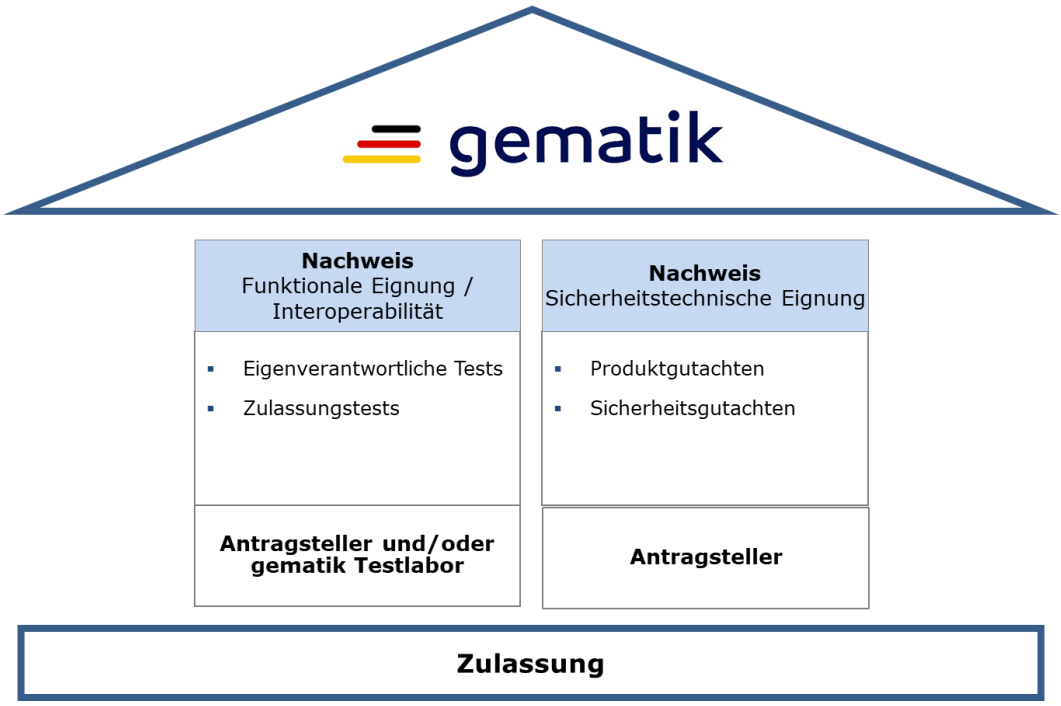

Abbildung 1: Prüfbereiche

3.2 Rollen

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

- Antragsteller (Hersteller),
- Zulassungsstelle,
- Testmanager,
- Testlabor
- Sicherheitsgutachter
- Produktgutachter

4 Zulassungsverfahren

Der folgende Verfahrensablauf umfasst die Antragstellung, das Zulassungsobjekt, notwendige Nachweise sowie die Zulassungserteilung.

Das Zulassungsverfahren Sektoraler Identity Provider steht in Abhängigkeit zu weiteren Verfahren. Die zwingende Reihenfolge bei der Durchführung ist:

vorausgesetzte Verfahren	**gegenwärtiges Verfahren**	**anschließende Verfahren**
Bestätigung Sicherheitsgutachten [gemZUL_Best_SiGu] als Nachweis für rechts stehendes Verfahren	**Zulassung Sektoraler Identity Provider** [gemZul_Anbieter]	**Anbieterzulassung Sektoraler Identity Provider** [gemZul_Anbieter]

Abbildung 2: Reihenfolge Zulassungsverfahren

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

4.1 Verfahrensübersicht

Nachfolgend die schematische Darstellung des Zulassungsverfahrens.

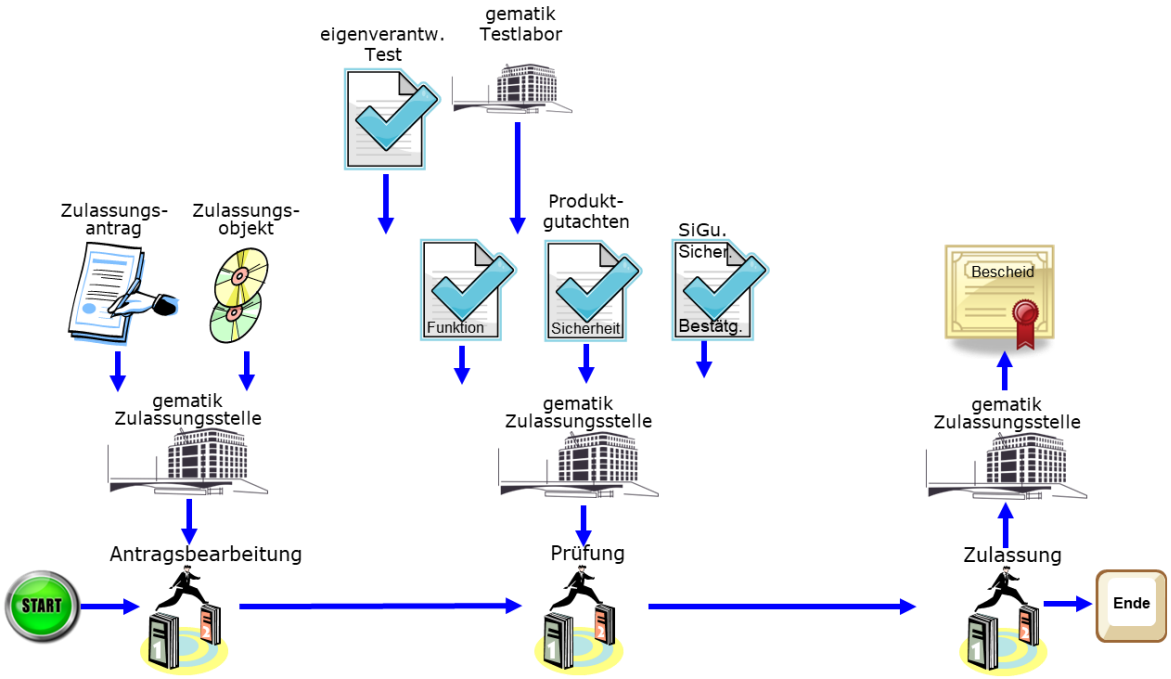

Abbildung 3: Schema Zulassungsverfahren

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 das Testlabor mit der Durchführung des Interoperabilitätstests.

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. Bei einem negativen Prüfergebnis wird der Antragsteller unter Angabe der Gründe informiert und kann nachbessern.

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:

- Austausch der Zugangsinformation für den Test des Dienstes erfolgt über den technischen Ansprechpartner gemäß Angaben im Antrag.
- Der Antragsteller wird im Rahmen eines Interoperabilitätstests gemeinsam mit dem gematik-Testlabor eine erfolgreiche Authentisierung am E-Rezept-Fachdienst mit einer Identität vom Sektoralen Identity Provider und das anschließende erfolgreiche Herunterladen eines E-Rezepts beim Fachdienst mit der E-Rezept-App (iOS und Android) durchführen.

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 sowie
- der sicherheitstechnischen Eignung

5.2 Nachweis der funktionalen Eignung

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

Der Antragsteller führt die Produkttests gemäß [gemProdT_IDP_Sek] eigenverantwortlich durch, bis sein entwickeltes Zulassungsobjekt die 100%ige Testabdeckung gemäß [gemProdT_IDP_Sek] erfüllt.

Das Zulassungsverfahren erfordert weiterhin den Nachweis erfolgreicher produktübergreifender Tests durch den Antragsteller. Der Testmanager der gematik unterstützt den Antragsteller bei der Durchführung dieser Tests. Die für diese Tests erforderlichen Use Cases werden durch die gematik festgelegt.

Die Testdokumentation ist gemäß [gemKPT_Test#4.7] zu erstellen und dem Testmanager zur Verfügung zu stellen.

Das Testlabor begleitet die Durchführung der produktübergreifenden Tests und fasst die Ergebnisse in einem Testbericht zusammen, der der Zulassungsstelle beigebracht wird.

5.3 Nachweis der sicherheitstechnischen Eignung

Die sicherheitstechnische Eignung wird festgestellt durch:

5.3.1 Produktgutachten

Das Zulassungsverfahren erfordert die sicherheitstechnische Prüfung des Produktes. Dafür sind im Produkttypsteckbrief [gemProdT_IDP_Sek]#3.2] Anforderungen gelistet, deren Einhaltung durch Sicherheitsgutachter gemäß [gemRL_PruefSichEig_DS#9.2.2] geprüft werden müssen. Hierbei werden die Sicherheitsanforderungen gemäß den Anforderungen aus dem Produkttypsteckbrief auf Einhaltung bzw. Umsetzung geprüft und bewertet.

Das Produktgutachten ist gemäß [gemRL_PruefSichEig_DS] zu erstellen. Es gilt als Nachweis und hat die Aussage zur sicherheitstechnischen Eignung entsprechend der Prüfgrundlage zu enthalten.

Die Zulassungsstelle beauftragt die Beurteilung des Produktgutachtens bei der gematik-Abteilung Datenschutz & Informationssicherheit, ob es vollständig, sorgfältig, objektiv und nachvollziehbar ist. Diese 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.

Der Produktgutachter prüft das Produkt und verifiziert somit auch die Umsetzung der Sicherheitsfunktionen und deren Änderung im Produkt, wenn die Sicherheitsfunktion durch die oben genannten Punkte adressiert wird. Die Änderung bezieht sich auf die Umsetzung der Sicherheitsfunktion (bspw. eines Verschlüsselungsalgorithmus), jedoch nicht auf Änderungen der Aufrufparameter bzw. der verarbeiteten Daten (bspw. geht es nicht um die Daten, die verschlüsselt werden) oder die Mehrfachverwendung dieser Sicherheitsfunktion.

Sicherheitsfunktionen, die personenbezogene Daten übertragen, verarbeiten, speichern oder anzeigen, erfahren besondere Beachtung bei der Umsetzung und Produktbegutachtung.

5.3.1.1 Wiederholung der Prüfung

Eine Wiederholung der Prüfung für das Produktgutachten wird aus folgenden Gründen notwendig:

- **periodische Wiederholung**
  Die Gültigkeitsdauer eines Produktgutachtens ist auf drei Jahre begrenzt. Deshalb ist ein erneutes Produktgutachten noch vor Ablauf der Gültigkeitsdauer einzureichen. Nach positivem Prüfungsergebnis durch die Zulassungsstelle wird der neue Gültigkeitszeitraum von drei Jahren intern vermerkt.
- **Wiederholung aufgrund von Änderungen**
  Beabsichtigt der Zulassungsnehmer Änderungen am Produkt vorzunehmen, die die Erfüllung der Anforderungen des Produkttyps betreffen, ist ggf. ein neues Produktgutachten beizubringen. Die Bewertung, ob ein neues Produktgutachten beizubringen ist, erfolgt nach der Änderungsanzeige durch den Zulassungsnehmer durch die gematik.

5.3.2 Sicherheitsgutachten

Die Erfüllung dieser 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 Bestätigungsbescheinigung wird auf Gültigkeit geprüft.

Anhang A

A1 – Abkürzungen

Kürzel	Erläuterung
IDP Sek	Sektoraler Identity Provider
TI	Telematikinfrastruktur
ZLS	Verfahrensschlüssel

Das übergreifende Glossar der gematik [gemGlossar] wird als eigenständiges Dokument zu 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 Test	Ergänzend zum Produkttest, der sich jeweils auf ein einzelnes Produkt bezieht, müssen Produkte auch integriert getestet werden.
JSON Web Token	Ein auf JSON basiertes und nach [RFC7519] (JWT) genormtes Access-Token. Das JWT ermöglicht den Austausch von verifizierbaren Claims innerhalb seines Payloads.
Access Token	Ein Access Token (nach [RFC6749 # section-1.4]) wird vom Client (Anwendungsfrontend) benötigt, um auf geschützte Daten eines Resource Servers zuzugreifen. Die Repräsentation kann als JSON Web Token erfolgen.
Claim	Ein Key/Value-Paar im Payload eines JSON Web Token.

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 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/dokumentensuche/#c2849).

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemProdT_IDP_Sek]	gematik: Produkttypsteckbrief Sektoraler Identity Provider
[gemSpec_OM]	gematik: Spezifikation Operations und Maintenance (Fehlermanagement, Versionierung, Monitoring)
[gemZul_übergrVerf]	gematik: übergeordnete Verfahrensbeschreibung für Zulassungs- und Bestätigungsverfahren
[gemRL_PruefSichEig_DS]	gematik: Richtlinie zur Prüfung der Sicherheitseignung
[gemZUL_Best_SiGu]	gematik: Bestätigung Sicherheitsgutachten
[gemZul_Anbieter]	gematik: Verfahrensbeschreibung Zulassungsverfahren für die Anbieter operativer Betriebsleistungen in der Telematikinfrastruktur

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 Fachportal gematik).

- „Antrag auf Zulassung eines Produktes der TI – Sektoraler Identity Provider"

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 als PDF-Datei versenden.	
5	Durchführung der eigenverantwortlichen Tests und Erstellen des unterschriebenen Testberichts.	
6	Nachweis der sicherheitstechnischen Eignung gemäß Definition im Zulassungsverfahren beauftragen und an die Zulassungsstelle versenden.	