Anwendungssteckbrief Digitale Gesundheitsanwendungen (nach §33a SGB V) in der Telematikinfrastruktur

Anwendung Version:	1.0.0
Anwendung Status:	freigegeben

Version:	1.0.0
Revision:	833099
Stand:	30.01.2024
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemAnw_DiGA_1.0.0

Historie Anwendungsversion und Anwendungssteckbrief

Historie Anwendungsversion

Die Anwendungsversion ändert sich, wenn sich die normativen Festlegungen für den Anwendungen ändern.

Anwendungsversion	Beschreibung der Änderung	**Referenz**
1.0.0	Initiale Version	gemAnw_DiGA_1.0.0

Historie Anwendungssteckbrief

Die Dokumentenversion des Anwendersteckbriefs ändert sich mit jeder inhaltlichen oder redaktionellen Änderung des Anwendersteckbriefs und seinen referenzierten Dokumenten. Redaktionelle Änderungen haben keine Auswirkung auf die Anwendungsversion.

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeiter
1.0.0	30.01.2024		Erstellt für **ePA für Alle**	gematik

Inhaltsverzeichnis

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Anbieter medizinischer Fachanwendungen können zur Authentisierung von Versicherten die GesundheitsID nutzen. Aktuell sind nur TI-Anwendungen sowie vom BfArM zugelassene Digitale Gesundheitsanwendungen (DiGA) zur Teilnahme als Fachanwendung in der TI-Föderation berechtigt.
Gemäß §6 Absatz 1 der "Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesundheitsanwendungen-Verordnung - DiGAV)" sind DiGA-Hersteller verpflichtet ihr Systeme derart anzupassen, dass die von der digitalen Gesundheitsanwendung verarbeiteten Daten mit Einwilligung des Versicherten in die elektronische Patientenakte des Versicherten übermittelt werden können. Zudem müssen DiGA Anbieter die Authentisierung von GKV-Versicherten als die die digitale Gesundheitsanwendung nutzenden Personen über digitale Identität nach § 291 Absatz 8 des Fünften Buches Sozialgesetzbuch unterstützen.
Hinweis: Perspektivisch sollen weitere Anwendungen des Gesundheitswesens die GesundheitsID nutzen bzw. integrieren können. Die fachlichen & gesetzlichen Grundlagen müssen hierzu allerdings erst geschaffen werden.
Die Voraussetzung für DiGA zur Nutzung von Diensten und Komponenten der Telematikinfrastruktur ist gemäß §327 SGB V die Bestätigung als „Digitale Gesundheitsanwendungen (nach §33a SGB V) in der Telematikinfrastruktur" durch die gematik. Der hier vorliegende Anwendungstypsteckbrief "Digitale Gesundheitsanwendungen (nach §33a SGB V) in der Telematikinfrastruktur" verzeichnet verbindlich Festlegungen der gematik an das Bestätigungsobjekt "Digitale Gesundheitsanwendungen (nach §33a SGB V) in der Telematikinfrastruktur" bzw. verweist auf Dokumente, in denen verbindliche Festlegungen mit ggf. anderer Notation zu finden sind. Die Festlegungen bilden die Grundlage für die Erteilung von Bestätigungen durch die gematik. Details über die Beantragung und Durchführung des Bestätigungsverfahrens sind der entsprechenden Verfahrensbeschreibung zu entnehmen.
Die normativen Festlegungen werden über ihren Identifier, ihren Titel sowie die Dokumentenquelle referenziert. Die normativen Festlegungen mit ihrem vollständigen, normativen Inhalt sind dem jeweils referenzierten Dokument zu entnehmen.

1.2 Zielgruppe

Der Anwendungstypsteckbrief DiGA richtet sich an Anbieter von Fachdiensten, die sich als Relying Party in der TI-Föderation registrieren möchten um damit ihren Anwendern die Möglichkeit einer Authentisierung mit der GesundheitsID zu ermöglich sowie behandlungsrelevante DiGA-Daten des Nutzers in seine/ihre ePA einzustellen.

Der Anwendungstypsteckbrief DiGA richtet sich an DiGA-Hersteller, welche die verpflichtenden Anwendungsfälle im Kontext der Telematikinfrastruktur umsetzen. Sie müssen sich zum einen als Relying Party in der TI-Föderation registrieren, um damit ihren Anwendern eine Authentisierung mit der GesundheitsID zu ermöglichen.
Zum anderen müssen Sie behandlungsrelevante DiGA-Daten des Nutzers in seine/ihre

ePA einstellen.

Hinweis: Aktuell sind nur vom BfArM zugelassene Digitale Gesundheitsanwendungen (DiGA) zur Teilnahme an der TI-Föderation vorgesehen.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung im Bestätigungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte) festgelegt und bekannt gegeben.

1.4 Abgrenzung des Dokumentes

Dieses Dokument macht keine Aussagen zur Aufteilung der Produktentwicklung bzw. Produktherstellung auf verschiedene Hersteller und Anbieter.

Dokumente zu den Zulassungsverfahren für die Anwendung sind nicht aufgeführt. Die geltenden Verfahren und Regelungen zur Beantragung und Durchführung von Bestätigungsverfahren können dem Fachportal der gematik entnommen werden.

1.5 Methodik

Die im Dokument verzeichneten normativen Festlegungen werden tabellarisch dargestellt. Die Tabellenspalten haben die folgende Bedeutung:

ID: Identifiziert die normative Festlegung eindeutig im Gesamtbestand aller Festlegungen der gematik.

Bezeichnung: Gibt den Titel einer normativen Festlegung informativ wieder, um die thematische Einordnung zu erleichtern. Der vollständige Inhalt der normativen Festlegung ist dem Dokument zu entnehmen, auf das die Quellenangabe verweist.

Quelle (Referenz): Verweist auf das Dokument, das die normative Festlegung definiert.

2 Dokumente

Die nachfolgenden Dokumente enthalten alle für den Anbietertyp normativen Festlegungen.

Tabelle 1: Dokumente mit normativen Festlegungen

Dokumentenkürzel	Bezeichnung des Dokumentes	Version
gemSpec_IDP_FD	Spezifikation Identity Provider – Fachdienste	1.7.0
gemKPT_Test	Testkonzept der TI	2.9.0
gemILF_PS_ePA	Implementierungsleitfaden Primärsysteme ePA	3.0.0
gemSpec_DS_Hersteller	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller	1.5.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.29.0
gemKPT_Betr	Betriebskonzept Online-Produktivbetrieb	3.29.0

Weiterhin sind die in folgender Tabelle aufgeführten Dokumente und Web-Inhalte normativ und gelten mit.

Tabelle 2: Mitgeltende Dokumente und Web-Inhalte

Quelle	Herausgeber: Bezeichnung / URL	Version Branch / Tag

Die Bestätigungsbedingungen für den Anwendungsteckbrief gemAnw_DiGA werden in der entsprechenden Verfahrensbeschreibung im Fachportal der gematik veröffentlicht.

Die in folgender Tabelle aufgeführten Dokumente und Web-Inhalte sind informative Beistellungen und sind nicht Gegenstand der Bestätigung / Zulassung.

Tabelle 3: Informative Dokumente und Web-Inhalte

Quelle	Herausgeber: Bezeichnung / URL	Version Branch / Tag
[gemSpec_IDP_Sek]	gematik: Spezifikation sektoraler IDP	2.2.0

Quelle	Herausgeber: Bezeichnung / URL	Version Branch / Tag
[gemSpec_IDP_FedMaster]	gematik: Spezifikation Federation Master	1.1.0
[gemSpec_IDP_Frontend]	gematik: Spezifikation Frontend	1.5.0
https://wiki.gematik.de/x/wxEEHg	gematik: Wissensdatenbank zur TI-Föderation	
https://service.gematik.de/servicedesk/customer/portal/33	gematik: Anfrageportal - Anfragen Identity Managment (Registrierung notwendig)	
https://wiki.gematik.de/pages/viewpage.action?pageId=512703175	TI-Leitfaden für DiGA-Hersteller	

Hinweis:

- Ist kein Herausgeber angegeben, wird angenommen, dass die gematik für Herausgabe und Veröffentlichung der Quelle verantwortlich ist.
- Ist keine Version angegeben, bezieht sich die Quellenangabe auf die aktuellste Version.
- Bei Quellen aus gitHub werden als Version Branch und / oder Tag verwendet.

3 Normative Festlegungen

Die folgenden Abschnitte verzeichnen alle für den Anbietertypen normativen Festlegungen der gematik an Anbieter zur Sicherstellung des Betriebes der von ihnen verantworteten Serviceeinheiten. Die Festlegungen sind gruppiert nach der Art der Nachweisführung ihrer Erfüllung als Grundlage der Zulassung.

3.1 Festlegungen zur funktionellen Eignung

3.1.1 Anbietererklärung funktionelle Eignung

Sofern in diesem Abschnitt Festlegungen verzeichnet sind, muss der Anbieter deren Umsetzung und Beachtung zum Nachweis der funktionalen Eignung durch eine Erklärung bestätigen bzw. zusagen.

Tabelle 4: Festlegungen zur funktionellen Eignung "Anbietererklärung"

ID	Bezeichnung	Quelle (Referenz)
A_14932	Bildung und Verwendung einer UUID für Dokumente	gemILF_PS_ePA
A_23131-01	DiGA-CS: Persistierung der DocumentEntry.entryUUID	gemILF_PS_ePA
GS-A_2162	Kryptographisches Material in Entwicklungs- und Testumgebungen	gemKPT_Test
TIP1-A_2803-01	Nachstellen von PU-Fehlern in der TU	gemKPT_Test
TIP1-A_4191	Keine Echtdaten in RU und TU	gemKPT_Test
TIP1-A_6523	Zulassungstest: Hersteller und Anbieter	gemKPT_Test
AF_10116	Bereitstellung Liste registrierte Identity Provider	gemSpec_IDP_FD
AF_10117	OAuth 2.0 Pushed Authorization Request	gemSpec_IDP_FD
AF_10118	Benutzerauthentifizierung und Erhalt des ID_TOKEN	gemSpec_IDP_FD
A_22860-01	Prüfung benötigter "scopes" und "claims"	gemSpec_IDP_FD
A_22861	Aktualisierung der bekannten Signaturschlüssel bei unbekannter "kid" der Signatur	gemSpec_IDP_FD
A_23004	Anforderung eines Vertrauensniveaus	gemSpec_IDP_FD
A_23005	Verifikation des durchgeführten Vertrauensniveaus	gemSpec_IDP_FD

A_23034	Entity Statement veröffentlichen	gemSpec_IDP_FD
A_23035	pseudonymes Attribut "sub"	gemSpec_IDP_FD
A_23036-01	Inhalte der "scopes" für Versicherte	gemSpec_IDP_FD
A_23037	Robustheit bei fehlenden Daten	gemSpec_IDP_FD
A_23038	Entity Statement abrufen	gemSpec_IDP_FD
A_23039	Entity Statement vorhalten	gemSpec_IDP_FD
A_23045-01	Registrierung des Fachdienstes	gemSpec_IDP_FD
A_23048	Response für OAuth 2.0 Pushed Authorization Requests	gemSpec_IDP_FD
A_23183	Veröffentlichen der TLS Authentisierungsschlüssel	gemSpec_IDP_FD
A_23185-01	Maximale Verwendungsdauer für Schlüssel von Fachdienst Authorization Servern	gemSpec_IDP_FD
A_23194	Veröffentlichen der öffentlichen Verschlüsselungsschlüssel	gemSpec_IDP_FD
A_23195	Entschlüsseln der ID_TOKEN	gemSpec_IDP_FD
A_23196	Zulässige Schlüssel	gemSpec_IDP_FD
A_23500	Ablehnung des PAR als "unauthorized" (HTTP 401)	gemSpec_IDP_FD
GS-A_5526	TLS-Renegotiation-Indication-Extension	gemSpec_Krypt

3.2 Festlegungen zur betrieblichen Eignung

3.2.1 Prozessprüfung betriebliche Eignung

Sofern in diesem Abschnitt Festlegungen mit Vorgaben zu organisatorischen Maßnahmen wie Prozessen und Strukturvorgaben verzeichnet sind, muss deren Erfüllung im Rahmen von Prozessprüfungen nachgewiesen werden.

Tabelle 5: Festlegungen zur betrieblichen Eignung "Prozessprüfung"

ID	Bezeichnung	Quelle (Referenz)
	Es liegen keine Festlegungen vor	

3.2.2 Anbietererklärung betriebliche Eignung

Sofern in diesem Abschnitt Festlegungen mit Vorgaben zu organisatorischen Maßnahmen wie Prozessen und Strukturvorgaben der Aufbauorganisation sowie der Umgebung verzeichnet sind, muss der Anbieter deren Umsetzung und Beachtung durch eine Anbietererklärung bestätigen bzw. zusagen.

Tabelle 6: Festlegungen zur betrieblichen Eignung "Anbietererklärung"

ID	Bezeichnung	Quelle (Referenz)
A_24349	Eigenverantwortliche Störungsabwendung einer DiGA	gemKPT_Betr
A_24351	Benennung von Ansprechpartnern der DiGA	gemKPT_Betr
A_24354	Kostenfreier Zugang zur DiGA für Fehlernachstellungen	gemKPT_Betr

3.2.3 Betriebshandbuch betriebliche Eignung

Sofern in diesem Abschnitt Festlegungen mit Vorgaben zu organisatorischen Maßnahmen wie Prozessen und Strukturvorgaben der Aufbauorganisation sowie der Umgebung verzeichnet sind, muss der Anbieter deren Umsetzung und Beachtung durch die Vorlage des Betriebshandbuches nachweisen.

Der Umfang und Inhalt des Betriebshandbuches ist der Definition in der Richtlinie Betrieb [gemRL_Betr_TI] zu entnehmen.

Tabelle 7: Festlegungen zur betrieblichen Eignung "Betriebshandbuch"

ID	Bezeichnung	Quelle (Referenz)
	Es liegen keine Festlegungen vor	

3.3 Festlegungen zur sicherheitstechnischen Eignung

3.3.1 Sicherheitsgutachten

Die in diesem Abschnitt verzeichneten Festlegungen sind Gegenstand der Prüfung der Sicherheitseignung gemäß [gemRL_PruefSichEig_DS]. Das entsprechende Sicherheitsgutachten ist der gematik vorzulegen.

Hinweis:

Einige Festlegungen sind sowohl in diesem Anwendungssteckbrief als auch in zugehörigen Produkttypsteckbriefen enthalten, da ein Nachweis der Erfüllung (ggf. auch anteilig) in Abhängigkeit von der Umsetzung sowohl durch die Anbieter der Produkte (Produktzulassung bzw. -bestätigung), als auch durch den Anbieter von Betriebsleistungen (Anbieterzulassung bzw. -bestätigung) erfolgen muss.

Abhängig von der konkreten Umsetzung können allerdings entsprechend [gemRL_PruefSichEig_DS] Festlegungen, die nur für die Anbieter der zugehörigen Produkte relevant sind, vom Sicherheitsgutachter als „entbehrlich" bewertet werden.

Weiterhin können Festlegungen, die zwar relevant sind, aber bereits vollständig vom Anbieter der zugehörigen Produkte erfüllt werden, vom Sicherheitsgutachter über Referenzieren der bestehenden Sicherheitsgutachten der Produktanbieter als umgesetzt bewertet werden.

Tabelle 8: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

ID	Bezeichnung	Quelle (Referenz)
	Es liegen keine Festlegungen vor	

3.3.2 Anbietererklärung sicherheitstechnische Eignung

Sofern in diesem Abschnitt Festlegungen verzeichnet sind, muss der Anbieter deren Umsetzung und Beachtung zum Nachweis der sicherheitstechnischen Eignung durch eine Erklärung bestätigen bzw. zusagen.

Tabelle 9: Festlegungen zur sicherheitstechnischen Eignung "Anbietererklärung"

ID	Bezeichnung	Quelle (Referenz)
A_17179	Auslieferung aktueller zusätzlicher Softwarekomponenten	gemSpec_DS_Hersteller
A_19147	Sicherheitstestplan	gemSpec_DS_Hersteller
A_19151	Implementierungsspezifische Sicherheitsanforderungen	gemSpec_DS_Hersteller
A_19152	Verwendung eines sicheren Produktlebenszyklus	gemSpec_DS_Hersteller
A_19154	Durchführung einer Bedrohungsanalyse	gemSpec_DS_Hersteller
A_19155	Durchführung sicherheitsrelevanter Quellcode-Reviews	gemSpec_DS_Hersteller
A_19158	Sicherheitsschulung für Entwickler	gemSpec_DS_Hersteller
A_19160	Änderungs- und Konfigurationsmanagementprozess	gemSpec_DS_Hersteller
A_19164	Mitwirkungspflicht bei Sicherheitsprüfung	gemSpec_DS_Hersteller
A_19165	Auditrechte der gematik zur Prüfung der Herstellerbestätigung	gemSpec_DS_Hersteller
A_22984	Unverzügliche Bewertung von Schwachstellen	gemSpec_DS_Hersteller
A_22985	Bereitstellung der Bewertung von Schwachstellen gegenüber der gematik	gemSpec_DS_Hersteller

A_22986	Meldung von erheblichen Schwachstellen und Bedrohungen	gemSpec_DS_Hersteller
A_23029	Bereitstellung von Updates abhängig von der Kritikalität der Schwachstellen	gemSpec_DS_Hersteller
GS-A_2330-02	Hersteller: Schwachstellen-Management	gemSpec_DS_Hersteller
GS-A_2525-01	Hersteller: Schließen von Schwachstellen	gemSpec_DS_Hersteller
GS-A_4944-01	Produktentwicklung: Behebung von Sicherheitsmängeln	gemSpec_DS_Hersteller
GS-A_4945-01	Produktentwicklung: Qualitätssicherung	gemSpec_DS_Hersteller
GS-A_4946-01	Produktentwicklung: sichere Programmierung	gemSpec_DS_Hersteller
A_23033	Integritätsschutz der IDP-Liste	gemSpec_IDP_FD
A_23040	Fachdienst: Prüfung der Signatur des Entity Statements	gemSpec_IDP_FD
A_23042	Verifikation der Certificate Transparency für TLS Verbindungen in die VAU	gemSpec_IDP_FD
A_23046	öffentlicher Schlüssel des Federation Master	gemSpec_IDP_FD
A_23049	Überprüfung des "ID_TOKEN" durch den Authorization-Server	gemSpec_IDP_FD
A_23050	Löschen personenbezogener Daten	gemSpec_IDP_FD
A_23078	Zugriffstoken ohne Personenbezogene Daten	gemSpec_IDP_FD
A_23204	Verwerfen der Token bei Inaktivität	gemSpec_IDP_FD
A_23336	Mindestvorgaben für Schlüssel von Fachdiensten als Teilnehmer der TI-Föderation	gemSpec_IDP_FD
A_17124-03	TLS-Verbindungen (ECC-Migration)	gemSpec_Krypt
A_18464	TLS-Verbindungen, nicht Version 1.1	gemSpec_Krypt
A_18467	TLS-Verbindungen, Version 1.3	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt
GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
GS-A_4387	TLS-Verbindungen, nicht Version 1.0	gemSpec_Krypt
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt

GS-A_5322	Weitere Vorgaben für TLS-Verbindungen	gemSpec_Krypt

4 Anhang – Verzeichnisse

4.1 Abkürzungen

Kürzel	Erläuterung
ID	Identifikation
CC	Common Criteria
DiGA	Digitale Gesundheitsanwendungen

4.2 Tabellenverzeichnis