

Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

Proof of Patient Presence- Service

Produkttyp Version: 2.0.0-0
Produkttyp Status: in Bearbeitung

Version: 1.0.0 CC2
Revision: 1712726
Stand: 03.09.2026
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemProdT_PoPP_Service_PTV_2.0.0-0

Historie Produkttypversion und Produkttypsteckbrief

Gender-Hinweis

Aus Gründen der besseren Lesbarkeit wird in diesem Dokument überwiegend die männliche Form verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Historie Produkttypversion

Die Produkttypversion ändert sich, wenn sich die normativen Festlegungen für den Produkttyp ändern und die Umsetzung durch Produktentwicklungen ebenfalls betroffen ist.

Produkttypversion	Beschreibung der Änderung	Referenz
1.0.0-0	Initiale Erstellung für Umsetzungsstufe 1	gemProdT_PoPP_Service_PTV_1.0.0-0
1.1.0-0	Umsetzungsstufe 1: PoPP1_26_1	gemProdT_PoPP_Service_PTV_1.1.0-0
2.0.0-0	Initiale Erstellung für Umsetzungsstufe 2	gemProdT_PoPP_Service_PTV_2.0.0-0

Historie Produkttypsteckbrief

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

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeiter
1.0.0 CC2	03.09.2026		Umsetzungsstufe 2: PoPP1_26_2	gematik

Inhaltsverzeichnis

1 Einführung	4
1.1 Zielsetzung und Einordnung des Dokumentes	4
1.2 Zielgruppe	4
1.3 Geltungsbereich	4
1.4 Abgrenzung des Dokumentes	5
1.5 Methodik	5
2 Dokumente	6
3 Normative Festlegungen	8
3.1 Festlegungen zur funktionalen Eignung.....	8
3.1.1 Produkttest/Produktübergreifender Test	8
3.1.2 Herstellererklärung funktionale Eignung	12
3.2 Festlegungen zur sicherheitstechnischen Eignung	16
3.2.1 Produktgutachten	16
3.2.2 Sicherheitsgutachten	22
3.2.3 Herstellererklärung sicherheitstechnische Eignung.....	23
3.2.4 Dokumentenprüfung.....	24
3.3 Festlegungen zur elektrischen, mechanischen und physikalischen Eignung	24
4 Produkttypspezifische Merkmale	25
5 Anhang – Verzeichnisse	26
5.1 Abkürzungen	26
5.2 Tabellenverzeichnis	26

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die normativen Festlegungen der gematik an Herstellung und Betrieb von Produkten des Produkttyps PoPP-Service oder verweist auf Dokumente, in denen verbindliche normative Festlegungen mit ggf. anderer Notation zu finden sind. Die normativen Festlegungen bilden die Grundlage für die Erteilung von Zulassungen, Zertifizierungen bzw. Bestätigungen durch die gematik. (Wenn im weiteren Dokument vereinfachend der Begriff „Zulassung“ verwendet wird, so ist dies der besseren Lesbarkeit geschuldet und umfasst übergreifend neben dem Verfahren der Zulassung auch Zertifizierungen und Bestätigungen der gematik-Zulassungsstelle.)

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 Produkttypsteckbrief richtet sich an den PoPP-Service-Hersteller und -Anbieter sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

Das Dokument ist außerdem zu verwenden von:

- der gematik im Rahmen des Zulassungsverfahrens,
- dem Bundesamt für Sicherheit in der Informationstechnik (BSI),
- akkreditierten Materialprüflaboren,
- Auditoren.

Bei zentralen Diensten der TI-Plattform und fachanwendungsspezifischen Diensten beziehen sich normative Festlegungen, die sowohl an Anbieter als auch Hersteller gerichtet sind, jeweils auf den Anbieter als Zulassungsnehmer, bei dezentralen Produkten auf den Hersteller.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Leistungsbeschreibung) 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 den Anbietertyp sind nicht aufgeführt. Die geltenden Verfahren und Regelungen zur Beantragung und Durchführung von Zulassungsverfahren können dem Fachportal der gematik (<https://fachportal.gematik.de/downloadcenter/zulassungs-bestaetigungsantraege-verfahrensbeschreibungen>) 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 Produkttyp normativen Festlegungen.

Tabelle 1: Dokumente mit normativen Festlegungen

Dokumenten Kürzel	Bezeichnung des Dokumentes	Version
gemF_PoPP_Online_Check-in	Feature Spezifikation PoPP Stufe 2 - Online Check-in	1.0.0 CC4
gemKPT_Test	Testkonzept der TI	3.6.0
gemSpec_DS_Hersteller	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller	1.7.0
gemSpec_FD_TI-Flow	Spezifikation: TI-Flow-Fachdienst	1.0.0_RC
gemSpec_IDP_FD	Spezifikation Identity Provider – Fachdienste	2.2.0
gemSpec_IDP_FedMaster	Spezifikation Federation Master	1.4.3
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.49.1
gemSpec_OM	Übergreifende Spezifikation Operations und Maintenance	1.19.0
gemSpec_Perf	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.86.0
gemSpec_PKI	Übergreifende Spezifikation – Spezifikation PKI	2.27.0
gemSpec_PoPP_Service	Spezifikation Proof of Patient Presence-Service	1.1.0
gemSpec_ZETA	Spezifikation Zero Trust Access (ZETA)	2.0.1_CC

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
[api-popp] - Stufe 1	GitHub-Pfad zu den Schnittstellen-Beschreibungen https://github.com/gematik/api-popp/tree/3.1.0	3.1.0

Quelle	Herausgeber: Bezeichnung / URL	Version Branch / Tag
[api-popp] - Stufe 2	GitHub-Pfad zu den Schnittstellen-Beschreibungen https://github.com/gematik/api-popp/tree/US-2_CC2	US-2_CC2

Die Bestätigungs-/Zulassungsbedingungen für das Bestätigungs-/Zulassungsobjekt PoPP_Service werden im Dokument [gemZul_Prod_PoPP-Service] im Fachportal der gematik im Abschnitt Zulassung 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	Versi on Branch / Tag
[gemRL_PruefSichEi g_DS]	gematik: Richtlinie zur Prüfung der Sicherheitseignung https://gemspec.gematik.de/docs/gemRL/gemRL_PruefSichEig_DS/latest/	latest

3 Normative Festlegungen

Die folgenden Abschnitte verzeichnen alle für den Produkttypen normativen Festlegungen, die für die Herstellung und den Betrieb von Produkten des Produkttyps notwendig sind. Die Festlegungen sind gruppiert nach der Art der Nachweisführung ihrer Erfüllung als Grundlage der Zulassung, Zertifizierung bzw. Bestätigung.

3.1 Festlegungen zur funktionalen Eignung

3.1.1 Produkttest/Produktübergreifender Test

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Festlegungen an den technischen Teil des Produkttyps verzeichnet, deren Umsetzung und Nachweiserbringung in Verantwortung des Zulassungsnehmers liegt.

Tabelle 4: Festlegungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

ID	Bezeichnung	Quelle (Referenz)
AF_10386-01	Online Check-in mit GesundheitsID	gemF_PoPP_Online_Check-in
AF_10390-01	PoPP-Token Erstellung bei Online Check-in	gemF_PoPP_Online_Check-in
AF_10425	Status der PoPP-Token-Erstellung nach Online Check-in ermitteln	gemF_PoPP_Online_Check-in
A_26361-01	PoPP-Service - Zero Trust Schutz des PoPP-Interfaces	gemF_PoPP_Online_Check-in
A_28659	PoPP-Service - Entgegennahme des HTTP-Request zur Ermittlung von Informationen zum Inhaber der Telematik-ID	gemF_PoPP_Online_Check-in
A_30040	PoPP-Service - Bereitstellung der Schnittstelle zum Abruf der PoPP-Token zu Online Check-ins	gemF_PoPP_Online_Check-in
A_30067	PoPP-Service - Push-Notification an PoPP-Modul nach Statuswechsel	gemF_PoPP_Online_Check-in
A_30145	PoPP-Service – StatusCodes	gemF_PoPP_Online_Check-in
A_30146	PoPP-Service – Zuordnung von Telematik-IDs zu WebSocket-Verbindungen	gemF_PoPP_Online_Check-in
A_30147	PoPP-Service – Auslieferung von PoPP-Token über bestehende WebSocket-Verbindungen	gemF_PoPP_Online_Check-in

ID	Bezeichnung	Quelle (Referenz)
A_30148	PoPP-Service – Entfernen ungültiger WebSocket-Verbindungen	gemF_PoPP_Online_Check-in
A_30149	PoPP-Service – Beenden von WebSocket-Verbindungen beim Wechsel von Verarbeitungskontexten	gemF_PoPP_Online_Check-in
A_30170	PoPP-Service - Status Code im WebSocket-Interface - 2	gemF_PoPP_Online_Check-in
A_26914	Integration von Zero Trust Komponenten	gemKPT_Test
A_27790-01	Schnittstelle zur ZETA Guard – Funktionale Eignung	gemKPT_Test
A_22482-02	Performance - Betriebsdatenlieferung - Erfassung von Betriebsdaten	gemSpec_Perf
A_26174	Performance - Selbstauskunft - Verpflichtung zur Erfassung	gemSpec_Perf
A_26333-01	Performance - Telemetriedatenlieferung - Spezifika PoPP-Service - Operation	gemSpec_Perf
A_26336	Performance - PoPP-Service - Robustheit gegenüber Lastspitzen	gemSpec_Perf
A_26532-01	Performance - Telemetriedatenlieferung - Spezifika PoPP-Service - Message	gemSpec_Perf
A_27316-01	Performance - Telemetriedatenlieferung - Spezifika PoPP-Service - Status	gemSpec_Perf
A_27722-04	Performance - Telemetriedatenlieferung - Status Code des Ressource Servers	gemSpec_Perf
A_27723-03	Performance - Telemetriedatenlieferung - Lieferung RS	gemSpec_Perf
A_27724-02	Performance - Telemetriedatenlieferung - Korrektheit der Datenlieferung	gemSpec_Perf
A_27729-01	Performance - Telemetriedatenlieferung - Selbstauskunft	gemSpec_Perf
A_28190-01	Performance - PoPP-Service - Import Hash-DB	gemSpec_Perf
A_28786	Performance - Telemetriedatenlieferung - Ausnahme der Vollständigkeit	gemSpec_Perf
A_28835	Telemetriedaten - Spezifika PoPP-Service - Metrik PoPP-vital	gemSpec_Perf

ID	Bezeichnung	Quelle (Referenz)
A_28860	Telemetriedaten - Spezifika PoPP-Service - Metrik PoPP-blockedItems	gemSpec_Perf
A_28889	Performance - Telemetriedaten - Spezifika PoPP-Service - RS Duration	gemSpec_Perf
AF_10387	PoPP-Token mittels eGK im Standard-Kartenleser	gemSpec_PoPP_Service
AF_10393	PoPP-Token mittels eGK im eH-KT	gemSpec_PoPP_Service
AF_10402	LEI am PoPP-Service registrieren / anmelden	gemSpec_PoPP_Service
A_26345	PoPP-Service - WebSocket Interface zur PoPP-Token-Erstellung EHC	gemSpec_PoPP_Service
A_26361	PoPP-Service - Zero Trust Schutz des PoPP-Interfaces	gemSpec_PoPP_Service
A_26362	PoPP-Service - Status Code im WebSocket-Interface	gemSpec_PoPP_Service
A_26431	PoPP-Service - PoPP-Token Claims	gemSpec_PoPP_Service
A_26432	PoPP-Service - PoPP-Token JWT	gemSpec_PoPP_Service
A_26433	PoPP-Service - PoPP-Token Header und Signatur	gemSpec_PoPP_Service
A_26434	PoPP-Service - Bereitstellung der öffentlichen Schlüssel zur Verifikation der PoPP-Token als JWKS	gemSpec_PoPP_Service
A_26508-01	PoPP-Service - Vertrauenswürdige Uhrzeit	gemSpec_PoPP_Service
A_26961	PoPP-Service - PoPP-Token Claims über Leistungserbringer (LE)	gemSpec_PoPP_Service
A_26962	PoPP-Service - PoPP-Token Claims über Versicherte	gemSpec_PoPP_Service
A_27000	PoPP-Service, StandardScenarioMessage	gemSpec_PoPP_Service
A_27001	PoPP-Service, Szenario SceReadCvc	gemSpec_PoPP_Service
A_27002	PoPP-Service, Szenario SceTC1	gemSpec_PoPP_Service
A_27003	PoPP-Service, Szenario SceReadX.509	gemSpec_PoPP_Service
A_27006	PoPP-Service, Szenario mit APDU innerhalb eines Trusted Channels	gemSpec_PoPP_Service

ID	Bezeichnung	Quelle (Referenz)
A_27008	PoPP-Service, Szenario SceOpenEgk, eGK öffnen	gemSpec_PoPP_Service
A_27009-01	PoPP-Service, Auswertung SceOpenEgk	gemSpec_PoPP_Service
A_27010	PoPP-Service, Auswertung SceReadCvc	gemSpec_PoPP_Service
A_27011	PoPP-Service, Auswertung SceTC1	gemSpec_PoPP_Service
A_27013	PoPP-Service, Auswertung SceReadX.509	gemSpec_PoPP_Service
A_27020	PoPP-Service, Szenario SceAuthG2	gemSpec_PoPP_Service
A_27021	PoPP-Service, Auswertung SceAuthG2	gemSpec_PoPP_Service
A_27022	PoPP-Service, Szenario SceAuthGx.y	gemSpec_PoPP_Service
A_27023	PoPP-Service, Auswertung SceAuthGx.y	gemSpec_PoPP_Service
A_27044-01	PoPP-Service, Schnittstelle I_PoPP_EHC_CertHash_Import	gemSpec_PoPP_Service
A_27045-01	PoPP-Service, Eintrag Lieferant	gemSpec_PoPP_Service
A_27046	PoPP-Service, eGK-Hash-Datenbank	gemSpec_PoPP_Service
A_27102	PoPP-Service - Verwenden der LEI Daten im Resource Server	gemSpec_PoPP_Service
A_27128	PoPP-Service, Codierung von Konnektor-Szenarien	gemSpec_PoPP_Service
A_27129	PoPP-Service, Codierung von Nicht-Konnektor-Szenarien	gemSpec_PoPP_Service
A_27202	PoPP-Service - TSL - Proxy für Verarbeitungskontexte	gemSpec_PoPP_Service
A_27296-01	PoPP-Service - Bereitstellung .well-known als Teilnehmer der TI-Föderation	gemSpec_PoPP_Service
A_27317-01	PoPP-Service - interne Fehlercodes	gemSpec_PoPP_Service
A_27622-01	PoPP-Service, eGK-Hash-Datenbank, check-Funktion	gemSpec_PoPP_Service
A_27623-01	PoPP-Service, eGK-Hash-Datenbank, import-Funktion	gemSpec_PoPP_Service
A_27624	PoPP-Service, eGK-Hash-Datenbank, Löschen veralteter Einträge	gemSpec_PoPP_Service

ID	Bezeichnung	Quelle (Referenz)
A_28893	PoPP-Service, Performanz während Import	gemSpec_PoPP_Service
A_28894	PoPP-Service, Zusatzeinträge während Import	gemSpec_PoPP_Service
A_28895	PoPP-Service, Blocken während Import	gemSpec_PoPP_Service
A_28896	PoPP-Service, Rückantwort	gemSpec_PoPP_Service
A_28897	PoPP-Service, Anzahl Lieferanten	gemSpec_PoPP_Service
A_28898	PoPP-Service, Ablauf eines Imports	gemSpec_PoPP_Service
A_28900	PoPP-Service, Kurzzeitprotokoll - check	gemSpec_PoPP_Service
A_28901	PoPP-Service, Kurzzeitprotokoll - import	gemSpec_PoPP_Service
A_28902	PoPP-Service, Kurzzeitprotokoll - Telemetriedaten	gemSpec_PoPP_Service
A_28908	PoPP-Service, Kommunikationskanal - HTTP	gemSpec_PoPP_Service
A_28909	PoPP-Service, Kommunikationskanal - Abbau der Verbindung	gemSpec_PoPP_Service
A_28977	PoPP-Service, Kurzzeitprotokoll - Mindestanzahl	gemSpec_PoPP_Service
A_29969	Resource Server – Nutzung der Notification-Service-Schnittstelle	gemSpec_ZETA

3.1.2 Herstellererklärung funktionale Eignung

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Festlegungen an den technischen Teil des Produkttyps verzeichnet, deren durchgeführte bzw. geplante Umsetzung und Beachtung der Hersteller bzw. der Anbieter durch eine Herstellererklärung bestätigt bzw. zusagt.

Tabelle 5: Festlegungen zur funktionalen Eignung "Herstellererklärung"

ID	Bezeichnung	Quelle (Referenz)
A_27030-04	Performance - PoPP-Service - Bearbeitungszeit unter Last	gemF_PoPP_Online_Check-in
A_28664	PoPP-Service - Registrierung am FHIR-VZD	gemF_PoPP_Online_Check-in
A_28665	PoPP-Service - Aktualisierung des FHIR-VZD Zugang	gemF_PoPP_Online_Check-in

ID	Bezeichnung	Quelle (Referenz)
A_28857	Maximale Gültigkeitsdauer und regelmäßige Erneuerung des Entity Statement eines TI-Föderation-Teilnehmers	gemF_PoPP_Online_Check-in
A_28911	Entity Statement eines TI-Fachdienstes als Protected Resource	gemF_PoPP_Online_Check-in
A_30076	Vorhalten VZD-Daten im PoPP-Service	gemF_PoPP_Online_Check-in
A_20061	Beschreibung Art und Umfang der Fehlerkorrektur	gemKPT_Test
A_25392-01	Nutzung Testfallmatrix-Template der gematik	gemKPT_Test
A_26241	Erstellung Performancetestbericht	gemKPT_Test
A_26674	Bereitstellung von Testkomponenten und Testartefakten in den Testumgebungen	gemKPT_Test
A_26675	Format der Testszenarien	gemKPT_Test
A_26676	Kontrollpunkte während der Entwicklungsphase	gemKPT_Test
A_26677	Herstellerspezifische Kontrollpunkte	gemKPT_Test
A_26680-01	Versionierung der Testkomponenten	gemKPT_Test
A_26684	Freie Nutzung der entwickelten Testartefakte	gemKPT_Test
A_26685	Automatisierung der Testartefakte	gemKPT_Test
A_26686	Verwendbarkeit von Testkomponenten und Testartefakten in automatisierten CI/CD-Pipelines	gemKPT_Test
A_26689	Keine Hardware-Abhängigkeiten bei Komponenten in Testumgebungen	gemKPT_Test
A_26690	Nutzung von Private oder Secret Keys in Testumgebungen	gemKPT_Test
A_26915	Integration von Monitoring Komponenten	gemKPT_Test
A_27053	Freie Nutzung der erworbenen Testartefakte	gemKPT_Test
A_27100	Übergreifende Testmaßnahmen	gemKPT_Test
A_27141	Testmanagementsystem des AN	gemKPT_Test
A_27142-01	Anforderungen an Testreporting	gemKPT_Test

ID	Bezeichnung	Quelle (Referenz)
A_27248	Güteprüfung Test	gemKPT_Test
A_27393	Bereitstellung als signiertes OCI konformes Image	gemKPT_Test
A_27394	Agiler Bereitstellungsprozess	gemKPT_Test
A_27438	Durchführung der Generalprobe	gemKPT_Test
A_27475	Fehlerbehebungsplan	gemKPT_Test
TIP1-A_6517-02	Eigenverantwortlicher Test: Zulassungsnehmer	gemKPT_Test
TIP1-A_6519	Eigenverantwortlicher Test: Hersteller und Anbieter	gemKPT_Test
TIP1-A_7335	Bereitstellung der Testdokumentation	gemKPT_Test
A_25392-01	Nutzung Testfallmatrix-Template der gematik	gemSpec_FD_TI-Flow
A_27141	Testmanagementsystem des AN	gemSpec_FD_TI-Flow
A_27142-01	Anforderungen an Testreporting	gemSpec_FD_TI-Flow
A_27248	Güteprüfung Test	gemSpec_FD_TI-Flow
A_27438	Durchführung der Generalprobe	gemSpec_FD_TI-Flow
A_27475	Fehlerbehebungsplan	gemSpec_FD_TI-Flow
TIP1-A_6517-02	Eigenverantwortlicher Test: Zulassungsnehmer	gemSpec_FD_TI-Flow
A_28911	Entity Statement eines TI-Fachdienstes als Protected Resource	gemSpec_IDP_FD
A_28857	Maximale Gültigkeitsdauer und regelmäßige Erneuerung des Entity Statement eines TI-Föderation-Teilnehmers	gemSpec_IDP_FedMaster
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM
GS-A_3696	Zeitpunkt der Erzeugung neuer Versionsnummern	gemSpec_OM
GS-A_3697	Anlass der Erhöhung von Versionsnummern	gemSpec_OM
GS-A_4541	Nutzung der Produkttypversion zur Kompatibilitätsprüfung	gemSpec_OM

ID	Bezeichnung	Quelle (Referenz)
GS-A_5025	Versionierung von Produkten auf Basis von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten durch die Produktidentifikation	gemSpec_OM
GS-A_5038	Festlegungen zur Vergabe einer Produktversion	gemSpec_OM
GS-A_5054	Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen	gemSpec_OM
A_23225	lokales Caching von Sperrinformationen und Toleranzzeiten	gemSpec_PKI
A_23349	Performance - Servicezeiten des Produktes - Hauptzeit - Montag bis Sonntag	gemSpec_Perf
A_27030-02	Performance - PoPP-Service - Bearbeitungszeit unter Last	gemSpec_Perf
A_28779-01	Performance - Telemetriedatenlieferung - Konfiguration Datenlieferung RS	gemSpec_Perf
A_28780-01	Performance - Telemetriedatenlieferung - Batchverarbeitung RS	gemSpec_Perf
A_28782-01	Performance - Telemetriedatenlieferung - Konfiguration Datenlieferung ZETA Guard	gemSpec_Perf
A_28785	Performance - Telemetriedatenlieferung - Bestandsdaten	gemSpec_Perf
A_28891	Verbindungsaufbau zum Telemetriedaten-Service des Produkts	gemSpec_Perf
A_28988	Performance - Telemetriedatenlieferung - Konfiguration Datenlieferung ZETA Guard - Sampling	gemSpec_Perf
A_27017	PoPP-Service, Erlaubnis für abweichende Szenarien	gemSpec_PoPP_Service
A_27018-01	PoPP-Service, Zulässige eGK Objektsystemversionen	gemSpec_PoPP_Service
A_27019-01	PoPP-Service, Unzulässige eGK Objektsystemversionen	gemSpec_PoPP_Service
A_28040	PoPP-Service - Verarbeiten von Prüfkarte eGK	gemSpec_PoPP_Service
A_28899	PoPP-Service, Kurzzeitprotokoll - Einträge	gemSpec_PoPP_Service

ID	Bezeichnung	Quelle (Referenz)
A_28923	PoPP-Service, Reihenfolge beim Import	gemSpec_PoPP_Service
A_28978	PoPP-Service, Kurzzeitprotokoll - Überlauf	gemSpec_PoPP_Service
A_28984	PoPP-Service, Kurzzeitprotokoll - ITSM-Meldung	gemSpec_PoPP_Service
A_27818	Unterstützung der Wartbarkeit des ZETA Guard-Dienstes	gemSpec_ZETA
A_29851	PEP HTTP Proxy, Ausschluss von Nicht-PEP-Fehlern	gemSpec_ZETA

3.2 Festlegungen zur sicherheitstechnischen Eignung

3.2.1 Produktgutachten

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

Tabelle 6: Festlegungen zur sicherheitstechnischen Eignung "Produktgutachten"

ID	Bezeichnung	Quelle (Referenz)
A_28848	Validierung der Vertrauensketten eines TI-Föderation-Teilnehmers	gemF_PoPP_Online_Check-in
A_30100	PoPP-Service - Abgleich client_id bei Statusabfrage	gemF_PoPP_Online_Check-in
A_30105	PoPP-Service - Löschen von Datensätzen nach deren Ablaufzeit	gemF_PoPP_Online_Check-in
A_30106	PoPP-Service - Abgleich der Telematik-ID PoPP-Datensatz und Nutzer-Anfrage	gemF_PoPP_Online_Check-in
A_30107	PoPP-Service - Unveränderte Datenübernahme und sichere Speicherung (GesundheitsID)	gemF_PoPP_Online_Check-in
A_30143	PoPP-Service - Rate-Limit Online Check-in pro Versichertem	gemF_PoPP_Online_Check-in
A_29779	Wechsel von Nutzerpseudonymen	gemSpec_FD_TI-Flow
A_28848	Validierung der Vertrauensketten eines TI-Föderation-Teilnehmers	gemSpec_IDP_FedMaster
A_18464	TLS-Verbindungen, nicht Version 1.1	gemSpec_Krypt

ID	Bezeichnung	Quelle (Referenz)
A_18467	TLS-Verbindungen, Version 1.3	gemSpec_Krypt
A_21275-01	TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake	gemSpec_Krypt
A_24779-02	PoPP, TI-Gateway-Zugangsmodule und eHealth-CardLink - TLS-Cipher-Suiten	gemSpec_Krypt
A_28578	PoPP-Service - Pseudonymisierung bei den Telemetriedaten (Anomalie-Erkennung)	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
GS-A_5526	TLS-Renegotiation-Indication-Extension	gemSpec_Krypt
GS-A_4640	Identifizierung/Validierung des TI-Vertrauensankers bei der initialen Einbringung	gemSpec_PKI
GS-A_4641	Initiale Einbringung TI-Vertrauensanker	gemSpec_PKI
GS-A_4748	Initiale Einbringung TSL-Datei	gemSpec_PKI
A_26468	PoPP-Service - Bereitstellung VAU-Image-Build-Pipeline und automatisiertes Einbinden des ZETA Guard	gemSpec_PoPP_Service
A_26469	PoPP-Service - Ausschließlich TLS-Verbindungen	gemSpec_PoPP_Service
A_26470	PoPP-Service - Schutz vor Angriffen auf Anwendungsebene	gemSpec_PoPP_Service
A_26471	PoPP-Service - VAU - Umsetzung einer VAU	gemSpec_PoPP_Service
A_26472	PoPP-Service - Eingeschränkte Speicherung von Daten	gemSpec_PoPP_Service
A_26498	PoPP-Service - Schlüsselpaare und X.509-Zertifikate immer auf Basis P-256	gemSpec_PoPP_Service
A_26499	PoPP-Service - CV-Identität für eGK-Kommunikation	gemSpec_PoPP_Service
A_26593	PoPP-Service - VAU - Ausschluss Manipulationen der Software bei Start eines Verarbeitungskontextes	gemSpec_PoPP_Service

ID	Bezeichnung	Quelle (Referenz)
A_26594	PoPP-Service - VAU - Import VAU-Image nur nach erfolgreicher Signaturprüfung	gemSpec_PoPP_Service
A_26595	PoPP-Service - VAU - Regelmäßiger Neustart der Verarbeitungskontexte	gemSpec_PoPP_Service
A_26596	PoPP-Service - VAU - Attestierung durch Systeme außerhalb der VAU	gemSpec_PoPP_Service
A_26597	PoPP-Service - VAU - Erkennen von Manipulationen an der HW der VAU - Softwareanteil	gemSpec_PoPP_Service
A_26598	PoPP-Service - VAU - Erkennen von Manipulationen an der Hardware der VAU - Hardwareanteil	gemSpec_PoPP_Service
A_26599	PoPP-Service - VAU - Isolation der VAU von Datenverarbeitungsprozessen des Anbieters	gemSpec_PoPP_Service
A_26600	PoPP-Service - VAU - Isolation zwischen Datenverarbeitungsprozessen mehrerer Verarbeitungskontexte der VAU	gemSpec_PoPP_Service
A_26601	PoPP-Service - VAU - Löschen aller Daten beim Beenden des Verarbeitungskontextes	gemSpec_PoPP_Service
A_26603	PoPP-Service - VAU - Verschlüsselung von Daten vor Speicherung außerhalb des Verarbeitungskontextes	gemSpec_PoPP_Service
A_26604	PoPP-Service - VAU - Ableitung Persistenzschlüssel durch ein HSM	gemSpec_PoPP_Service
A_26605	PoPP-Service - VAU - Nutzung Persistenzschlüssel ausschließlich im Verarbeitungskontext	gemSpec_PoPP_Service
A_26606	PoPP-Service - VAU - Sicherer VAU-Kanal vom Kommunikationspartner in den Verarbeitungskontext	gemSpec_PoPP_Service
A_26607	PoPP-Service - VAU - Authentisierung gegenüber VAU-Clients	gemSpec_PoPP_Service
A_26609	PoPP-Service - VAU - Sichere Kommunikation zwischen Komponenten	gemSpec_PoPP_Service
A_26610	PoPP-Service - VAU - Identitäten zur Authentisierung für Kommunikation zwischen Verarbeitungskontexten	gemSpec_PoPP_Service

ID	Bezeichnung	Quelle (Referenz)
A_26611	PoPP-Service - VAU - Sichere Verbindung zwischen bekannten VAU-Image und HSM	gemSpec_PoPP_Service
A_26612	PoPP-Service - VAU - Datenschutzkonformes Logging und Monitoring des Verarbeitungskontextes der VAU	gemSpec_PoPP_Service
A_26613	PoPP-Service - VAU - Protokollierung VAU-Image-Hashwerte und öffentliche Schlüssel im HSM	gemSpec_PoPP_Service
A_26614	PoPP-Service - VAU - Exportierbarkeit Protokoll für VAU-Image-Hashwerte und öffentliche Schlüssel aus HSM	gemSpec_PoPP_Service
A_26615	PoPP-Service - VAU - Einspielen von VAU-Image durch den Anbieter	gemSpec_PoPP_Service
A_26617	PoPP-Service - VAU - Hersteller - Schlüsselqualität Attestierungs- und Autorisierungs-Schlüssel	gemSpec_PoPP_Service
A_26618	PoPP-Service - VAU - Hersteller - Einbringen und Speichern von Attestierungs-Schlüsseln in VAU	gemSpec_PoPP_Service
A_26619	PoPP-Service - VAU - Hersteller - Speichern von Autorisierungs- und CA-Schlüsseln	gemSpec_PoPP_Service
A_26620	PoPP-Service - VAU - Hersteller - Bereitstellung Prüfschlüssel für Attestierung und Autorisierung	gemSpec_PoPP_Service
A_26621	PoPP-Service - VAU - Hersteller - kryptografische Autorisierung von VAU-Image	gemSpec_PoPP_Service
A_26622	PoPP-Service - VAU - Hersteller - Übermittlung autorisierter VAU-Image an Anbieter und gematik	gemSpec_PoPP_Service
A_26631-01	PoPP-Service - APDU-Paket-Signatur - Einbetten OCSP-Response	gemSpec_PoPP_Service
A_26687	PoPP-Service - VAU - Schlüssel- und CSR-Erzeugung im HSM durch Verarbeitungskontext	gemSpec_PoPP_Service
A_26692	PoPP-Service - VAU - Hersteller - Protokollierung sicherheitsrelevanter Hersteller-Aktivitäten	gemSpec_PoPP_Service
A_26822	PoPP-Service - Sichere VAU-Image-Erzeugung (Prozess)	gemSpec_PoPP_Service

ID	Bezeichnung	Quelle (Referenz)
A_26954	PoPP-Service - Schlüsselpaare für CV-Zertifikate immer auf Basis von Brainpool	gemSpec_PoPP_Service
A_26975	PoPP-Service - OCSP-Stapling an Client-Schnittstelle	gemSpec_PoPP_Service
A_27006	PoPP-Service, Szenario mit APDU innerhalb eines Trusted Channels	gemSpec_PoPP_Service
A_27010	PoPP-Service, Auswertung SceReadCvc	gemSpec_PoPP_Service
A_27011	PoPP-Service, Auswertung SceTC1	gemSpec_PoPP_Service
A_27013	PoPP-Service, Auswertung SceReadX.509	gemSpec_PoPP_Service
A_27021	PoPP-Service, Auswertung SceAuthG2	gemSpec_PoPP_Service
A_27023	PoPP-Service, Auswertung SceAuthGx.y	gemSpec_PoPP_Service
A_27038	PoPP-Service - VAU - Aktivierung außerhalb des HSM gespeicherter Schlüssel	gemSpec_PoPP_Service
A_27039	PoPP-Service - VAU - Nutzung außerhalb des HSMs gespeicherter Schlüssel	gemSpec_PoPP_Service
A_27042	PoPP-Service - VAU - Gehärtete Schnittstellen für Anbieter	gemSpec_PoPP_Service
A_27130	PoPP-Service, Prüfen von X.509-Zertifikaten einer eGK	gemSpec_PoPP_Service
A_27150	PoPP-Service - TSL - Aktualisierung	gemSpec_PoPP_Service
A_27151	PoPP-Service - TSL - Prüfung auf Aktualität	gemSpec_PoPP_Service
A_27152	PoPP-Service - TSL - Keine abgelaufene TSL verwenden	gemSpec_PoPP_Service
A_27201	PoPP-Service - eGK-Hash-Datenbank Aspekte für Produktgutachten	gemSpec_PoPP_Service
A_27373	PoPP-Service - VAU - Temporäre Möglichkeit des Rollback auf vorherige Version	gemSpec_PoPP_Service
A_27613	PoPP-Service - Maßnahmen gegen Datenverlust	gemSpec_PoPP_Service
A_28547-01	PoPP-Service, eGK-Hash-Datenbank, Client-Zertifikatsprüfung im TLS-Handshake	gemSpec_PoPP_Service
A_28548	PoPP-Service, eGK-Hash-Datenbank, Signatur-Zertifikatsprüfung	gemSpec_PoPP_Service

ID	Bezeichnung	Quelle (Referenz)
A_25410	ZETA Guard - Verbot von Werbe- und Usability-Tracking	gemSpec_ZETA
A_28405	ZETA Guard – Umwandlung für Ziel-VAU-Architektur	gemSpec_ZETA
A_28406-01	ZETA Guard – Verification der ZETA Guard Images	gemSpec_ZETA
A_28744	ZETA Guard - Ressourcenserver-Zugriff nur von freigegebenen Komponenten	gemSpec_ZETA
A_28745	ZETA Guard - Zugriff nur von freigegebenen Ressourcenservern	gemSpec_ZETA
A_28746	ZETA Guard - HSM Proxy in einer VAU	gemSpec_ZETA
A_28747	HSM-Proxy - Zugriff auf ZETA-Schlüssel über HSM-Proxy	gemSpec_ZETA
A_28756	Umsetzung ZETA Guard in Sicherheits- und Datenschutzkonzept	gemSpec_ZETA
A_28757	ZETA Guard - Zugriff nur zwischen attestierten Komponenten	gemSpec_ZETA
A_28797-01	HSM-Proxy - Isolation HSM Proxy	gemSpec_ZETA
A_28814	HSM-Proxy - Sealing von Credentials	gemSpec_ZETA
A_28816	HSM-Proxy - Minimale Trusted-Computing-Base	gemSpec_ZETA
A_28817	HSM-Proxy – Keine Persistierung von Request/Response Daten	gemSpec_ZETA
A_28819	HSM-Proxy - Integrität und Authentizität der Konfiguration und Rollback-Schutz	gemSpec_ZETA
A_28820	HSM-Proxy - Eingabe Validierung von Operationen	gemSpec_ZETA
A_28821	HSM-Proxy - Schutzmaßnahmen gegen die OWASP Top 10 Risiken	gemSpec_ZETA
A_28822	HSM-Proxy - Datenschutzkonformes Logging und Monitoring	gemSpec_ZETA
A_28826	HSM Proxy, Übergabe PDP-Datenbank-Schlüssel an ZETA Guard Authorization Server	gemSpec_ZETA
A_28962	ZETA GUARD - Nachweis der Umsetzung von Anforderungen in dem Build-Pipeline	gemSpec_ZETA

3.2.2 Sicherheitsgutachten

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

Tabelle 7: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

ID	Bezeichnung	Quelle (Referenz)
A_19147	Sicherheitstestplan	gemSpec_DS_Hersteller
A_19148	Sicherheits- und Datenschutzkonzept	gemSpec_DS_Hersteller
A_19150	Umsetzung Sicherheitstestplan	gemSpec_DS_Hersteller
A_19151	Implementierungsspezifische Sicherheitsanforderungen	gemSpec_DS_Hersteller
A_19152	Verwendung eines sicheren Produktlebenszyklus	gemSpec_DS_Hersteller
A_19153	Sicherheitsrelevanter Softwarearchitektur-Review	gemSpec_DS_Hersteller
A_19154	Durchführung einer Bedrohungsanalyse	gemSpec_DS_Hersteller
A_19155	Durchführung sicherheitsrelevanter Quellcode-Reviews	gemSpec_DS_Hersteller
A_19156	Durchführung automatisierter Sicherheitstests	gemSpec_DS_Hersteller
A_19157	Dokumentierter Plan zur Sicherheitsschulung für Entwickler	gemSpec_DS_Hersteller
A_19158	Sicherheitsschulung für Entwickler	gemSpec_DS_Hersteller
A_19159	Dokumentation des sicheren Produktlebenszyklus	gemSpec_DS_Hersteller
A_19160	Änderungs- und Konfigurationsmanagementprozess	gemSpec_DS_Hersteller
A_22984	Unverzögliche 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
A_27429	Sicherer Softwareentwicklungsprozess bei Zulieferern	gemSpec_DS_Hersteller

ID	Bezeichnung	Quelle (Referenz)
A_27430	Supply-Chain Angriffe verhindern	gemSpec_DS_Hersteller
A_27431	SBOM nach Vorgaben des BSI	gemSpec_DS_Hersteller
A_27433	Codemodifikationen nur durch autorisierte Mitarbeiter	gemSpec_DS_Hersteller

3.2.3 Herstellererklärung sicherheitstechnische Eignung

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

Tabelle 8: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung"

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4191	Keine Echtdaten in RU und TU	gemKPT_Test
A_17178	Produktentwicklung: Basisschutz gegen OWASP Top 10 Risiken	gemSpec_DS_Hersteller
A_17179	Auslieferung aktueller zusätzlicher Softwarekomponenten	gemSpec_DS_Hersteller
A_19163	Rechte der gematik zur sicherheitstechnischen Prüfung des Produktes	gemSpec_DS_Hersteller
A_19164	Mitwirkungspflicht bei Sicherheitsprüfung	gemSpec_DS_Hersteller
A_19165	Auditrechte der gematik zur Prüfung der Herstellerbestätigung	gemSpec_DS_Hersteller
A_23445	Beteiligung der Hersteller am Coordinated Vulnerability Disclosure Programm	gemSpec_DS_Hersteller
A_27432	SBOM der gematik zur Verfügung stellen	gemSpec_DS_Hersteller
GS-A_2330-02	Hersteller: Schwachstellen-Management	gemSpec_DS_Hersteller
GS-A_2350-01	Produktunterstützung der Hersteller	gemSpec_DS_Hersteller
GS-A_2354-01	Produktunterstützung mit geeigneten Sicherheitstechnologien	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

ID	Bezeichnung	Quelle (Referenz)
GS-A_4946-01	Produktentwicklung: sichere Programmierung	gemSpec_DS_Hersteller
GS-A_4947-01	Produktentwicklung: Schutz der Vertraulichkeit und Integrität	gemSpec_DS_Hersteller
A_28407	ZETA Guard – Nachweisbarkeit verwendete Version des ZETA-Images	gemSpec_ZETA

3.2.4 Dokumentenprüfung

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

Tabelle 9: Festlegungen zur sicherheitstechnischen Eignung "Dokumentenprüfung"

ID	Bezeichnung	Quelle (Referenz)
	Es liegen keine Festlegungen vor	

3.3 Festlegungen zur elektrischen, mechanischen und physikalischen Eignung

Der Produkttyp erfordert den Nachweis der elektrischen, mechanischen und physikalischen Eignung. Sofern dabei spezifische Festlegungen der gematik zu beachten sind, werden diese nachfolgend aufgeführt. Der Nachweis erfolgt durch die Vorlage des Prüfberichts.

Tabelle 10: Festlegungen zur elektrischen, mechanischen und physikalischen Eignung

ID	Bezeichnung	Quelle (Referenz)
	Es liegen keine Festlegungen vor	

4 Produktypspezifische Merkmale

Es liegen keine optionalen Ausprägungen des Produktyps vor.

5 Anhang – Verzeichnisse

5.1 Abkürzungen

Kürzel	Erläuterung
ID	Identifikation
CC	Common Criteria

5.2 Tabellenverzeichnis

Tabelle 1: Dokumente mit normativen Festlegungen	6
Tabelle 2: Mitgeltende Dokumente und Web-Inhalte	6
Tabelle 3: Informative Dokumente und Web-Inhalte	7
Tabelle 4: Festlegungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"	8
Tabelle 5: Festlegungen zur funktionalen Eignung "Herstellererklärung"	12
Tabelle 6: Festlegungen zur sicherheitstechnischen Eignung "Produktgutachten"	16
Tabelle 7: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"	22
Tabelle 8: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung"	23
Tabelle 9: Festlegungen zur sicherheitstechnischen Eignung "Dokumentenprüfung"	24
Tabelle 10: Festlegungen zur elektrischen, mechanischen und physikalischen Eignung ..	24