

Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

Proof of Patient Presence Modul

Produkttyp Version: 1.0.0-0
Produkttyp Status: in Bearbeitung

Version: 1.0.0 CC2
Revision: 1714032
Stand: 03.09.2026
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemProdT_PoPP_Modul_PTV_1.0.0-0

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 Version auf Dokumentenebene	gemProdT_PoPP_Modul_PTV_1.0.0-0

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		zur Abstimmung freigegeben	gematik

Inhaltsverzeichnis

1 Einführung	4
1.1 Zielsetzung und Einordnung des Dokumentes	4
1.2 Zielgruppe	4
1.3 Geltungsbereich	5
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	11
3.2 Festlegungen zur sicherheitstechnischen Eignung	14
3.2.1 Produktgutachten	14
3.2.2 Sicherheitsgutachten	16
3.2.3 Herstellererklärung sicherheitstechnische Eignung.....	17
3.3 Festlegungen zur elektrischen, mechanischen und physikalischen Eignung	20
4 Produkttypspezifische Merkmale	21
5 Anhang – Verzeichnisse	22
5.1 Abkürzungen	22
5.2 Tabellenverzeichnis	22

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-Modul 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.

Offener Punkt: OP-PoPP-X (Hinweis)

Die gematik entwickelt derzeit ein neues Zulassungsverfahren für Apps für Versicherte. In diesem Zusammenhang wird zunächst ein allgemeiner App-Steckbrief erstellt, der künftig durch spezifische Steckbriefe für einzelne Module, beispielsweise das PoPP-Modul, ergänzt werden soll.

Der vorliegende Steckbrief umfasst derzeit noch sämtliche Anforderungen an das PoPP-Modul. Die Aufteilung in einen allgemeinen App-Steckbrief und modulspezifische Steckbriefe wird zu einem späteren Zeitpunkt erfolgen, voraussichtlich vor der geplanten Veröffentlichung der Dokumente zur PoPP-Stufe 2 im November 2026.

1.2 Zielgruppe

Der Produkttypsteckbrief richtet sich an PoPP-Modul-Hersteller und -Anbieter sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen. (Da der PoPP-Modul integraler Bestandteil der Versicherten-Apps der Kostenträger sein sollen, in denen auch das Authenticator-Modul der sektoralen IDPs implementiert ist, sind die Hersteller der Apps der Kostenträger und die Hersteller der sektoralen IDPs implizit ebenfalls gemeint.)

Das Dokument ist außerdem zu verwenden von:

- der gematik im Rahmen des Zulassungsverfahrens,
- dem Bundesamt für Sicherheit in der Informationstechnik (BSI),
- 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. gemPTV_ATV_Festlegungen, 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
gemKPT_Test	Testkonzept der TI	3.6.0
gemSpec_DS_Hersteller	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller	1.7.0
gemSpec_IDP_Frontend	Spezifikation Identity Provider - Frontend	2.0.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.49.1
gemSpec_Perf	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.86.0
gemSpec_PoPP_Modul	Spezifikation PoPP (Proof of Patient Presence) - Modul	1.0.0_CC4
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 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_Modul werden im Dokument [gemZul_Best_Titel] 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	Version Branch / Tag
[gemRL_PruefSichEig_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)
A_26673	Testumgebung in der Produktentwicklungsphase	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_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_27053	Freie Nutzung der erworbenen Testartefakte	gemKPT_Test
A_27100	Übergreifende Testmaßnahmen	gemKPT_Test
AF_10119	Abruf des "ACCESS_TOKEN"	gemSpec_IDP_Frontend

ID	Bezeichnung	Quelle (Referenz)
A_22294-01	Ermöglichen der Nutzung von sektoralen Identity Providern zur Authentisierung	gemSpec_IDP_Frontend
A_23086	Aufruf des Authorization-Servers	gemSpec_IDP_Frontend
A_28501	PoPP-Modul - Erstellen eines HTTP-Request zum Auslösen der Erstellung eines PoPP-Token mit GesundheitsID	gemSpec_PoPP_Modul
A_28503	PoPP-Modul - Ergebnisinterpretation nach Abschluss der Erstellung eines PoPP-Token mit GesundheitsID	gemSpec_PoPP_Modul
A_28511	PoPP-Modul - Anzeige einer Historie der erstellten PoPP-Token	gemSpec_PoPP_Modul
A_28512	PoPP-Modul - Anlage, Anzeige und Auswahl von Favoriten	gemSpec_PoPP_Modul
A_28514	PoPP-Modul - Erstellen eines HTTP-Request zur VZD-Abfrage	gemSpec_PoPP_Modul
A_28515	PoPP-Modul - Suche nach Inhabern einer Telematik-ID im FHIR-VZD	gemSpec_PoPP_Modul
A_28516	PoPP-Modul - Darstellung des Ergebnis der PoPP-Token-Erzeugung	gemSpec_PoPP_Modul
A_28600	Ergebnisverarbeitung der VZD-Abfrage	gemSpec_PoPP_Modul
A_28675	PoPP-Modul - unterstützte Authentisierungsverfahren	gemSpec_PoPP_Modul
A_29037	PoPP-Modul - Informationen zum Nachrichten-Datensatz	gemSpec_PoPP_Modul
A_29044	PoPP-Modul - "Push Notifications"	gemSpec_PoPP_Modul
A_30120	PoPP-Modul, QR-Code einlesen	gemSpec_PoPP_Modul
A_25339	ZETA Client - Exponential Backoff	gemSpec_ZETA
A_25732	ZETA Client - Unterstützung des Nutzers bei der Client-Registrierung	gemSpec_ZETA
A_25735-01	mobiler Client- Push-Benachrichtigung	gemSpec_ZETA
A_25758	ZETA Client - Erfassung Kontaktinformation für Offband-Verifikation	gemSpec_ZETA
A_25762-01	ZETA Client - Nutzerauthentifizierung - Unterstützung etablierter Identitäten und Dienste	gemSpec_ZETA

ID	Bezeichnung	Quelle (Referenz)
A_25781-01	ZETA Clients - OAuth2 Autorisierung	gemSpec_ZETA
A_25782	ZETA Client - OAuth2 Session Management	gemSpec_ZETA
A_25783-02	ZETA Client - Anweisungen aus HTTP Response Status Codes und Header folgen	gemSpec_ZETA
A_27007	ZETA Client - HTTP Statuscodes	gemSpec_ZETA
A_28425-01	ZETA Client, Service Discovery – if-none-match und etag	gemSpec_ZETA
A_28465	ZETA Client, Registrierung mit mehreren ZETA Guard	gemSpec_ZETA
A_29374	ZETA, Ablauf Service Discovery	gemSpec_ZETA
A_29380	ZETA, Ablauf Zugriff auf den RS mit ZETA/ASL	gemSpec_ZETA
A_29381	ZETA, Ablauf Zugriff auf den RS ohne ZETA/ASL	gemSpec_ZETA
A_29692	ZETA Client - Versionierung der Token Ausstellung	gemSpec_ZETA
A_29781	ZETA Client, Android Ablauf zur Schlüsselgenerierung	gemSpec_ZETA
A_29782	ZETA Client, Ablauf Apple OS Schlüsselgenerierung	gemSpec_ZETA
A_29809	ZETA Client, Ablauf Android Attestierung	gemSpec_ZETA
A_29810	ZETA Client, Ablauf Apple OS Attestierung	gemSpec_ZETA
A_29849	ZETA Client, Reaktion auf terminierte Session	gemSpec_ZETA
A_29852	ZETA Client, Auswertung des PEP-Fehler-Headers	gemSpec_ZETA
A_29853	ZETA Client, Weiterleitung von Fachdienst-Fehlern	gemSpec_ZETA
A_29859	ZETA Client, Behandlung von Step-Up-Fehlermeldungen	gemSpec_ZETA
A_29862	ZETA Client, zusätzliches DPoP Token bei ZETA/ASL Terminierung am Resource Server	gemSpec_ZETA
A_29933	ZETA Client – Ersatzgerät bei E-Mail-Verlust	gemSpec_ZETA
A_30002	ZETA Client - Serverseitiger Token-Widerruf bei Logout	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. zugesagt.

Tabelle 5: Festlegungen zur funktionalen Eignung "Herstellererklärung"

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_6519	Eigenverantwortlicher Test: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6519-01	Eigenverantwortlicher Test: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6526-03	Produkttypen: Bereitstellung	gemKPT_Test
A_23083	Auslösung der Benutzerauthentifizierung	gemSpec_IDP_Frontend
A_23084-01	Aufruf des Authenticator-Moduls	gemSpec_IDP_Frontend
A_23085-01	Registrierung des Anwendungsfrontends	gemSpec_IDP_Frontend
A_28782-01	Performance - Telemetriedatenlieferung - Konfiguration Datenlieferung ZETA Guard	gemSpec_Perf
A_28988	Performance - Telemetriedatenlieferung - Konfiguration Datenlieferung ZETA Guard - Sampling	gemSpec_Perf
A_27605	PoPP-Modul - Authentifizierung mit SSO im ePA-FdV	gemSpec_PoPP_Modul
A_28502	PoPP-Modul - Erstellen der "authorization_details" zum Auslösen der Erstellung eines PoPP-Token mit GesundheitsID	gemSpec_PoPP_Modul
A_28507	PoPP-Modul - Aufruf der Initialisierungs-Methode des ZETA Client	gemSpec_PoPP_Modul
A_28508	PoPP-Modul - Aufruf des ZETA Client zum Auslösen der Erstellung eines PoPP-Token mit GesundheitsID	gemSpec_PoPP_Modul
A_28510	PoPP-Modul - Erzeugung und Versand eines HTTP-Request an callBackURL einer Anbieter-App	gemSpec_PoPP_Modul
A_28618	PoPP-Modul - Aufruf des ZETA Client für die FHIR-VZD-Anfrage	gemSpec_PoPP_Modul
A_28677	PoPP-Modul - Abfrage des Status der Erstellung eines PoPP-Token	gemSpec_PoPP_Modul

ID	Bezeichnung	Quelle (Referenz)
A_29040	Implementierung des PoPP-Moduls in Kassen-App mit Authenticator-Modul des sektoralen IDP	gemSpec_PoPP_Modul
A_29041	Erreichbarkeit des PoPP-Modul aus Anbieter-App	gemSpec_PoPP_Modul
A_29045	PoPP-Modul - Unveränderbarkeit der WorkplaceID	gemSpec_PoPP_Modul
A_30012	Unterstützung von Anbieter-Apps	gemSpec_PoPP_Modul
A_30025	PoPP-Modul - Umsetzung anerkannter Standards zur Barrierefreiheit	gemSpec_PoPP_Modul
A_30075	PoPP-Modul - Zulassungsunterlagen	gemSpec_PoPP_Modul
A_30102	Anbieter-APP - Implementierung der Callback Schnittstelle	gemSpec_PoPP_Modul
A_30177	PoPP-Modul – Integration in Kassen-App bei Nutzung der GesundheitsID	gemSpec_PoPP_Modul
A_25338-01	ZETA Client - Authentifizierung beim Token Exchange	gemSpec_ZETA
A_25339	ZETA Client - Exponential Backoff	gemSpec_ZETA
A_25432-01	ZETA Client - Ablauf Client-Registrierung	gemSpec_ZETA
A_25434	ZETA Client - Client-Registrierung mit bestätigten Umgebungseigenschaften Android	gemSpec_ZETA
A_25732	ZETA Client - Unterstützung des Nutzers bei der Client-Registrierung	gemSpec_ZETA
A_25733	ZETA Client - Clientverwaltung und manuelle De-Registrierung	gemSpec_ZETA
A_25734	ZETA Client - Zugriffsprotokoll Client-Registrierung	gemSpec_ZETA
A_25758	ZETA Client - Erfassung Kontaktinformation für Offband-Verifikation	gemSpec_ZETA
A_25761	ZETA Client - Nutzerauthentifizierung mittels etablierter Standards	gemSpec_ZETA
A_25762-01	ZETA Client - Nutzerauthentifizierung - Unterstützung etablierter Identitäten und Dienste	gemSpec_ZETA
A_25766	ZETA Client - Client Credentials in TI Qualität	gemSpec_ZETA
A_25767	ZETA Client - Clientkey in JWT	gemSpec_ZETA

ID	Bezeichnung	Quelle (Referenz)
A_25768	ZETA Client - Client-Registrierung mit bestätigten Umgebungseigenschaften Apple	gemSpec_ZETA
A_25769	ZETA Client - Client Credentials sicher generieren und schützen	gemSpec_ZETA
A_25783-02	ZETA Client - Anweisungen aus HTTP Response Status Codes und Header folgen	gemSpec_ZETA
A_27379-03	ZETA Client - TLS OCSP Stapling Unterstützung	gemSpec_ZETA
A_28425-01	ZETA Client, Service Discovery – if-none-match und etag	gemSpec_ZETA
A_28426	ZETA Client, Service Discovery	gemSpec_ZETA
A_28524	ZETA Client, Konfigurationsdaten pro ZETA Guard Registrierung	gemSpec_ZETA
A_29376	ZETA, Ablauf Token Exchange mit Attestation	gemSpec_ZETA
A_29377	ZETA, Ablauf Token Exchange mit Refresh Token	gemSpec_ZETA
A_29380	ZETA, Ablauf Zugriff auf den RS mit ZETA/ASL	gemSpec_ZETA
A_29381	ZETA, Ablauf Zugriff auf den RS ohne ZETA/ASL	gemSpec_ZETA
A_29658	ZETA, Ablauf Client Registrierung für mobile Clients	gemSpec_ZETA
A_29659	ZETA, Ablauf OIDC Authentifizierung für mobile Clients	gemSpec_ZETA
A_29660	ZETA, Ablauf Authorization Request mit PAR	gemSpec_ZETA
A_29671	ZETA, Ablauf Nutzerauthentisierung am sektoralen IDP	gemSpec_ZETA
A_29672	ZETA, Ablauf Token-Bezug und Ausstellung der ZETA Token	gemSpec_ZETA
A_29692	ZETA Client - Versionierung der Token Ausstellung	gemSpec_ZETA
A_29723	Hersteller Clientsystem, Meldung von Client-Metadaten	gemSpec_ZETA
A_29733	ZETA, Ablauf OAuth Client Authentifizierung ohne Nutzer	gemSpec_ZETA
A_29849	ZETA Client, Reaktion auf terminierte Session	gemSpec_ZETA

ID	Bezeichnung	Quelle (Referenz)
A_29862	ZETA Client, zusätzliches DPoP Token bei ZETA/ASL Terminierung am Resource Server	gemSpec_ZETA
A_29921	Authorization Server - Schlüssel-Rollover mit Proof-of-Possession	gemSpec_ZETA
A_29933	ZETA Client – Ersatzgerät bei E-Mail-Verlust	gemSpec_ZETA
A_30001	ZETA, Ablauf Token Revocation	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_18464	TLS-Verbindungen, nicht Version 1.1	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
GS-A_4387	TLS-Verbindungen, nicht Version 1.0	gemSpec_Krypt
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt
A_27595	PoPP-Modul - QR-Code, Validierung und Warnung der VER	gemSpec_PoPP_Modul
A_27621	PoPP-Modul - Einmalige Einwilligung der VER in die Datennutzung durch PoPP-Service	gemSpec_PoPP_Modul
A_28488	PoPP-Modul - Anzeige von VZD-Informationen zu einer Telematik-ID	gemSpec_PoPP_Modul
A_29036	PoPP-Modul - Löschen von Einträgen in der Historie	gemSpec_PoPP_Modul
A_30033	PoPP-Modul - App - Unveränderte Kommunikation zum ZETA Client	gemSpec_PoPP_Modul

ID	Bezeichnung	Quelle (Referenz)
A_30048	PoPP-Modul - Einwilligung der VER in die Datennutzung durch SMC-B-Inhaber	gemSpec_PoPP_Modul
A_30130	PoPP-Modul - Sichere Speicherung von Informationen	gemSpec_PoPP_Modul
A_25338-01	ZETA Client - Authentifizierung beim Token Exchange	gemSpec_ZETA
A_25340-02	ZETA Client- Zertifikatsprüfung	gemSpec_ZETA
A_25733	ZETA Client - Clientverwaltung und manuelle De-Registrierung	gemSpec_ZETA
A_25734	ZETA Client - Zugriffsprotokoll Client-Registrierung	gemSpec_ZETA
A_25766	ZETA Client - Client Credentials in TI Qualität	gemSpec_ZETA
A_25769	ZETA Client - Client Credentials sicher generieren und schützen	gemSpec_ZETA
A_25782	ZETA Client - OAuth2 Session Management	gemSpec_ZETA
A_27378-01	ZETA Client - TLS	gemSpec_ZETA
A_27379-03	ZETA Client - TLS OCSP Stapling Unterstützung	gemSpec_ZETA
A_28426	ZETA Client, Service Discovery	gemSpec_ZETA
A_28465	ZETA Client, Registrierung mit mehreren ZETA Guard	gemSpec_ZETA
A_28524	ZETA Client, Konfigurationsdaten pro ZETA Guard Registrierung	gemSpec_ZETA
A_29374	ZETA, Ablauf Service Discovery	gemSpec_ZETA
A_29376	ZETA, Ablauf Token Exchange mit Attestation	gemSpec_ZETA
A_29377	ZETA, Ablauf Token Exchange mit Refresh Token	gemSpec_ZETA
A_29658	ZETA, Ablauf Client Registrierung für mobile Clients	gemSpec_ZETA
A_29659	ZETA, Ablauf OIDC Authentifizierung für mobile Clients	gemSpec_ZETA
A_29660	ZETA, Ablauf Authorization Request mit PAR	gemSpec_ZETA

ID	Bezeichnung	Quelle (Referenz)
A_29671	ZETA, Ablauf Nutzerauthentisierung am sektoralen IDP	gemSpec_ZETA
A_29672	ZETA, Ablauf Token-Bezug und Ausstellung der ZETA Token	gemSpec_ZETA
A_29733	ZETA, Ablauf OAuth Client Authentifizierung ohne Nutzer	gemSpec_ZETA
A_29781	ZETA Client, Android Ablauf zur Schlüsselgenerierung	gemSpec_ZETA
A_29782	ZETA Client, Ablauf Apple OS Schlüsselgenerierung	gemSpec_ZETA
A_29809	ZETA Client, Ablauf Android Attestierung	gemSpec_ZETA
A_29810	ZETA Client, Ablauf Apple OS Attestierung	gemSpec_ZETA
A_30001	ZETA, Ablauf Token Revocation	gemSpec_ZETA
A_30002	ZETA Client - Serverseitiger Token-Widerruf bei Logout	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

ID	Bezeichnung	Quelle (Referenz)
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_27429	Sicherer Softwareentwicklungsprozess bei Zulieferern	gemSpec_DS_Hersteller
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
A_25335	Hersteller Clientsystem - Hinweise und Maßnahmen sicherer Betrieb	gemSpec_ZETA
A_25336	Hersteller Clientsystem - Regelmäßige Updates	gemSpec_ZETA
A_25337	Hersteller Clientsystem - Registrierung für product_id	gemSpec_ZETA
A_28461-01	Informationspflicht des Client-Herstellers gegenüber Nutzern	gemSpec_ZETA

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

ID	Bezeichnung	Quelle (Referenz)
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_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_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
GS-A_4946-01	Produktentwicklung: sichere Programmierung	gemSpec_DS_Hersteller
GS-A_4947-01	Produktentwicklung: Schutz der Vertraulichkeit und Integrität	gemSpec_DS_Hersteller
A_23081	Automatisches Löschen von Token bei Inaktivität	gemSpec_IDP_Frontend
A_23082	Abruf und Anzeige der IDP Liste	gemSpec_IDP_Frontend

ID	Bezeichnung	Quelle (Referenz)
A_24756	Unterstützung eines SSO innerhalb eines Anwendungskontextes	gemSpec_IDP_Frontend
A_24916	Annahme eines Authorization Code	gemSpec_IDP_Frontend
A_18467	TLS-Verbindungen, Version 1.3	gemSpec_Krypt
GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
GS-A_5322	Weitere Vorgaben für TLS-Verbindungen	gemSpec_Krypt
GS-A_5526	TLS-Renegotiation-Indication-Extension	gemSpec_Krypt
A_25335	Hersteller Clientsystem - Hinweise und Maßnahmen sicherer Betrieb	gemSpec_ZETA
A_25336	Hersteller Clientsystem - Regelmäßige Updates	gemSpec_ZETA
A_25337	Hersteller Clientsystem - Registrierung für product_id	gemSpec_ZETA
A_25340-02	ZETA Client- Zertifikatsprüfung	gemSpec_ZETA
A_25432-01	ZETA Client - Ablauf Client-Registrierung	gemSpec_ZETA
A_25434	ZETA Client - Client-Registrierung mit bestätigten Umgebungseigenschaften Android	gemSpec_ZETA
A_25761	ZETA Client - Nutzerauthentifizierung mittels etablierter Standards	gemSpec_ZETA
A_25767	ZETA Client - Clientkey in JWT	gemSpec_ZETA
A_25768	ZETA Client - Client-Registrierung mit bestätigten Umgebungseigenschaften Apple	gemSpec_ZETA
A_25781-01	ZETA Clients - OAuth2 Autorisierung	gemSpec_ZETA
A_25802	ZETA Client - Einhaltung der BSI Steckbriefe.TR-03161-1	gemSpec_ZETA
A_26681-02	ZETA Client - Umsetzen eines ZETA/ASL-Kanals	gemSpec_ZETA
A_27378-01	ZETA Client - TLS	gemSpec_ZETA
A_28461-01	Informationspflicht des Client-Herstellers gegenüber Nutzern	gemSpec_ZETA
A_29723	Hersteller Clientsystem, Meldung von Client-Metadaten	gemSpec_ZETA

ID	Bezeichnung	Quelle (Referenz)
A_29921	Authorization Server - Schlüssel-Rollover mit Proof-of-Possession	gemSpec_ZETA

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 9: 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"	11
Tabelle 6: Festlegungen zur sicherheitstechnischen Eignung "Produktgutachten"	14
Tabelle 7: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"	16
Tabelle 8: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung"	17
Tabelle 9: Festlegungen zur elektrischen, mechanischen und physikalischen Eignung	20