Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

KOM-LE-Clientmodul

Produkttyp Version:	1.3.0-0
Produkttyp Status:	freigegeben
Version:	1.0.0
Revision:	111375
Stand:	15.05.2019
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemProdT_CM_KOMLE_PTV_1.3.0-0

Historie Produkttypversion und Produkttypsteckbrief

Historie Produkttypversion

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

Produkttypversion	Beschreibung der Änderung	Referenz
1.0.0	Initiale Version	[gemProdT_CM_KOMLE_PTV1.0.0]
1.1.0	Afo ergänzt	[gemProdT_CM_KOMLE_PTV1.1.0]
1.2.0	Weitere Anforderungen ergänzt, ORS1-Release 1.4	[gemProdT_CM_KOMLE_PTV1.2.0]
1.2.0-1	Anpassung auf Releasestand 1.6.4	[gemProdT_CM_KOMLE_PTV1.2.0-1]
1.2.1-0	Anpassung auf Releasestand 2.1.2	[gemProdT_CM_KOMLE_PTV1.2.1-0]
1.3.0-0	Anpassung auf Releasestand 3.1.0	[gemProdT_CM_KOMLE_PTV1.3.0-0]

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	15.05.2019		freigegeben	gematik

Inhaltsverzeichnis

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die Anforderungen der gematik an die Herstellung des Bestätigungsobjektes KOM-LE-Clientmodul oder verweist auf Dokumente, in denen verbindliche Anforderungen mit ggf. anderer Notation zu finden sind. Die Anforderungen bilden die Grundlage für die Erteilung von Bestätigungen durch die gematik.

Die Anforderungen werden über ihren Identifier, ihren Titel sowie die Dokumentenquelle referenziert. Die Anforderungen mit ihrem vollständigen, normativen Inhalt sind dem jeweils referenzierten Dokument zu entnehmen.

1.2 Zielgruppe

Der Produkttypsteckbrief für das Bestätigungsobjekt KOM-LE-Clientmodul richtet sich an KOM-LE-Clientmodul-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 Bestätigungsverfahrens
- dem Bundesamt für Sicherheit in der Informationstechnik (BSI)
- akkreditierten Materialprüflaboren
- Auditoren

Die Anforderungen beziehen sich auf den Hersteller des Bestätigungsobjektes KOM-LE-Clientmodul.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Bestätigungsverfahren 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 Bestätigungsverfahren für das Bestätigungsobjekt KOM-LE-Clientmodul sind nicht aufgeführt. Die geltenden Verfahren und Regelungen zur

Beantragung und Durchführung von Bestätigungsverfahren können der Homepage der gematik entnommen werden.

1.5 Methodik

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

Afo-ID: Identifiziert die Anforderung eindeutig im Gesamtbestand aller Festlegungen der gematik.

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

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

2 Dokumente

Die nachfolgenden Dokumente enthalten alle für das Bestätigungsobjekt KOM-LE-Clientmodul normativen Anforderungen.

Tabelle 1: Dokumente mit Anforderungen zu dem Bestätigungsobjekt

Dokumentenkürzel	Bezeichnung des Dokumentes	Version
gemSpec_DS_Hersteller	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller	1.1.0
gemSpec_CM_KOMLE	Spezifikation KOM-LE-Clientmodul	1.6.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.13.0
gemKPT_Test	Testkonzept der TI	2.3.0
gemSpec_OM	Übergreifende Spezifikation Operations und Maintenance	1.12.0
gemSpec_Perf	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.7.0
gemSpec_Net	Übergreifende Spezifikation Netzwerk	1.15.0
gemSMIME_KOMLE	S/MIME-Profil Kommunikation Leistungserbringer (KOM-LE)	1.1.0

Die Bestätigungsbedingungen für das Bestätigungsobjekt KOM-LE-Clientmodul werden im Dokument [gemZul_Best_KOM-LE] auf der Internetseite der gematik im Abschnitt Zulassung veröffentlicht.

Errata

Neben den vorgenannten Dokumenten werden auf der Internetseite der gematik bei Bedarf Errata-Dokumente mit normativen Ergänzungen bzw. Korrekturen zu den Spezifikationsdokumenten veröffentlicht. Sofern in den Errata der vorliegende Produkttyp benannt wird, sind diese bei der Umsetzung des Produkttyps entsprechend der Vorgabe in der Dokumentenlandkarte zu berücksichtigen. Dabei kann eine abweichende Produkttypversion festgelegt werden.

3 Blattanforderungen

Die folgenden Abschnitte verzeichnen alle für das Bestätigungsobjekt KOM-LE-Clientmodul normativen Anforderungen, die für die Entwicklung und den Betrieb von Produkten des Bestätigungsobjektes KOM-LE-Clientmodul notwendig sind (Blattanforderungen). Die Anforderungen sind gruppiert nach der Art der Nachweisführung ihrer Erfüllung als Grundlage der Bestätigung.

3.1 Anforderungen zur funktionalen Eignung

3.1.1 Produkttest/Produktübergreifender Test

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Anforderungen an den technischen Teil des Bestätigungsobjektes KOM-LE-Clientmodul verzeichnet, deren Umsetzung im Zuge von Bestätigungstests durch die gematik geprüft wird.

Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_17239	ECC-Migration, Unterstützung verschiedener kryptografischer Verfahren bei der TLS-Verwendung	gemSpec_CM_KOMLE
A_17464	ECC-Migration, Prüfung der ECC-Fähigkeit des Konnektors	gemSpec_CM_KOMLE
A_17472	ECC-Migration, Keine Verwendung von ECC-Verschlüsselungszertifikaten bei Konnektoren ohne ECC-Unterstützung	gemSpec_CM_KOMLE
KOM-LE-A_2004	Größe einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM-LE-A_2012	Authentisierung gegenüber dem MTA mit Benutzernamen und Passwort	gemSpec_CM_KOMLE
KOM-LE-A_2013	Unterstützung der Clientteile der Mechanismen PLAIN und LOGIN	gemSpec_CM_KOMLE
KOM-LE-A_2016	Schließen der SMTP-Verbindung mit dem Clientsystem	gemSpec_CM_KOMLE
KOM-LE-A_2017	Schließen der SMTP-Verbindung mit dem MTA	gemSpec_CM_KOMLE
KOM-LE-A_2021	Verhalten, wenn Nachricht nicht signiert werden kann	gemSpec_CM_KOMLE
KOM-LE-A_2022	Verschlüsseln der Nachricht mit den Verschlüsselungszertifikaten C.HCI.ENC bzw. C.HP.ENC	gemSpec_CM_KOMLE
KOM-LE-A_2024	Information des Absenders über Empfänger, für die	gemSpec_CM_KOMLE

	nicht verschlüsselt werden kann	
KOM−LE−A_2025	Abbruch des Sendens, wenn keine Verschlüsselung möglich	gemSpec_CM_KOMLE
KOM−LE−A_2028	Entfernen von Empfängern aus dem Header der Nachricht	gemSpec_CM_KOMLE
KOM−LE−A_2034	Authentifizierung gegenüber POP3-Server mit Benutzernamen und Passwort	gemSpec_CM_KOMLE
KOM−LE−A_2038	Schließen der POP3-Verbindung mit dem Clientsystem	gemSpec_CM_KOMLE
KOM−LE−A_2039	Schließen der POP3-Verbindung mit dem POP3-Server	gemSpec_CM_KOMLE
KOM−LE−A_2042	Entschlüsselung einer KOM-LE-SMIME-Nachricht	gemSpec_CM_KOMLE
KOM−LE−A_2046	Aufbau der Fehlernachricht bei fehlgeschlagener Entschlüsselung	gemSpec_CM_KOMLE
KOM−LE−A_2047	Fehlertexte bei fehlgeschlagener Entschlüsselung	gemSpec_CM_KOMLE
KOM−LE−A_2048	Prüfung der Signatur einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM−LE−A_2049	Ergebnis der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM−LE−A_2050	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM−LE−A_2057	Abbrechen des Signierens, wenn keine SM-B verfügbar ist	gemSpec_CM_KOMLE
KOM−LE−A_2058	Abbrechen des Signierens, wenn Freischaltung der erforderlichen SM-B fehlschlägt	gemSpec_CM_KOMLE
KOM−LE−A_2062	Abbrechen des Entschlüsseln, wenn die erforderliche Karte nicht verfügbar ist	gemSpec_CM_KOMLE
KOM−LE−A_2063	Abbrechen des Entschlüsseln, wenn Freischaltung der erforderlichen Karte fehlschlägt	gemSpec_CM_KOMLE
KOM−LE−A_2066	Verwendung von TLS für SMTP-Verbindungen mit Clientsystemen	gemSpec_CM_KOMLE
KOM−LE−A_2067	Verwendung von TLS für POP3-Verbindungen mit Clientsystemen	gemSpec_CM_KOMLE
KOM−LE−A_2070	Verbindungsaufbau mit dem Konnektor mit TLS	gemSpec_CM_KOMLE
KOM−LE−A_2071	TLS-Verbindung mit dem Konnektor mit oder ohne zertifikatsbasierter Client-Authentifizierung	gemSpec_CM_KOMLE
KOM−LE−A_2072	Verwendung von HTTP-Basic-Authentifizierung für TLS-Verbindungen mit dem Konnektor	gemSpec_CM_KOMLE

KOM−LE−A_2074	Verbindung zu KOM-LE-Fachdiensten immer über TLS	gemSpec_CM_KOMLE
KOM−LE−A_2079	Protokolldateien für Ablauf, Performance und Fehler	gemSpec_CM_KOMLE
KOM−LE−A_2080	Keine Protokollierung sensibler Daten	gemSpec_CM_KOMLE
KOM−LE−A_2081	Format der Protokolldateien	gemSpec_CM_KOMLE
KOM−LE−A_2082	Zugriff auf Protokolldateien einschränken	gemSpec_CM_KOMLE
KOM−LE−A_2083	Kopien der Protokolldateien	gemSpec_CM_KOMLE
KOM−LE−A_2084	Aktivierung und Deaktivierung der Protokollierung von Performanceinformationen	gemSpec_CM_KOMLE
KOM−LE−A_2085	Begrenzung des Speicherplatzes für Protokolldateien	gemSpec_CM_KOMLE
KOM−LE−A_2086	Vorgangsnummer für Protokolleinträge	gemSpec_CM_KOMLE
KOM−LE−A_2087	Felder zur Protokollierung des Ablaufs	gemSpec_CM_KOMLE
KOM−LE−A_2088	Felder zur Protokollierung der Performance	gemSpec_CM_KOMLE
KOM−LE−A_2089	Aktionen zur Protokollierung der Performance	gemSpec_CM_KOMLE
KOM−LE−A_2090	Felder zur Protokollierung der Fehler	gemSpec_CM_KOMLE
KOM−LE−A_2091	Konfigurationsparameter	gemSpec_CM_KOMLE
KOM−LE−A_2094	Skalierbarkeit	gemSpec_CM_KOMLE
KOM−LE−A_2176	Prüfen auf gültiges ENC-Zertifikat für den Empfänger im RCPT-Kommando	gemSpec_CM_KOMLE
KOM−LE−A_2178	Kein Versenden an Empfänger mit unterschiedlichen Telematik-IDs in den Verschlüsselungszertifikaten	gemSpec_CM_KOMLE
KOM−LE−A_2179	Vermerk in der Nachricht bei erfolgreicher Entschlüsselung	gemSpec_CM_KOMLE
KOM−LE−A_2180	Struktur des Signaturprüfberichts	gemSpec_CM_KOMLE
KOM−LE−A_2181	Authentifizierung von Clientsystemen gegenüber dem Clientmodul	gemSpec_CM_KOMLE
KOM−LE−A_2184	Standardwerte der Konfigurationsparameter	gemSpec_CM_KOMLE
KOM−LE−A_2192	Fehlernachricht bei Empfänger mit unterschiedlichen Telematik-IDs in den Verschlüsselungszertifikaten	gemSpec_CM_KOMLE
KOM−LE−A_2225	Update-Mechanismen	gemSpec_CM_KOMLE
KOM−LE−A_2230	Synchronisation mit der Systemzeit des Konnektors	gemSpec_CM_KOMLE
GS−A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt

GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt
GS-A_5530	TLS-Verbindungen, Version 1.1	gemSpec_Krypt
GS-A_5136	Performance – KOM-LE-Clientmodul – Bearbeitungszeit unter Last	gemSpec_Perf

3.1.2 Herstellererklärung funktionale Eignung

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Anforderungen an den technischen Teil des Bestätigungsobjektes KOM-LE-Clientmodul verzeichnet, deren Erfüllung der Hersteller bzw. der Anbieter durch eine Herstellererklärung belegt.

Tabelle 3: Anforderungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_2162	Kryptographisches Material in Entwicklungs- und Testumgebungen	gemKPT_Test
TIP1-A_4191	Keine Echtdaten in RU und TU	gemKPT_Test
TIP1-A_4929	Nachweis über Qualität der Zufallszahlen	gemKPT_Test
TIP1-A_5052	Dauerhafte Verfügbarkeit in der RU	gemKPT_Test
TIP1-A_6079	Updates von Referenzobjekten	gemKPT_Test
TIP1-A_6080	Softwarestand von Referenzobjekten	gemKPT_Test
TIP1-A_6081	Bereitstellung der Referenzobjekte	gemKPT_Test
TIP1-A_6082	Versionen der Referenzobjekte	gemKPT_Test
TIP1-A_6088	Unterstützung bei Fehlernachstellung	gemKPT_Test
TIP1-A_6093	Ausprägung der Referenzobjekte	gemKPT_Test
TIP1-A_6517	Eigenverantwortlicher Test: TBV	gemKPT_Test
TIP1-A_6518	Eigenverantwortlicher Test: TDI	gemKPT_Test
TIP1-A_6519	Eigenverantwortlicher Test: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6523	Zulassungstest: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6524	Testdokumentation gemäß Vorlagen	gemKPT_Test
TIP1-A_6526	Produkttypen: Bereitstellung	gemKPT_Test
TIP1-A_6529	Produkttypen: Mindestumfang der Interoperabilitätsprüfung	gemKPT_Test

TIP1−A_6532	Zulassung eines neuen Produkts: Aufgaben der TDI	gemKPT_Test
TIP1−A_6533	Zulassung eines neuen Produkts: Aufgaben der Hersteller und Anbieter	gemKPT_Test
TIP1−A_6536	Zulassung eines geänderten Produkts: Aufgaben der TDI	gemKPT_Test
TIP1−A_6537	Zulassung eines geänderten Produkts: Aufgaben der Hersteller und Anbieter	gemKPT_Test
TIP1−A_6538	Durchführung von Produkttests	gemKPT_Test
TIP1−A_6539	Durchführung von Produktübergreifenden Tests	gemKPT_Test
TIP1−A_6772	Partnerprodukte bei Interoperabilitätstests	gemKPT_Test
TIP1−A_7335	Bereitstellung der Testdokumentation	gemKPT_Test
TIP1−A_7358	Qualität des Produktmusters	gemKPT_Test
KOM−LE−A_2095	Reihenfolge Signatur und Verschlüsselung	gemSMIME_KOMLE
KOM−LE−A_2096	Signatur und Verschlüsselung entsprechend S/MIME V3.2	gemSMIME_KOMLE
KOM−LE−A_2097	Verschlüsselter Body	gemSMIME_KOMLE
KOM−LE−A_2098	Header der äußeren Nachricht	gemSMIME_KOMLE
KOM−LE−A_2099	Header-Element X-KOM-LE-Version	gemSMIME_KOMLE
KOM−LE−A_2100	Wert Header-Element X-KOM-LE-Version	gemSMIME_KOMLE
KOM−LE−A_2101	Neues message-id Element	gemSMIME_KOMLE
KOM−LE−A_2102	Wert subject Header-Element	gemSMIME_KOMLE
KOM−LE−A_2103	Opak-Signatur	gemSMIME_KOMLE
KOM−LE−A_2104	Typ S/MIME-Verschlüsselung	gemSMIME_KOMLE
KOM−LE−A_2106	AuthenticatedEnvelopedData ohne originatorInfo	gemSMIME_KOMLE
KOM−LE−A_2107	AuthenticatedEnvelopedData mit unauthAttrs	gemSMIME_KOMLE
KOM−LE−A_2108	Schlüsselverwaltungsalgorithmus	gemSMIME_KOMLE
KOM−LE−A_2109	Zertifikatsidentifizierung bei keyTransRecipientInfo	gemSMIME_KOMLE
KOM−LE−A_2111	RecipientInfo Element für Sender	gemSMIME_KOMLE
KOM−LE−A_2112	Inhalt von authEncryptedContentInfo	gemSMIME_KOMLE
KOM−LE−A_2114	Attribut recipient-emails	gemSMIME_KOMLE
KOM−LE−A_2115	Referenzierte Zertifikate in RecipientEmail	gemSMIME_KOMLE

KOM−LE−A_2116	E-Mail-Adresse des Zertifikatsinhabers	gemSMIME_KOMLE
KOM−LE−A_2117	Zertifikatsidentifikation über Aussteller und Seriennummer	gemSMIME_KOMLE
KOM−LE−A_2118	Keine crls in signed-data	gemSMIME_KOMLE
KOM−LE−A_2119	Signed-data muss certificates enthalten	gemSMIME_KOMLE
KOM−LE−A_2121	Signierte Daten im Element eContent	gemSMIME_KOMLE
KOM−LE−A_2122	Signaturzertifikat im Element Zertifikate	gemSMIME_KOMLE
KOM−LE−A_2123	Genau ein signerInfo Element	gemSMIME_KOMLE
KOM−LE−A_2124	Inhalt Element sid aus Unterzeichnerinformationen	gemSMIME_KOMLE
KOM−LE−A_2125	Aussteller und Seriennummer entsprechend Signaturzertifikat	gemSMIME_KOMLE
KOM−LE−A_2126	Unterzeichnerinformationen ohne unsignedAttrs	gemSMIME_KOMLE
KOM−LE−A_2127	Unterzeichnerinformationen mit signiertem Attribut recipient-emails	gemSMIME_KOMLE
KOM−LE−A_2128	Zertifikate für Verschlüsselung	gemSMIME_KOMLE
KOM−LE−A_2129	Signaturzertifikat	gemSMIME_KOMLE
KOM−LE−A_2003	Unterstützung von E-Mail-Clients	gemSpec_CM_KOMLE
KOM−LE−A_2005	Keine persistente Speicherung von Nachrichten	gemSpec_CM_KOMLE
KOM−LE−A_2006	Einzuhaltende Standards beim Senden und Empfangen	gemSpec_CM_KOMLE
KOM−LE−A_2007	SMTP Begrüßung	gemSpec_CM_KOMLE
KOM−LE−A_2008	Initialer SMTP-Dialog	gemSpec_CM_KOMLE
KOM−LE−A_2009	Unterstützung der Serverteile der Mechanismen PLAIN und LOGIN	gemSpec_CM_KOMLE
KOM−LE−A_2010	Extrahieren von MTA-Adresse, Portnummer und Kartenaufrufkontext	gemSpec_CM_KOMLE
KOM−LE−A_2011	Verbindungsaufbau mit dem MTA über MTA-Adresse und Portnummer	gemSpec_CM_KOMLE
KOM−LE−A_2014	Authentifizierung gegenüber MTA mit anderen Mechanismen als PLAIN und LOGIN	gemSpec_CM_KOMLE
KOM−LE−A_2015	Ergebnis des Verbindungsaufbaus mit dem MTA	gemSpec_CM_KOMLE
KOM−LE−A_2018	Weiterleitung von SMTP-Meldungen und Antwortcodes	gemSpec_CM_KOMLE

KOM−LE−A_2019	Signatur und Verschlüsselung entsprechend KOM-LE-S/MiME-Profil	gemSpec_CM_KOMLE
KOM−LE−A_2020	Signieren der Nachricht mit dem Schlüssel Prk.HCI.OSIG	gemSpec_CM_KOMLE
KOM−LE−A_2023	Verschlüsselungszertifikate aus dem Verzeichnisdienst	gemSpec_CM_KOMLE
KOM−LE−A_2026	Cachen von Verschlüsselungszertifikaten	gemSpec_CM_KOMLE
KOM−LE−A_2027	Befüllung des recipient-emails Attributs	gemSpec_CM_KOMLE
KOM−LE−A_2029	Aufbereitung einer vom Clientsystem erhaltenen KOM-LE-S/MIME-Nachricht	gemSpec_CM_KOMLE
KOM−LE−A_2030	POP3-Dialog zur Authentifizierung	gemSpec_CM_KOMLE
KOM−LE−A_2031	Unterstützung der Serverteile der Mechanismen USER/PASS und SASL PLAIN	gemSpec_CM_KOMLE
KOM−LE−A_2032	Extrahieren der Zugangsdaten des POP3-Servers und des Kartenaufrufkontextes	gemSpec_CM_KOMLE
KOM−LE−A_2033	Verbindungsaufbau mit POP3-Server über Adresse und Portnummer	gemSpec_CM_KOMLE
KOM−LE−A_2035	Unterstützung der Clientteile der Mechanismen USER/PASS und SASL PLAIN	gemSpec_CM_KOMLE
KOM−LE−A_2036	Authentifizierung gegenüber POP3-Server mit anderen Mechanismen als USER/PASS oder SASL PLAIN	gemSpec_CM_KOMLE
KOM−LE−A_2037	Antwortcodes des Verbindungsaufbaus mit dem POP3-Server	gemSpec_CM_KOMLE
KOM−LE−A_2040	Übermittlung von POP3-Kommandos und -Meldungen nach erfolgreicher Authentifizierung	gemSpec_CM_KOMLE
KOM−LE−A_2041	Setzen des Parameters <N> des TOP-Kommandos auf Null	gemSpec_CM_KOMLE
KOM−LE−A_2043	Beachtung des recipient-emails Attributs bei der Entschlüsselung	gemSpec_CM_KOMLE
KOM−LE−A_2044	E-Mail-Adresse des den Abholvorgang auslösenden Nutzers	gemSpec_CM_KOMLE
KOM−LE−A_2052	Quellen zur Ermittlung der SM-B des Senders beim Signieren	gemSpec_CM_KOMLE
KOM−LE−A_2059	Verwendung des recipient-emails Attributs beim Entschlüsseln	gemSpec_CM_KOMLE
KOM−LE−A_2060	Quellen zur Ermittlung der erforderlichen Karte beim Entschlüsseln	gemSpec_CM_KOMLE

KOM−LE−A_2061	Speichern von Zuordnungen im Cache beim Entschlüsseln	gemSpec_CM_KOMLE
KOM−LE−A_2064	Verwendung von X.509-Identitäten bei der TLS-Authentifizierung	gemSpec_CM_KOMLE
KOM−LE−A_2076	Ermittlung der Serviceendpunkte des Konnektors	gemSpec_CM_KOMLE
KOM−LE−A_2077	Auswahl der unterstützten Version einer Dienstschnittstelle des Konnektors	gemSpec_CM_KOMLE
KOM−LE−A_2190	Übergabe des recipient-emails Attributs beim Signieren	gemSpec_CM_KOMLE
KOM−LE−A_2191	Übergabe des recipient-emails Attributs beim Verschlülsseln	gemSpec_CM_KOMLE
KOM−LE−A_2193	Verpacken des verschlüsselten CMS-Objektes	gemSpec_CM_KOMLE
KOM−LE−A_2300	Import des Schlüsselmaterial für TLS-Verbindungen	gemSpec_CM_KOMLE
KOM−LE−A_2301	Individuelles Schlüsselmaterial für TLS-Verbindungen	gemSpec_CM_KOMLE
A_17124	TLS-Verbindungen (ECC-Migration)	gemSpec_Krypt
A_17205	Signatur der TSL: Signieren und Prüfen (ECC-Migration)	gemSpec_Krypt
A_17206	XML-Signaturen (ECC-Migration)	gemSpec_Krypt
A_17220	Verschlüsselung binärer Daten (ECIES) (ECC-Migration)	gemSpec_Krypt
A_17221	XML-Verschlüsselung (ECIES) (ECC-Migration)	gemSpec_Krypt
A_17322	TLS-Verbindungen zulässige Ciphersuiten (ECC-Migration)	gemSpec_Krypt
A_17360	XML-Signaturen (Dokumente) (ECC-Migration)	gemSpec_Krypt
A_17775	TLS-Verbindungen Reihenfolge Ciphersuiten (ECC-Migration)	gemSpec_Krypt
GS−A_4359	X.509-Identitäten für die Durchführung einer TLS-Authentifizierung	gemSpec_Krypt
GS−A_5526	TLS-Renegotiation-Indication-Extension	gemSpec_Krypt
GS−A_5542	TLS-Verbindungen (fatal Alert bei Abbrüchen)	gemSpec_Krypt
GS−A_4831	Standards für IPv4	gemSpec_Net
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
GS−A_5038	Festlegungen zur Vergabe einer Produktversion	gemSpec_OM
GS−A_5039	Änderung der Produktversion bei Änderungen der Produkttypversion	gemSpec_OM

3.2 Anforderungen zur sicherheitstechnischen Eignung

3.2.1 Sicherheitstechnische Eignung: Zertifizierung nach Technischer Richtlinie

In diesem Abschnitt sind Anforderungen verzeichnet, deren Umsetzung im Zuge einer Prüfung gemäß TR TR-03143 „eHealth G2-COS Konsistenz-Prüftool“ nachgewiesen werden muss. Der Nachweis erfolgt durch die Vorlage des Prüfberichts eines für diese Prüfung zugelassenen Prüflabors.

Tabelle 4: Anforderungen zur sicherheitstechnischen Eignung " Sich.techn. Eignung: Zertifizierung nach Technischer Richtlinie"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_17124	TLS-Verbindungen (ECC-Migration)	gemSpec_Krypt
A_17220	Verschlüsselung binärer Daten (ECIES) (ECC-Migration)	gemSpec_Krypt

3.2.2 CC-Evaluierung

In diesem Abschnitt sind Anforderungen verzeichnet, deren Umsetzung im Zuge einer Zertifizierung gemäß Common Criteria [CC] nachgewiesen werden muss. Der Nachweis erfolgt durch die Vorlage des IT-Sicherheitszertifikats bei der gematik.

Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "CC-Evaluierung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_17206	XML-Signaturen (ECC-Migration)	gemSpec_Krypt
A_17221	XML-Verschlüsselung (ECIES) (ECC-Migration)	gemSpec_Krypt

3.2.3 Herstellererklärung sicherheitstechnische Eignung

In diesem Abschnitt sind alle Anforderungen an das Bestätigungsobjekt KOM-LE-Clientmodul verzeichnet, deren Erfüllung der Hersteller bzw. der Anbieter zum Nachweis der sicherheitstechnischen Eignung durch eine Herstellererklärung belegt.

Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
KOM−LE−A_2045	Entschlüsselung nur mit Schlüsseln des abholenden Nutzers	gemSpec_CM_KOMLE
KOM−LE−A_2048	Prüfung der Signatur einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM−LE−A_2050	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM−LE−A_2065	Schutz des Schlüsselspeichers für TLS-Verbindungen	gemSpec_CM_KOMLE
KOM−LE−A_2075	Prüfung von TLS-Server-Zertifikaten	gemSpec_CM_KOMLE
KOM−LE−A_2177	Verwenden von SignDocument und EncryptDocument	gemSpec_CM_KOMLE
KOM−LE−A_2182	Verwendung des vom KOM-LE-Anbieter zur Verfügung gestellten Zertifikats für die clientseitige TLS-Authentifizierung	gemSpec_CM_KOMLE
KOM−LE−A_2299	Vorgehen bei Signatur und Verschlüsselung einer KOM-LE Nachricht	gemSpec_CM_KOMLE
A_17178	Produktentwicklung: Basisschutz gegen OWASP Top 10 Risiken	gemSpec_DS_Hersteller
A_17179	Auslieferung aktueller zusätzlicher Softwarekomponenten	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_2524−01	Produktunterstützung: Nutzung des Problem-Management-Prozesses	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_17205	Signatur der TSL: Signieren und Prüfen (ECC-Migration)	gemSpec_Krypt

A_17322	TLS-Verbindungen zulässige Ciphersuiten (ECC-Migration)	gemSpec_Krypt
A_17360	XML-Signaturen (Dokumente) (ECC-Migration)	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_5526	TLS-Renegotiation-Indication-Extension	gemSpec_Krypt
GS-A_5530	TLS-Verbindungen, Version 1.1	gemSpec_Krypt

3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung

In diesem Abschnitt sind Anforderungen verzeichnet, deren Umsetzung im Zuge einer elektrischen, mechanischen und physikalischen Prüfung nachgewiesen werden muss. Der Nachweis erfolgt durch die Vorlage des Prüfberichts.

Tabelle 7: Anforderungen zur elektrischen, mechanischen und physikalischen Eignung

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Es liegen keine Anforderungen vor	

4 Produkttypspezifische Merkmale

Nachfolgend werden die optionalen Ausprägungen des Produkttyps beschrieben oder (nicht Zutreffendes streichen)

Es liegen keine optionalen Ausprägungen des Produkttyps vor.

5 Anhang A – Verzeichnisse

5.1 Abkürzungen

Kürzel	Erläuterung
Afo-ID	Anforderungs-Identifikation
CC	Common Criteria

5.2 Tabellenverzeichnis

5.3 Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

[Quelle]	Herausgeber: Titel, Version
[CC]	Internationaler Standard: Common Criteria for Information Technology Security Evaluation https://www.commoncriteriaportal.org/cc/
[gemRL_PruefSichEig]	gematik: Richtlinie zur Prüfung der Sicherheitseignung
[gemZul_Best_KOM-LE]	gematik: Bestätigung Produkte hier: Fachdienst-KOM-LE bzw. KOM-LE-Clientmodul