Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

Integriertes Clientmodul KIM (KIM-iCM)

Produkttyp Version:	1.0.0-1
Produkttyp Status:	freigegeben

Version:	1.0.1
Revision:	1168359
Stand:	18.03.2025
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemProdT_iCM_KIM_PTV_1.0.0-1

gemProdT_iCM_KIM_PTV

Historie Produkttypversion

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

Produkttypversion	Beschreibung der Änderung	Referenz
1.0.0-0	Initiale Version auf Dokumentenebene	gemProdT_iCM_KIM_PTV_1.0.0-0
1.0.0-1	Anpassung auf Releasestand KIM 1.5.2-9-1	gemProdT_iCM_KIM_PTV_1.0.0-1

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	14.03.2025		freigegeben für Releasestand KIM 1.5.2-9-1	gematik
1.0.1	18.03.2025		Ergänzung von Afos	gematik

Inhaltsverzeichnis

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Steckbrief enthält alle verbindlichen normativen Festlegungen der gematik an die Herstellung eines Integriertes KIM-Clientmoduls.

Die normativen Festlegungen sind die Grundlage für die Erteilung einer Zulassung durch die gematik.

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 für das Zulassungsobjekt Integriertes KIM-Clientmodul richtet sich an Hersteller von Integriertes KIM-Clientmodulen sowie an Hersteller 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)
- Auditoren

Die normativen Festlegungen beziehen sich auf den Hersteller des Zulassungsobjektes Integriertes KIM-Clientmodul.

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 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 das Zulassungsobjekt Integriertes KIM-Clientmodul 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

Dokumentenkürzel	Bezeichnung des Dokumentes	Version
gemSMIME_KOMLE	S/MIME-Profil Kommunikation Leistungserbringer (KOM-LE)	1.7.0
gemSpec_CM_KOMLE	Spezifikation KOM-LE-Clientmodul	1.16.6
gemSpec_DS_Hersteller	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller	1.5.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.27.0
gemSpec_Perf	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.27.0

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
[kim openapi]	KIM OpenAPI Schnittstellen-Definitionen: https://github.com/gematik/api-kim/tree/main/src/openapi	main

***) vorherige Registrierung notwendig*

Die Zulassungsbedingungen für das Zulassungsobjekt Integriertes KIM-Clientmodul werden im Dokument [gemZul_Prod_KOM-LE] 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

[api-kim]	KIM - Dokumentation: https://github.com/gematik/api-kim	main
[gemZul_Prod_KOM-LE]	gematik: Zulassung Produkte hier: Integriertes KOM-LE-Clientmodul: https://fachportal.gematik.de/schnelleinstieg/downloadcenter/zulassungs-bestaetigungsantraege-verfahrensbeschreibungen	

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 das Bestätigungsobjekt Integriertes KIM-Clientmodul normativen Festlegungen, die für die Entwicklung und den Betrieb von Produkten des Bestätigungsobjektes Integriertes KIM-Clientmodul notwendig sind. Die Festlegungen sind gruppiert nach der Art der Nachweisführung ihrer Erfüllung als Grundlage der 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 Bestätigungsobjektes Integriertes KIM-Clientmodul verzeichnet, deren Umsetzung im Zuge von Bestätigungstests durch die gematik geprüft wird.

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

ID	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
A_18783	Import Schlüssel und Zertifikat als PKCS#12 Datei	gemSpec_CM_KOMLE
A_19355-01	Prüfen der Nachrichtengröße	gemSpec_CM_KOMLE
A_19356-06	Prüfen der Version des Empfängers	gemSpec_CM_KOMLE
A_19357-02	Verarbeitung einer Client-Mail größer 15 MiB	gemSpec_CM_KOMLE
A_19358-01	Erzeugung symmetrischer Schlüssel	gemSpec_CM_KOMLE
A_19359-10	Einbetten von Informationen großer Nachrichten	gemSpec_CM_KOMLE
A_19360-02	Verschlüsselung der E-Mail-Daten	gemSpec_CM_KOMLE
A_19361-01	Lokalisierung des KIM Fachdienstes	gemSpec_CM_KOMLE
A_19362-01	Client Authentifizierung für Upload am KAS	gemSpec_CM_KOMLE

A_19364-02	Freigabelink in die Mail aufnehmen	gemSpec_CM_KOMLE
A_19365-02	Senden der KOM-LE-Nachricht	gemSpec_CM_KOMLE
A_19367	Empfangen der Nachricht	gemSpec_CM_KOMLE
A_19368-01	Client Authentifizierung für Download am KAS	gemSpec_CM_KOMLE
A_19369-02	Ermittlung von Informationen der auf dem KAS abgelegten E-Mail-Daten	gemSpec_CM_KOMLE
A_19370-04	Download von E-Mail-Daten	gemSpec_CM_KOMLE
A_19371-04	Entschlüsselung vom KAS abgerufener E-Mail-Daten	gemSpec_CM_KOMLE
A_19372-03	Prüfen der E-Mail-Daten	gemSpec_CM_KOMLE
A_19374-03	Zusammensetzen der Mail	gemSpec_CM_KOMLE
A_19453	Aktualisierung PKCS#12-Datei Administrationsmodul	gemSpec_CM_KOMLE
A_19456-03	Domain Fachdienst Administrationsmodul	gemSpec_CM_KOMLE
A_19457-04	Client Authentisierung Administrationsmodul	gemSpec_CM_KOMLE
A_19458-03	Initiale Anmeldung KOM-LE-Teilnehmer Administrationsmodul	gemSpec_CM_KOMLE
A_19459	Registrierung Aufruf KOM-LE-Teilnehmer Administrationsmodul	gemSpec_CM_KOMLE
A_19460	Registrierungsdialog KOM-LE-Teilnehmer Administrationsmodul	gemSpec_CM_KOMLE
A_19462	Registrierungsfehler KOM-LE-Teilnehmer Administrationsmodul	gemSpec_CM_KOMLE
A_19463	Deregistrierung Aufruf KOM-LE-Teilnehmer Administrationsmodul	gemSpec_CM_KOMLE
A_19464-03	Deregistrierungsdialog KOM-LE-Teilnehmer Administrationsmodul	gemSpec_CM_KOMLE
A_19468-02	Beantragen und Herunterladen der PKCS#12 Datei	gemSpec_CM_KOMLE
A_19488-02	E-Mail-Kategorisierung	gemSpec_CM_KOMLE
A_19513	Bereitstellung Zertifikate aus PKCS#12-Datei	gemSpec_CM_KOMLE
A_19523	Service-Discovery Administrationsmodul	gemSpec_CM_KOMLE

A_20628	Beachtung des received-Header-Attributs bei der Entschlüsselung	gemSpec_CM_KOMLE
A_20650-07	Übermittlung von Fehlernachrichten	gemSpec_CM_KOMLE
A_21223-01	Verbindungen mit dem Konnektor bei LDAP	gemSpec_CM_KOMLE
A_21236-01	Headerfeld „Return-Path“ der äußeren Nachricht	gemSpec_CM_KOMLE
A_21380	Verwaltung von Abwesenheitsnotizen	gemSpec_CM_KOMLE
A_21381-01	Automatischer Abruf der PKCS#12-Datei	gemSpec_CM_KOMLE
A_21382	Generierung eines symmetrischen Schlüssels für die PKCS#12-Datei	gemSpec_CM_KOMLE
A_21387-01	Prüfung der verwendeten Clientmodul-Version beim Senden	gemSpec_CM_KOMLE
A_21388-03	Übermittlung der Produkt- und Produkttypversion	gemSpec_CM_KOMLE
A_21390	Prüfung auf eine KOM-LE-S/MIME-Nachricht	gemSpec_CM_KOMLE
A_21391-02	Auswertung des X-KOM-LE-Version Header Elements	gemSpec_CM_KOMLE
A_21396	Darstellung von Ereignissen	gemSpec_CM_KOMLE
A_22340	Cachen vom KOM-LE-Versionen	gemSpec_CM_KOMLE
A_22412-01	Behandlung von Zugriffs-Limitierung	gemSpec_CM_KOMLE
A_22416	Anfragen von technischen Konfigurationsdaten	gemSpec_CM_KOMLE
A_22417-01	Einfügen des Ablaufdatums in den äußeren Mail-Header	gemSpec_CM_KOMLE
A_22427-01	I_Attachment_Services - Content-Length	gemSpec_CM_KOMLE
A_23165	Verhalten bei fehlgeschlagener Integritätsprüfung	gemSpec_CM_KOMLE
A_23467	Übermittlung der KAS-Datenmenge	gemSpec_CM_KOMLE
A_23505	Bereitschaft zum Empfang großer Nachrichten	gemSpec_CM_KOMLE
A_23512-02	Auswertung der KOM-LE-Version bei Nachrichten mit KAS-Content	gemSpec_CM_KOMLE
A_24332	Vertrauenswürdige Konnektor-Serverzertifikate	gemSpec_CM_KOMLE

A_24795	Vereinfachung Fingerprint-Abgleich - Einheitliche Darstellung	gemSpec_CM_KOMLE
A_27360	Übermittlung der Größe der verschlüsselten KAS-Datenmenge	gemSpec_CM_KOMLE
KOM-LE-A_2004-01	Verarbeitung einer Client-Mail bis zu 15 MiB	gemSpec_CM_KOMLE
KOM-LE-A_2013	Unterstützung der Clientteile der Mechanismen PLAIN und LOGIN	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_2028	Entfernen von Empfängern aus dem Header der Nachricht	gemSpec_CM_KOMLE
KOM-LE-A_2042	Entschlüsselung einer KOM-LE-SMIME-Nachricht	gemSpec_CM_KOMLE
KOM-LE-A_2047-02	Fehlertexte bei fehlgeschlagener Entschlüsselung	gemSpec_CM_KOMLE
KOM-LE-A_2048-01	Prüfung der Signatur und Integrität 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_2064-02	Verwendung von X.509-Identitäten bei der TLS-Authentifizierung	gemSpec_CM_KOMLE
KOM-LE-A_2070-01	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_2074-01	Verbindung zu KOM-LE-Fachdiensten immer über TLS	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_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_2176-01	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_2225	Update-Mechanismen	gemSpec_CM_KOMLE
A_21275-01	TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake	gemSpec_Krypt
GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
GS-A_5035	Nichtverwendung des SSL-Protokolls	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 Festlegungen an den technischen Teil des Bestätigungsobjektes Integriertes KIM-Clientmodul verzeichnet, deren Erfüllung der Hersteller bzw. der Anbieter durch eine Herstellererklärung belegt.

Tabelle 5: Festlegungen zur funktionalen Eignung "Herstellererklärung"

ID	Bezeichnung	Quelle (Referenz)
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_2098-03	Header der äußeren Nachricht	gemSMIME_KOMLE
KOM-LE-A_2099	Header-Element X-KOM-LE-Version	gemSMIME_KOMLE
KOM-LE-A_2100-02	Wert Header-Element X-KOM-LE-Version	gemSMIME_KOMLE
KOM-LE-A_2101-01	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_2111-01	RecipientInfo Element für Sender	gemSMIME_KOMLE
KOM-LE-A_2112	Inhalt von authEncryptedContentInfo	gemSMIME_KOMLE
KOM-LE-A_2114-01	Attribut recipient-emails	gemSMIME_KOMLE
KOM-LE-A_2115-02	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
A_19454	Dialoggestaltung Administrationsmodul	gemSpec_CM_KOMLE
A_19455	Formulardialoge Administrationsmodul	gemSpec_CM_KOMLE
A_20188	Formulardialoge Administrationsmodul - außerhalb der Leistungserbringerumgebung	gemSpec_CM_KOMLE
A_20773	I_AccountManager_Service Zeichensatz Clientmodul	gemSpec_CM_KOMLE
A_22348-01	Caching der Prüfergebnisse der TLS-Server-Zertifikate	gemSpec_CM_KOMLE
A_24333	CA Prüfung für Konnektor-Serverzertifikate	gemSpec_CM_KOMLE
A_24796	Vereinfachung Fingerprint-Abgleich - Vergleichstool	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_2014	Authentifizierung gegenüber MTA mit anderen Mechanismen als PLAIN und LOGIN	gemSpec_CM_KOMLE
KOM-LE-A_2015-01	Ergebnis des Verbindungsaufbaus mit dem MTA	gemSpec_CM_KOMLE
KOM-LE-A_2019	Signatur und Verschlüsselung entsprechend KOM-LE-S/MiME-Profil	gemSpec_CM_KOMLE
KOM-LE-A_2020-01	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_2035	Unterstützung der Clientteile der Mechanismen	gemSpec_CM_KOMLE

	USER/PASS und SASL PLAIN	
KOM-LE-A_2036	Authentifizierung gegenüber POP3-Server mit anderen Mechanismen als USER/PASS oder SASL PLAIN	gemSpec_CM_KOMLE
KOM-LE-A_2043	Beachtung des recipient-emails Attributs bei der Entschlüsselung	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_2060-01	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_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_2091-01	Konfigurationsparameter	gemSpec_CM_KOMLE
KOM-LE-A_2184	Standardwerte der Konfigurationsparameter	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 Verschlüsseln	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_2301-03	Individuelles Schlüsselmaterial für TLS-Verbindungen	gemSpec_CM_KOMLE
A_17124-01	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_17221-01	XML-Verschlüsselung (ECIES) (ECC-Migration)	gemSpec_Krypt
A_17322	TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (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_4359-02	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

3.2 Festlegungen zur sicherheitstechnischen Eignung

3.2.1 Herstellererklärung sicherheitstechnische Eignung

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

Tabelle 6: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung"

ID	Bezeichnung	Quelle (Referenz)
KOM-LE-A_2048-01	Prüfung der Signatur und Integrität einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM-LE-A_2065	Schutz des Schlüsselspeichers für TLS-Verbindungen	gemSpec_CM_KOMLE
KOM-LE-A_2075-01	Prüfung von TLS-Server-Zertifikaten	gemSpec_CM_KOMLE
KOM-LE-A_2177	Verwenden von SignDocument und EncryptDocument	gemSpec_CM_KOMLE
KOM-LE-A_2182-01	Verwendung des vom KOM-LE-Anbieter zur Verfügung gestellten Zertifikats für die clientseitige TLS-Authentifizierung	gemSpec_CM_KOMLE
KOM-LE-A_2299-02	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	gemSpec_DS_Hersteller

	Softwarekomponenten	
A_23445	Beteiligung der Hersteller am Coordinated Vulnerability Disclosure Programm	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_17124-01	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_17221-01	XML-Verschlüsselung (ECIES) (ECC-Migration)	gemSpec_Krypt
A_17322	TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration)	gemSpec_Krypt
A_17360	XML-Signaturen (Dokumente) (ECC-Migration)	gemSpec_Krypt
A_18464	TLS-Verbindungen, nicht Version 1.1	gemSpec_Krypt
A_19644	Hashfunktion für Hashwert-Referenzen beim Fachdienst Download-Server (KAS)	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_5526	TLS-Renegotiation-Indication-Extension	gemSpec_Krypt

4 Anhang A – Verzeichnisse

4.1 Abkürzungen

Kürzel	Erläuterung
ID	Identifikation
CC	Common Criteria

4.2 Tabellenverzeichnis