

Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Fachdienst KOM-LE

Version: 1.910.0 CC
Revision: 198557230715
Stand: 02.0330.04.2020
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemSpec_FD_KOMLE

Dokumentinformationen

Änderungen zur Vorversion

Die Änderungen/Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion basieren auf können Sie der Änderungsliste P21.1 in nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.1.0	02.12		Ersterstellung	Projekt KOM-LE
	04. 13		Einfügen Anforderungen mit Afo-Makro	Projekt KOM-LE
1.0.0	27.01.14		Einarbeitung Kommentare	Projekt KOM-LE
1.1.0	28.02.14	3.1	Hinweis ergänzt	Projekt KOM-LE
1.2.0	25.07.14	4.3	Afo zu Schnittstellen der TI-Plattform ergänzt	Projekt KOM-LE
1.3.0	22.09.14		Begriff Betreiber durch Anbieter ersetzt	
1.4.0	06.05.15		Anpassung Anforderung KOM-LE-A_2146	Projekt KOM-LE
1.5.0	24.07.15	3.1	Präzisierung der Erstellung von Abwesenheitsnotizen (2 neue Afos)	P74
1.6.0	28.10.16	4.3	Anpassungen gemäß Änderungsliste	gematik
1.7.0	14.05.18		Anpassungen gemäß Änderungsliste	gematik
1.8.0	15.05.19		Anpassungen gemäß Änderungsliste P18.1	gematik
1.9.0	02.03.20		Anpassungen gemäß Änderungsliste P21.1	gematik

1.10.0 CC	02.0330.04.20		freigegeben Anpassungen gemäß Änderungsliste P22.1 und Scope- Themen aus Systemdesign R4.0.0	gematik
--------------	---------------	--	--	---------

ENTWURF

Inhaltsverzeichnis

1 Einordnung des Dokuments	7
1.1 Zielsetzung und Einordnung des Dokuments	7
1.2 Zielgruppe	7
1.3 Geltungsbereich	7
1.4 Arbeitsgrundlagen	7
1.5 Abgrenzung des Dokuments	8
1.6 Methodik	8
1.6.1 Anforderungsmanagement	9
1.6.2 Diagramme	9
1.6.3 Nomenklatur	9
1.6.4 Hinweis auf offene Punkte <optional>	9
2 Systemüberblick	10
3 Funktionen	12
3.1 Funktionen des Mail Servers	12
3.2 Funktionen des Account Managers	13
3.3 Fehlerbehandlung	16
3.4 Protokollierung	17
3.5 Monitoring	17
3.6 Konfiguration	18
4 Schnittstellen	20
4.1 Schnittstelle I_Message_Service	20
4.1.1 Operation send_Message	21
4.1.2 Operation receive_Message	23
4.2 Schnittstelle zur Registrierung und Deregistrierung von KOM-LE-Teilnehmern	23
4.3 Genutzte Schnittstellen der TI-Plattform	30
5 Nicht-Funktionale Anforderungen	32
5.1 Skalierbarkeit	32
5.2 Performance	32
5.3 Mengengerüst	32
6 Anhang A Verzeichnisse	33
6.1 Abkürzungen	33
6.2 Glossar	34
6.3 Abbildungsverzeichnis	34

67	6.4 Tabellenverzeichnis.....	34
68	6.5 Referenzierte Dokumente.....	35
69	6.5.1 Dokumente der gematik.....	35
70	6.5.2 Weitere Dokumente.....	35
71	1 Einordnung des Dokuments	7
72	1.1 Zielsetzung und Einordnung des Dokuments	7
73	1.2 Zielgruppe	7
74	1.3 Geltungsbereich	7
75	1.4 Arbeitsgrundlagen	7
76	1.5 Abgrenzung des Dokuments	8
77	1.6 Methodik	8
78	1.6.1 Anforderungsmanagement	9
79	1.6.2 Diagramme	9
80	1.6.3 Nomenklatur	9
81	1.6.4 Hinweis auf offene Punkte <optional>	9
82	2 Systemüberblick	10
83	3 Funktionen.....	12
84	3.1 Funktionen des Mail Servers.....	12
85	3.2 Funktionen des Account Managers	13
86	3.3 Funktionen des KOM-LE Attachment Services.....	14
87	3.4 Service Lokalisierung	14
88	3.5 Fehlerbehandlung.....	16
89	3.6 Protokollierung.....	17
90	3.7 Monitoring.....	17
91	3.8 Konfiguration	18
92	4 Schnittstellen.....	20
93	4.1 Schnittstelle I_Message_Service	20
94	4.1.1 Operation send_Message	21
95	4.1.2 Operation receive_Message	23
96	4.2 Schnittstelle I_Attachment_Services.....	23
97	4.3 Schnittstelle I_AccountManager_Service	27
98	4.4 Genutzte Schnittstellen der TI-Plattform.....	30
99	5 Nicht-Funktionale Anforderungen	32
100	5.1 Skalierbarkeit	32
101	5.2 Performance	32
102	5.3 Mengengerüst.....	32

103	6 Anhang A – Verzeichnisse	33
104	6.1 Abkürzungen	33
105	6.2 Glossar	34
106	6.3 Abbildungsverzeichnis	34
107	6.4 Tabellenverzeichnis	34
108	6.5 Referenzierte Dokumente	35
109	6.5.1 Dokumente der gematik.....	35
110	6.5.2 Weitere Dokumente.....	35
111		
112		

ENTWURF

1 Einordnung des Dokuments

1.1 Zielsetzung und Einordnung des Dokuments

Dieses Dokument enthält die Anforderungen an den Produkttyp Fachdienst KOM-LE. Der Fachdienst ist verantwortlich für die Speicherung und Bereitstellung von KOM-LE-Nachrichten sowie für die Registrierung und Deregistrierung von KOM-LE-Teilnehmern.

Aus den Kommunikationsbeziehungen mit Clientmodul, Konnektor und Verzeichnisdienst resultieren vom Fachdienst anzubietende Schnittstellen, die in diesem Dokument normativ beschrieben werden. Vom Fachdienst genutzte Schnittstellen liegen zumeist in anderen Verantwortungsbereichen (z.B. Verzeichnisdienst). Diese werden in der entsprechenden Produktspezifikationen definiert.

1.2 Zielgruppe

Dieses Dokument richtet sich neben Personengruppen, die grundsätzlich am Fachdienst Kommunikation Leistungserbringer interessiert sind, an

- Hersteller und Entwickler des Fachdienstes
- Anbieter
- Verantwortliche für Zulassung und Test

1.3 Geltungsbereich

Das vorliegende Dokument enthält normative Anforderungen und Festlegungen, die von Herstellern und Anbietern von Komponenten und Diensten im Rahmen der Projekte der Neuausrichtung zur Einführung der elektronischen Gesundheitskarte und der Telematikinfrastruktur zu beachten sind. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Produktypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

1.4 Arbeitsgrundlagen

Grundlagen für die Ausführungen dieses Dokumentes sind

- das systemspezifische Konzept KOM-LE [gemSysL_KOMLE]
- KOM-LE S/MIME Profil [gemSMIME_KOMLE]
- Gesamtarchitektur der TI [gemÜK_Arch_TI]
- Konzept Architektur der TI-Plattform [gemKPT_Arch_TIP]
- Konzept PKI der TI-Plattform [gemKPT_PKI_TIP]

1.5 Abgrenzung des Dokuments

Spezifiziert werden in dem Dokument die vom Produkttyp bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert.

Die Systemlösung der Fachanwendung KOM-LE ist im systemspezifischen Konzept [gemSysL_KOMLE] beschrieben. Dieses Konzept setzt die fachlichen Anforderungen des Lastenheftes auf Systemebene um, zerlegt die Fachanwendung KOM-LE in die zugehörigen Produkttypen, darunter das KOM-LE-Clientmodul und der KOM-LE-Fachdienst. Ferner definiert es die Schnittstellen zwischen den einzelnen Produkttypen. Für das Verständnis dieser Spezifikation wird die Kenntnis von [gemSysL_KOM-LE] vorausgesetzt.

Die Anforderungen an das Clientmodul werden separat in der Spezifikation KOM-LE-Clientmodul [gemSpec_CM_KOMLE] beschrieben.

Die Anforderungen an das Format der KOM-LE-Nachrichten, die zwischen dem Clientmodul und dem Fachdienst übermittelt werden, werden separat im KOM-LE-S/MIME-Profil [gemSMIME_KOMLE] beschrieben.

Abbildung 1 zeigt schematisch die Einbettung des vorliegenden Dokuments in die Dokumentenlandschaft der Lastenheft- und Pflichtenheftphase in Form einer Dokumentenhierarchie.

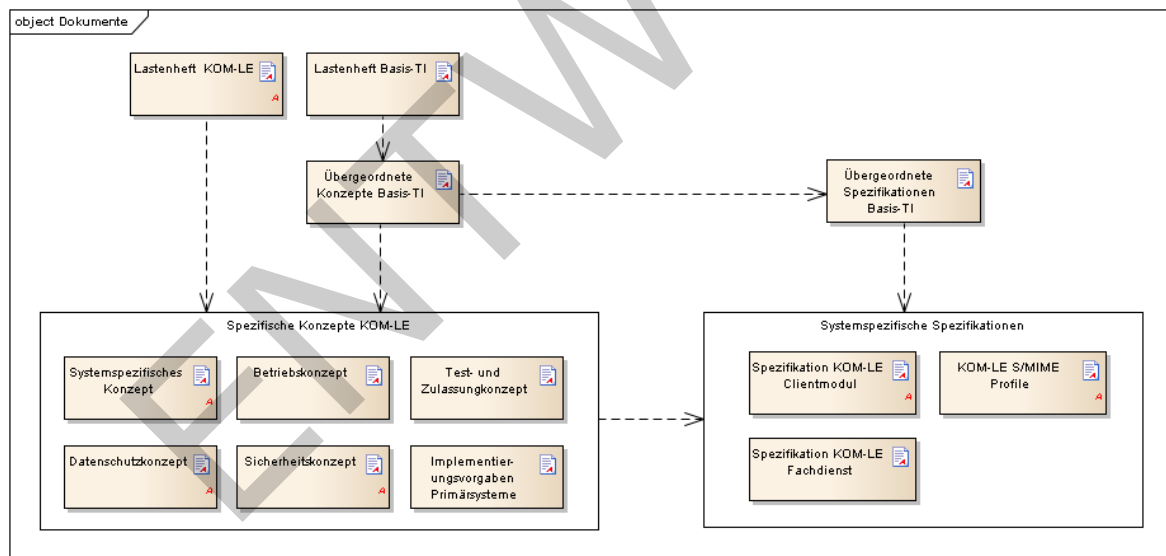


Abbildung 1: Abb_Dok_Hierarchie_KOMLE Dokumentenhierarchie KOM-LE

1.6 Methodik

Das Vorgehen zur Erstellung dieser Spezifikation verwendet einen anforderungszentrierten und modellbasierten Entwicklungsprozess. Dabei werden Auftragsanforderungen über Umsetzungsanforderungen bis hin zu Blattanforderungen verfeinert. Auf Basis der vollständigen und nachvollziehbaren Anforderungen werden

173 verbindliche Artefakte zur Fachanwendung modelliert. Der gesamte Prozess wird durch
174 eine Qualitätssicherung begleitet.

175 **1.6.1 Anforderungsmanagement**

176 Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID
177 sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen
178 deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN
179 gekennzeichnet.

180 Sie werden im Dokument wie folgt dargestellt:

181 **<AFO-ID> - <Titel der Afo>**

182 Text / Beschreibung

183 [**<=**]

184

185 Dabei umfasst die Anforderung sämtliche innerhalb der Afo-ID und der Textmarke
186 angeführten Inhalte.

187 **1.6.2 Diagramme**

188 Die Darstellung der Spezifikationen von Komponenten erfolgt auf der Grundlage einer
189 durchgängigen Use-Case-Modellierung als

- 190 • technische Use Cases (eingebundene Graphik sowie tabellarische Darstellung mit
- 191 Vor- und Nachbedingungen gemäß Modellierungsleitfaden),
- 192 • Sequenz- und Aktivitätendiagramme sowie
- 193 • Klassendiagramme
- 194 • XML-Strukturen und Schnittstellenbeschreibungen.

195 **1.6.3 Nomenklatur**

196 Sofern im Text dieser Spezifikation auf die Ausgangsanforderungen verwiesen wird,
197 erfolgt dies in eckigen Klammern, z.B. [KOMLE-A_2015]. Wird auf
198 Eingangsanforderungen verwiesen, erfolgt dies in runden Klammern, z.B. (KOMLE-
199 A_202).

200 **1.6.4 Hinweis auf offene Punkte <optional>**

201 *Das Kapitel wird in einer späteren Version des Dokumentes ergänzt.*

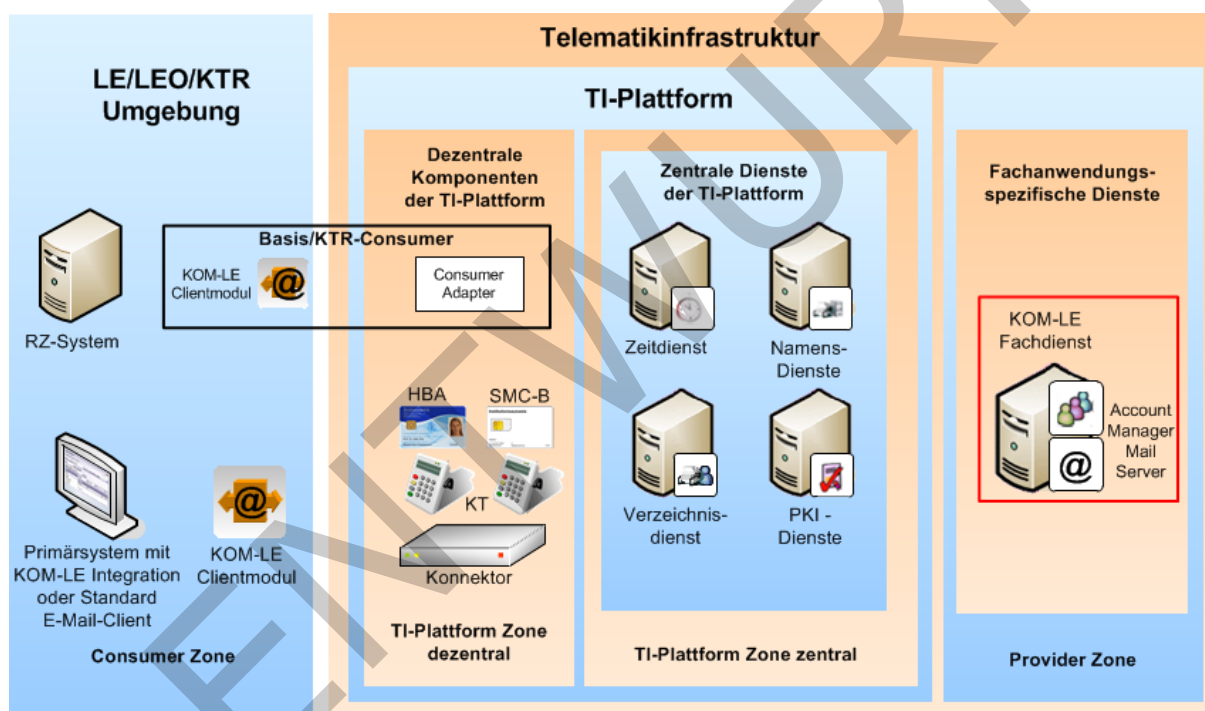
202

2 Systemüberblick

Der Fachdienst KOM-LE ist in der Provider Zone an das zentrale Netz der TI-Plattform angeschlossen und besteht aus den Teilkomponenten Account Manager und Mail Server (SMTP und POP3-Server) und dem KOM-LE Attachment Service (KAS).

Die Teilkomponente Account Manager prüft die Authentizität des Leistungserbringers/KOM-LE-Teilnehmers sowie dessen Registrierungs- bzw. Deregistrierungsdaten. Nach erfolgreicher Prüfung der Daten erfolgt die Registrierung bzw. Deregistrierung des KOM-LE-Teilnehmers inklusive der Aktualisierung seines Verzeichniseintrages bezüglich der E-Mail-Adresse.

Die Teilkomponente Mail Server stellt dem KOM-LE-Clientmodul eine Schnittstelle zum Versenden und Abholen von E-Mails zur Verfügung. Die technische Umsetzung erfolgt über die Bereitstellung von entsprechenden TCP-Ports für SMTP- bzw. POP3.



Die Teilkomponente KOM-LE Attachment Service stellt dem Clientmodul eine Schnittstelle zum Ablegen bzw. Herunterladen von Anhängen größer 25 MB zur Verfügung.

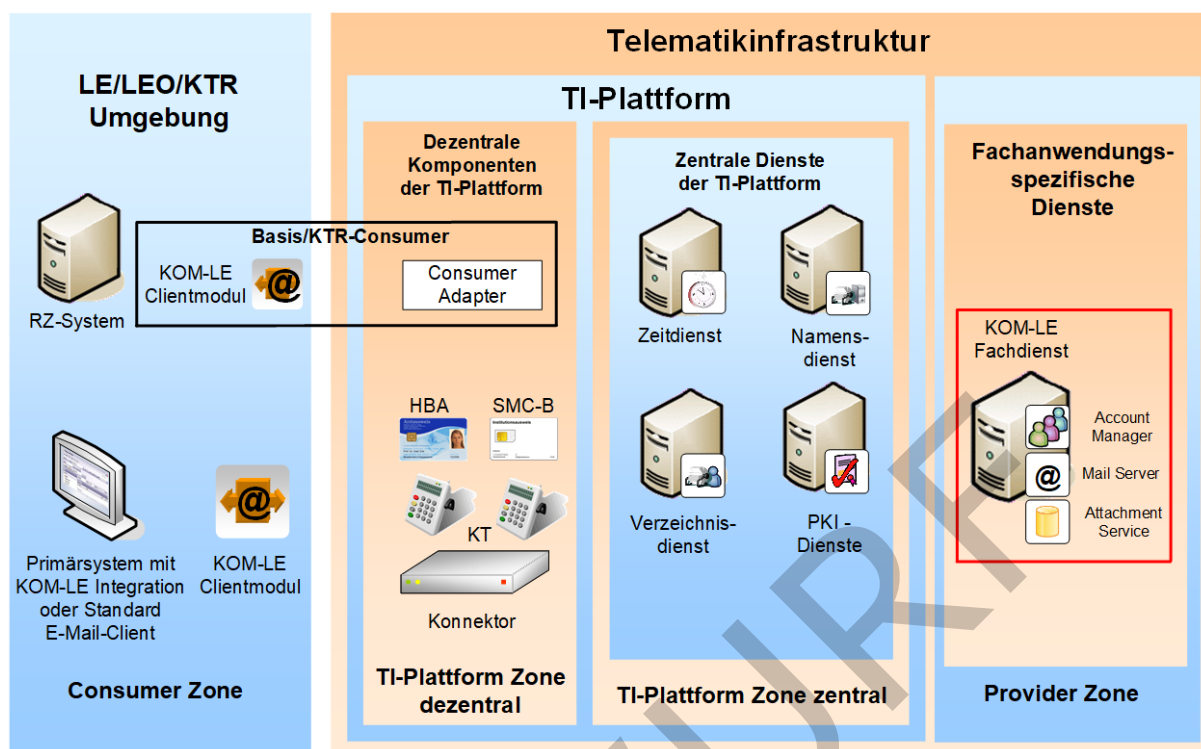


Abbildung 2: Abb_FD_Systemkontext Fachdienst KOM-LE im Systemkontext

223

3 Funktionen

3.1 Funktionen des Mail Servers

225 Der Mail Server nimmt SMTP-Nachrichten von Clientmodulen oder anderen KOM-LE-
226 Fachdiensten entgegen und leitet diese an die Ziel-Mail-Server weiter. Empfangene
227 Nachrichten werden vom Mail Server zur Abholung bereitgestellt und auf Anforderung
228 über POP3 an Clientmodule ausgeliefert. Die zugehörigen Anwendungsfälle sind im
229 systemspezifischen Konzept [gemSysL_KOM-LE#3.1.1, 3.1.5] beschrieben.

230 **KOM-LE-A_2185 - Mail Server darf nur Nachrichten aus der TI verarbeiten**

231 Der Mail Server des KOM-LE-Fachdienstes MUSS ausschließlich Nachrichten, die innerhalb
232 der TI versendet werden, verarbeiten. Der Zugriff auf einen Mail Server von außerhalb
233 der TI ist nicht zulässig.

234 [\leq]

235 **KOM-LE-A_2130 - Generieren einer Zustellbestätigung**

236 Der Ziel-Mail-Server MUSS, wenn die eingehende Nachricht eine Zustellbestätigung
237 anfordert, diese entsprechend Delivery Status Notification vom Typ Success (RFC3461-
238 3464) generieren und an den Absender übermitteln.

239 [\leq]

240 **KOM-LE-A_2131 - Fehlernachricht bei fehlerhafter E-Mail-Adresse**

241 Können Nachrichten aufgrund einer fehlerhaften E-Mail-Adresse nicht weitergeleitet
242 werden, MUSS der Mail Server eine Fehlernachricht entsprechend Delivery Status
243 Notification erzeugen und diese an den Absender übermitteln.

244 [\leq]

245 **KOM-LE-A_2132 - Identifikation der Originalnachricht**

246 Zur Identifikation der Originalnachricht MUSS eine entsprechend Delivery Status
247 Notification erzeugte Nachricht den Empfänger und das Versanddatum der
248 Ursprungsnachricht enthalten.

249 [\leq]

250 **KOM-LE-A_2223 - Unterstützung Autoreply für Abwesenheitsnotiz**

251 Der Mail Server SOLL eine Autoreply-Funktionalität für das Versenden von
252 Abwesenheitsnotizen nach RFC5230 unterstützen.

253 [\leq]

254 **KOM-LE-A_2278 - Aufbau Autoreply für Abwesenheitsnotiz**

255 Der Mail Server MUSS beim Versenden von automatischen Abwesenheitsnotizen folgende
256 Bedingungen erfüllen:

257 SMTP MAIL FROM = <> (leer)

258 Subject = „Auto: “ + Betreff der Nachricht beim Mailserver

259 Auto-Submitted field = „auto-replied“ (siehe RFC5230, section 5).

260 [\leq]

261 **KOM-LE-A_2224 - Einstellen von Abwesenheitsnotizen**

262 Der Mail Server SOLL es dem Nutzer ermöglichen, Abwesenheitsnotizen einstellen zu
263 können.

264 [\leq]

KOM-LE-A_2277 - Versenden von Abwesenheitsnotizen ohne Signatur und Verschlüsselung

Der Mail Server MUSS den Nutzer beim Einrichten von automatischen Abwesenheitsnotizen informieren, dass diese nicht als verschlüsselte und signierte Nachrichten versendet werden.

[<=]

Die Pflege der Abwesenheitsfunktionen (z.B. Aktivieren, Deaktivieren und Notiztext) kann nicht mit dezentralen Komponenten der TI vorgenommen werden.

3.2 Funktionen des Account Managers

~~Der Über die Teilkomponente Account Manager ist für des Fachdienstes wird die Kontoverwaltung eines KOM-LE-Teilnehmers durchgeführt. Zu dem Funktionsumfang gehören: die Registrierung und (mit inkludiertem Herunterladen der PKCS#12-Datei), die Deregistrierung der KOM-LE-Teilnehmer zuständig. Im Rahmen, die Registerstatusabfrage sowie die Kennwortänderung. Eine weitere Aufgabe des Account Managers ist die Übertragung der vom Administrationsmodul gelieferte Clientversion in den Verzeichnisdienst. Die Operationen werden durch ein Webservice des Account Managers bereitgestellt. Ein weiterer wesentlicher Bestandteil dieser Prozesse müssen sich die KOM-LE-Teilnehmer authentisieren sowie Registrierungs- bzw. Deregistrierungsdaten übermittelt und geprüft werden. Bestandteile dieser Prozesse sind zwingend die Operationen ist die zwingende Authentifizierung des KOM-LE Teilnehmers über sein AUT-Zertifikat durch eine webbasierte Anwendung sowie die Aktualisierung des Verzeichnisdiensteintrages bezüglich der E-Mail-Adresse. Die zugehörigen Anwendungsfälle sind im systemspezifischen Konzept [gemSysL_KOM-LE#3.1.7, 3.1.8] beschrieben.~~

KOM-LE-A_2133 - Durchführung eines Accountings zur Abrechnung

Führt der Anbieter ein Accounting für die Abrechnung unter Einhaltung der geltenden Anforderungen an Datenschutz und Informationssicherheit durch, KANN der Fachdienst die dafür notwendigen Funktionen implementieren.

[<=]

KOM-LE-A_2304 - Information an Nutzer zur bcc-Funktionalität

Der KOM-LE-Anbieter MUSS die KOM-LE-Teilnehmer im Rahmen der Registrierung zu KOM-LE und im KOM-LE-Nutzerhandbuch darüber informieren, dass auf eine Nutzung der bcc-Funktionalität eines E-Mail-Clients verzichtet werden sollte, da es technisch nicht ausgeschlossen ist, dass Nachrichtempfänger ggf. auch alle bcc (blind carbon copy) Empfänger der Nachricht ermitteln werden können.[<=]

Es kann zusätzlich darauf hingewiesen werden, dass dies nicht die Klartext-Nachricht betrifft, die ein Empfänger letztlich in seinem Mail-Client empfängt, sondern nur die Daten, die das KOM-LE-Clientmodul verarbeitet. Es ist also durch den Empfänger ein Eingriff zur Analyse des Clientmoduls (z.B. mit Hilfe eines Debuggers) durchzuführen, um an die Daten zu gelangen.

A_19591 - Eintrag Clientmodul-Version in VZD, Account Manager

Der Account Manager MUSS die vom Client übermittelte cm_Version gemeldetet Clientmodul-Version im Verzeichnisdienst in die KOM-LE-Version der KOM-LE-Fachdaten für die betroffenen "mail"-Adresse eintragen. [<=]

Es gelten die Festlegungen aus Kap.4.4., da der Verzeichnisdienst zur TI-Plattform gehört.

3.3 Funktionen des KOM-LE Attachment Services

Die Teilkomponente KAS des Fachdienstes dient als Speicherort für verschlüsselte Anhänge von Mails größer 25 MByte. Damit wird die Übertragung von großen Mails ermöglicht. Das sendende KOM-LE Clientmodul legt die großen Anhänge in verschlüsselter Form auf den KAS ab. Das empfangende KOM-LE Clientmodul lädt die Anhänge beim Empfang der Mail und stellt sie dem Client in entschlüsselter Form zusammen mit der Mail zur Verfügung.

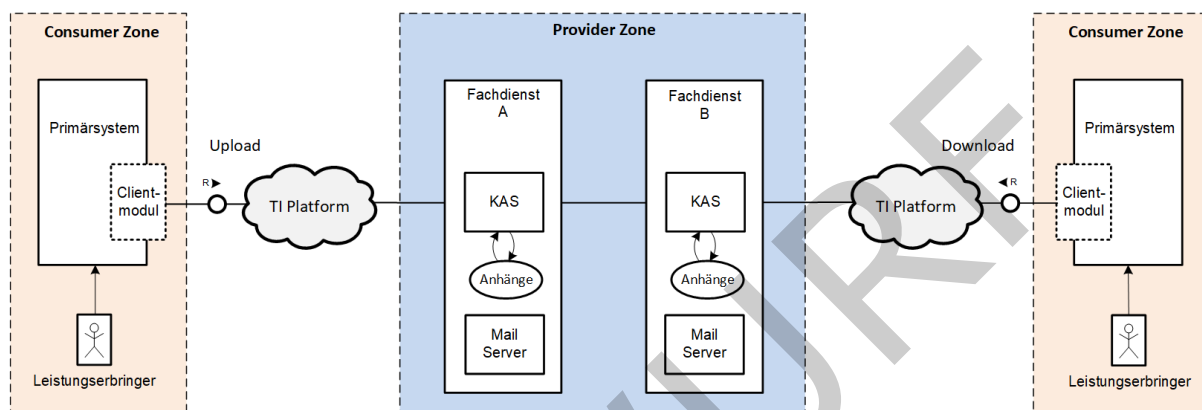


Abbildung 3 Abb_FD_KAS Funktionsweise des Attachment Service

Das sendende KOM-LE Clientmodul legt die großen Anhänge auf dem KAS seines Fachdienstes A ab. Das empfangende KOM-LE Clientmodul lädt die Anhänge der Mail vom KAS des Fachdienstes A, auch wenn der Empfänger einen anderen Fachdienst nutzt. Zur Kommunikation der Clientmodule mit den KAS Servern werden für TLS die TI Zertifikate analog zu Schnittstelle I_Message_Service genutzt, was die Kommunikation über Anbietergrenzen hinaus ermöglicht.

Die maximale Gesamtgröße einer Mail wird durch den Fachdienst definiert und über die Operation I_Attachment_Services::read_MaxMailSize den Client Modulen zur Verfügung gestellt. Die Client Module prüfen die Gesamtgröße der Mail - inklusive aller Anhänge - vor dem Versenden. Mittels der Operation I_Attachment_Services::add_Attachment prüft der KAS die Größe der einzelnen Anlagen beim Laden auf den Fachdienst.

3.4 Service Lokalisierung

A_19524 - Verwaltung Resource Records Typs für Service Discovery, KIM

Der KOM-LE-Fachdienst MUSS die aufgeführten Resource Records Types im Namensraum der TI gemäß folgender Tabelle verwalten.

Tabelle 1: Tab_KOMLE_Service Discovery

Resource Record Bezeichner	Resource Record Type	Beschreibung
----------------------------	----------------------	--------------

_accmgr._tcp.kim.telematik	PTR	Ermittlung aller Account Manager Dienste aller KOM-LE-Anbieter.
<accmgr_service_name>.<hrst_domain>.kim.telematik	SRV und TXT	SRV Resource Record zur Ermittlung der Ports und des FQDN des Account Managers
_kas._tcp.kim.telematik	PTR	Ermittlung aller KAS-Dienste aller KOM-LE-Anbieter.
<kas_service_name>.<hrst_domain>.kim.telematik	SRV und TXT	SRV Resource Record zur Ermittlung der Ports und des FQDN des KAS

[<=]

Der Einträge in < > sind als Variable zu verstehen und durch konkrete Bezeichner zu ersetzen, z.B. für den Account Manager

```
_accmgr._tcp.kim.telematik 86400 IN PTR _accmgr._tcp.hrst1.kim.telematik
_accmgr._tcp.hrst1.kim.telematik 86400 IN SRV 5 10 8443 account-
manager.hrst1.kim.telematik
```

```
_accmgr._tcp.hrst1.kim.telematik 86400 IN TXT „txtvers=1“ „path=/“
```

oder z.B. für den KAS

```
kas._tcp.kim.telematik 86400 IN PTR _hrst1_kas._tcp.hrst1.kim.telematik
_kas._tcp.hrst1.kim.telematik 86400 IN SRV 5 10 8443
kas.hrst1.kim.telematik
```

```
_kas._tcp.hrst1.kim.telematik 86400 IN TXT „txtvers=1“ „path=/“
```

A_19533 - Verwaltung Resource Records FQDN, KIM

Der KOM-LE-Fachdienst MUSS im Namensraum der TI die Resource Records gemäß nachstehender Tabelle verwalten.

Tabelle 2: Tab_KOMLE_FQDN

Resource Record Typ	Beschreibung
---------------------	--------------

FQDN	A Resource Records zur Namensauflösung von FQDN des KOM-LE-Fachdienstes des jeweiligen Anbieters in IP-Adressen
------	---

[<=]

Nachfolgend sind exemplarisch FQDNs für den Account Manager und KAS dargestellt:

account-manager.hrst1.kim.telematik IN A 10.30.20.10

kas.hrst1.kim.telematik IN A 10.30.20.20

3.3.5 Fehlerbehandlung

KOM-LE-A_2134 - Aktionen bei Fehlerzuständen

Der Fachdienst KOM-LE MUSS mindestens die in Tabelle Tab_Fehler_Behandlung beschriebenen Fehlerzustände erkennen und die zugehörigen Aktionen durchführen.

[<=]

Tabelle 3: Tab_Fehler_Behandlung Fehlerbehandlung Fachdienst KOM-LE

Teilkomponente	Fehlerbeschreibung	durchzuführende Aktionen
Mail Server	Aufbau der TLS-Verbindung schlägt fehl	Protokollierung des Fehlers, Übermittlung Fehlercode an den Aufrufer (z.B. Clientmodul)
Mail Server	Authentifizierung über Benutzername und Passwort schlägt fehl	Protokollierung des Fehlers, Übermittlung Fehlercode an den Aufrufer (z.B. Clientmodul)
Mail Server	Nachricht ist nicht verschlüsselt	Protokollierung des Fehlers, Generierung einer entsprechenden Fehlernachricht an den Absender, Verwerfen der Originalnachricht
Mail Server	Absenderadresse fehlerhaft	Protokollierung des Fehlers, Verwerfen der Originalnachricht
Mail Server	Empfängeradresse fehlerhaft	Protokollierung des Fehlers, Generierung einer entsprechenden Fehlernachricht an den Absender mit der Originalnachricht im Anhang, Verwerfen der Originalnachricht

Mail Server	Nachricht kann nicht weitergeleitet werden (z. B.: empfangender Mail Server oder TI-Netz nicht verfügbar)	Protokollierung des Fehlers, Versuch der erneuten Weiterleitung der Nachricht nach einem konfigurierbarem Zeitraum
Account Manager	Verzeichnisdienst nicht erreichbar	Protokollierung des Fehlers

367

368 **3.43.6 Protokollierung**369 **KOM-LE-A_2135 - Protokollierung von Vorgängen**

370 Für die Nachvollziehbarkeit der Vorgänge am Fachdienst KOM-LE MÜSSEN Maßnahmen
 371 und Verfahren gemäß DSGVO i.V.m. BDSG installiert werden. Die Protokollierung der
 372 folgenden Informationen ist dabei zulässig:

- 373 • Anmeldung von Nutzern (Nutzername und Uhrzeit),
- 374 • Informationen über empfangene, weitergeleitete und abgeholte Nachrichten
 375 Absender, Empfänger, Uhrzeit) und
- 376 • Fehlermeldungen (Fehler mit Beschreibung und Uhrzeit).

377 [**<=**]378 **KOM-LE-A_2136 - Protokollierung außerhalb gesetzlicher und vertraglicher**
379 **Pflichten**

380 Der KOM-LE-Fachdienst MUSS sicherstellen, dass eine Protokollierung von
 381 personenbezogenen Daten außerhalb der gesetzlichen und vertraglichen Pflichten nur
 382 dann erfolgt, wenn dies zum Zwecke der Fehler- bzw. Störungsbehebung erforderlich ist.

383 [**<=**]384 **KOM-LE-A_2137 - Protokollierung zum Zwecke der Fehler- bzw.**
385 **Störungsbehebung**

386 Falls im KOM-LE-Fachdienst eine Protokollierung zum Zwecke der Fehler- bzw.
 387 Störungsbehebung erfolgt, MUSS der KOM-LE-Fachdienst unter Berücksichtigung des Art.
 388 25 Abs. 2 DSGVO sicherstellen, dass in den Protokolldaten entsprechend dem
 389 Datenschutzgrundsatz nach Art. 5 DSGVO nur personenbezogene Daten in der Art und
 390 dem Umfang enthalten sind, wie sie zur Behebung erforderlich sind und dass die
 391 erzeugten Protokolldaten im Fachdienst nach der Behebung unverzüglich gelöscht
 392 werden.

393 [**<=**]394 **3.53.7 Monitoring**395 **KOM-LE-A_2138 - Auskunftsfähigkeit über den Systemzustand**

396 Die Administratoren des KOM-LE-Fachdienstes sind verpflichtet, zu jedem Zeitpunkt
 397 auskunftsfähig über den Systemzustand des Fachdienstes zu sein. Zur Unterstützung
 398 dieser Auskunftsfähigkeit KANN der KOM-LE-Fachdienst Monitoringfunktionen
 399 implementieren.

400 [**<=**]

3-63.8 Konfiguration

KOM-LE-A_2139 - Konfiguration Fachdienst

Der Fachdienst KOM-LE MUSS dem Anbieter mindestens die in der Tabelle Tab_Konfig_Parameter dargestellten Parameter zur Konfiguration zur Verfügung stellen. [\leq]

Tabelle 4: Tab_Konfig_Parameter Konfigurationsparameter Fachdienst KOM-LE

Parameter	Standardwert	Beschreibung
Maximale Größe von Nachrichten	35 MB	Die maximale Größe von Nachrichten in KOM-LE soll laut Lastenheft [gemLH_KOM-LE] mindestens 25 MB betragen. Die Nachrichten werden unter Verwendung von S/MIME transportiert und auf dem Fachdienst gespeichert. Die Verwendung von S/MIME schließt die base64-Kodierung der Nachricht ein. Deshalb erhöht sich die Nachrichtengröße ca. um den Faktor 1,4.
Zeitraum für erneuten Weiterleitungsversuch	1 Stunde	Nach Ablauf des Zeitraums soll der Mail Server erneut versuchen Nachrichten weiterzuleiten, die nicht zugestellt werden konnten, weil der empfangende Mail Server oder das TI-Netz nicht verfügbar waren.
Löschfrist von Nachrichten	90 Tage	Nachrichten, die vom Fachdienst nicht abgeholt werden oder nach dem Abholen auf dem Fachdienst verbleiben, müssen nach der angegebenen Frist gelöscht werden.
Löschfrist von Logfiles	90 Tage	Die im Rahmen der Nachrichtenverarbeitung erzeugten Logfiles müssen nach der angegebenen Frist gelöscht werden.
Download- und Prüfzyklus der TSL	1 Tag	Regelmäßiger Zyklus in dem die aktuelle TSL zu laden und zu prüfen ist.
Downloadpunkt der TSL	-	IP-Adresse des verwendeten Downloadpunktes der TSL
IP-Adresse DNS-Server	-	IP-Adresse des verwendeten DNS-Servers der TI
IP-Adresse NTP-Server	-	IP-Adresse des verwendeten NTP-Servers der TI

IP-Adresse Verzeichnisdienst	-	IP-Adresse des Verzeichnisdienstes der TI
---------------------------------	---	---

408

ENTWURF

409

4 Schnittstellen

A_17240 - ECC-Migration, Unterstützung verschiedener kryptografischer Verfahren bei der TLS-Verwendung

Der Fachdienst KOM-LE MUSS parallel RSA und ECC unterstützen. Als TLS-Client MUSS der Fachdienst KOM-LE bevorzugt ECC verwenden, falls er auf einen TLS-Server, der beide Verfahren unterstützt, trifft. [≤]

4.1 Schnittstelle I_Message_Service

KOM-LE-A_2140 - Schnittstelle I_Message_Service

Die Teilkomponente Mail Server des KOM-LE-Fachdiensts MUSS die Schnittstelle I_Message_Service anbieten. I_Message_Service ist eine logische Schnittstelle, die Funktionalitäten zum Versenden und Empfangen von E-Mail-Nachrichten bereitstellt. Die Schnittstelle bietet die folgenden Operationen:

- send_Message(Nachricht, Anmeldedaten) und
- receive_Message(Anmeldedaten): Nachricht[].

Die Schnittstelle kann sowohl seitens des KOM-LE-Clientmoduls als auch eines anderen KOM-LE-Fachdienstes (nur send_Message Operation) aufgerufen werden. Erfolgt der Aufruf der Operation send_Message durch einen anderen Fachdienst, entfällt der Parameter Anmeldedaten.

[≤]

KOM-LE-A_2141 - Technische Umsetzung der Schnittstelle I_Message_Service

Die technische Umsetzung der Schnittstelle I_Message_Service erfolgt über die Bereitstellung von entsprechenden TCP-Ports am KOM-LE-Fachdienst für SMTP-bzw. POP3-Verbindungen. Die Schnittstelle MUSS ausschließlich über eine sichere Verbindung unter Verwendung von TLS mit beidseitiger zertifikatsbasierter Authentifizierung zugänglich sein.

[≤]

KOM-LE-A_2226 - Zuordnung TLS-Client-Zertifikat für Clientmodul

Der KOM-LE-Anbieter MUSS das KOM-LE Clientmodul mit einem TLS-Client-Zertifikat aus der Komponenten-PKI der TI für die TLS-Kommunikation mit dem KOM-LE Fachdienst ausstatten.

[≤]

KOM-LE-A_2227 - Zuordnung TLS-Server-Zertifikat für Clientmodul

Der KOM-LE-Anbieter MUSS das KOM-LE Clientmodul mit einem TLS-Server-Zertifikat aus der Komponenten-PKI der TI für die TLS-Kommunikation mit Clientsystemen ausstatten.

[≤]

KOM-LE-A_2228 - Ausschließliche Akzeptanz von TLS-Client-Zertifikaten von KOM-LE Clientmoduln

Der Fachdienst MUSS beim Aufbau einer TLS-Verbindung mit dem KOM-LE Clientmodul ausschließlich Client-Zertifikate akzeptieren, die KOM-LE Clientmoduln zugeordnet sind.

[≤]

KOM-LE-A_2186 - Verwendung des C.FD.TLS-S Server-Zertifikats bei der TLS-Authentifizierung mit dem Clientmodul

Beim Aufbau der TLS-Verbindung mit dem Clientmodul MUSS sich der Fachdienst KOM-LE mit seinem C.FD.TLS-S Server-Zertifikat authentifizieren.

[<=]

KOM-LE-A_2142 - Ports der Schnittstelle I_Message_Service

Die Schnittstelle I_Message_Service MUSS folgende Ports benutzen:

- SMTPS: 465 und
- POP3S: 995.

[<=]

KOM-LE-A_2143 - Aufbau der TLS-Verbindung

Der Aufbau der TLS-Verbindung für die Schnittstelle I_Message_Service DARF NICHT über STARTTLS erfolgen.

[<=]

KOM-LE-A_2144 - Schritte beim Aufbau der TLS-Verbindung

Beim Aufbau der TLS-Verbindung MUSS der KOM-LE-Fachdienst folgende Schritte bei der Prüfung des vorgelegten Clientzertifikats (C.CM.TLS-CS-Zertifikat des Clientmoduls oder C.FD.TLS-C Client-Zertifikat eines anderen KOM-LE-Fachdienstes) durchführen:

- Prüfung des Vertrauensstatus der Aussteller-CA gegen die TSL,
- mathematische Prüfung der Zertifikatssignatur,
- Prüfung der zeitlichen Gültigkeit des Zertifikats und
- Prüfung des Zertifikatsstatus durch Abfrage des relevanten OCSP-Responders.

Die Reihenfolge ist empfohlen z. B. hinsichtlich wirtschaftlicher Umsetzbarkeit (Offline-Schritte vor Online-Schritten), aber nicht zwingend vorgegeben. Vorbedingung für die Zertifikatsprüfung ist, dass eine validierte TSL in Form eines Trust Stores vorliegt.

[<=]

KOM-LE-A_2145 - Validierung der TSL

Unabhängig von der Zertifikatsprüfung MUSS der KOM-LE-Fachdienst in regelmäßigen Zyklen die TSL-Validierung durchführen. Dabei sind folgende Schritte auszuführen:

- Download der aktuellen Liste vom relevanten Downloadpunkt,
- Validierung gegen das XML-Schema der TSL,
- Prüfung des Vertrauensstatus des TSL-Signaturzertifikats gegen einen sicher verwahrten TSL-Root-Schlüssel und
- Prüfung der XML-Signatur.

[<=]

4.1.1 Operation send_Message

Die Operation send_Message ermöglicht das Versenden von KOM-LE-Nachrichten über den Mail Server des KOM-LE-Fachdienstes. Die logischen Parameter dieser Operation werden in Tabelle 3 beschrieben. Die technische Implementierung dieser Operation erfolgt über die Bereitstellung eines TCP-Ports über den eine SMTP-Verbindung für das Versenden von KOM-LE-Nachrichten aufgebaut wird [RFC 5321].

492 **Tabelle 5: Tab_Para_send_Msg Parameter send_Message Fachdienst KOM-LE**

Parameter		Beschreibung
Eingangsparameter	Anmeldedaten (optional)	Benutzername und Passwort für Authentifizierung des Clients gegenüber dem SMTP-Server seines KOM-LE-Anbieters. Bei der Kommunikation zwischen Clientmodul und SMTP-Server des Senders ist dieser Parameter zwingend erforderlich. Bei Dienst-zu-Dienst-Kommunikation (SMTP-Server des Senders und SMTP-Server des Empfängers) entfällt der Parameter.
	Nachricht	KOM-LE-Nachricht

493 **KOM-LE-A_2146 - Verarbeitung von Nachrichten entsprechend S/MIME-Profil**

494 Der Mail Server DARF Nachrichten, die nicht entsprechend S/MIME-Profil
 495 [gemSMIME_KOMLE] verschlüsselt sind, NICHT weiterleiten bzw. im Postfach des
 496 Empfängers hinterlegen. Für alle servergenerierten Nachrichten wie
 497 Zustellbestätigungen, Fehlermeldungen und Abwesenheitsnotizen sowie vom Clientmodul
 498 generierte Fehlernachrichten, gilt diese Anforderung nicht.

500 [\leq]

501 **KOM-LE-A_2147 - Generierung von Zustellbestätigungen**

502 Erhält der Mail Server eine Nachricht, die eine Zustellbestätigung fordert, MUSS er diese
 503 unter Verwendung folgender Informationen aus der empfangenen Nachricht:

- 504 • Empfänger und
- 505 • Empfangszeitpunkt

506 generieren und unverschlüsselt an den Absender weiterleiten.

507 [\leq]

508 **KOM-LE-A_2148 - Authentifizierungsmechanismen beim Nachrichtenversand**

509 Der Mail Server MUSS die Authentifizierungsmechanismen PLAIN [RFC 4616], CRAM-MD5
 510 [RFC 2195] und SCRAM-SHA-1 [RFC 5802] von SMTP-Auth [RFC 4954] unterstützen.

511 [\leq]

512 **KOM-LE-A_2149 - Kein Empfang von Nachrichten bei deregistriertem Konto**

513 Der KOM-LE-Fachdienst MUSS Nachrichten, die an ein deregistriertes Konto gerichtet
 514 sind, bei Eingang verwerfen und an den Absender eine Fehler-E-Mail senden.

515 [\leq]

516 **KOM-LE-A_2150 - Kein Versenden von Nachrichten bei deregistriertem Konto**

517 Der KOM-LE-Fachdienst DARF Nachrichten NICHT von einem deregistrierten Konto aus
 518 verschicken.

519 [\leq]

4.1.2 Operation receive_Message

Die Operation receive_Message ermöglicht das Abholen von KOM-LE-Nachrichten vom Mail Server des KOM-LE-Fachdiensts. Die logischen Parameter dieser Operation werden in Tabelle 4 beschrieben. Die technische Implementierung dieser Operation erfolgt über Bereitstellung eines TCP-Ports über den eine POP3-Verbindung für das Abholen von KOM-LE-Nachrichten aufgebaut wird [RFC 1939].

Tabelle 6: Tab_Para_recive_Msg Parameter receive_Message Fachdienst KOM-LE

Parameter		Beschreibung
Eingangsparameter	Anmeldedaten	Benutzername und Passwort für Authentifizierung gegenüber dem POP3-Server.
Ausgangsparameter	Nachricht[]	KOM-LE-Nachrichten

KOM-LE-A_2151 - Unterstützung des POP3-Kommandos APOP

Der Mail Server MUSS sowohl die Authentifizierung mit Benutzername und Passwort als auch über das POP3-Kommando APOP ermöglichen.

[<=]

KOM-LE-A_2152 - Unterstützung des POP3-Kommandos UIDL

Um die Kompatibilität mit dem KOM-LE-Clientmodul sicherzustellen MUSS der Mail Server das POP3-Kommando UIDL unterstützen.

[<=]

KOM-LE-A_2154 - Versand von Löschenbenachrichtigungen

Der KOM-LE-Fachdienst DARF den Sender NICHT über das automatische Löschen einer von ihm versendeten aber nicht abgeholten Nachricht informieren.

[<=]

KOM-LE-A_2155 - Nicht abgeholte Nachrichten nach der Deregistrierung

Der KOM-LE-Fachdienst MUSS bereits eingegangene Nachrichten, die noch nicht vom Teilnehmer abgerufen wurden, auch nach der Deregistrierung des Teilnehmers bis Ablauf der Löschfrist der jeweiligen Nachricht zum Abrufen bereit halten und dann löschen.

[<=]

4.2 Schnittstelle zur Registrierung I_Attachment_Services

Der KAS ermöglicht das hoch- und Deregistrierungrunterladen von KOM-LE-Teilnehmern verschlüsselten Anhängen von Mails größer 25 MB. Zum Bereitstellen der Funktionen wird die REST-Schnittstelle I_Attachment_Services definiert. Der Aufruf der Schnittstelle ist ausschließlich vom Clientmodul zulässig. Die Schnittstellenbeschreibung ist in [AttachmentServices.yaml] definiert.

KOM-LE-A_2156 – Schnittstelle zur Registrierung und Deregistrierung In der folgenden Tabelle sind alle Ressourcen mit den jeweiligen HTTP-Methoden dargestellt. Die jeweilige Operation ist eine Abstraktion auf einen Webservice Endpunkt. Die Teilkomponente Account Manager des Fachdienstes KOM-LE MUSS eine Schnittstelle für die Registrierung und Deregistrierung von KOM-LE Teilnehmern anbieten.

[<=]

Tabelle 7 Operationen vom KAS

Operation	URI	Method e	Reques t	Response	Beschreibun g
add_Attachment	/	POST	binary <File>	string <Freigabelink>	Fügt einen verschlüsselte n Anhang im KAS hinzu
read_Attachmen t	/ID_der_Ressour ce (Teil des Freigabelinks)	GET	-	binary <File>	Lädt einen unter einem Freigabelink erreichbaren verschlüsselte n Anhang herunter
read_MaxMailSi ze	/MaxMailSize	GET	-	integer	Gibt die maximal unterstützte Größe einer Mail (inklusive Anhänge und base64-Kodierung) zurück.

A_19375 - KAS – Implementierung der Schnittstelle

KOM-LE-A_2157 – Aufgaben der Schnittstelle zur Registrierung und Deregistrierung Der KAS MUSS die Schnittstelle I_Attachment_Services als REST- Webservices über HTTPS gemäß [AttachmentServices.yaml] implementieren.

[<=]

A_19377 - KAS – TLS-gesicherte Verbindung

Der KAS zur Registrierung und Deregistrierung MUSS die Schnittstelle I_Attachment_Services durch Verwendung von TLS mit beidseitiger Authentisierung sichern. Der KAS MUSS für diese TLS-Verbindungen TI-Zertifikate (analog zu Schnittstelle I_Message_Service) nutzen. Der KAS MUSS sich mit der Server-Identität von Schnittstelle I_Attachment_Services authentisieren.

[<=]

folgende Aufgaben erfüllen:

- Prüfung der Authentizität des KOM-LE Teilnehmers,

- Authentisierung gegenüber dem KOM-LE-Teilnehmer,
- Übertragung der Registrierungs- bzw. Deregistrierungsdaten unter Gewährleistung von Vertraulichkeit, Integrität und Authentizität
- Prüfung der Registrierungs- bzw. Deregistrierungsdaten,
- Vergabe von Benutzername und Passwort zur Authentifizierung am Mail Server und
- Änderung des Verzeichniseintrages des KOM-LE-Teilnehmers (Eintragen bzw. Entfernen der E-Mail-Adresse(n)).

[<=]

A_13540 – Pflege der Basisdaten des Verzeichnisdienstes

Zusätzlich zur Schnittstelle für die Registrierung und Deregistrierung MUSS der Fachdienst dem KOM-LE-Teilnehmer eine Schnittstelle zur Pflege (erzeugen, lesen, ändern und löschen) der Basisdaten des Verzeichnisdienstes der TI anbieten. [<=]

A_19378 - KAS – Dokumentengröße prüfen

Der KAS MUSS die Dateigröße jedes übergebenen Dokumentes ermitteln, bevor das Dokument gespeichert wird. Der KAS MUSS die Verarbeitung ablehnen, wenn die Gesamtgröße des Dokumentes dieses Konfigurationswerts des KAS übersteigt. [<=]

A_19519 - KAS – Maximale Mail Größe bereitstellen

Der KAS MUSS seinen Clients die maximale Gesamtgröße einer Mail mit Operation read_MaxMailSize bereitstellen. Dieser Wert MUSS konfigurierbar sein.

[<=]

A_19379 - KAS – Dokumentenzugriff

Der KAS MUSS sicherstellen, dass nur über den dazugehörigen Freigabelink auf das Dokument zugegriffen werden kann. [<=]

Erzeugung des Freigabelinks

Der KAS generiert für jeden Upload eines Anhangs einen zufälligen und eindeutigen Freigabelink und sendet diesen als Antwort an den Client zurück. Durch Verwendung des Freigabelinks kann der Anhang vom KAS heruntergeladen werden.

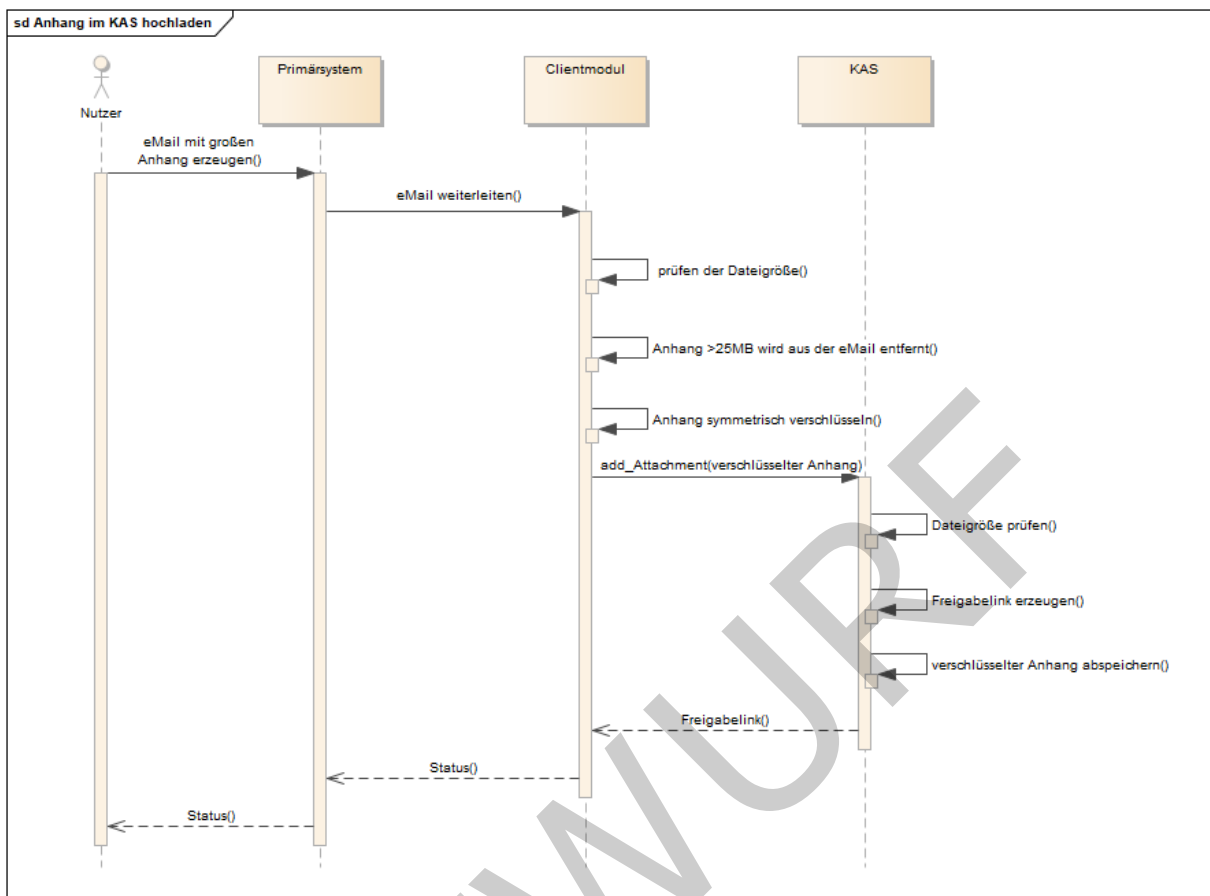


Abbildung 4 Abb_Anw_Dokument auf dem KAS hochladen

A_19380 - KAS – Erzeugung Freigabelink

Der KAS MUSS bei Aufruf der REST-Operation add_Attachment einen Freigabelink erzeugen, die aus dem FQDN der Teilkomponente KAS und einer zufälligen und eindeutigen ID der Ressource (Anhang) z.B. einer UUID [RFC4122] besteht und diesen an den aufrufenden Client zurückgeben.

[<=]

A_19381 - KAS – Freigabelink Transportsicherheit

Der KAS MUSS in den Freigabelink das https-Protokoll hinein generieren: "HTTPS://".

[<=]

A_19382 - KAS – Freigabelink löschen

Der KAS MUSS bei Löschung einer Ressource (Anhang) im KAS-Speicher gewährleisten, dass unter dem Freigabelink der gelöschten Ressource für ein Jahr keine Ressource abrufbar ist.

[<=]

A_19383 - KAS – Keine Kopien von gelöschten Daten

Der KAS DARF von gelöschten Daten KEINE Kopien speichern.

[<=]

Anforderungen an den Anbieter

Im Folgenden werden weitere Anforderungen an den Anbieter der KAS-Komponente gestellt:

A_19384 - KAS – Sicher gegen Datenverlust

Der Anbieter des KAS MUSS den Dienst gegen Datenverlust absichern.

[<=]

A_19385 - KAS – Löschen von Ressource

Der Anbieter des KAS KANN Regeln zum Löschen der Ressourcen auf dem KAS Server definieren und diese seinen Kunden in geeigneter Form mitteilen.

[<=]

4.3 Schnittstelle I_AccountManager_Service

Der Account Manager stellt ein Webservices zur einfachen Verwaltung des Accounts eines KOM-LE-Teilnehmers bereit. Die Schnittstellenbeschreibung I_AccountManager_Service ist in [AccountManager.yaml] definiert. Der Aufruf der REST-Schnittstelle ist ausschließlich vom Clientmodul (Administrationsmodul) zulässig.

In der folgenden Tabelle sind alle Ressourcen mit den jeweiligen HTTP-Methoden dargestellt. Die jeweilige Operation ist eine Abstraktion auf einen Webservice Endpunkt.

Tabelle 8 Operationen vom Account Manager

Operation	URI	Method	Request	Response	Beschreibung
register	/accmgr/register/	POST	username password	<Status> <PKCS#12-Datei>	Registrierung des Teilnehmers am KOM-LE-Fachdienst.
deregister	/accmgr/deregister/	POST	username password	<Status>	Deregistrierung des Teilnehmers am KOM-LE-Fachdienst.
register_State	/accmgr/register-state/	GET	username password	<Status>	Abfrage des Registrierungsstatus.
cm_Version	/accmgr/cm-version/	PUT	username password KOM-LE-Version	<Status>	Übermittlung der KOM-LE-Version.
pw_Change	/accmgr/pw/	PUT	username password newPassword	<Status>	Änderung des Passworts.

A_20063 - Account Manager - Implementierung der Schnittstelle

Die Teilkomponente Account Manager des Fachdienstes MUSS die Schnittstelle I_AccountManager_Service als REST-Webservice über HTTPS gemäß [AccountManager.yaml] implementieren.
[<=]

A_20064 - Account Manager - TLS-gesicherte Verbindung

Die Teilkomponente Account Manager des Fachdienstes MUSS die Schnittstelle I_AccountManager_Service bei der Registrierung durch Verwendung von TLS mit halbseitiger Authentisierung sichern.[<=]

Mit den folgenden Anforderungen wird die Funktionsweise der Operationen des Webservices festgelegt.

KOM-LE-A_2187 - Authentifizierung des KOM-LE-Teilnehmers über AUT-Zertifikat

Zur Pflege der Basisdaten des Verzeichnisdienstes und bei der Registrierung und Deregistrierung MUSS der Fachdienst die Authentizität des KOM-LE-Teilnehmers über das AUT-Zertifikat des HBA bzw. der SM-B des Teilnehmers prüfen. Über die aus dem AUT-Zertifikat ermittelte Telematik-ID ist anschließend der Zugriff auf den Verzeichnisdienst möglich.
[<=]

KOM-LE-A_2305 - Mehrere KOM-LE Postfächer für einen KOM-LE-Teilnehmer

Der KOM-LE Fachdienst MUSS die Möglichkeit anbieten für einen KOM-LE-Teilnehmer, repräsentiert durch dasselbe AUTH Zertifikat, mehrere Postfächer mit jeweils eigener E-Mail-Adresse und eigenen Anmeldecredentials nutzen zu können.[<=]

~~**A_13541 - Verwendung der Schnittstelle I_Directory_Maintenance**~~~~Für die Pflege der Basisdaten des Verzeichniseintrages MUSS der KOM-LE-Fachdienst die Schnittstelle I_Directory_Maintenance der TI-Plattform verwenden.[<=]~~**KOM-LE-A_2158 - Protokollieren von Registrierung und Deregistrierung**

Der KOM-LE-Fachdienst MUSS das Registrieren und Deregistrieren von KOM-LE-Teilnehmern protokollieren.
[<=]

KOM-LE-A_2159 - Verwendung der Schnittstelle**I_Directory_Application_Maintenance**

Für die Änderung des Verzeichniseintrages (Eintragen bzw. Löschen der E-Mail-Adresse des KOM-LE-Teilnehmers) MUSS der KOM-LE-Fachdienst die Schnittstelle I_Directory_Application_Maintenance der TI-Plattform verwenden.
[<=]

KOM-LE-A_2160 - Kommunikation mit dem Verzeichnisdienst über TLS

Der Fachdienst KOM-LE MUSS bei der Änderung des Verzeichniseintrages über die Schnittstelle I_Directory_Application_Maintenance immer eine sichere Verbindung unter Verwendung von TLS mit beidseitiger zertifikatsbasierter Authentifizierung benutzen.
[<=]

KOM-LE-A_2189 - Verwendung des C.FD.TLS-C Client-Zertifikats bei der TLS-Authentifizierung mit dem Verzeichnisdienst

Beim Aufbau der TLS-Verbindung mit dem Verzeichnisdienst MUSS sich der Fachdienst KOM-LE mit seinem C.FD.TLS-C Client-Zertifikat authentifizieren.
[<=]

696 **KOM-LE-A_2161 - Benutzername der KOM-LE-Teilnehmers**

697 Der KOM-LE-Fachdienst MUSS bei der Registrierung die E-Mail-Adresse des KOM-LE-
698 Teilnehmers als Benutzernamen verwenden.

699 [\leq]

700 **KOM-LE-A_2162 - Übermittlung der Passwörter zum Fachdienst**

701 Die Fachanwendung KOM-LE MUSS gewährleisten, dass Passwörter der Teilnehmer nur
702 vertraulichkeits-, integritäts- und authentizitätsgeschützt vom Client zum Fachdienst
703 übermittelt werden.

704 [\leq]

705 **KOM-LE-A_2163 - Vorgaben zur Minimum-Qualität des Passwortes**

706 Der KOM-LE-Anbieter MUSS Vorgaben zur Minimum-Qualität des Passwortes
707 (entsprechend BSI GS M 2.11 „Regelung des Passwortgebrauchs“) machen und die
708 Einhaltung dieser Vorgaben gewährleisten.

709 [\leq]

710 **KOM-LE-A_2164 - Passwörter nicht im Klartext speichern**

711 Der Fachdienst KOM-LE DARF Passwörter der KOM-LE-Teilnehmer NICHT im Klartext
712 speichern.

713 [\leq]

714 **KOM-LE-A_2165 - Möglichkeit der Änderung des Passwortes**

715 Die Teilkomponente Account Manager des Fachdienstes KOM-LE MUSS dem KOM-LE-
716 Teilnehmer die Möglichkeit anbieten das Passwort für die Anmeldung am KOM-LE-
717 Fachdienst zu ändern.

718 [\leq]

719 **KOM-LE-A_2166 - Keine Änderung oder Löschung des Passwortes durch Dritte**

720 Der KOM-LE-Fachdienst DARF das Ändern oder Löschen der bei ihm gespeicherten
721 Passwörter der KOM-LE-Konten durch Dritte NICHT zulassen.

722 [\leq]

723 **KOM-LE-A_2302 - Erzeugung Schlüssel und Bezug TLS-Zertifikate für
724 Clientmodule**

725 Der KOM-LE-Anbieter MUSS die Schlüsselpaare für die Zertifikate für KOM-LE-
726 Clientmodule erzeugen und für diese aus der Komponenten-PKI der TI die C.CM.TLS-CS-
727 Zertifikate beziehen, sodass die Zertifikate vor der Registrierung eines Nutzers zur
728 Verfügung stehen. [\leq]

729 **KOM-LE-A_2303 - Übermittlung Schlüssel und TLS-Zertifikat für Clientmodule**

730 Der KOM-LE-Anbieter MUSS über einen beidseitig authentisierten Kanal unter Wahrung
731 der Vertraulichkeit und Integrität den privaten Schlüssel und das C.CM.TLS-CS-Zertifikat
732 für das Clientmodul – sowohl initial für die Ersteinrichtung als auch periodisch vor Ablauf
733 des jeweils aktuell verwendeten Zertifikats – an den KOM-LE-Nutzer übermitteln. [\leq]

734 Dies kann bspw. mittels der Übertragung einer PKCS#12-Datei über einen beidseitig
735 authentisierten TLS-Kanal unter Nutzung des Auth-Clients realisiert werden, wobei die
736 Möglichkeit der Authentifizierung des Fachdienstes durch den Nutzer gegeben sein muss.

737 **KOM-LE-A_2167 - Sperrung des Accounts**

738 Der Fachdienst KOM-LE MUSS den Account eines Teilnehmers nach drei
739 aufeinanderfolgenden Fehleingaben des Passwortes temporär sperren. Nach dem Sperren
740 des Accounts kann der Nutzer keine E-Mails mehr versenden bzw. abholen. Die
741 Benutzerinformationen bleiben aber erhalten, so dass später ein Entsperren des Accounts
742 möglich ist.

743 [\leq]

KOM-LE-A_2168 - Entsperren des Accounts

Der KOM-LE-Anbieter MUSS praktikable Mechanismen zum Entsperren eines aufgrund fehlerhafter Passworteingaben gesperrten Accounts anbieten.

[<=]

KOM-LE-A_2169 - Authentifizierungsdaten beim Versenden und Empfangen von Nachrichten

Der KOM-LE-Fachdienst MUSS die im Registrierungsprozess vergebenen Daten für Benutzernamen und Passwort sowohl beim Versenden von Nachrichten über SMTP als auch beim Abholen von Nachrichten über POP3 für die Authentifizierung verwenden.

[<=]

A_18784 - Bereitstellung Schlüssel und Zertifikat für Clientmodul als passwortgeschützte PKCS#12 Datei

Der KOM-LE-Anbieter MUSS dem KOM-LE-Teilnehmer das Schlüsselmateriale und das Zertifikat für das KOM-LE-Clientmodul im Registrierungsprozess als passwortgeschützte PKCS#12-Datei zur Verfügung stellen. Die Übermittlung des zur p12-Datei gehörigen Passworts muss dabei auf einem anderem Übertragungsweg als die Bereitstellung der p12-Datei erfolgen.

[<=]

A_19542 - Schnittstelle für den Download

Der Account Manager MUSS eine Operation für das Herunterladen der PKCS#12-Datei bereitstellen.

[<=]

4.24.4 Genutzte Schnittstellen der TI-Plattform

Hier werden die durch den Fachdienst genutzten Schnittstellen der TI-Plattform aufgelistet. Die Spezifikation dieser Schnittstellen erfolgt durch das Projekt Basis-TI und wird in [gemKPT_Arch_TIP] beschrieben.

KOM-LE-A_2231 - Schnittstellen der TI-Plattform

Der Fachdienst KOM-LE MUSS die in der Tabelle Tab_Interface_TIP aufgeführten Schnittstellen der TI-Plattform benutzen.

[<=]

Tabelle 9: Tab_Interface_TIP Schnittstellen zur TI-Plattform des Fachdienstes KOM-LE

Schnittstelle	Operation	benutzt durch
I_Directory_Application_Maintenance	add_Directory_FA-Attributes delete_Directory_FA-Attributes modify_Directory_FA-Attributes	Account Manager bei der Registrierung bzw. Deregistrierung
I_Directory_Query	search_Directory	Account Manager bei der Registrierung bzw. Deregistrierung

I_Directory_Maintenance	add_Directory_FA-Attributes delete_Directory_FA-Attributes modify_Directory_FA-Attributes	Account Manager zur Pflege der Basisdaten des Verzeichnisdienstes
I_NTP_Time_Information	sync_Time	Fachdienst für die Verwendung der korrekten Zeit z.B. beim Versenden und Weiterleiten von E-Mails/Empfangsbestätigungen oder bei der Erstellung von Logging-Einträgen
I_DNS_Name_Resolution	get_IP_Address	Mail Server beim Versenden und Weiterleiten von E-Mails
I_OCSP_Request	check_Revocation_Status	Mail Server beim Aufbau der TLS-Verbindung
I_TSL_Download	download_TSL	Mail Server als Vorbedingung beim Aufbau der TLS-Verbindung

775 **5 Nicht-Funktionale Anforderungen**

776 **5.1 Skalierbarkeit**

777 **KOM-LE-A_2171 - Skalierbarkeit KOM-LE-Fachdienst**

778 Der KOM-LE-Fachdienst MUSS mit einer zunehmenden Anzahl von beteiligten
 779 Teilnehmern skalieren.
 780 [\leq]

781 **5.2 Performance**

782 Die durch den Fachdienst KOM-LE zu erfüllenden Performance-Anforderungen befinden
 783 sich in [gemSpec_Perf#4.4].

784 **5.3 Mengengerüst**

785 Das für den Fachdienst KOM-LE relevante Mengengerüst befindet sich in
 786 [gemSpec_Perf#3.1].

787

6 Anhang A – Verzeichnisse

788

6.1 Abkürzungen

Abkürzung	Bedeutung
base64	Verfahren zur Kodierung von Binärdaten in eine Zeichenfolge, die nur aus lesbaren ASCII-Zeichen besteht
DNS	Domain Name System
HBA	Heilberufsausweis
ID	Identification
IP	Internet Protocol
MIME	Multipurpose Internet Mail Extensions
ISO	International Organization for Standardization
KB	Kilobyte
KAS	KOM-LE Attachment Service
MB	Megabyte
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
POP3	Post Office Protocol Version 3
RFC	Request for Comments
SMC (B/A/KTR)	Security Module Card
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
TI	Telematikinfrastuktur
TLS	Transport Layer Security, die Vorgängerbezeichnung ist SSL

TSL	Trusted Service List
S/MIME	Secure Multipurpose Internet Mail Extensions
XML	Extensible Markup Language

6.2 Glossar

Das Glossar wird als eigenständiges Dokument, vgl [gemGlossar_TI] zur Verfügung gestellt.

6.3 Abbildungsverzeichnis

Abbildung 1: Abb_Dok_Hierarchie_KOMLE Dokumentenhierarchie KOM-LE	8
Abbildung 2: Abb_FD_Systemkontext Fachdienst KOM-LE im Systemkontext	11
Abbildung 1: Abb_Dok_Hierarchie_KOMLE Dokumentenhierarchie KOM-LE	8
Abbildung 2 Abb_FD_Systemkontext Fachdienst KOM-LE im Systemkontext	11
Abbildung 3 Abb_FD_KAS Funktionsweise des Attachment Service	14
Abbildung 4 Abb_Anw_Dokument auf dem KAS hochladen	26

6.4 Tabellenverzeichnis

Tabelle 1: Tab_Fehler_Behandlung Fehlerbehandlung Fachdienst KOM-LE	16
Tabelle 2: Tab_Konfig_Parameter Konfigurationsparameter Fachdienst KOM-LE	18
Tabelle 3: Tab_Para_send_Msg Parameter send_Message Fachdienst KOM-LE	22
Tabelle 4: Tab_Para_recive_Msg Parameter receive_Message Fachdienst KOM-LE	23
Tabelle 5: Tab_Interface_TIP Schnittstellen zur TI-Plattform des Fachdienstes KOM-LE	30
Tabelle 1: Tab_KOMLE_Service Discovery	14
Tabelle 2: Tab_KOMLE_FQDN	15
Tabelle 3: Tab_Fehler_Behandlung Fehlerbehandlung Fachdienst KOM-LE	16
Tabelle 4: Tab_Konfig_Parameter Konfigurationsparameter Fachdienst KOM-LE	18
Tabelle 5: Tab_Para_send_Msg Parameter send_Message Fachdienst KOM-LE	22
Tabelle 6: Tab_Para_recive_Msg Parameter receive_Message Fachdienst KOM-LE	23
Tabelle 7 Operationen vom KAS	24
Tabelle 8 Operationen vom Account Manager	27
Tabelle 9: Tab_Interface_TIP Schnittstellen zur TI-Plattform des Fachdienstes KOM-LE	30

6.5 Referenzierte Dokumente

6.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummer entnehmen Sie bitte der aktuellen, auf der Internetseite der gematik veröffentlichten Dokumentenlandkarte, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemGlossar_TI]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemLH_KOM-LE]	gematik: Lastenheft Kommunikation Leistungserbringer (KOM-LE)
[gemSysL_KOM-LE]	gematik: Systemspezifisches Konzept Kommunikation Leistungserbringer (KOM-LE)
[gemSpec_CM_KOMLE]	gematik: Spezifikation Clientmodul KOM-LE
[gemSMIME_KOM-LE]	gematik: S/MIME-Profil Kommunikation Leistungserbringer (KOM-LE)
[AttachmentServices.yaml]	gematik:
[AccountManager.yaml]	gematik:

6.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[DESTATIS_KRK]	Statistisches Bundesamt Deutschland, Eckdaten der Krankenhäuser 2010 http://www.destatis.de/
[RFC1939]	RFC 1939: Post Office Protocol – Version 3, J. Myers, M. Rose, Mai 1996

[RFC 2195]	J. Klensin, R. Catoe, P. Krumviede, RFC 2195: IMAP/POP AUTHorize Extension for Simple Challenge/Response, September 1997
[RFC4122]	A Universally Unique IDentifier (UUID) URN Namespace
[RFC 4616]	K. Zeilenga, RFC 4616: The PLAIN Simple Authentication and Security Layer (SASL) Mechanism, August 2006
[RFC 4954]	R. Siemborski, A. Melnikov, RFC 4954: SMTP Service Extension for Authentication, July 2007
[RFC 5321]	J. Klensin, RFC 5321: Simple Mail Transfer Protocol, October 2008
[RFC 5802]	C. Newman, A. Menon-Sen, A. Melnikov, N. Williams, RFC 5802: Salted Challenge Response Authentication Mechanism (SCRAM) SASL and GSS-API Mechanisms, July 2010