

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Fachdienst KOM- LE

Version: 1.8.0
Revision: 109011
Stand: 15.05.2019
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemSpec_FD_KOMLE

Dokumentinformationen

Änderungen zur Vorversion

Die Änderungen zur Vorversion aufgrund der Änderungsliste P18.1 sind gelb markiert.

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 |
| | | | Anpassungen gemäß Änderungsliste P18.1 | gematik |
| 1.8.0 | 15.05.2019 | | freigegeben | gematik |

Inhaltsverzeichnis

| | | |
|----------|--|-----------|
| 1 | Einordnung des Dokuments | 5 |
| 1.1 | Zielsetzung und Einordnung des Dokuments | 5 |
| 1.2 | Zielgruppe | 5 |
| 1.3 | Geltungsbereich | 5 |
| 1.4 | Arbeitsgrundlagen | 5 |
| 1.5 | Abgrenzung des Dokuments | 6 |
| 1.6 | Methodik | 6 |
| 1.6.1 | Anforderungsmanagement | 7 |
| 1.6.2 | Diagramme | 7 |
| 1.6.3 | Nomenklatur | 7 |
| 1.6.4 | Hinweis auf offene Punkte <optional> | 7 |
| 2 | Systemüberblick | 8 |
| 3 | Funktionen | 9 |
| 3.1 | Funktionen des Mail Servers | 9 |
| 3.2 | Funktionen des Account Managers | 10 |
| 3.3 | Fehlerbehandlung | 10 |
| 3.4 | Protokollierung | 11 |
| 3.5 | Monitoring | 12 |
| 3.6 | Konfiguration | 12 |
| 4 | Schnittstellen | 14 |
| 4.1 | Schnittstelle I_Message_Service | 14 |
| 4.1.1 | Operation send_Message | 15 |
| 4.1.2 | Operation receive_Message | 16 |
| 4.2 | Schnittstelle zur Registrierung und Deregistrierung von KOM-LE-Teilnehmern | 17 |
| 4.3 | Genutzte Schnittstellen der TI-Plattform | 20 |
| 5 | Nicht-Funktionale Anforderungen | 22 |
| 5.1 | Skalierbarkeit | 22 |
| 5.2 | Performance | 22 |
| 5.3 | Mengengerüst | 22 |
| 6 | Anhang A – Verzeichnisse | 23 |
| 6.1 | Abkürzungen | 23 |
| 6.2 | Glossar | 24 |

6.3 Abbildungsverzeichnis.....24

6.4 Tabellenverzeichnis.....24

6.5 Referenzierte Dokumente.....24

 6.5.1 Dokumente der gematik.....24

 6.5.2 Weitere Dokumente25

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 Produktypspezifikationen 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.

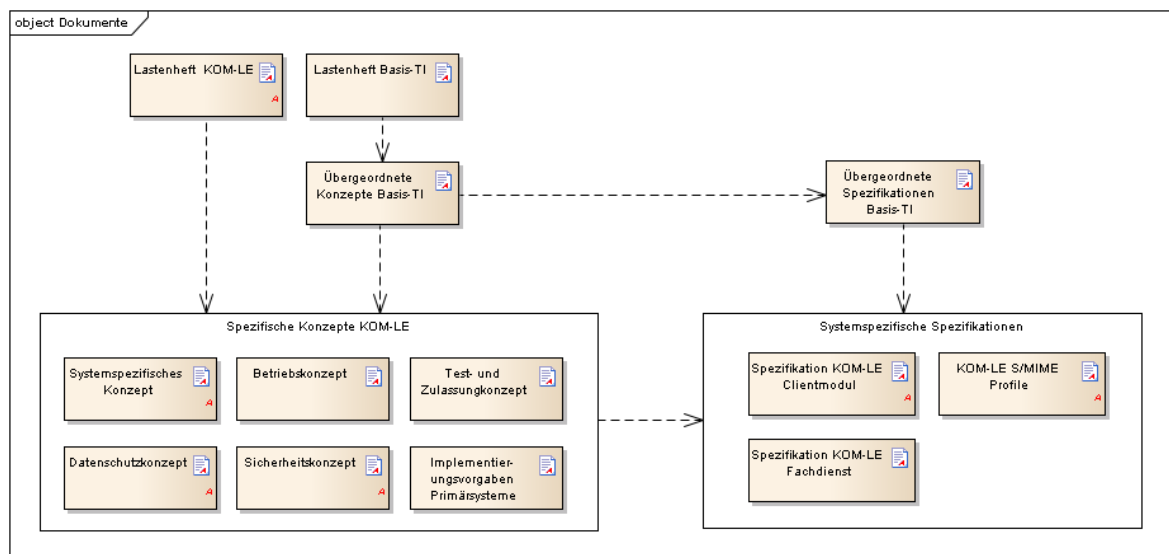


Abbildung 1: Abb_Dok_Hierarchie_KOMLE Dokumentenhierarchie KOM-LE

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

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

1.6.1 Anforderungsmanagement

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

Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>

Text / Beschreibung

[<=]

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

1.6.2 Diagramme

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

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

1.6.3 Nomenklatur

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

1.6.4 Hinweis auf offene Punkte <optional>

Das Kapitel wird in einer späteren Version des Dokumentes ergänzt.

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).

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.

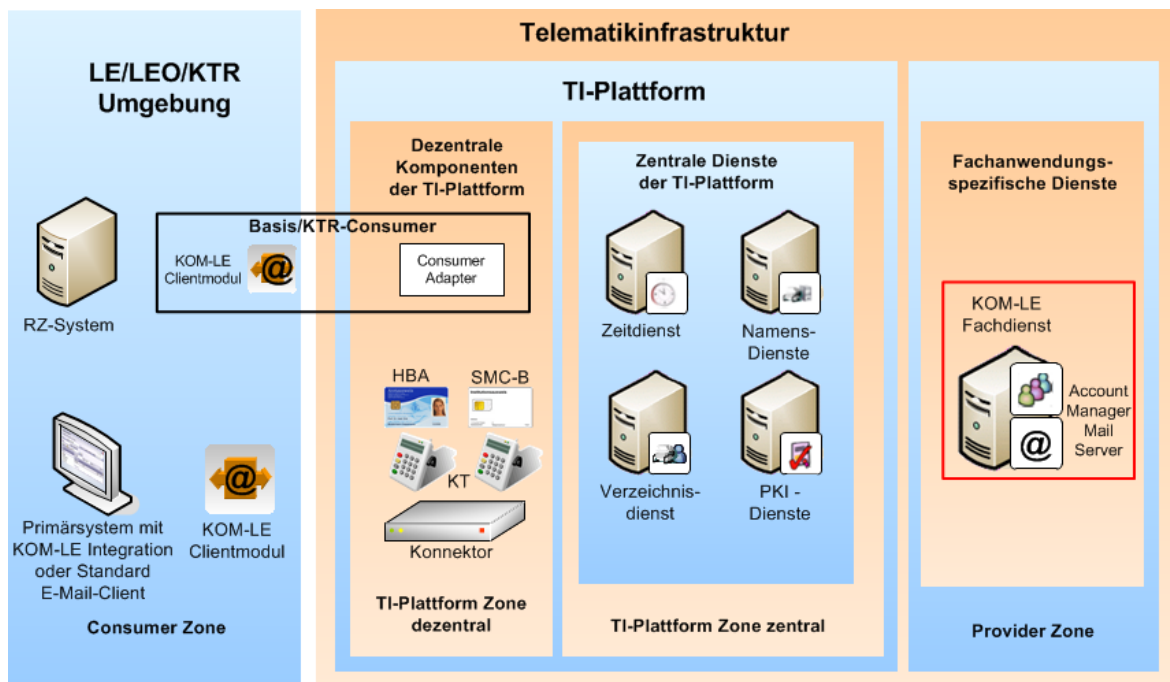


Abbildung 2: Abb_FD_Systemkontext Fachdienst KOM-LE im Systemkontext

3 Funktionen

3.1 Funktionen des Mail Servers

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

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

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

[<=]

KOM-LE-A_2130 - Generieren einer Zustellbestätigung

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

[<=]

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

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

[<=]

KOM-LE-A_2132 - Identifikation der Originalnachricht

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

[<=]

KOM-LE-A_2223 - Unterstützung Autoreply für Abwesenheitsnotiz

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

[<=]

KOM-LE-A_2278 - Aufbau Autoreply für Abwesenheitsnotiz

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

SMTP MAIL FROM = <> (leer)

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

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

[<=]

KOM-LE-A_2224 - Einstellen von Abwesenheitsnotizen

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

[<=]

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 Account Manager ist für die Registrierung und Deregistrierung der KOM-LE-Teilnehmer zuständig. Im Rahmen dieser Prozesse müssen sich die KOM-LE-Teilnehmer authentisieren sowie Registrierungs- bzw. Deregistrierungsdaten übermittelt und geprüft werden. Bestandteile dieser Prozesse sind zwingend die 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 Nachrichteneempfänger 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.

3.3 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 1: 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 |

3.4 Protokollierung

KOM-LE-A_2135 - Protokollierung von Vorgängen

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

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

[<=]

KOM-LE-A_2136 - Protokollierung außerhalb gesetzlicher und vertraglicher Pflichten

Der KOM-LE-Fachdienst MUSS sicherstellen, dass eine Protokollierung von personenbezogenen Daten außerhalb der gesetzlichen und vertraglichen Pflichten nur

dann erfolgt, wenn dies zum Zwecke der Fehler- bzw. Störungsbehebung erforderlich ist.
 [≤]

KOM-LE-A_2137 - Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung

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

[≤]

3.5 Monitoring

KOM-LE-A_2138 - Auskunftsfähigkeit über den Systemzustand

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

[≤]

3.6 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.

[≤]

Tabelle 2: 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 |

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].

Tabelle 3: 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 |

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

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

[<=]

KOM-LE-A_2147 - Generierung von Zustellbestätigungen

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

- Empfänger und
- Empfangszeitpunkt

generieren und unverschlüsselt an den Absender weiterleiten.

[<=]

KOM-LE-A_2148 - Authentifizierungsmechanismen beim Nachrichtenversand

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

[<=]

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

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

[<=]

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

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

[<=]

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 4: 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 und Deregistrierung von KOM-LE-Teilnehmern

KOM-LE-A_2156 - Schnittstelle zur Registrierung und Deregistrierung

Die Teilkomponente Account Manager des Fachdienstes KOM-LE MUSS eine Schnittstelle für die Registrierung und Deregistrierung von KOM-LE-Teilnehmern anbieten.

[<=]

KOM-LE-A_2157 - Aufgaben der Schnittstelle zur Registrierung und Deregistrierung

Die Schnittstelle zur Registrierung und Deregistrierung MUSS 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.[<=]

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.

[<=]

KOM-LE-A_2161 - Benutzername der KOM-LE-Teilnehmers

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

[<=]

KOM-LE-A_2162 - Übermittlung der Passwörter zum Fachdienst

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

[<=]

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

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

[<=]

KOM-LE-A_2164 - Passwörter nicht im Klartext speichern

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

[<=]

KOM-LE-A_2165 - Möglichkeit der Änderung des Passwortes

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

[<=]

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

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

[<=]

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

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

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

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

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

KOM-LE-A_2167 - Sperrung des Accounts

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

[<=]

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.

[<=]

4.3 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 5: 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 |

5 Nicht-Funktionale Anforderungen

5.1 Skalierbarkeit

KOM-LE-A_2171 - Skalierbarkeit KOM-LE-Fachdienst

Der KOM-LE-Fachdienst MUSS mit einer zunehmenden Anzahl von beteiligten Teilnehmern skalieren.

[<=]

5.2 Performance

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

5.3 Mengengerüst

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

6 Anhang A – Verzeichnisse

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 |
| 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 | Telematikinfrastruktur |
| 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 | 6 |
| Abbildung 2: Abb_FD_Systemkontext Fachdienst KOM-LE im Systemkontext | 8 |

6.4 Tabellenverzeichnis

| | |
|--|----|
| Tabelle 1: Tab_Fehler_Behandlung Fehlerbehandlung Fachdienst KOM-LE | 10 |
| Tabelle 2: Tab_Konfig_Parameter Konfigurationsparameter Fachdienst KOM-LE | 12 |
| Tabelle 3: Tab_Para_send_Msg Parameter send_Message Fachdienst KOM-LE | 15 |
| Tabelle 4: Tab_Para_recive_Msg Parameter receive_Message Fachdienst KOM-LE..... | 17 |
| Tabelle 5: Tab_Interface_TIP Schnittstellen zur TI-Plattform des Fachdienstes KOM-LE20 | |

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) |

6.5.2 Weitere Dokumente

| [Quelle] | Herausgeber (Erscheinungsdatum): Titel |
|----------------|--|
| [DESTATIS_KRK] | Statistisches Bundesamt Deutschland, Eckdaten der Krankenhäuser 2010 http://www.destatis.de/ |
| [KBV] | Kassenärztliche Bundesvereinigung, Grunddaten 2006, http://www.kbv.de/publikationen/125.html |
| [KZBV] | KZBV: Zahnärztliche Versorgung 2006, DATEN&FAKTEN http://www.bzaek.de/list/presse/datenfakten/df2006.pdf |
| [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 |
| [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 |