Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Systemspezifisches Konzept

Kommunikation Leistungs-erbringer (KOM-LE)

Version:	1.3.0
Revision	\main\rel_online\rel_ors1\1
Stand:	24.07.2015
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemSysL_KOM-LE]

Dokumentinformationen

Änderungen zur Vorversion

Die türkisenen Markierungen kennzeichnen die Änderungen zur letzten Veröffentlichung.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
			Erstellung TEAM	
			Review Team	
	13.09.11		Formale QS	QM
	16.09.11		I_FES_Operation Schnittstelle und deren Operationen werden umbenannt („FES“ wird durch „Sign“ ersetzt)	
0.5.0	19.11.13		zur Abstimmung freigegeben	gematik
			Einarbeitung Kommentare	
1.0.0	29.01.14		zur Angebotserstellung freigegeben	gematik
	14.02.14		Verzeichnisdienst entfernt	P74
1.1.0	28.02.14		zur Angebotserstellung freigegeben	gematik
	09.09.14		Ergänzung Anforderungen externe Partner	
1.2.0	22.09.14		zur Angebotserstellung freigegeben	gematik
1.2.1_ SMC-B(Org)	16.03.15		Erweiterung Teilnehmerkreis um Organisation der Gesellschafter	gematik
	13.05.15		zur Angebotserstellung freigegeben	gematik
1.3.0			freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments

1.1 Zielsetzung

Dieses Dokument beschreibt basierend auf den Anforderungen des Lastenheftes KOM-LE [gemLH_KOM-LE] und des Konzepts der Architektur der TI-Plattform [gemKPT_Arch_TIP] die systemspezifische Lösung des Projektes KOM-LE. Dabei werden insbesondere die Komponenten der Lösung von KOM-LE und ihre Schnittstellen mit der TI-Plattform beschrieben.

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

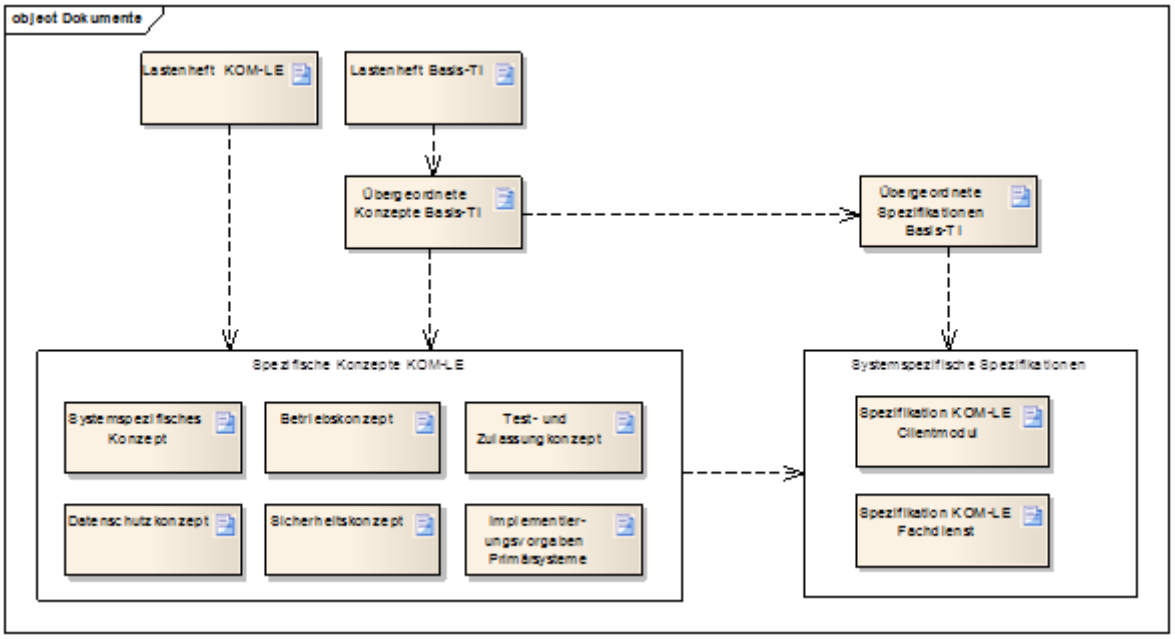

Abbildung 1 Dokumentenhierarchie KOM-LE

1.2 Zielgruppe

Dieses Dokument richtet sich neben Personengruppen, die grundsätzlich an den Verfahren von KOM-LE interessiert sind, an

- Entwickler von fachspezifischen Clientmodulen,
- Entwickler von Fachdiensten,
- Primärsystemhersteller,
- Anbieter und Betreiber sowie

- Verantwortliche für Zulassung und Test.

1.3 Geltungsbereich

Das vorliegende Dokument enthält Festlegungen, die von Herstellern und Betreibern von Komponenten und Diensten der Telematikinfrastruktur im Rahmen der Projekte der Neuausrichtung zur Einführung der elektronischen Gesundheitskarte und der Telematikinfrastruktur zu beachten sind. Es gilt somit nicht für den Basis-Rollout.

1.4 Arbeitsgrundlagen

Grundlagen für die Ausführungen dieses Dokuments sind

- das Lastenheft KOM-LE [gemLH_KOM-LE]
- das Lastenheft Basis-TI [gemLH_Basis-TI]
- das Konzept der Architektur der TI-Plattform [gemKPT_Arch_TIP]

Mitgeltend für die Ausführungen dieses Dokumentes und begleitend dazu erstellt wurde das Dokument Schutzbedarfsfeststellung in der Telematikinfrastruktur [gemMeth_Schutzbed].

1.5 Abgrenzung des Dokuments

Innerhalb des Dokuments wird auf die systemspezifische Lösung des Projektes Kommunikation Leistungserbringer (KOM-LE) eingegangen. Für Informationen zum fachlichen Gesamtkontext wird auf das Lastenheft KOM-LE [gemLH_KOM-LE] verwiesen.

1.6 Methodik

Das Vorgehen zur Erstellung des systemspezifischen Konzepts verwendet den anforderungszentrierten und modellbasierten Entwicklungsprozess der gematik. Dabei werden auf Basis von vollständigen und nachvollziehbaren Anforderungen Lösungen dargestellt, aus denen in der Designphase verbindliche Artefakte zur Fachanwendung modelliert werden. Der gesamte Prozess wird durch eine Qualitätssicherung begleitet.

1.6.1 Diagramme

Die Darstellung der Facharchitektur erfolgt prinzipiell auf der Grundlage einer durchgängigen UML-Modellierung unter Nutzung der folgenden Diagrammtypen:

- Komponentendiagramme (CMP) zur Darstellung der beteiligten Komponenten und ihrer Schnittstellen
- Verteilungsdiagramme zur Darstellung der Verteilung von Komponenten auf Systeme

- Use-Case-Diagramme (UC) zur Darstellung der technische Anwendungsfälle
- Aktivitätsdiagramme (ACT) zur Abbildung der technischen Abläufe eines Anwendungsfalls. Die Aktivitätsdiagramme werden durch Tabellen ergänzt, die die funktionalen Ergänzungen beinhalten.
- Sequenzdiagramme (SD) zur Abbildung der Schnittstellen zwischen den Komponenten innerhalb eines Anwendungsfalls
- Klassendiagramme zur Abbildung der Infomodelle
- Objektdiagramme zur exemplarischen Darstellung von Informationsobjekten

Die Modelle sind in einem zentralen Werkzeug (Enterprise Architect) projektübergreifend abgelegt.

1.6.2 Anforderungsmanagement

Die Lösungsanalyse von KOM-LE entwirft eine Lösungsskizze, mit der die Anforderungen des Lastenheftes umgesetzt werden können. KOM-LE hat eine separate Liste erstellt, in der für jede Lastenheftanforderungen geprüft wurde, ob die Anforderung in der Analysephase betrachtet wurde und ob sie durch den gewählten Lösungsansatz umgesetzt werden kann. Ein Verweis auf konkrete Umsetzungsanforderungen erfolgt in dem systemspezifischen Konzept nicht.

Die Lastenheftanforderungen, die aufgrund der gewählten technischen Umsetzungen oder aus anderen Gründen nicht oder nicht vollständig umsetzbar sind, werden im Anhang B dokumentiert.

Neue Festlegungen gegenüber dem Lastenheft werden ebenfalls im Anhang B dokumentiert.

2 Systemüberblick

2.1 Übergreifende Anforderungen

Für die Fachanwendung KOM-LE gelten weiterhin die im Lastenheft KOM-LE aufgeführten Rahmenbedingungen ([gemLH_KOM-LE#3]) und Projektanforderungen ([gemLH_KOM-LE#AnhB1]).

Die projektübergreifenden Anforderungen werden während der Designphase vom Basis-TI-Projekt erstellt.

2.2 Komponentenmodell

Abbildung 2 gibt einen Überblick auf die Telematikinfrastruktur aus Sicht der KOM-LE-Anwendung. Die Abbildung zeigt die für die KOM-LE-Anwendungsfälle relevanten Dienste und Komponenten und ihre Platzierung in den Tiers der TI. Das Primärsystem und die TI-Plattform sind für einen vollständigen Überblick aufgeführt, liegen aber nicht im Verantwortungsbereich des Projektes KOM-LE.

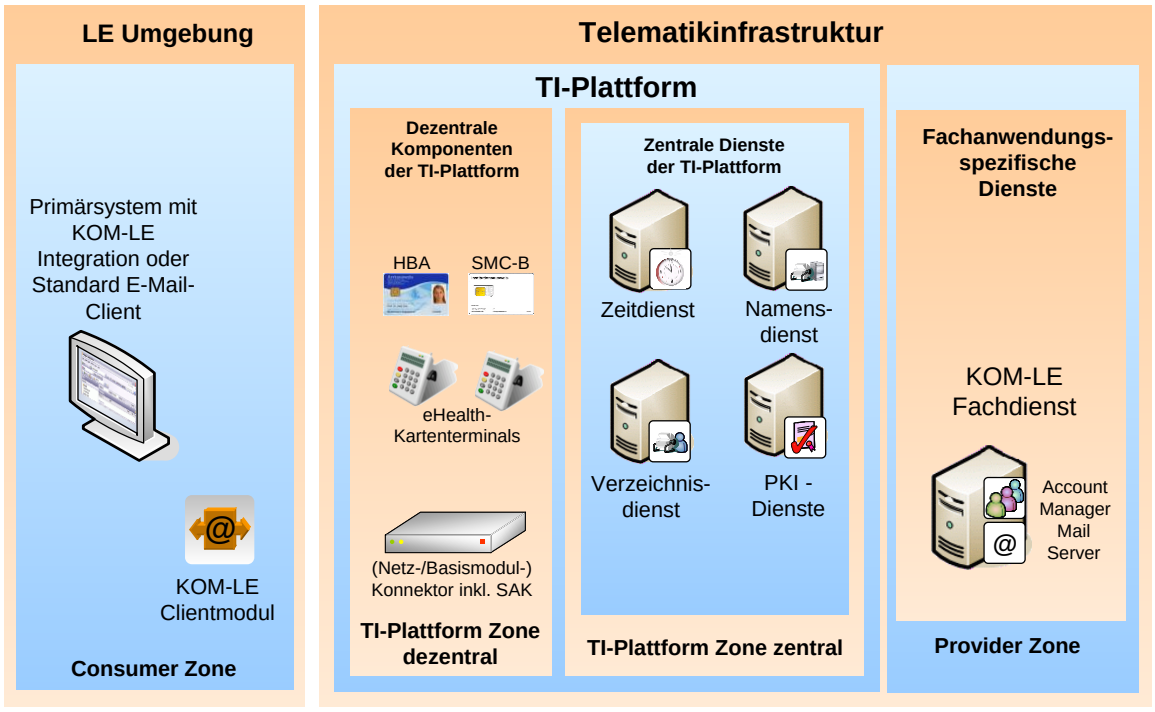

Abbildung 2: Abb_KOM-LE_Sicht_TI KOM-LE-Sicht auf die Telematikinfrastruktur

In

Abbildung 3 ist das Komponentendiagramm mit für die Anwendung KOM-LE relevanten Komponenten und Schnittstellen dargestellt. Eine Beschreibung der Schnittstellen erfolgt im Kapitel 4.

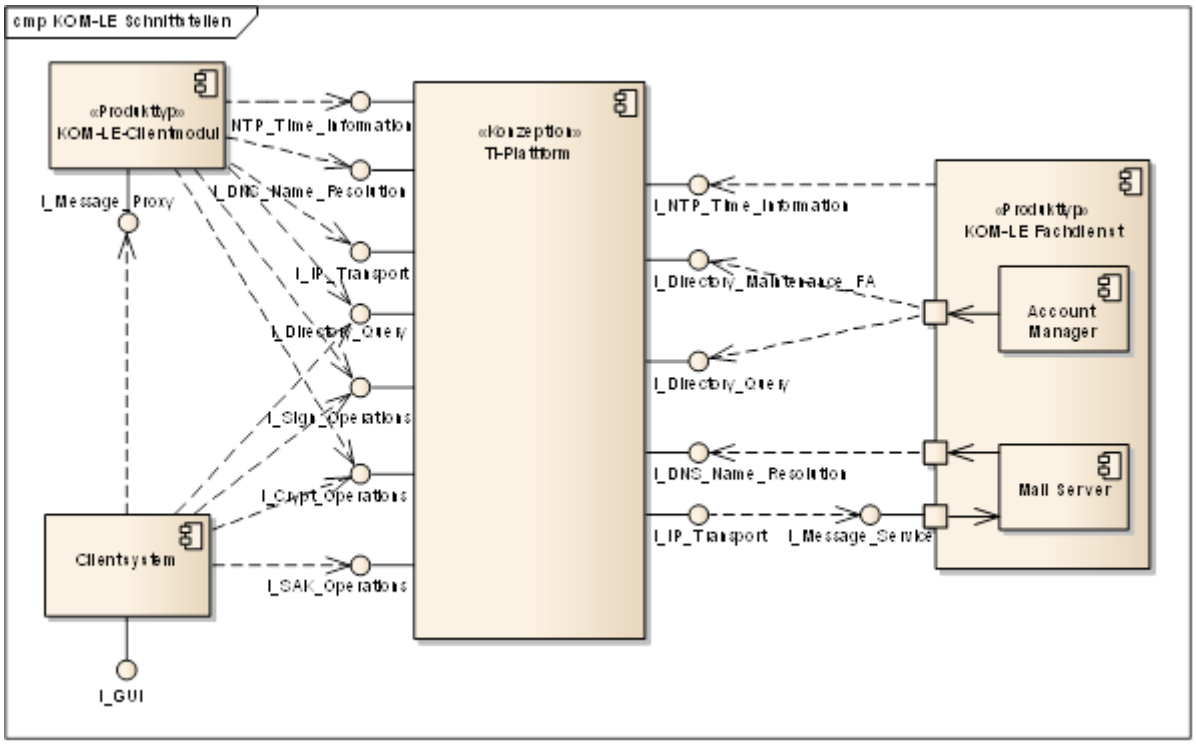

Abbildung 3: Abb_Komp_KOM-LE Komponentendiagramm KOM-LE

Die TI-Plattform ist entsprechend dem Konzept der Architektur der TI-Plattform [gem-KPT_Arch_TIP] als „Black Box“ mit ihren Außenschnittstellen visualisiert. Dargestellt sind nur diejenigen Außenschnittstellen, die im Rahmen der Anwendung KOM-LE genutzt werden.

Die Komponenten werden im Kapitel 5 den Produkttypen der Fachanwendung KOM-LE zugeordnet.

2.2.1 Komponente Clientsystem

Die Komponente Clientsystem stellt dem KOM-LE-Teilnehmern ~~(Leistungserbringer und ihre Mitarbeiter)~~ die Schnittstelle I_GUI zur Nutzung der KOM-LE-Leistungsmerkmale zur Verfügung.

Das Leistungsmerkmal „Adressierte Kommunikation Leistungserbringer“ kann von einem Clientsystem sowohl durch die Nutzung marktüblicher E-Mail-Clients als auch durch die Integration der E-Mail-Funktionalität in die PVS, KIS und AVS umgesetzt werden. Das Clientsystem benutzt hierzu die Schnittstelle I_Message_Proxy, die durch das KOM-LE-Clientmodul angeboten wird.

Das Leistungsmerkmal „Dokument schützen“ wird durch das Clientsystem unter ausschließlicher Verwendung von Schnittstellen, die durch die TI-Plattform zur Verfügung gestellt werden, realisiert.

2.2.2 Komponente KOM-LE-Clientmodul

Das KOM-LE-Clientmodul fungiert als SMTP und POP3-Proxy. Das Clientmodul stellt

dem KOM-LE-Teilnehmer die Funktionalität für den automatischen Schutz von KOM-LE-Nachrichten zur Verfügung. Beim Versenden der Nachrichten führt das Clientmodul die Verschlüsselung und das Signieren der E-Mails durch [gemSpec_CM_KOMLE#3.2.4.1.1]. Beim Abholen der Nachrichten führt das Clientmodul die Entschlüsselung und Signaturprüfung der E-Mails durch [gemSpec_CM_KOMLE#3.3.4.2].

Zur Realisierung dieser Funktionalität stellt das Clientmodul die Schnittstelle I_Message_Proxy mit den Operationen send_Message und receive_Message zur Verfügung.

Für Ver-/Entschlüsselung und Signaturerzeugung/Signaturprüfung benutzt das Clientmodul Schnittstellen der TI-Plattform, die die tatsächlichen kryptographischen Operationen durchführen.

2.2.3 Komponente TI-Plattform

Die Komponente TI-Plattform stellt als „Black Box“ die Funktionen der TI-Plattform mit ihren Außenschnittstellen zur Verfügung. Ihr detaillierter Aufbau ist im Konzept Architektur der TI-Plattform [gemKPT_Arch_TIP] beschrieben.

Durch KOM-LE werden dezentral folgende Schnittstellen benutzt:

- I_Directory_Query (Clientmodul: Ermittlung ENC-Zertifikate zur E-Mail-Verschlüsselung, PS: Ermittlung E-Mail-Adressen der Empfänger),
- I_SAK_Operations (PS: qualifizierte Signatur Dokumente),
- I_Sign_Operations (Clientmodul: Signatur MIME Objekte, PS: Signatur Dokumente),
- I_Crypt_Operations (Clientmodul: Verschlüsselung/Entschlüsselung MIME Objekte, PS: Verschlüsselung/Entschlüsselung Dokumente),
- I_IP_Transport (Voraussetzung für die Kommunikation zwischen Clientmodul und Fachdienst in der TI),
- I_NTP_Time_Information (Clientmodul: Zeitinformation).
- I_DNS_Name_Resolution (Auflösung von DNS-Anfragen)

Fachdienstseitig werden folgende Schnittstellen benutzt:

- I_IP_Transport (Voraussetzung für die Kommunikation zwischen Clientmodul und Fachdienst in der TI),
- I_DNS_Name_Resolution (Auflösung von DNS-Abfragen),
- I_Directory_Query (Einsicht in die Verzeichniseinträge),
- I_Directory_Application_Maintenance (Pflege der Verzeichniseinträge - Registrieren, Deregistrieren und Verzeichniseinträge ändern),
- I_NTP_Time_Information (Zeitinformation).

2.2.4 Komponente Fachdienst KOM-LE

Die Komponente Fachdienst KOM-LE Provider besteht aus den Teilkomponenten Account Manager und Mail Server (SMTP und POP3-Server).

Die Teilkomponente Account Manager nutzt die Schnittstellen I_Directory_Application_Maintenance und I_Directory_Query der TI-Plattform, um die Registrierung, Deregistrierung und die Änderung von Verzeichniseinträgen der KOM-LE-Teilnehmer vorzunehmen.

Die Teilkomponente Mail Server stellt die Schnittstelle I_Message_Service zum Versenden und Abholen von E-Mails zur Verfügung.

2.3 Akteure und Berechtigungen

Für die Leistungsmerkmale der Fachanwendung KOM-LE sind die folgenden Akteure relevant:

- Leistungserbringer,
- medizinische Institution,
- ~~Leistungerbringerorganisation~~Organisation der Gesellschafter,
- KOM-LE-Teilnehmer (Leistungserbringer bzw. medizinische Institution oder ~~Leistungerbringerorganisation~~Organisation der Gesellschafter, die bei einem KOM-LE-Anbieter registriert sind) und
- KOM-LE-Fachdienst.

In der folgenden Tabelle werden für diese Akteure die fachlichen Berechtigungen dargestellt.

Tabelle 1: Tab_Fachl_Berech Fachliche Berechtigungsmatrix KOM-LE

		Akteure				
Anwendungsfälle		Leistungserbringer	medizinische Institution	~~Leistungerbringerorganisation~~Organisation der Gesellschafter	KOM-LE-Teilnehmer	KOM-LE-Fachdienst
	KOM-LE_AF_1 Nachricht senden				X	
	KOM-LE_AF_2 Nachricht empfangen				X	
	KOM-LE_AF_3 Teilnehmer registrieren	X	X	X		X
	KOM-LE_AF_4 Teilnehmer deregistrieren				X	X

Bei der Durchführung der Anwendungsfälle zum Schutz der Inhalte von Nachrichten und

Dokumenten müssen in KOM-LE ausschließlich die folgenden (privaten) Schlüssel und Zertifikate verwendet werden:

Tabelle 2: Tab_Mtrx_Zert Matrix Zertifikatsbenutzung KOM-LE

		Sender				Empfänger			
		HBA QES		SMC-B O-SIG		HBA ENC		SMC-B ENC	
		ID.HP.QES		ID.HCI.OSIG		ID.HP.ENC		ID.HCI.ENC	
		Zertifikat	privater Schlüssel	Zertifikat	privater Schlüssel	Zertifikat	privater Schlüssel	Zertifikat	privater Schlüssel
KOM-LE_AF_1 Nachricht versenden (an LE)	S/MIME Signatur			K	K				
	S/MIME Verschlüsselung					R			
KOM-LE_AF_1 Nachricht versenden (an Institution/Organisation)	S/MIME Signatur			K	K				
	S/MIME Verschlüsselung							R	
KOM-LE_AF_2 Nachricht empfangen (LE)	S/MIME Signatur validieren			P					
	S/MIME Entschlüsselung						K		
KOM-LE_AF_2 Nachricht empfangen (Institution/Organisation)	S/MIME Signatur validieren			P					
	S/MIME Entschlüsselung								K

Legende: K – Gespeichert auf der Karte
R – Gespeichert im Verzeichnisdienst (remote)
P – Prüfung Zertifikat (Gespeichert außerhalb der Karte)

2.4 Zusammenhang der Anwendungsfälle

Der Zusammenhang der Anwendungsfälle wird als UML-Use-Case-Diagramm dargestellt. Abbildung 4 zeigt die für die Fachanwendung relevanten Anwendungsfälle und ihre Beziehungen untereinander. Die detaillierte Darstellung der Anwendungsfälle erfolgt in Kapitel 3.

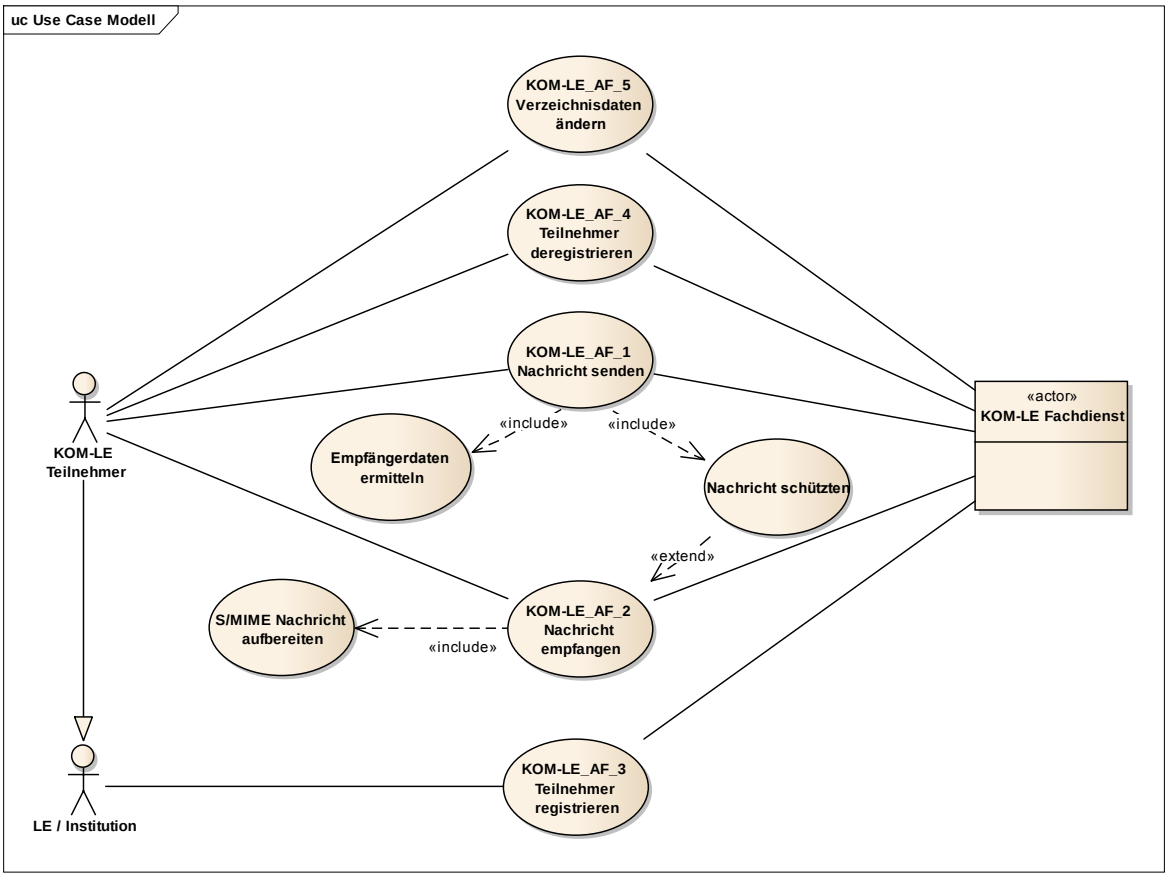

Abbildung 4: Abb_UseCases_KOM-LE Anwendungsfalldiagramm KOM-LE

3 Anwendungsfälle

In diesem Kapitel werden die Anwendungsfälle des Lastenheftes, gruppiert nach Leistungsmerkmalen, beschrieben. Für die Anwendungsfälle des Leistungsmerkmals „Adressierte Kommunikation Leistungserbringer“ existieren jeweils ein Aktivitätsdiagramm und ein Sequenzdiagramm. Die Aktivitätsdiagramme können auf weitere Prozesse verweisen, die dann wiederum in gesonderten Kapiteln durch Aktivitätsdiagramme und Sequenzdiagramme beschrieben werden.

Die Aktivitätsdiagramme zeigen die verwendeten Prozesse und die verwendeten Informationsobjekte des Anwendungsfalls auf. In den jeweiligen Sequenzdiagrammen wird derselbe Ablauf als technische Sequenz von parametrisierten Schnittstellenaufrufen abgebildet. Die Schnittstellen sind die logischen Schnittstellen der TI-Plattform und der Komponenten von KOM-LE.

Des Weiteren werden jeweils funktionale Ergänzungen zu den Bildern sowie die verfeinerten nicht funktionalen Anforderungen aufgeführt. In die nichtfunktionalen Anforderungen fließen die verfeinerten Performance-Anforderungen sowie die Ergebnisse der Schutzbedarfsfeststellung für die Prozesse ein.

3.1 Leistungsmerkmal adressierte Kommunikation Leistungserbringer

3.1.1 Anwendungsfall KOM-LE_AF_1 „Nachricht senden“

Im folgenden Aktivitätsdiagramm werden die notwendigen Aktivitäten und die beteiligten Informationsobjekte des Anwendungsfalls „Nachricht senden“ dargestellt.

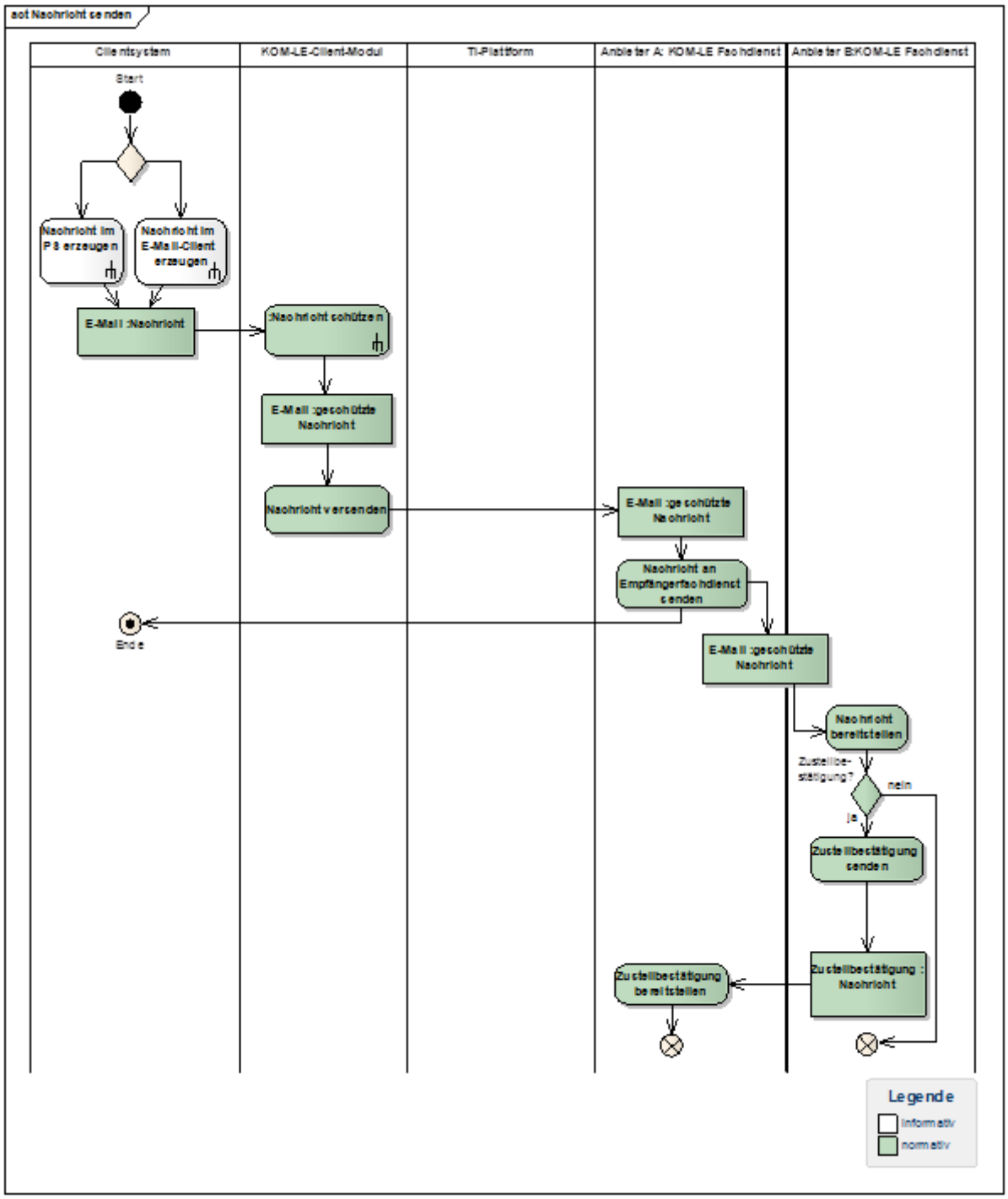

Abbildung 5: Abb_ADia_Snd_Msg Aktivitätsdiagramm Anwendungsfall KOM-LE_AF_1 Nachricht senden

⌦ KOM-LE-A_2174 Anwendungsfall KOM-LE_AF_1 „Nachricht senden“

Die Fachanwendung KOM-LE MUSS den Anwendungsfall KOM-LE_AF_1 "Nachricht senden" umsetzen und dabei die funktionalen Ergänzungen aus Tab_Snd_Msg Nachricht senden beachten**.** ⌫

Das Sequenzdiagramm in Abbildung 6 stellt die zu verwendenden Schnittstellen bei den Aktivitäten des Anwendungsfalls „Nachricht senden“ dar.

Die zusammengesetzten Aktivitäten „Nachricht im Primärsystem erzeugen“ und „Nachricht im E-Mail-Client erzeugen“ entsprechen dem Sequenzdiagramm „Nachricht im PS/E-Mail-Client erzeugen“. Die entsprechenden Aktivitäts- und Sequenzdiagramme werden im Kapitel 3.1.2 dargestellt.

Die zusammengesetzte Aktivität „Nachricht schützen“ entspricht dem Sequenzdiagramm „Nachricht schützen“. Die entsprechenden Aktivitäts- und Sequenzdiagramme werden im Kapitel 3.1.4 dargestellt.

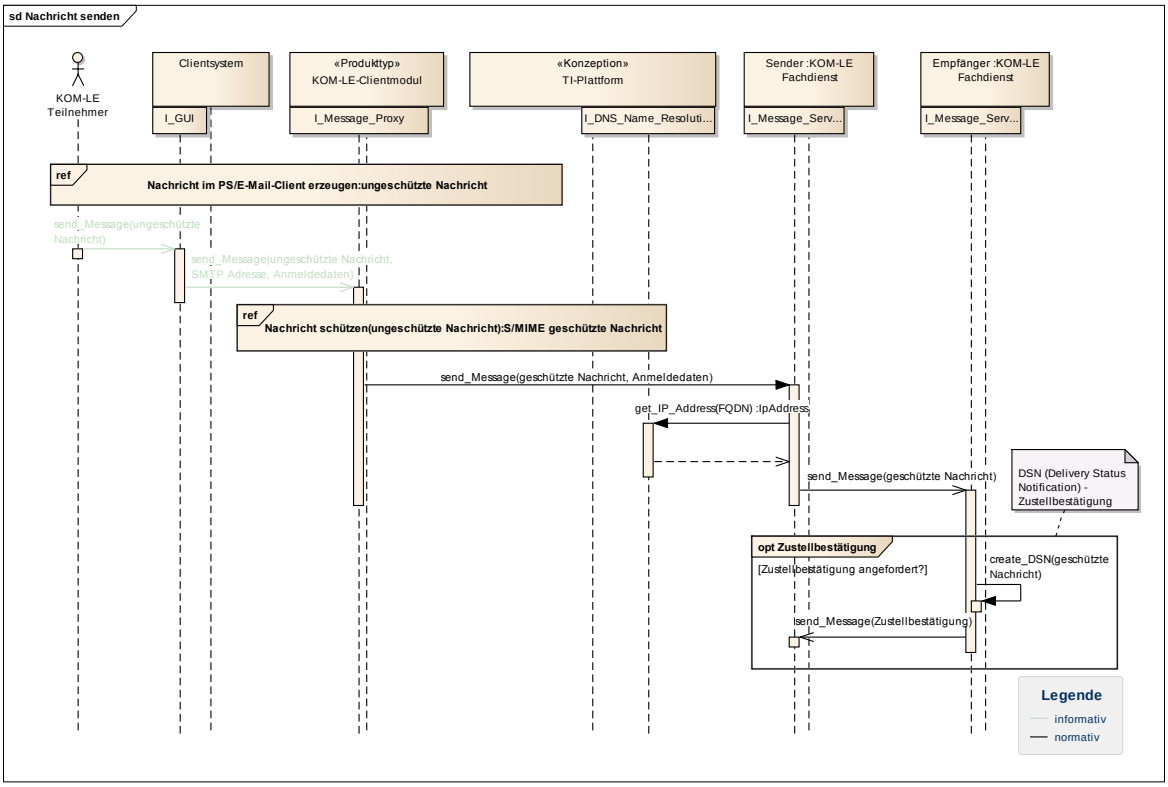

Abbildung 6: Abb_SDia_Snd_Msg Sequenzdiagramm Anwendungsfall KOM-LE_AF_1 „Nachricht senden“

Abbildung 7 zeigt wie Signatur und Verschlüsselung der im Client erzeugten Nachricht im KOM-LE-Clientmodul erfolgen. Der dafür relevante Subprozess „Nachricht schützen“ wird im Kapitel 3.1.4 detailliert beschrieben.

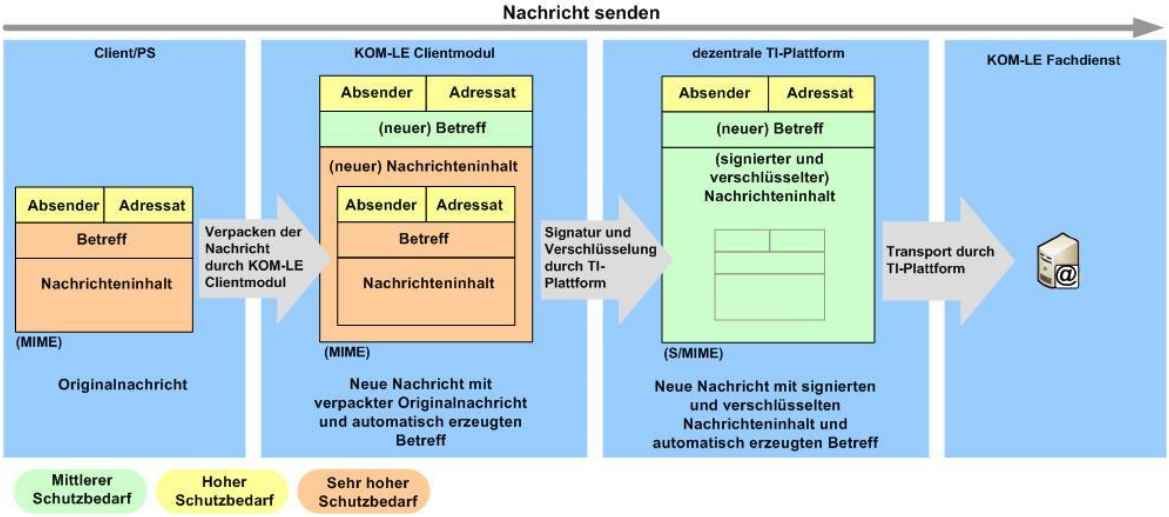

Abbildung 7: Abb_Integr_Vertr_Snd Anbringen des Integritäts- und Vertraulichkeitsschutzes beim Senden einer KOM-LE-Nachricht

3.1.1.1 Funktionale Ergänzungen zum Anwendungsfall

Die nachfolgende Tabelle führt zum Anwendungsfall normativ funktionale Ergänzungen auf, welche durch die Anwendung KOM-LE zu erfüllen sind

Tabelle 3: Tab_Snd_Msg Nachricht senden

KOM-LE_AF_1 Nachricht senden	
Kurzbeschreibung	Eine Nachricht, die im Primärsystem eines Teilnehmers oder durch einen E-Mail-Client erzeugt wird, wird an den durch den Teilnehmer ausgewählten Empfängerkreis versendet. Zum Versenden werden die Nachrichten automatisch durch das KOM-LE-Clientmodul verschlüsselt und signiert. Zusätzlich kann der Teilnehmer wählen, ob eine Zustell- und/oder Lesebestätigung erzeugt werden soll. Um die Zuordnung zwischen der Zustellbestätigung und der ursprünglichen Nachricht zu ermöglichen, muss die Zustellbestätigung die geschützte Ursprungsnachricht als Anhang beinhalten. Der Nachrichtentransport erfolgt unter Verwendung von TLS.
Initiierender Akteur	KOM-LE-Teilnehmer ~~(Leistungserbringer oder Mitarbeiter Leistungserbringer)~~
Auslöser	KOM-LE-Teilnehmer möchte eine Nachricht versenden.
Ergebnis	Nachricht steht den Empfängern zur Abholung bereit. Angeforderte Zustellbestätigungen wurden durch die KOM-LE-Fachdienste erzeugt. Falls die Nachricht nicht zugestellt werden konnte, muss der Sender darüber informiert werden.
Beteiligte Informationsobjekte	Nachricht (unsigniert, unverschlüsselt), S/MIME-geschützte Nachricht, ENC-Zertifikate Empfänger (ID.HP.ENC auf HBA oder ID.HCI.ENC auf SMC-B), Signaturschlüssel (ID.HCI.OSIG auf SMC-B), Anmeldedaten E-Mail-Account, Zustellbestätigung
Vorbedingungen	Sender und Empfänger sind bei einem KOM-LE-Anbieter regis-

KOM-LE_AF_1 Nachricht senden	
	triert. ENC-Zertifikate der Empfänger stehen zur Verfügung. Die SMC-B ist freigeschaltet.
Verwendete Standards	SMTP für Senden einer Nachricht ([RFC5321]) S/MIME Version 3.2 für Schutz einer Nachricht Delivery Status Notification für Zustellbestätigung ([RFC3464]) Standards, die Struktur einer Nachricht beschreiben, sind in Kapitel 6 erwähnt.
Fehlerfälle	Verschlüsselungszertifikat nicht verfügbar SMC-B ist nicht verfügbar Nachricht nicht zustellbar Falsche Anmeldedaten

3.1.1.2 Performanceanforderungen

Die für den Anwendungsfall geltenden Performancevorgaben sind in [gemSpec_Perf#4.4] beschrieben.

3.1.2 Subprozesse „Nachricht im Primärsystem erzeugen“ und Nachricht im „E-Mail-Client erzeugen“

Das Primärsystem (PVS, KIS, AVS) kann den KOM-LE-Teilnehmern Funktionen zum Erstellen und Versenden von E-Mails anbieten. Hier kann vor allem die Generierung der zu sendenden Inhalte direkt durch das Primärsystem erfolgen. Das Senden der Nachricht kann hier direkt aus dem Primärsystem heraus erfolgen.

Bietet das Primärsystem eines Teilnehmers diese Funktionen nicht an, kann dafür ein Standard-E-Mail-Client verwendet werden. Allerdings müssen hierzu durch den KOM-LE-Teilnehmer die zu sendenden Informationen ohne integrierte Unterstützung durch das Primärsystem an den E-Mail-Client übergeben werden.

Im folgenden Aktivitätsdiagramm werden die notwendigen Aktivitäten und die beteiligten Informationsobjekte des Subprozesses „Nachricht im Primärsystem erzeugen“ beschrieben.

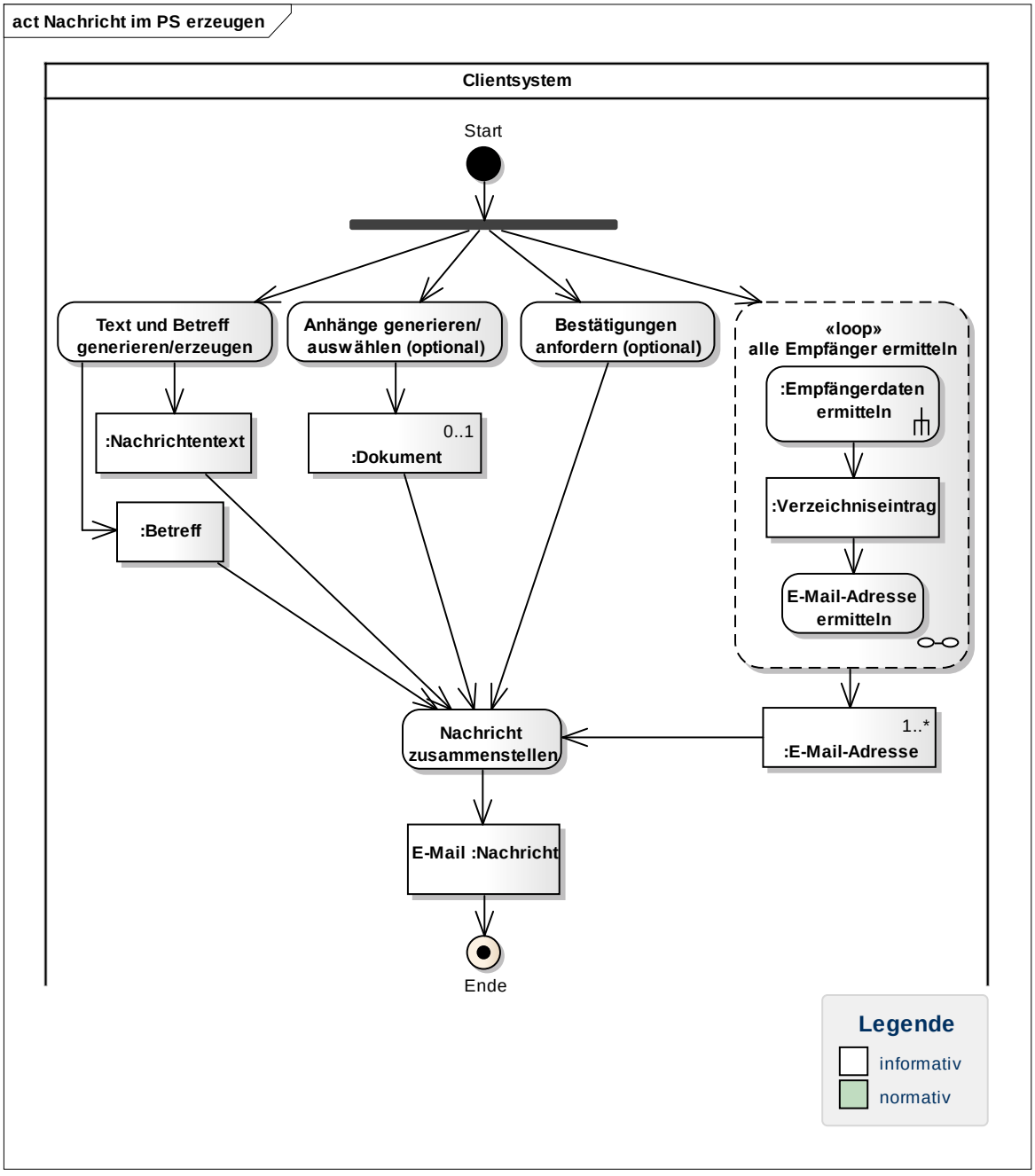

Abbildung 8: Abb_ADia_Msg_PS Aktivitätsdiagramm Subprozess "Nachricht im PS erzeugen"

Im folgenden Aktivitätsdiagramm werden die notwendigen Aktivitäten und die beteiligten Informationsobjekte des Subprozesses „Nachricht im E-Mail-Client erzeugen“ beschrieben.

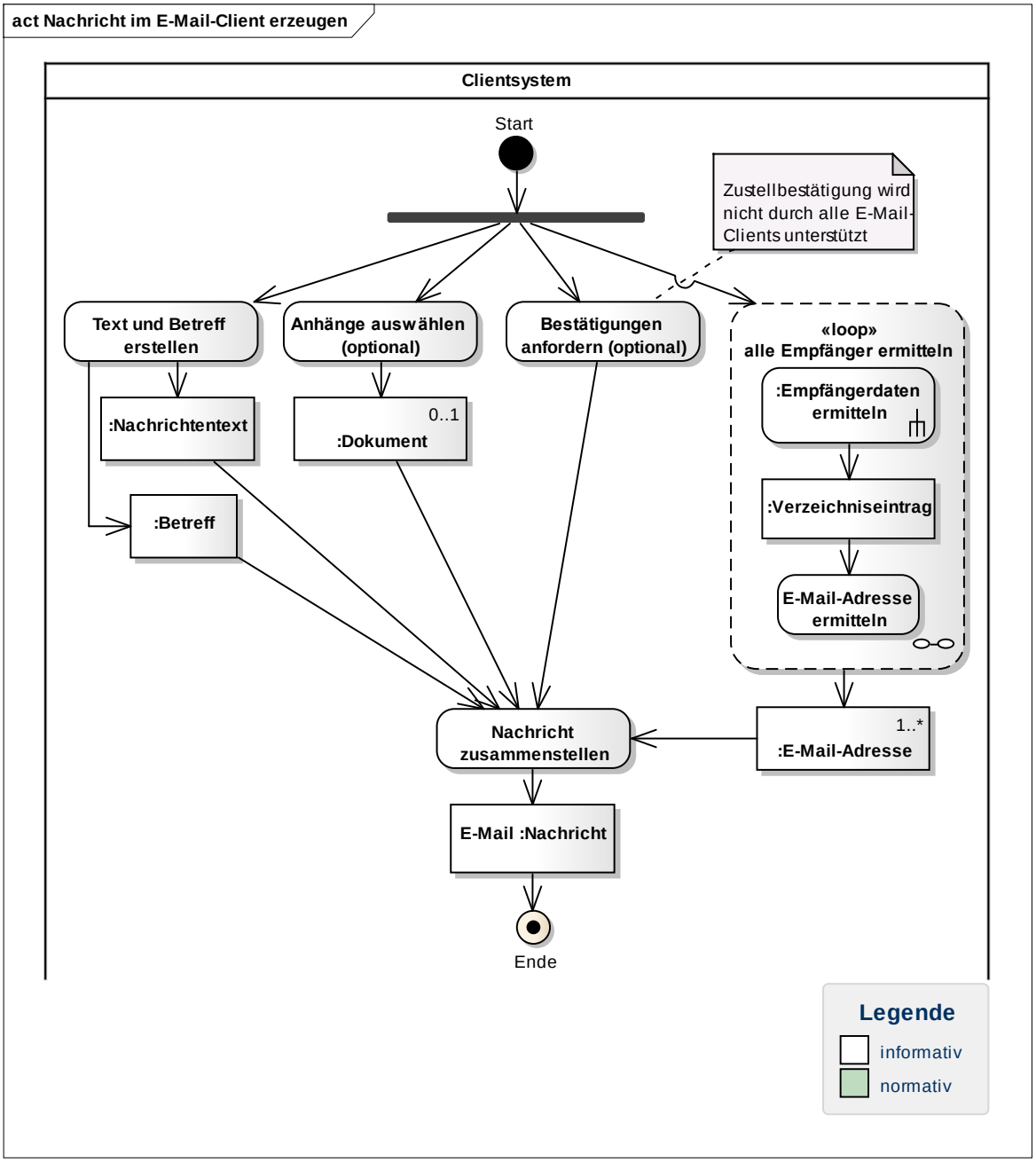

Abbildung 9: Abb_ADia_Msg_MC Aktivitätsdiagramm Subprozess "Nachricht im E-Mail-Client erzeugen"

Unabhängig davon, ob die Nachricht im Primärsystem oder im E-Mail-Client erzeugt wird, werden die gleichen Schnittstellen benutzt. Im Sequenzdiagramm „Nachricht im PS/E-Mail-Client erzeugen“ (Abbildung 10) ist dies berücksichtigt.

Die zusammengesetzte Aktivität „Empfänger ermitteln“ entspricht dem Sequenzdiagramm „Empfänger ermitteln“. Die entsprechenden Aktivitäts- und Sequenzdiagramme werden im Kapitel 3.1.4 dargestellt.

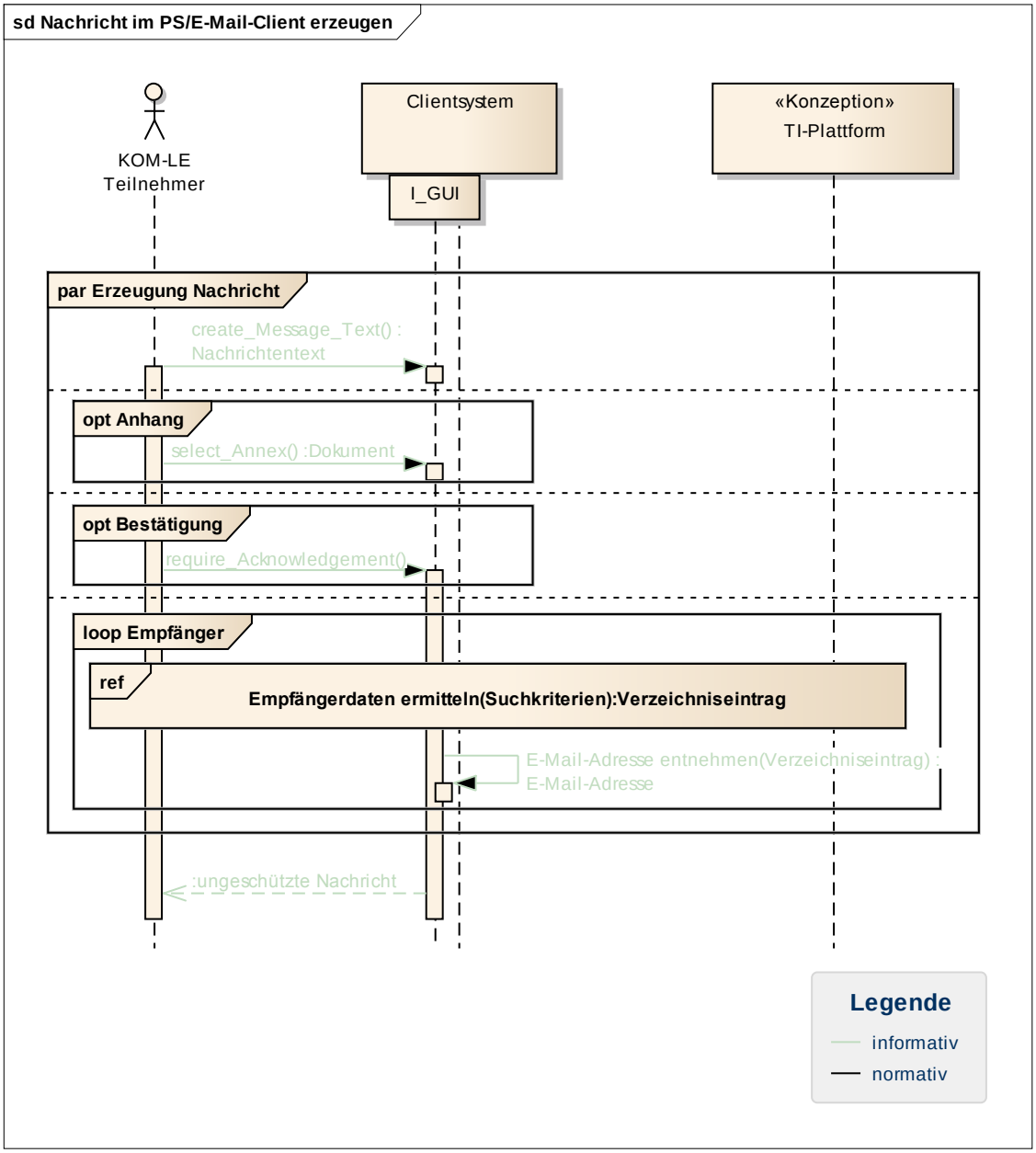

Abbildung 10: Abb_SDia_Msg_CS Sequenzdiagramm Subprozess "Nachricht im PS/E-Mail-Client erzeugen"

3.1.2.1 Funktionale Ergänzungen zum Subprozess

Die nachfolgende Tabelle führt zum Subprozess normativ funktionale Ergänzungen auf, welche durch die Anwendung KOM-LE zu erfüllen sind.

Tabelle 4: Tab_Msg_CS Subprozess "Nachricht im PS/E-Mail-Client erzeugen"

Nachricht im E-Mail-Client erzeugen	
Kurzbeschreibung	Erstellung einer E-Mail unter Verwendung des Primärsystems (PVS, KIS, AVS) oder eines Standard-E-Mail-Clients. Der Teilnehmer schreibt den Nachrichtentext, wählt optional

Nachricht im E-Mail-Client erzeugen	
	Anhänge aus, fordert optional Zustell- und/oder Lesebestätigung an und ermittelt die Empfänger.
Initiierender Akteur	KOM-LE-Teilnehmer ~~(Leistungserbringer oder Mitarbeiter Leistungserbringer)~~
Auslöser	KOM-LE-Teilnehmer wollen eine Nachricht erstellen.
Ergebnis	Nachricht steht im E-Mail-Client zum Versenden bereit.
Beteiligte Informationsobjekte	Nachricht (unsigniert, unverschlüsselt), E-Mail-Adressen Empfänger, Nachrichtentext, Betreff, Anhangsdokumente (optional), Verzeichniseintrag
Vorbedingungen	Empfänger sind bei einem KOM-LE-Anbieter registriert. E-Mail-Adressen der Empfänger sind bekannt oder können über den Verzeichnisdienst ermittelt werden.
Verwendete Standards	Standards, welche die Struktur einer Nachricht beschreiben, sind in Kapitel 6 erwähnt.
Fehlerfälle	Empfängerermittlung schlägt fehl

3.1.3 Subprozess „Empfängerdaten ermitteln“

Im folgenden Aktivitätsdiagramm werden die notwendigen Aktivitäten und die beteiligten Informationsobjekte des Subprozesses „Empfängerdaten ermitteln“ beschrieben.

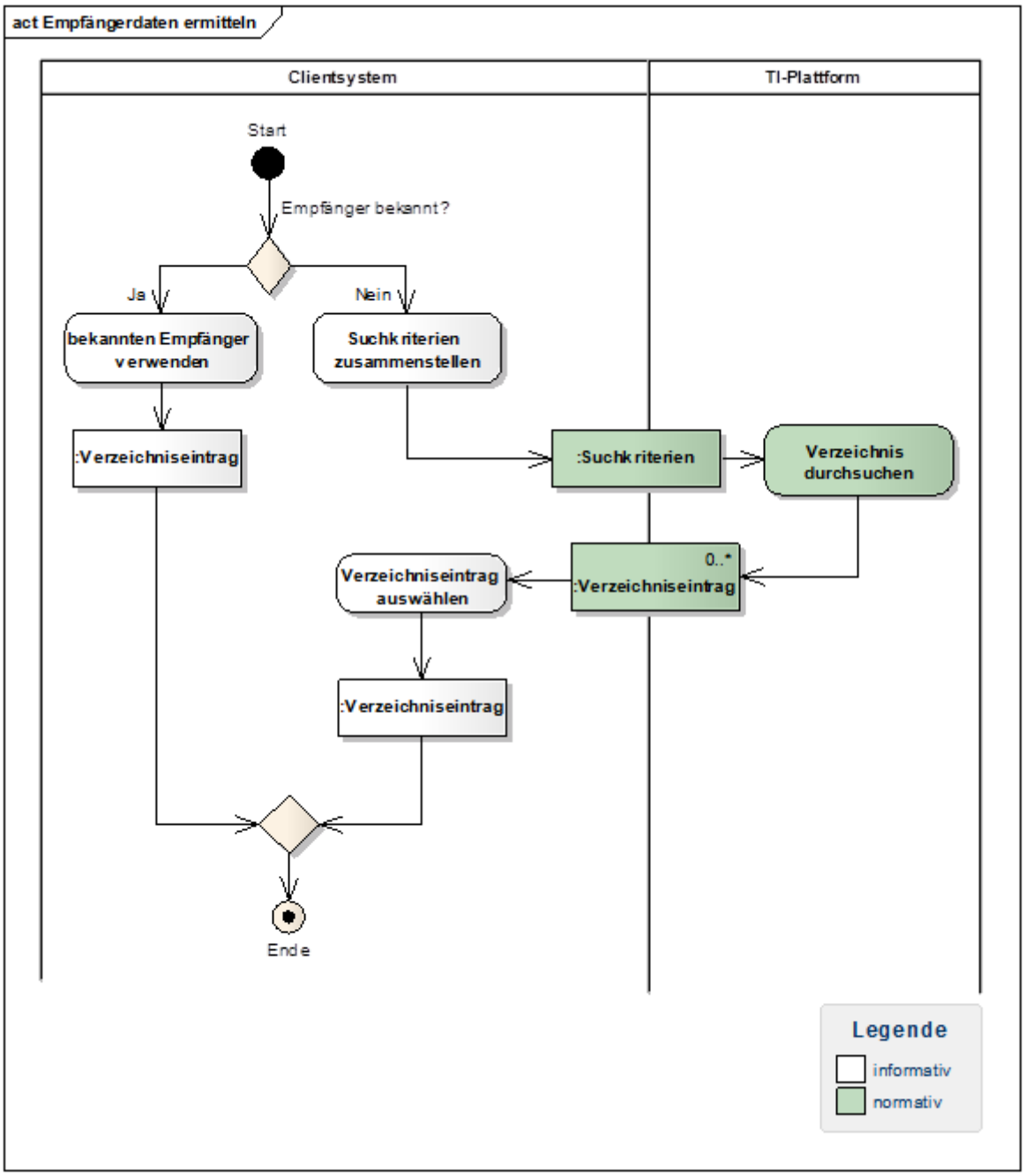

Abbildung 11: Abb_ADia_Rcpt Aktivitätsdiagramm Subprozess "Empfängerdaten ermitteln"

Das folgende Sequenzdiagramm stellt die zu verwendenden Schnittstellen bei den Aktivitäten des Subprozesses „Empfängerdaten ermitteln“ dar.

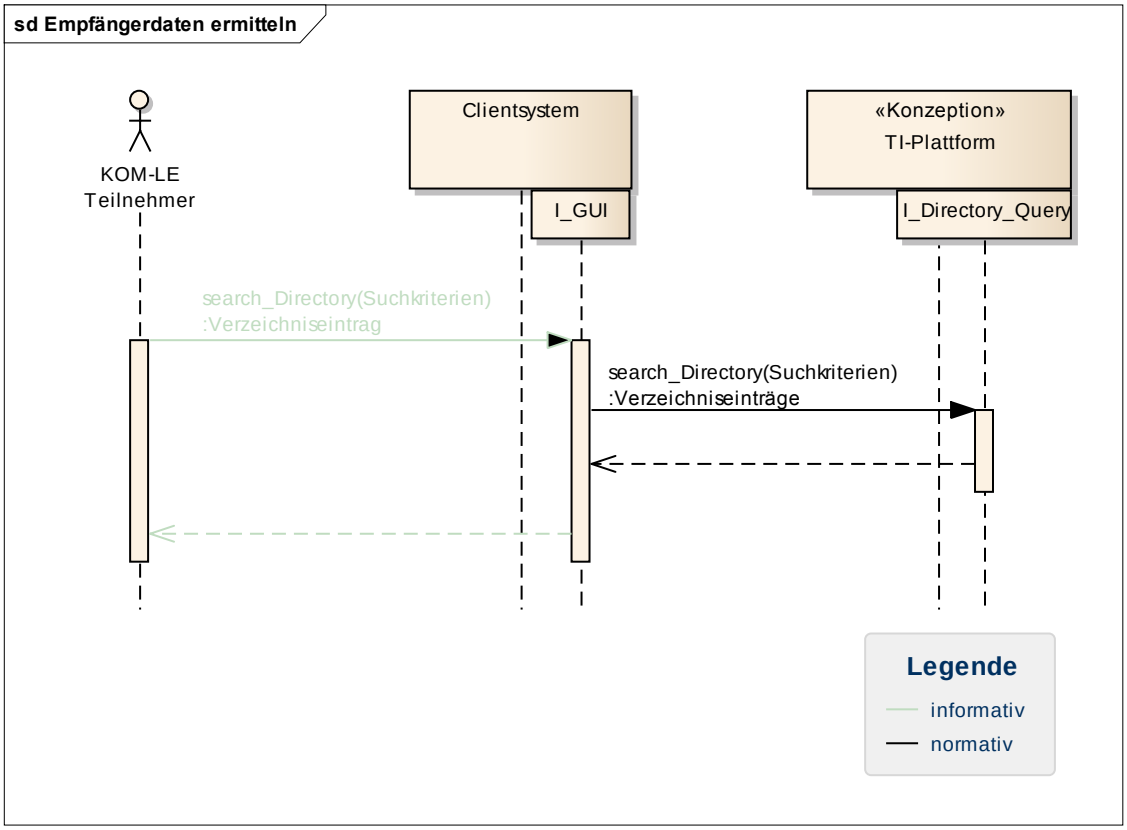

Abbildung 12: Abb_SDia_Rcpt Sequenzdiagramm Subprozess "Empfängerdaten ermitteln"

3.1.3.1 Funktionale Ergänzungen zum Subprozess

Die nachfolgende Tabelle führt zum Subprozess normativ funktionale Ergänzungen auf, welche durch die Anwendung KOM-LE zu erfüllen sind.

Tabelle 5: Tab_Rcpt Subprozess "Empfängerdaten ermitteln"

Nachricht im E-Mail-Client erzeugen	
Kurzbeschreibung	Der Subprozess liefert anhand von Suchkriterien passende Verzeichniseinträge aus dem Teilnehmerverzeichnis.
Initiierender Akteur	KOM-LE-Teilnehmer ~~(Leistungserbringer oder Mitarbeiter Leistungserbringer)~~
Auslöser	Nachricht soll an Empfänger versendet werden oder ein Dokument soll für einen Empfänger verschlüsselt werden.
Ergebnis	Gesuchte Empfängerinformationen wie E-Mail-Adresse und Verschlüsselungszertifikat stehen durch Lieferung der entsprechenden Verzeichniseinträge zur Verfügung.
Beteiligte Informationsobjekte	Suchkriterien, Verzeichniseintrag
Vorbedingungen	Die gesuchten Empfänger sind mit ihren Informationen im Teilnehmerverzeichnis eingetragen.
Fehlerfälle	Verzeichnisdienst nicht verfügbar, kein Eintrag entsprechend Suchkriterien vorhanden

3.1.4 Subprozess „Nachricht schützen“

Im folgenden Aktivitätsdiagramm werden die notwendigen Aktivitäten und die beteiligten Informationsobjekte des Subprozesses „Nachricht schützen“ beschrieben.

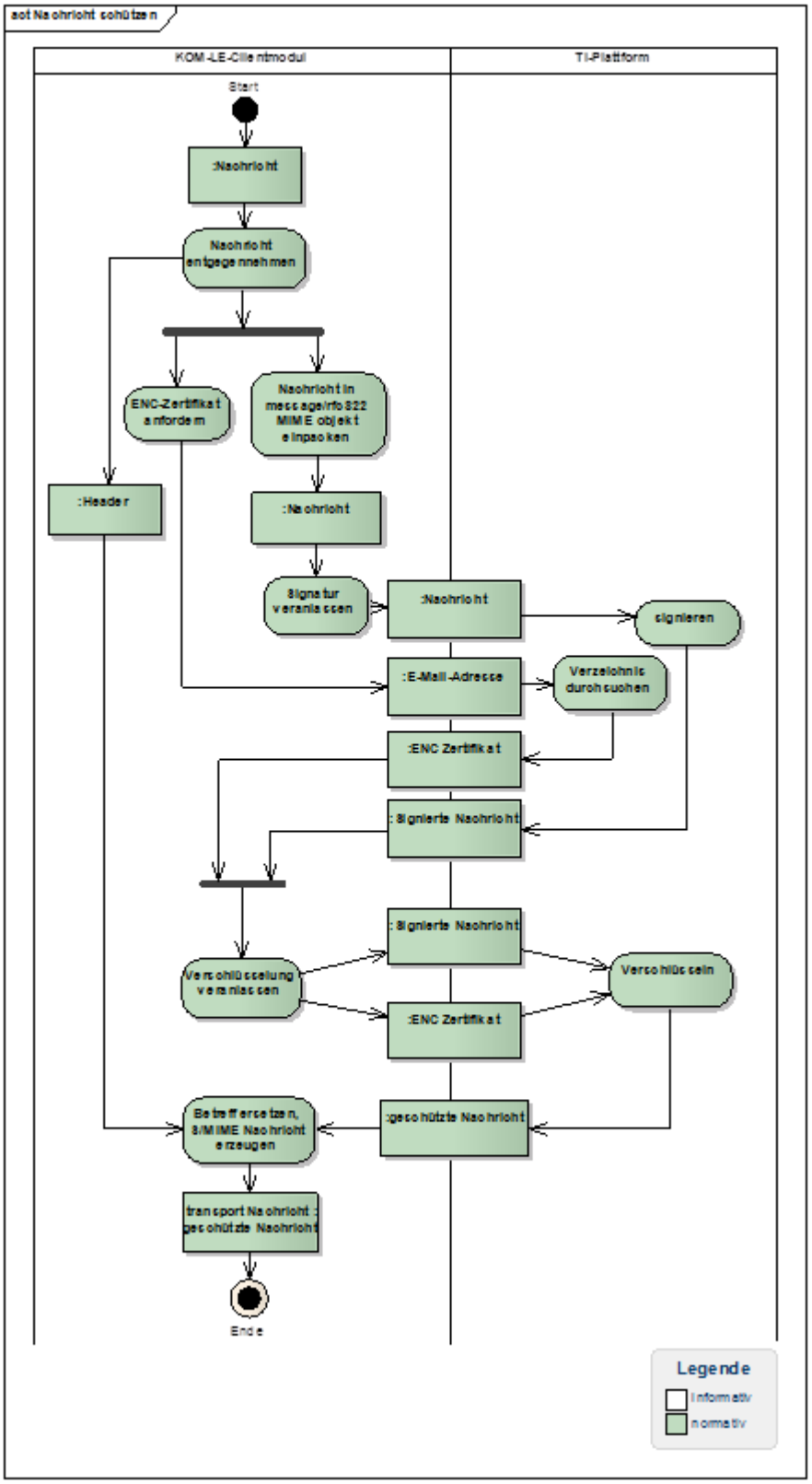

Abbildung 13: Abb_ADia_Prot_Msg Aktivitätsdiagramm Subprozess "Nachricht schützen"

Das folgende Sequenzdiagramm stellt die zu verwendenden Schnittstellen bei den Aktivitäten des Subprozesses „Nachricht schützen“ dar.

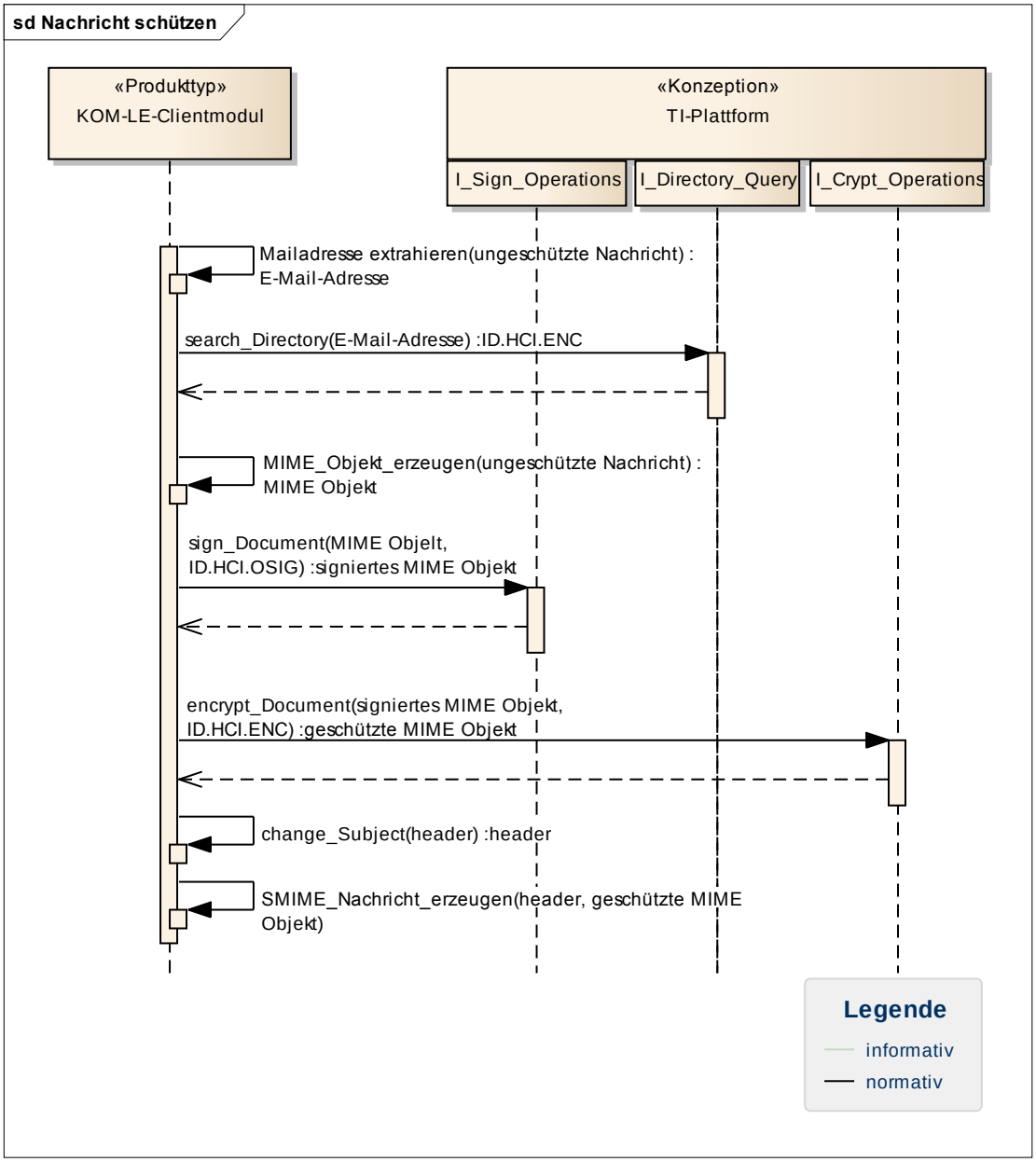

Abbildung 14: Abb_SDia_Prot_Msg Sequenzdiagramm Subprozess "Nachricht schützen"

Bei der Verschlüsselung muss die Nachricht auch für den Sender verschlüsselt werden. Dies ist erforderlich, um sicherzustellen, dass beim Empfangen einer Zustellbestätigung, die die ursprüngliche Nachricht als Anhang enthält, das Clientmodul des Senders der ursprünglichen Nachricht diese Nachricht entschlüsseln und in lesbarer Form als Teil der Zustellbestätigung an das Clientsystem weiterleiten kann.

3.1.4.1 Funktionale Ergänzungen zum Subprozess

Die nachfolgende Tabelle führt zum Subprozess normativ funktionale Ergänzungen auf, welche durch die Anwendung KOM-LE zu erfüllen sind.

Tabelle 6: Tab_Prot_MSG Subprozess "Nachricht schützen"

Nachricht schützen	
Kurzbeschreibung	Der Subprozess verpackt die übergebene Nachricht als MIME-Objekt in eine Transportnachricht. Die Transportnachricht erhält beim Verpacken die Adressinformationen des Original-Headers und einen generierten Betreff ohne personenbezogene medizinische Informationen. Anschließend wird die Transportnachricht signiert und verschlüsselt und somit eine S/MIME geschützte Nachricht erzeugt. Die Signatur der Transportnachricht erfolgt mit dem OSIG-Zertifikat der SMC-B und dient ausschließlich dem Integritätsschutz der Nachricht.
Initiierender Akteur	Aufruf durch übergeordneten Subprozess „Nachricht übertragen“
Auslöser	Nachricht soll an Empfänger versendet werden.
Ergebnis	geschützte Nachricht
Beteiligte Informationsobjekte	Nachricht, signierte Nachricht, geschützte Nachricht, E-Mail-Adresse, ENC-Zertifikat (ID.HP.ENC oder ID.HCI.ENC), Header
Vorbedingungen	ENC-Zertifikat des Empfängers ist für den KOM-LE-Clientmodul zugänglich.
Verwendete Standards	S/MIME Version 3.2 für Schutz einer Nachricht
Fehlerfälle	ENC-Zertifikat des Empfängers kann nicht ermittelt werden Fehler beim Signieren/Verschlüsseln des Bodies

3.1.5 Anwendungsfall KOM-LE_AF_2 „Nachricht empfangen“

Im folgenden Aktivitätsdiagramm werden die notwendigen Aktivitäten und die beteiligten Informationsobjekte des Anwendungsfalls „Nachricht empfangen“ dargestellt.

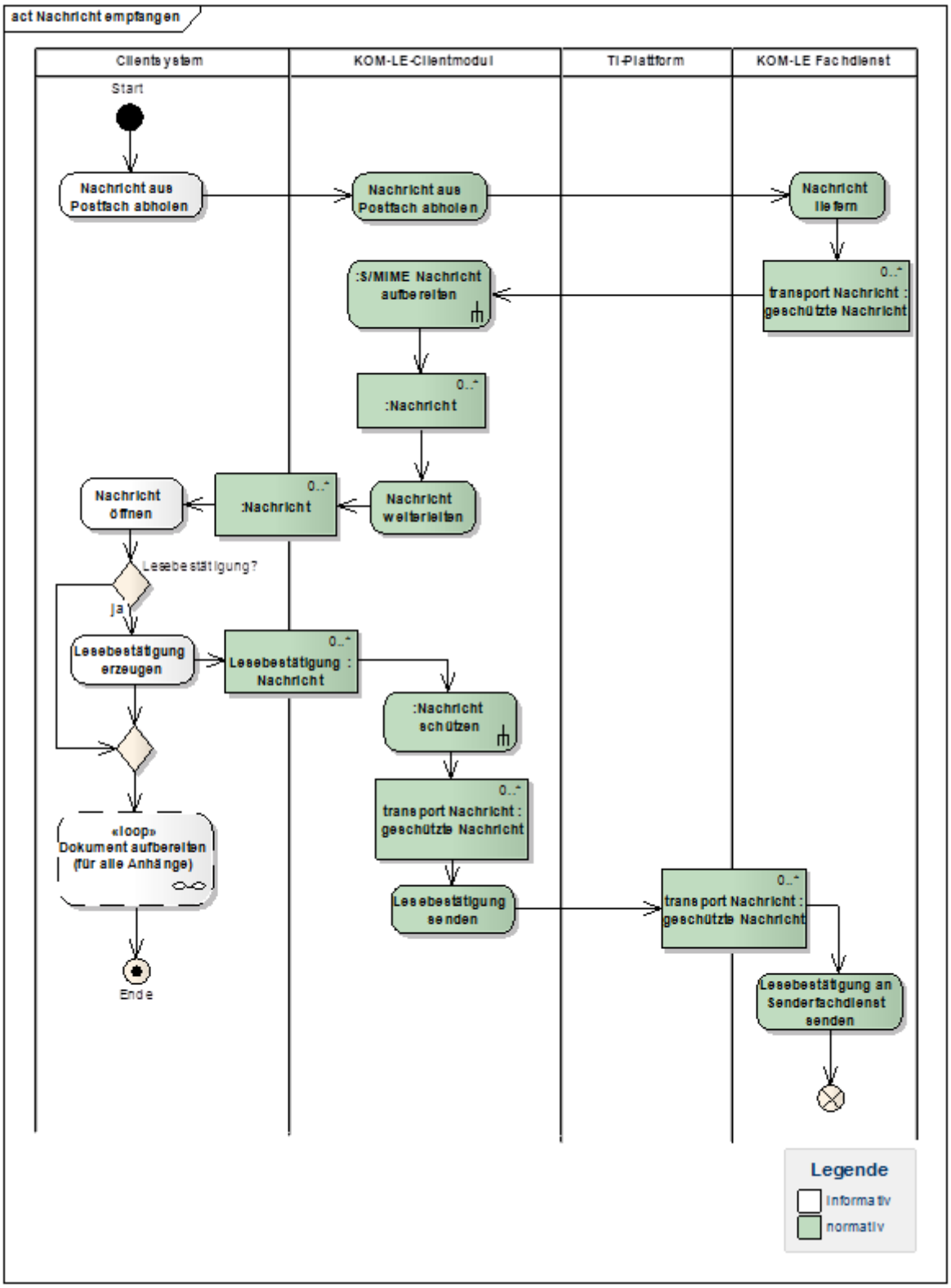

Abbildung 15: Abb_ADia_Rcv_Msg Aktivitätsdiagramm Anwendungsfall KOM-LE_AF_2 "Nachricht empfangen"

⌦ KOM-LE-A_2175 Anwendungsfall KOM-LE_AF_2 „Nachricht empfangen“

Die Fachanwendung KOM-LE MUSS den Anwendungsfall KOM-LE_AF_2 "Nachricht empfangen" umsetzen und dabei die funktionalen Ergänzungen aus Tab_Rcv_Msg Nachricht empfangen beachten. ⌫

Die zusammengesetzte Aktivität „S/MIME-Nachricht aufbereiten“ entspricht dem Sequenzdiagramm „S/MIME-Nachricht aufbereiten“. Die entsprechenden Aktivitäts- und Sequenzdiagramme werden im Kapitel 3.1.6 dargestellt.

Die zusammengesetzte Aktivität „Nachricht schützen“ und das entsprechende Sequenzdiagramm wurden in Kapitel 3.1.4 beschrieben.

Das Sequenzdiagramm im Abbildung 16 stellt die zu verwendenden Schnittstellen bei den Aktivitäten des Anwendungsfalls „Nachricht empfangen“ dar.

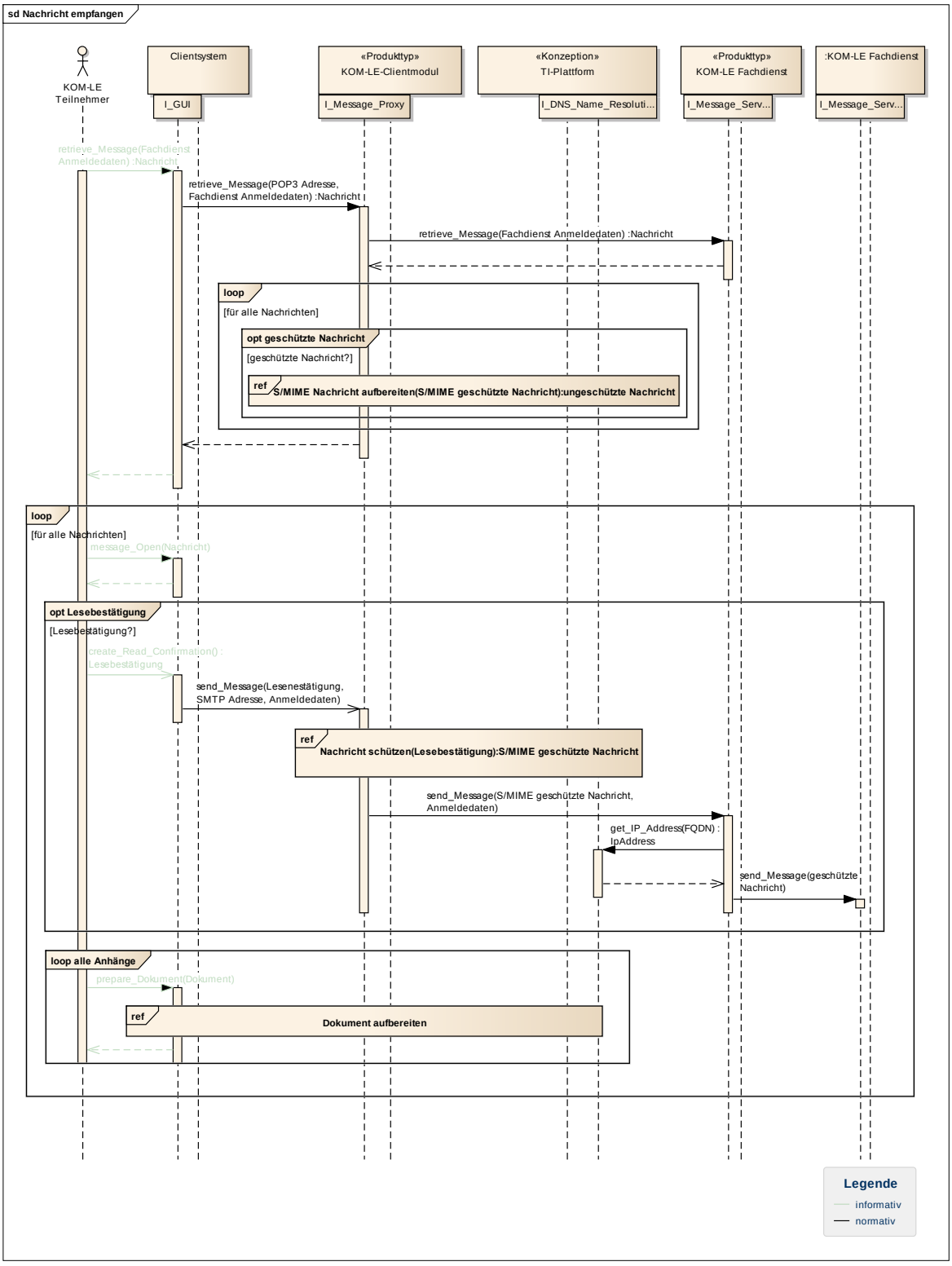

Abbildung 16: Abb_SDia_Rcv_Msg Sequenzdiagramm Anwendungsfall KOM-LE_AF_2 "Nachricht empfangen"

Abbildung 17 zeigt, wie die verpackte Originalnachricht entschlüsselt, ihre Signatur geprüft und ausgepackt wird. Der dafür relevante Subprozess „S/MIME-Nachricht aufbereiten“ wird im Kapitel 3.1.6 beschrieben.

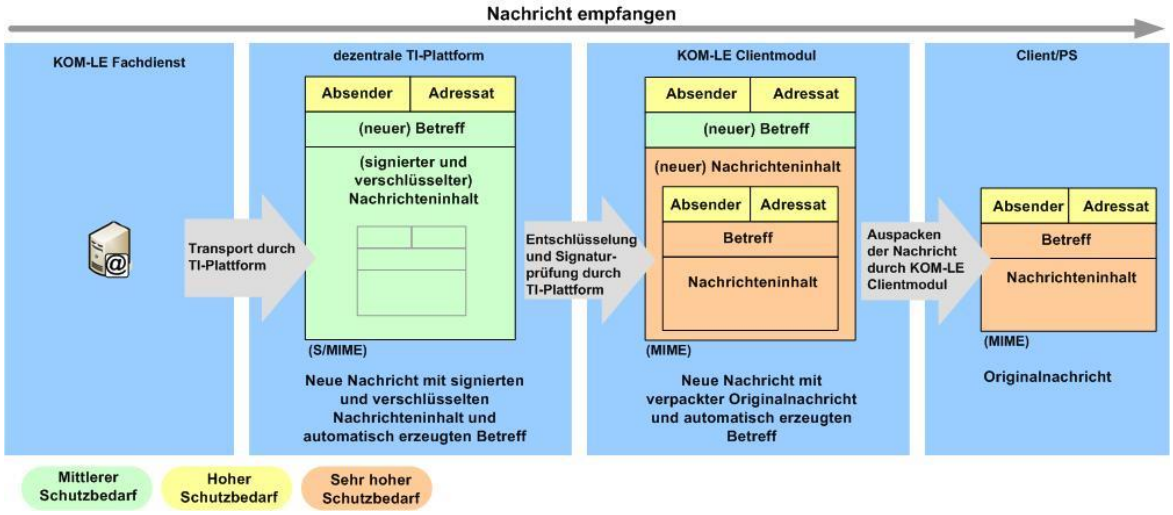

Abbildung 17: Abb_Del_Integr_Vertr Entfernen des Integritäts- und Vertraulichkeitsschutzes beim Empfangen einer KOM-LE-Nachricht

Das Versenden der Lesebestätigung erfolgt analog zum Versenden einer normalen KOM-LE-Nachricht (siehe Kapitel 3.1.1). Die Aufbereitung der Nachrichtenanhänge erfolgt wie in Kapitel 3.2.2 Anwendungsfall „Dokument aufbereiten“ beschrieben.

3.1.5.1 Funktionale Ergänzungen zum Anwendungsfall

Die nachfolgende Tabelle führt zum Subprozess normativ funktionale Ergänzungen auf, welche durch die Anwendung KOM-LE zu erfüllen sind.

Tabelle 7: Tab_Rcv_Msg Nachricht empfangen

KOM-LE_AF_2 Nachricht empfangen	
Kurzbeschreibung	Nachrichten, die beim KOM-LE-Provider für den Empfänger bereitstehen, werden abgeholt. Dabei werden die Nachrichten durch das KOM-LE-Clientmodul automatisch entschlüsselt sowie deren Signatur geprüft. Die entschlüsselten E-Mails werden an das Primärsystem (AVS, KIS, AVS) bzw. den E-Mail-Client weitergeleitet. Der Nachrichtentransport erfolgt unter Verwendung von TLS.
Initiierender Akteur	KOM-LE-Teilnehmer ~~(Leistungserbringer oder Mitarbeiter Leistungserbringer)~~
Auslöser	KOM-LE-Teilnehmer will seine Nachrichten abholen.
Ergebnis	Abgeholte Nachrichten stehen im Primärsystem (AVS, KIS, AVS) bzw. E-Mail-Client zur weiteren Bearbeitung zur Verfügung.
Beteiligte Informationsobjekte	Nachricht (unsigniert, unverschlüsselt), S/MIME-geschützte Nachricht, Anmeldedaten E-Mail-Account, Lesebestätigung, S/MIME-geschützte Lesebestätigung
Vorbedingungen	Empfänger ist bei einem KOM-LE-Anbieter registriert. Die SMC-B ist freigeschaltet.

KOM-LE_AF_2 Nachricht empfangen	
	Die Karte mit dem entsprechenden ENC-Schlüssel (ID.HP.ENC oder ID.HCI.ENC) ist zugänglich
Verwendete Standards	POP3 für Empfangen einer Nachricht [RFC1939] Message Disposition Notification für Lesebestätigung [RFC3798]
Fehlerfälle	KOM-LE-Provider nicht erreichbar Nachricht nicht entschlüsselbar Signaturprüfung der Nachricht fehlerhaft Falsche Anmeldedaten

3.1.5.2 Performanceanforderungen

Die für den Anwendungsfall geltenden Performancevorgaben sind in [gemSpec_Perf#4.4] beschrieben.

3.1.6 Subprozess „S/MIME-Nachricht aufbereiten“

Im folgenden Aktivitätsdiagramm werden die notwendigen Aktivitäten und die beteiligten Informationsobjekte des Subprozesses „S/MIME-Nachricht aufbereiten“ beschrieben.

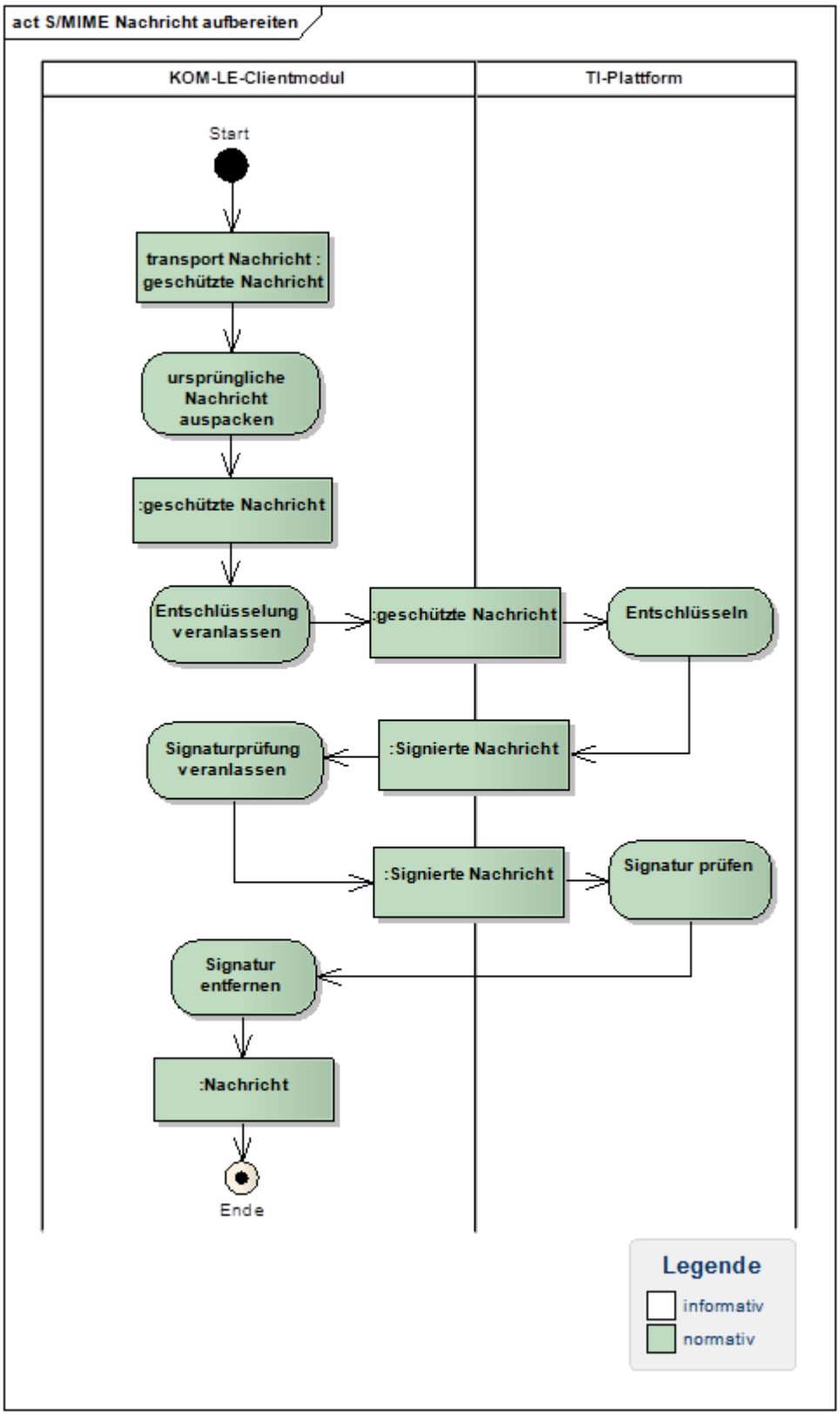

Abbildung 18: Abb_ADia_Prep_Msg Aktivitätsdiagramm Subprozess "S/MIME-Nachricht aufbereiten“

Das folgende Sequenzdiagramm stellt die zu verwendenden Schnittstellen bei den Aktivitäten des Subprozesses „S/MIME-Nachricht aufbereiten“ dar.

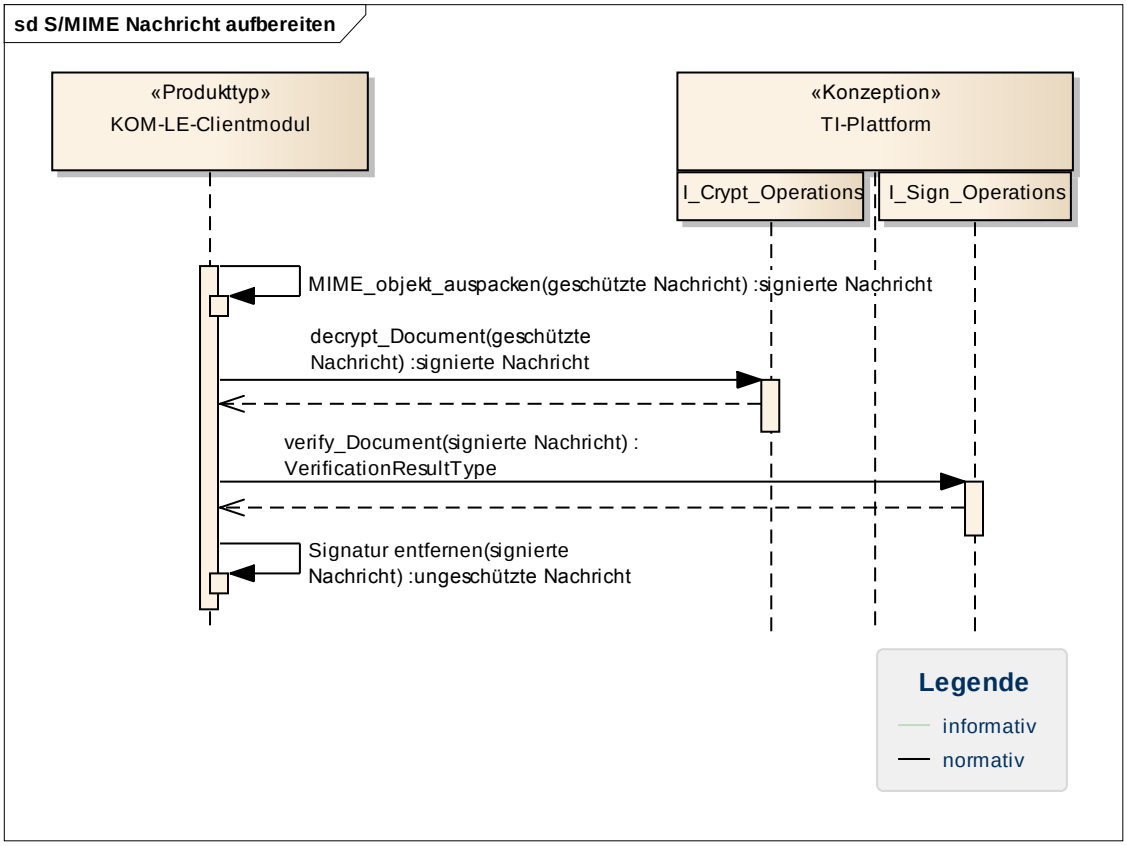

Abbildung 19: Abb_SDia_Prep_Msg Sequenzdiagramm Subprozess "S/MIME-Nachricht aufbereiten“

3.1.6.1 Funktionale Ergänzungen zum Subprozess

Die nachfolgende Tabelle führt zum Subprozess normativ funktionale Ergänzungen auf, welche durch die Anwendung KOM-LE zu erfüllen sind.

Tabelle 8: Tab_Prep_Msg Subprozess "S/MIME-Nachricht aufbereiten"

S/MIME-Nachricht aufbereiten	
Kurzbeschreibung	Der Subprozess entschlüsselt die Transportnachricht und prüft ihre Signatur. Nach der Signaturprüfung wird die Signatur von der Transportnachricht entfernt und anschließend die ursprüngliche Nachricht aus der Transportnachricht ausgepackt.
Initiierender Akteur	Aufruf durch übergeordneten Anwendungsfall „Nachricht empfangen“
Auslöser	Nachricht wird vom Empfänger abgeholt.
Ergebnis	(ungeschützte) Nachricht

S/MIME-Nachricht aufbereiten	
Beteiligte Informationsobjekte	Nachricht, signierte Nachricht, geschützte Nachricht, E-Mail-Adresse, ENC-Zertifikat (ID.HP.ENC oder ID.HCI.ENC)
Vorbedingungen	Empfänger ist bei einem KOM-LE-Anbieter registriert. Die SMC-B ist freigeschaltet.
Fehlerfälle	Nachricht nicht entschlüsselbar Signaturprüfung der Nachricht fehlerhaft

3.1.7 Anwendungsfall KOM-LE_AF_3 „Teilnehmer registrieren“

Im folgenden Aktivitätsdiagramm werden die notwendigen Aktivitäten und die beteiligten Informationsobjekte des Anwendungsfalls „Teilnehmer registrieren“ beschrieben.

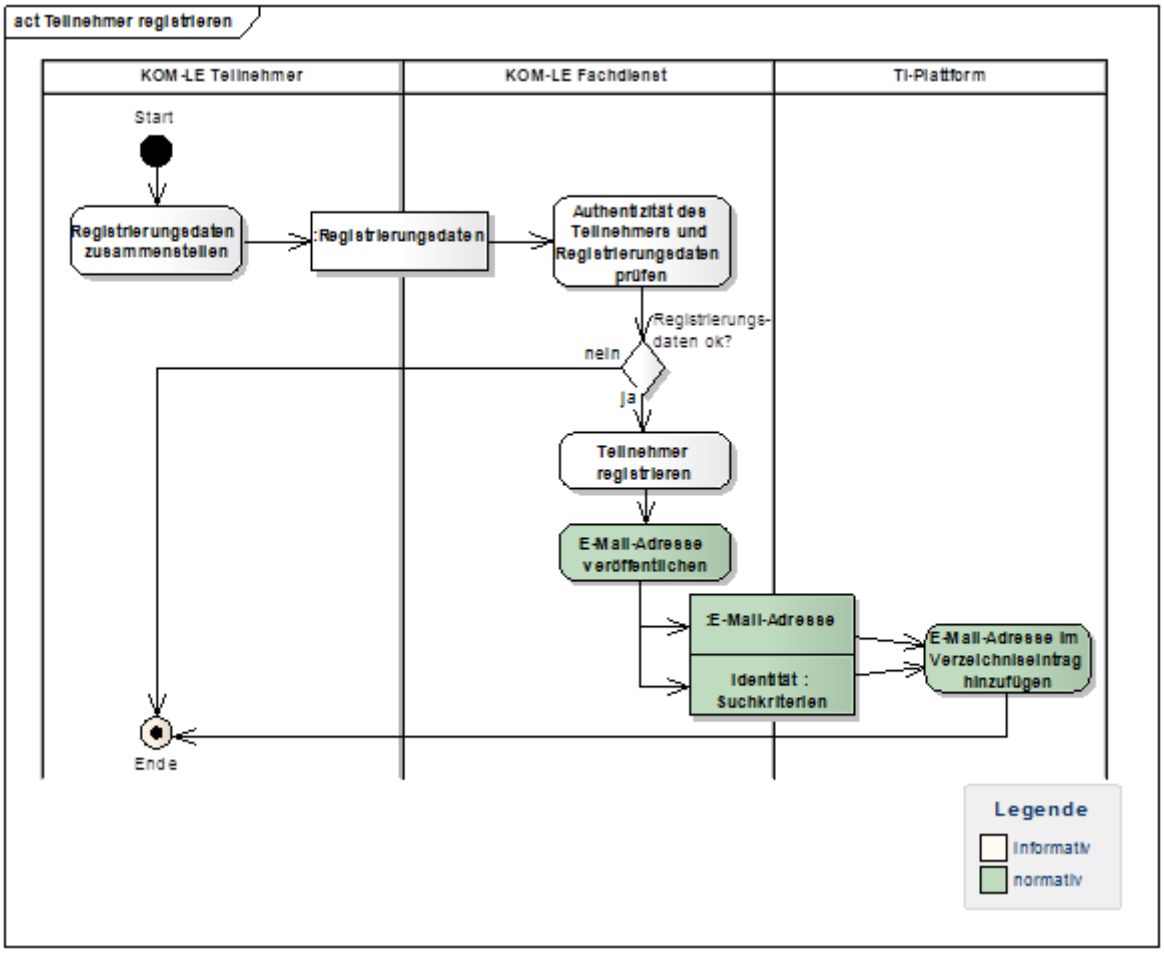

Abbildung 20: Abb_ADia_Reg_Usr Aktivitätsdiagramm Anwendungsfall KOM-LE_AF_3 "Teilnehmer registrieren"

⌦ KOM-LE-A_2194 Anwendungsfall KOM-LE_AF_3 „Teilnehmer registrieren“

Die Fachanwendung KOM-LE MUSS den Anwendungsfall KOM-LE_AF_3 "Teilnehmer registrieren" umsetzen und dabei die funktionalen Ergänzungen aus Tab_Reg_Usr Teilnehmer registrieren beachten. ⌫

Das folgende Sequenzdiagramm stellt die zu verwendenden Schnittstellen bei den Aktivitäten des Anwendungsfalls „Teilnehmer registrieren“ dar.

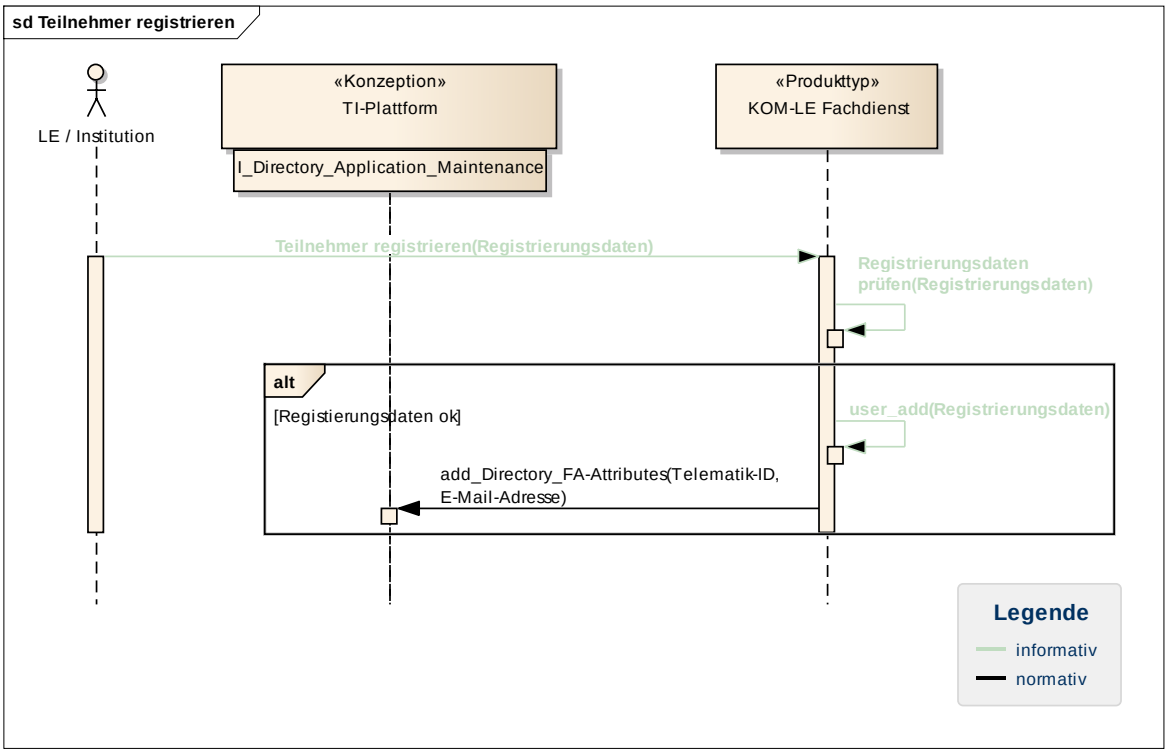

Abbildung 21: Abb_SDia_Reg_Usr Sequenzdiagramm Anwendungsfall KOM-LE_AF_3 "Teilnehmer registrieren"

3.1.7.1 Funktionale Ergänzungen zum Anwendungsfall

Die nachfolgende Tabelle führt zum Subprozess normativ funktionale Ergänzungen auf, welche durch die Anwendung KOM-LE zu erfüllen sind.

Tabelle 9: Tab_Reg_Usr Teilnehmer registrieren

KOM-LE_AF_3 Teilnehmer registrieren	
Kurzbeschreibung	Leistungserbringer, ~~oder~~ medizinische Institutionen oder ~~Leistungerbringerorganisation~~Organisation der Gesellschafter müssen sich bei einem KOM-LE-Anbieter registrieren, um Teilnehmer an KOM-LE zu werden. Dazu stellen sie ihre Registrierungsdaten zusammen und übergeben sie ihrem KOM-LE-Anbieter. Der KOM-LE-Anbieter prüft die Authentizität des Antragstellers sowie dessen Registrierungsdaten. Ist die Prüfung erfolgreich wird der Antragsteller als Teilnehmer registriert. Wie die Registrierungsdaten vom Leistungserbringer bzw. der medizinischen Institution oder ~~Leistungerbringerorganisation~~einer Organisation der Gesellschafter zum KOM-LE-Anbieter übertragen werden, legt der jeweilige KOM-LE-Anbieter fest. Der KOM-LE-Anbieter trägt somit auch die Verantwortung dafür, dass die Registrierungsdaten sicher unter Einhaltung der Datenschutzanforderungen übertragen werden. Um den KOM-LE-Anbieter bei der Durchführung dieses Prozesses zu unterstützen, bietet die TI den AUTH-Client

KOM-LE_AF_3 Teilnehmer registrieren	
	an, der es dem Leistungserbringer ermöglicht, sich mit Hilfe des HBA bzw. der SMC-B webbasiert, z.B. an einem Web-Portal, zu authentifizieren. Abweichend von der Lastenheftanforderung KOM-LE-A_1023, müssen alle KOM-LE-Teilnehmer einen Eintrag im Teilnehmerverzeichnis haben. Voraussetzung zur Teilnahme an KOM-LE ist, dass seine Basisdaten im Verzeichniseintrag vorliegen. Anhand der Informationen aus den Registrierungsdaten wird der Antragsteller identifiziert und erhält vom KOM-LE-Anbieter seine E-Mail-Adresse. Der Fachdienst des KOM-LE-Anbieters muss diese E-Mail-Adresse dem Verzeichniseintrag des Antragstellers hinzufügen. Der KOM-LE-Fachdienst muss dazu die Schnittstelle I_Directory_Application_Maintenance der TI-Plattform benutzen. Zur Identifizierung des Verzeichniseintrages des Antragstellers verwendet der KOM-LE-Fachdienst Identitätsinformationen des Antragstellers, die im Rahmen der Authentifizierung ermittelt wurden (Telematik-ID).
Initiierender Akteur	Leistungserbringer/medizinische Institution oder ~~Leistungerbringerorganisation~~Organisation der Gesellschafter für die Zusammenstellung der Registrierungsdaten. KOM-LE-Fachdienst für das Einbringen der E-Mail-Adresse in den Verzeichniseintrag.
Auslöser	Leistungserbringer/medizinische Institution oder ~~Leistungerbringerorganisation~~Organisation der Gesellschafter möchte bei einem bestimmten Provider an KOM-LE teilnehmen.
Ergebnis	Teilnehmer ist beim KOM-LE-Anbieter registriert und der zugehörige Verzeichniseintrag im Teilnehmerverzeichnis enthält die E-Mail-Adresse.
Beteiligte Informationsobjekte	Registrierungsdaten, E-Mail-Adresse, Verzeichniseintrag
Vorbedingungen	Leistungserbringer/medizinische Institution oder ~~Leistungerbringerorganisation~~Organisation der Gesellschafter können sich bei einem KOM-LE-Anbieter mit einem HBA oder einer SMC-B authentifizieren. Für den Antragsteller muss bereits ein Verzeichniseintrag im Teilnehmerverzeichnis existieren.
Fehlerfälle	Registrierungsdaten fehlerhaft Authentizitätsprüfung nicht erfolgreich Verzeichnisdienst der TI-Plattform nicht erreichbar Verzeichnisdaten fehlerhaft Verzeichniseintrag für Antragsteller nicht vorhanden

3.1.7.2 Performanceanforderungen

Die für den Anwendungsfall geltenden Performancevorgaben sind in [gemSpec_Perf#4.2.1] beschrieben.

3.1.8 Anwendungsfall KOM-LE_AF_4 „Teilnehmer deregistrieren“

Im folgenden Aktivitätsdiagramm werden die notwendigen Aktivitäten und die beteiligten

Informationsobjekte des Anwendungsfalls „Teilnehmer deregistrieren“ beschrieben.

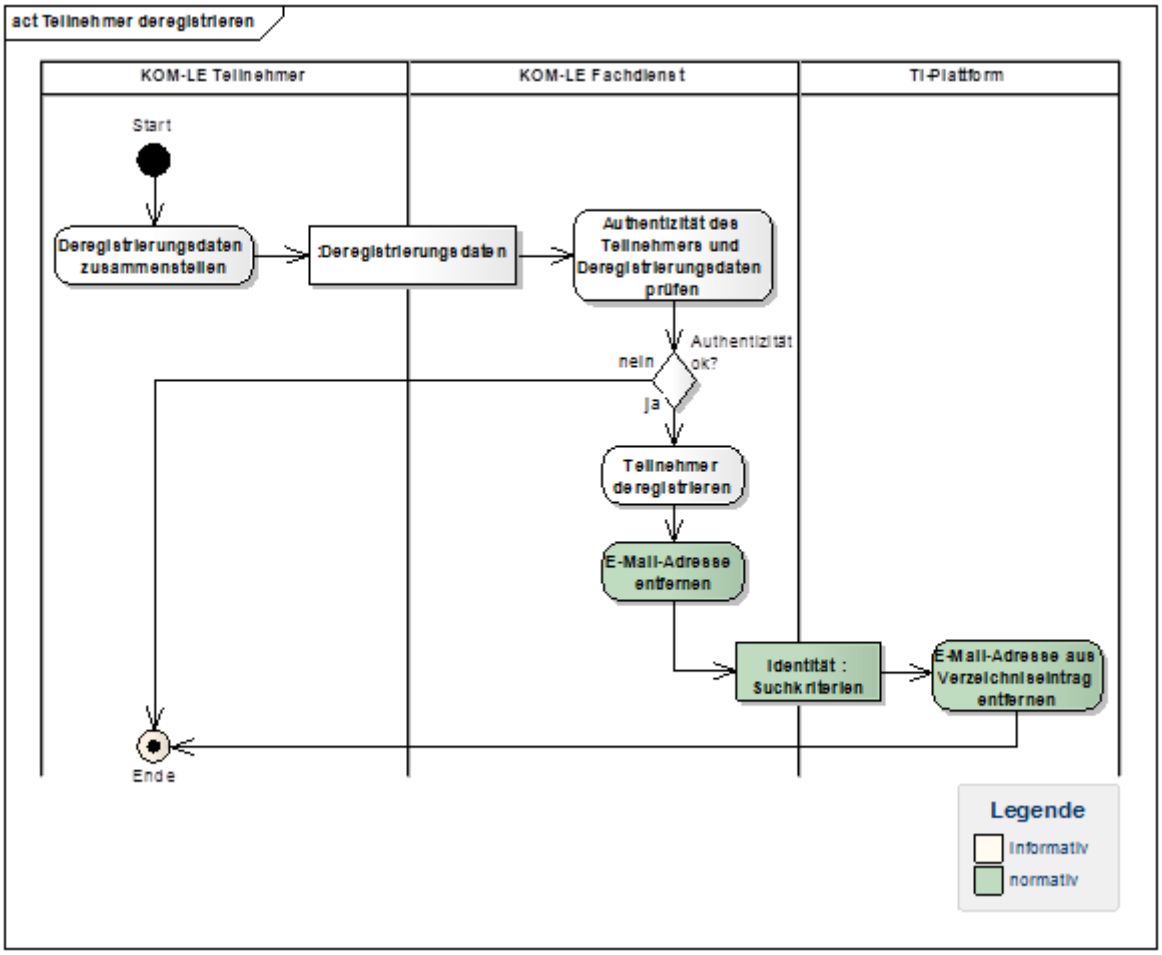

Abbildung 22: Abb_ADia_Dereg_Usr Aktivitätsdiagramm Anwendungsfall KOM-LE_AF_4 "Teilnehmer deregistrieren"

⌦ KOM-LE-A_2195 Anwendungsfall KOM-LE_AF_4 "Teilnehmer deregistrieren"

Die Fachanwendung KOM-LE MUSS den Anwendungsfall KOM-LE_AF_4 "Teilnehmer deregistrieren" umsetzen und dabei die funktionalen Ergänzungen aus Tab_Dereg_Usr Teilnehmer deregistrieren beachten**.** ⌫

Das folgende Sequenzdiagramm stellt die zu verwendenden Schnittstellen bei den Aktivitäten des Anwendungsfalls „Teilnehmer deregistrieren“ dar.

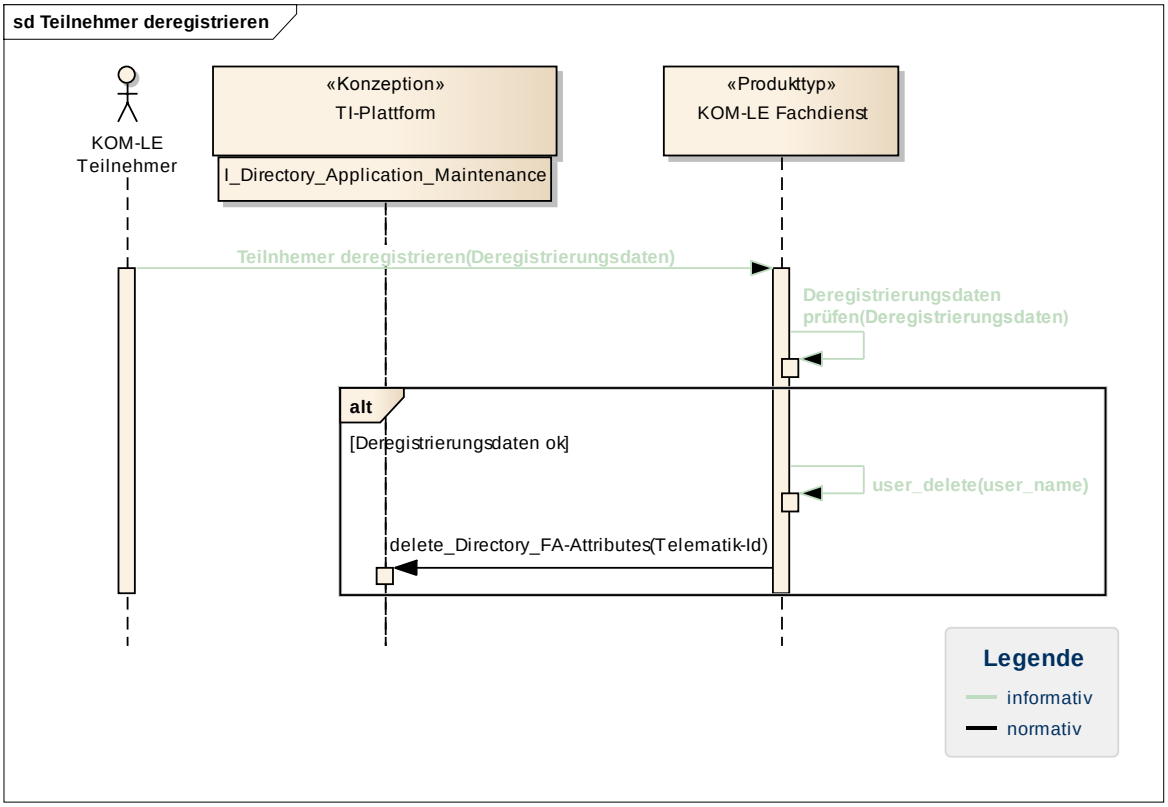

Abbildung 23: Abb_SDia_Dereg_Usr Sequenzdiagramm Anwendungsfall KOM-LE_AF_4 "Teilnehmer deregistrieren"

3.1.8.1 Funktionale Ergänzungen zum Anwendungsfall

Die nachfolgende Tabelle führt zum Anwendungsfall normativ funktionale Ergänzungen auf, welche durch die Anwendung KOM-LE zu erfüllen sind.

Tabelle 10: Tab_Dereg_Usr Teilnehmer deregistrieren

KOM-LE_AF_4 Teilnehmer deregistrieren	
Kurzbeschreibung	KOM-LE-Teilnehmer, die nicht mehr an KOM-LE teilnehmen wollen, müssen sich bei ihrem KOM-LE-Anbieter deregistrieren. Dazu stellen sie ihre Deregistrierungsdaten (wie Vertragsnummer, Beendigungsdatum) zusammen und übergeben sie ihrem KOM-LE-Anbieter. Der KOM-LE-Anbieter prüft die Authentizität des Teilnehmers. Ist die Prüfung erfolgreich, wird der Teilnehmer deregistriert. Wie die Deregistrierungsdaten vom KOM-LE-Teilnehmer zum KOM-LE-Anbieter übertragen werden, legt der jeweilige KOM-LE-Anbieter fest. Der KOM-LE-Anbieter trägt somit auch die Verantwortung dafür, dass die Deregistrierungsdaten sicher unter Einhaltung der Datenschutzanforderungen übertragen werden. Zur Unterstützung des KOM-LE-Anbieters bei der Durchführung dieses Prozesses bietet die TI den AUTH-Client an, der es dem Leistungserbringer ermöglicht, sich mit Hilfe des HBA bzw. der SMC-B webbasiert, z.B. an einem Web-Portal, zu authentifizieren. Bei Verlust des/der HBA/SMC-B muss eine Authentifizierung in diesem Anwendungsfall auch auf

KOM-LE_AF_4 Teilnehmer deregistrieren	
	anderem Wege möglich sein (z.B. über Nutzername und Passwort). Der Fachdienst des KOM-LE-Anbieters muss die E-Mail-Adresse aus dem Verzeichniseintrag des KOM-LE-Teilnehmers löschen. Der KOM-LE-Fachdienst muss dazu die Schnittstelle I_Dirctory_Application_Maintenance der TI-Plattform benutzen. Zur Identifizierung des Verzeichniseintrages des KOM-LE-Teilnehmers verwendet der KOM-LE-Fachdienst Identitätsinformationen des Teilnehmers, die entweder im Rahmen der Authentifizierung ermittelt wurden oder beim KOM-LE-Anbieter hinterlegt wurden (Telematik-ID).
Initiierender Akteur	KOM-LE-Teilnehmer für die Zusammenstellung der Deregistrierungsdaten. KOM-LE-Fachdienst für das Löschen der E-Mail-Adresse im Verzeichniseintrag.
Auslöser	Leistungserbringer/medizinische Institution oder ~~Leistungerbringerorganisation~~Organisation der Gesellschafter möchte den Vertrag mit seinem KOM-LE-Anbieter beenden.
Ergebnis	Teilnehmer ist beim KOM-LE-Anbieter deregistriert und aus dem zugehörigen Verzeichniseintrag im Teilnehmerverzeichnis wurde die E-Mail-Adresse entfernt.
Beteiligte Informationsobjekte	Deregistrierungsdaten, Verzeichniseintrag, Suchkriterien
Vorbedingungen	Leistungserbringer/medizinische Institution oder ~~Leistungerbringerorganisation~~Organisation der Gesellschafter sind bei einem KOM-LE-Anbieter registriert.
Fehlerfälle	Deregistrierungsdaten fehlerhaft Authentizitätsprüfung nicht erfolgreich Verzeichnisdienst der TI-Plattform nicht erreichbar

3.1.8.2 Performanceanforderungen

Die für den Anwendungsfall geltenden Performancevorgaben sind in [gemSpec_Perf#4.2.1] beschrieben.

3.1.9 Anwendungsfall KOM-LE_AF_5 „Verzeichnisdaten ändern“

Im Anwendungsfall KOM-LE_AF_5 „Verzeichnisdaten ändern“ kann der KOM-LE-Teilnehmer seine Daten zur Postadresse im Teilnehmerverzeichnis ändern. Dieser Anwendungsfall wird nicht durch KOM-LE umgesetzt, sondern durch die TI-Plattform, die hierfür die Schnittstelle I_Directory_Maintenance anbietet.

3.2 Leistungsmerkmal Dokumente schützen

3.2.1 Anwendungsfall KOM-LE_AF_6 „Dokument schützen“

Im Anwendungsfall KOM-LE_AF_6 „Dokument schützen“ können Dokumente signiert und/oder verschlüsselt werden. Dieser Anwendungsfall wird nicht durch KOM-LE umge-

setzt, sondern durch die TI-Plattform, die hierfür die Schnittstellen I_Sign_Operations, I_SAK_Operations und I_Crypt_Operations anbietet.

3.2.2 Anwendungsfall KOM-LE_AF_7 „Dokument aufbereiten“

Im Anwendungsfall KOM-LE_AF_7 „Dokument aufbereiten“ werden Dokumente falls sie verschlüsselt waren, entschlüsselt und ggf. vorhandene Signaturen geprüft. Dieser Anwendungsfall wird nicht durch KOM-LE umgesetzt, sondern durch die TI-Plattform, die hierfür die Schnittstellen I_Sign_Operations, I_SAK_Operations und I_Crypt_Operations anbietet.

4 Externe Schnittstellen

Die externen Schnittstellen sind die Schnittstellen, die die Kommunikation zwischen Primärsystemen und dem KOM-LE-Clientmodul, der TI-Plattform und dem Fachdienst sowie Fachdienst und zentralen Diensten der TI-Plattform ermöglichen.

4.1 Schnittstellen des KOM-LE-Clientmoduls zum Clientsystem

Die Kommunikation zwischen dem KOM-LE-Clientmodul und dem Primärsystem erfolgt über die Schnittstelle I_Message_Proxy (Abbildung 24). Die Schnittstelle muss vom KOM-LE-Clientmodul bereitgestellt werden.

4.1.1 Schnittstelle I_Message_Proxy

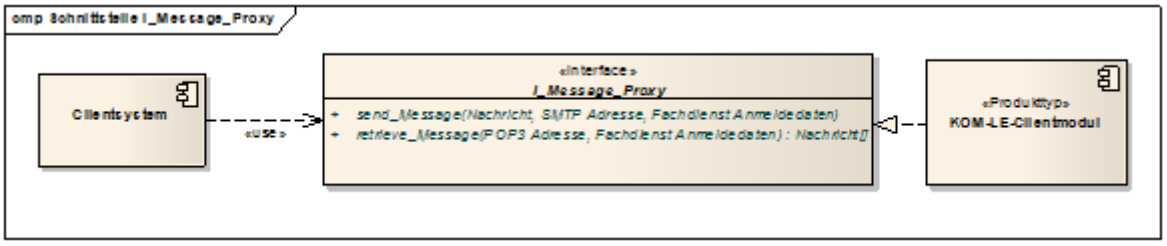

Abbildung 24: Abb_Intf_PS_CM Schnittstelle zwischen dem KOM-LE-Clientmodul und dem Primärsystem

I_Message_Proxy ist eine logische Schnittstelle, die Funktionalitäten zum Versenden und Empfangen von E-Mail-Nachrichten bereitstellt. Die Schnittstelle wird vom KOM-LE-Clientmodul angeboten und enthält folgende Operationen:

- send_Message(Nachricht, SMTP-Adresse, Anmeldedaten)
- retrieve_Message(POP3-Adresse, Anmeldedaten): Nachricht[ ]

Die technische Umsetzung dieser Schnittstelle erfolgt über die Bereitstellung von entsprechenden TCP-Ports am KOM-LE-Clientmodul für die SMTP- bzw. POP3-Verbindungen.

Die logische Schnittstelle muss den Zugang über eine sichere Verbindung (TLS) ermöglichen.

Die Anmeldedaten können im Primärsystem oder dem E-Mail-Client abgespeichert werden, wenn das Sicherheitsniveau der Einsatzumgebung und des Clients eine sichere Aufbewahrung der Anmeldedaten ermöglichen. Eine Eingabe der Anmeldedaten vor jedem Zugriff auf I_Message_Proxy sollte vermieden werden.

4.1.1.1 Operation send_Message

send_Message ist eine Operation, die das Versenden von KOM-LE-Nachrichten über das KOM-LE-Clientmodul zum KOM-LE-Fachdienst ermöglicht. Die technische Implementie-

rung dieser Operation erfolgt über die Bereitstellung eines TCP-Ports über den eine SMTP-Verbindung für das Versenden von KOM-LE-Nachrichten aufgebaut wird.

Tabelle 11: Tab_Para_Snd_Msg_CM Parameter der Operation send_Message

Parameter		Beschreibung
Eingangs-Parameter	SMTP-Adresse	FQDN (Fully Qualified Domain Name) und Portnummer, die auf den SMTP-Server des entsprechenden KOM-LE-Fachdienstes verweisen
	Anmeldedaten	Benutzername und Passwort für Authentifizierung gegenüber dem SMTP-Server.
	Nachricht	KOM-LE-Nachricht

4.1.1.2 Operation retrieve_Message

retrieve_Message ist eine Operation, die das Empfangen von KOM-LE-Nachrichten ermöglicht. Die technische Implementierung dieser Operation erfolgt über die Bereitstellung eines TCP-Ports über den eine POP3-Verbindung für das Empfangen von KOM-LE-Nachrichten aufgebaut wird.

Tabelle 12: Tab_Para_Rcv_Msg_CM Parameter der Operation retrieve_Message

Parameter		Beschreibung
Eingangs-Parameter	POP3-Adresse	FQDN und Portnummer, die auf den POP3-Server des entsprechenden KOM-LE-Fachdienstes verweisen
	Anmeldedaten	Benutzername und Passwort für Authentifizierung gegenüber dem POP3-Server
Ausgangs-Parameter	Nachricht[ ]	KOM-LE-Nachrichten

4.2 Schnittstellen des KOM-LE-Fachdienstes zum KOM-LE-Clientmodul

Die Kommunikation zwischen dem KOM-LE-Clientmodul und dem KOM-LE-Fachdienst erfolgt über die I_Message_Service-Schnittstelle (Abbildung 25). Die Schnittstelle muss vom KOM-LE-Fachdienst bereitgestellt werden.

4.2.1 Schnittstelle I_Message_Service

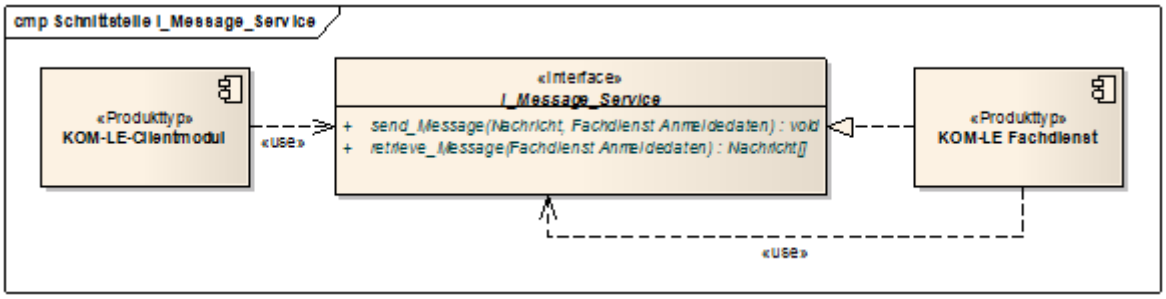

Abbildung 25: Abb_Intf_CM_FD Schnittstellen zwischen die TI-Plattform und dem KOM-LE-Fachdienst

I_Message_Service ist eine logische Schnittstelle, die Funktionalitäten zum Versenden und Empfangen von E-Mail-Nachrichten bereitstellt. Die Schnittstelle wird vom KOM-LE-Fachdienst angeboten. Die Schnittstelle enthält folgende Operationen:

- send_Message(Nachricht, Anmeldedaten)
- retrieve_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.

Die technische Umsetzung dieser Schnittstelle 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 (TLS) zugänglich sein.

4.2.1.1 Operation send_Message

send_Message ist eine Operation, die das Versenden von KOM-LE-Nachrichten über den KOM-LE-Fachdienst ermöglicht. Die technische Implementierung dieser Operation erfolgt über Bereitstellung eines TCP-Ports über den eine SMTP-Verbindung für das Versenden von KOM-LE-Nachrichten aufgebaut wird. Der KOM-LE-Fachdienst darf nur Nachrichten (außer Zustellbestätigungen) entgegennehmen und verarbeiten, die verschlüsselt sind.

Tabelle 13: Tab_Para_Snd_Msg_FD Parameter der Operation send_Message

Parameter		Beschreibung
Eingangs-Parameter	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

4.2.1.2 Operation retrieve_Message

retrieve_Message ist eine Operation, die das Empfangen von KOM-LE-Nachrichten ermöglicht. Die technische Implementierung dieser Operation erfolgt über Bereitstellung eines TCP-Ports über den eine POP3-Verbindung für das Empfangen von KOM-LE-Nachrichten aufgebaut wird.

Tabelle 14: Tab_Para_Rcv_Msg_FD Parameter der Operation retrieve_Message

Parameter		Beschreibung
Eingangs-Parameter	Anmeldedaten	Benutzername und Passwort für Authentifizierung gegenüber dem POP3-Server
Ausgangs-Parameter	Nachricht[ ]	KOM-LE-Nachrichten

4.3 Genutzte Schnittstellen der Basis-TI-Plattform

Hier werden die innerhalb der Anwendungsfälle und Prozesse genutzten Schnittstellen der Basis-TI-Plattform aufgelistet. Die Spezifikation dieser Schnittstellen erfolgt in [gem-KPT_Arch_TIP].

Tabelle 15: Tab_Intf_TIP Genutzten Basis-TI-Plattform-Schnittstellen und -Operationen

Genutzt durch	Schnittstelle	Operation
Primärsystem	I_Directory_Query	search_Directory
	I_Sign_Operations	sign_Document
		verify_Document
	I_Crypt_Operations	encrypt_Document
		decrypt_Document
	I_SAK_Operations	sign_Document_QES
		verify_Document_QES
KOM-LE-Clientmodul	I_Directory_Query	search_Directory
	I_Sign_Operations	sign_Document
		verify_Document
	I_Crypt_Operations	encrypt_Document
		decrypt_Document
	I_NTP_Time_Information	sync_Time
	I_IP_Transport	send_Data
	I_DNS_Name_Resolution	get_IP_Address
Fachanwendungsspezifische Dienste	I_Directory_Application_Maintenance	change
	I_Directory_Query	search_Directory
	I_NTP_Time_Information	sync_Time
	I_IP_Transport	send_Data

Genutzt durch	Schnittstelle	Operation
	I_DNS_Name_Resolution	get_IP_Address

5 Systemzerlegung (Deployment)

Dieses Kapitel stellt die Zerlegung von KOM-LE-Komponenten in der TI dar. Abbildung 26 zeigt die Strukturierung der KOM-LE-Architektur in Tiers der TI.

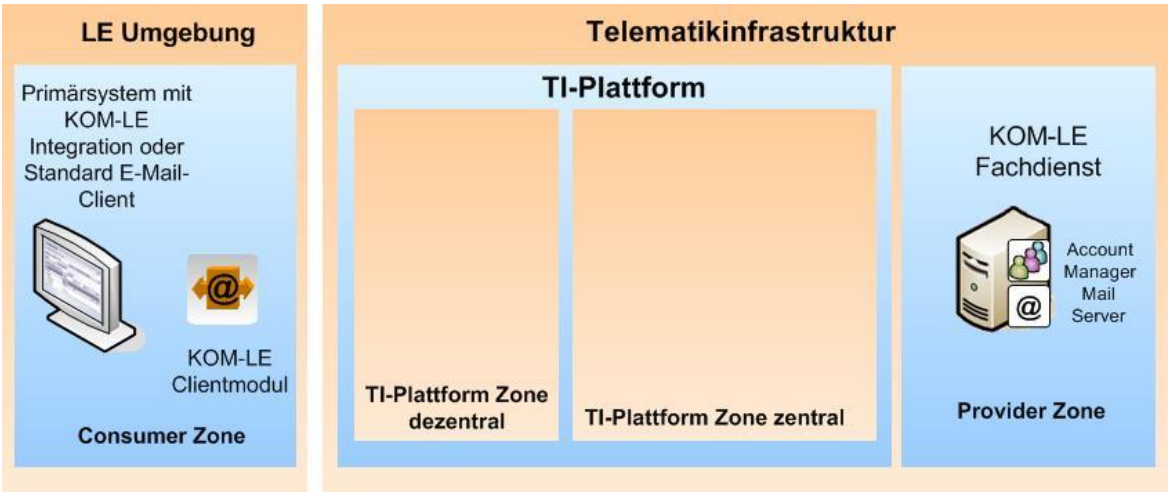

Abbildung 26: Abb_Depl_KOM-LE KOM-LE-Systemzerlegung

Die formale Beschreibung der Zerlegungsvarianten der KOM-LE-Komponenten erfolgt in Kapitel 5.1.

Die Fachanwendung KOM-LE unterteilt sich in zwei Produkttypen, die die normativ beschriebenen, versionierten und für die TI konkret realisierten Einheiten darstellen:

- KOM-LE-Clientmodul
- KOM-LE-Fachdienst.

Die Beschreibung der Produkttypen erfolgt in Kapitel 5.2 und 5.3.

5.1 Zerlegungsvarianten

Abbildung 27 entspricht der Variante, in der das KOM-LE-Clientmodul lokal auf der Primärsystemumgebung läuft. Beispielsweise, kann diese Variante in kleineren Arztpraxen auftreten, wo die KOM-LE-Nachrichten von einer sehr geringen Anzahl von Arbeitsplätzen versendet und empfangen werden.

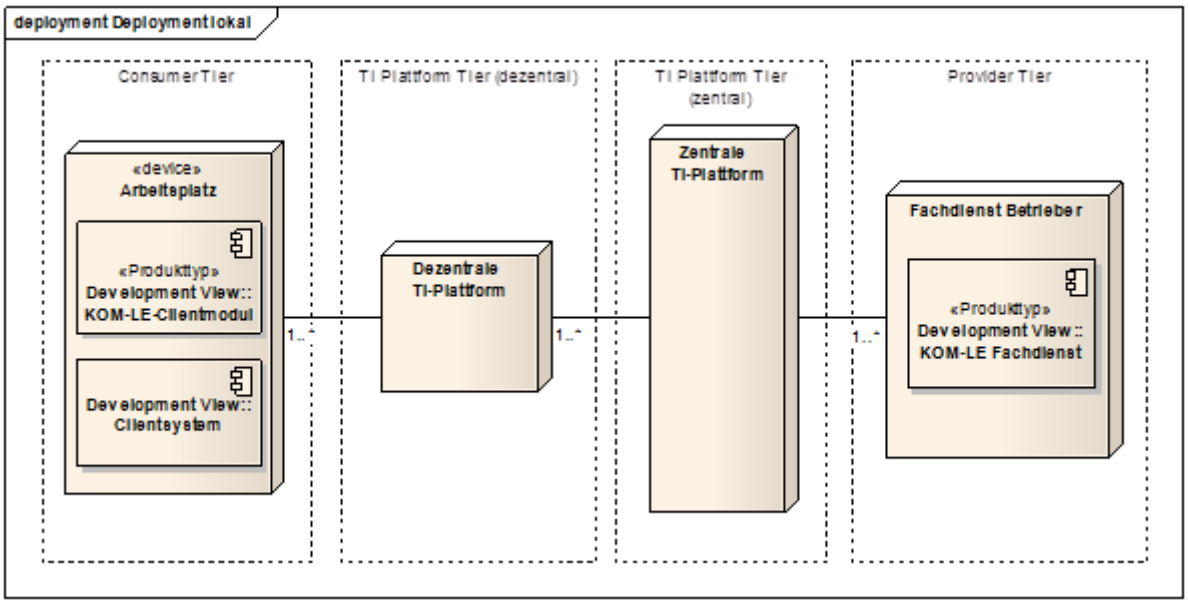

Abbildung 27: Abb_Depl_KOM-LE_V1 Lokales Deployment von KOM-LE-Clientmodul

Abbildung 28 zeigt die Variante, in der ein KOM-LE-Clientmodul gleichzeitig mehrere Arbeitsplätze bedient. Diese Konfiguration kann in größeren Arztpraxen oder Krankenhäusern verwendet werden.

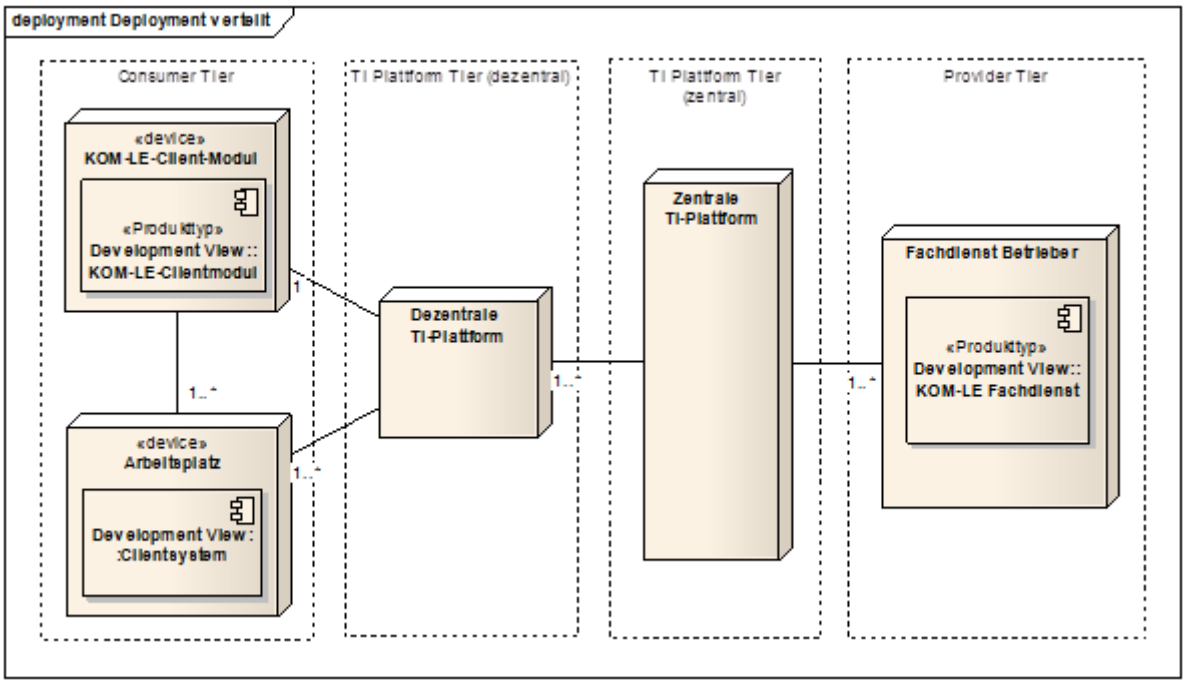

Abbildung 28: Abb_Depl_KOM-LE_V2 Verteiltes Deployment von KOM-LE-Clientmodul

5.2 Produkttyp KOM-LE-Clientmodul

Ein KOM-LE-Clientmodul kann sowohl lokal auf dem Arbeitsplatz als auch in einer separaten Umgebung laufen.

Um Vertraulichkeit und Integrität der KOM-LE-Nachrichten und Anmeldedaten zu schützen muss das Clientmodul in der Lage sein, die Verbindungen zum Arbeitsplatz und zum Basis-TI-Konnektor über TLS zu sichern.

Für die Verbindung zwischen dem Clientmodul und dem Konnektor muss auch eine beidseitige Authentifizierung möglich sein.

5.3 Produkttyp KOM-LE-Fachdienst

Der KOM-LE-Fachdienst kapselt die E-Mail- und Nutzerverwaltungskomponenten. Der Fachdienst ist direkt an das Zentrale Netz angeschlossen und bietet Funktionalitäten zum Senden bzw. Empfangen von E-Mail-Nachrichten über SMTP- bzw. POP3-Protokolle. Die Nutzerverwaltungskomponente bietet Funktionalitäten zu Registrierung und Deregistrierung von KOM-LE-Teilnehmern, der Änderung von Nutzerdaten sowie das Einbringen von KOM-LE relevanten Attributen in den Verzeichnisdienst.

Die im Fachdienst eingesetzten Komponenten bieten lediglich eine logische Sicht auf Funktionalitäten des Dienstes und dienen nicht als Implementierungsvorgaben.

Der Fachdienst darf keine Nachrichten von Clients weiterleiten, die nicht vertraulichkeitsgeschützt sind und muss diese löschen (vernichten).

6 Informationsmodelle

6.1 Fachliches Informationsmodell

Das fachliche Infomodell bietet eine logische Sicht auf fachlich relevante Daten und dient als Basis für das technische Infomodell. Das Infomodell stellt die in KOM-LE-Anwendungsfällen referenzierten Dateneinheiten dar sowie die statischen Beziehungen über sie zueinander.

6.1.1 Nachricht

`Infomodell Nachricht` (Abbildung 29) stellt die Struktur einer KOM-LE-Nachricht dar. Es beschreibt Teile einer E-Mail-Nachricht (ungeschützte und mit über S/MIME gewährleistete Vertraulichkeit und Integrität) mit mehreren Anhängen, deren Vertraulichkeit und Integrität ebenfalls geschützt werden kann.

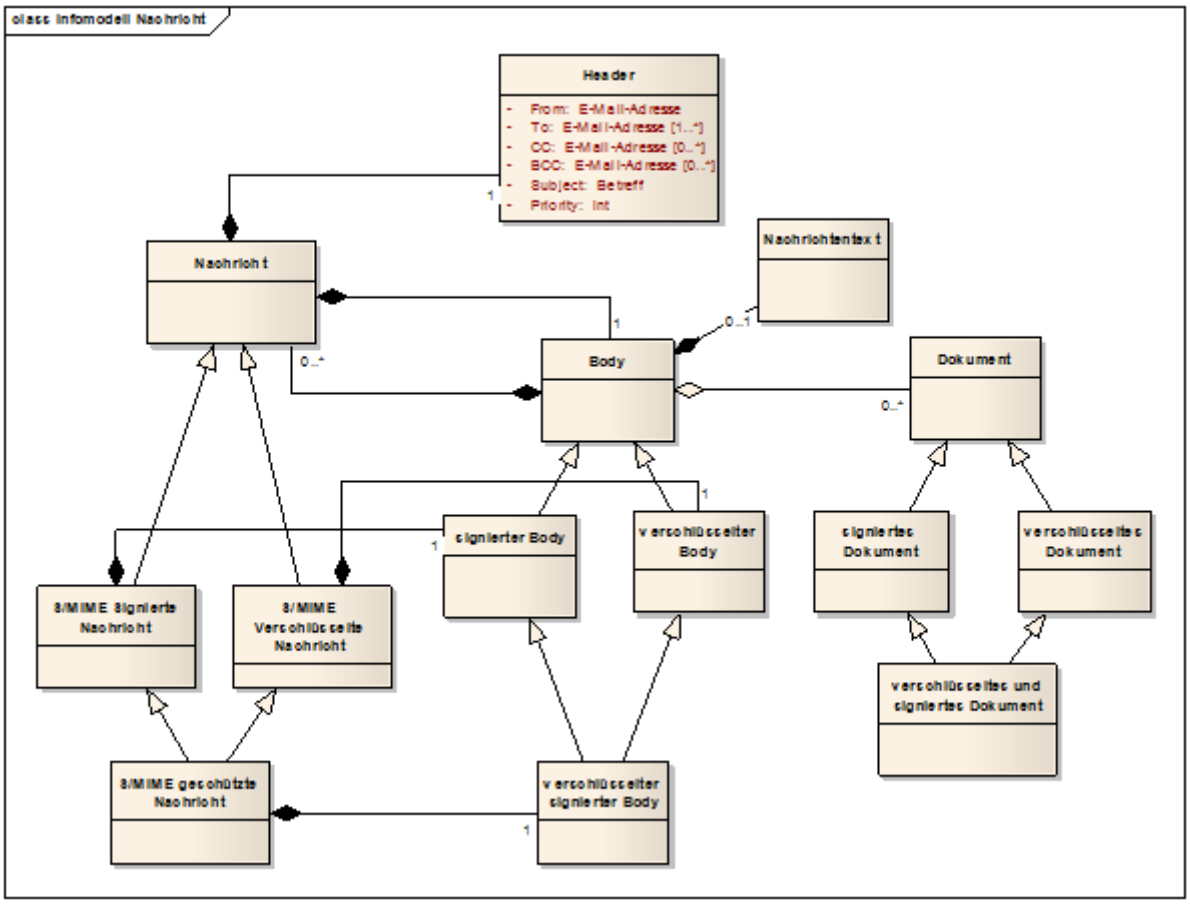

Abbildung 29: Abb_Info_Msg Infomodell Nachricht

Abbildung 30 zeigt das Beispiel einer ungeschützten KOM-LE-Nachricht. Die Nachricht enthält E-Mail-Adressen von Absender und Empfänger, Betreff mit medizinischen perso-

nenbezogenen Daten, Nachrichtentext und einen mit QES signierten Arztbrief im PDF/A-Format im Anhang.

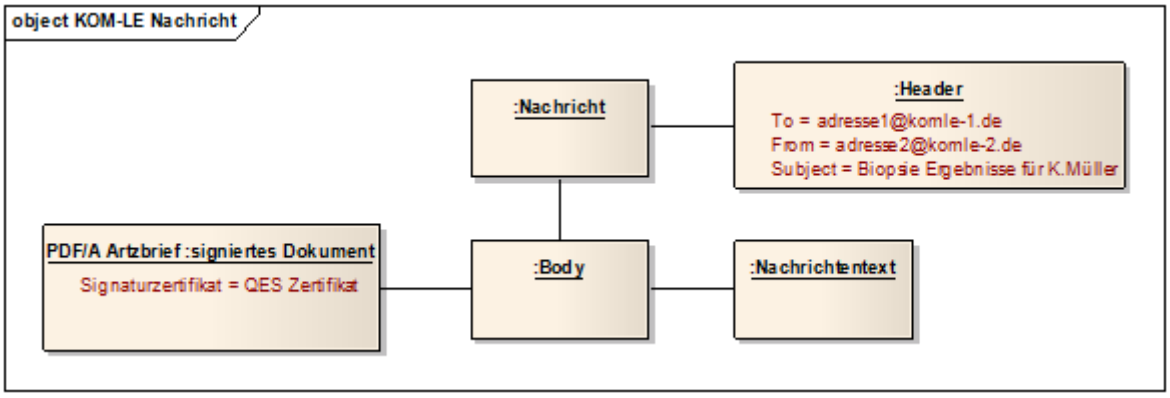

Abbildung 30: Abb_Bsp_unprot_Msg Beispiel einer ungeschützten KOM-LE-Nachricht

Abbildung 31 zeigt die ursprüngliche Nachricht, die durch das KOM-LE-Clientmodul integritäts- und vertraulichkeitsgeschützt wurde.

Um sicher zu stellen, dass Header-Elemente der ursprünglichen Nachricht auch integritäts- und vertraulichkeitsgeschützt sind, wird die ursprüngliche Nachricht als MIME-Anhang in eine neue, durch S/MIME geschützte Nachricht verpackt. Die äußere Nachricht übernimmt den Header der ursprünglichen Nachricht bis auf dem Betreff, der durch einen Text ohne Bezug auf Person und medizinische Daten ersetzt wird. Die äußere Nachricht wird danach entsprechend S/MIME-Standard signiert und verschlüsselt, indem der neue Body (als Transport-Body bezeichnet) signiert und verschlüsselt wird. Der Header (als Transport-Header bezeichnet) bleibt unverschlüsselt und unsigniert. Dadurch dass der ursprüngliche Header im Transport-Body mitsigniert wird und der äußere Header keine personbezogenen und medizinischen Daten enthält, hat die neue Nachricht einen mittleren Schutzbedarf.

Die Möglichkeit Header-Elemente einer E-Mail-Nachricht durch die Verpackung in eine neue Nachricht zu schützen, wird ab S/MIME Version 3.1 unterstützt ([RFC5750], Kapitel 3.1). Die KOM-LE-Umsetzung muss diese Version unterstützen.

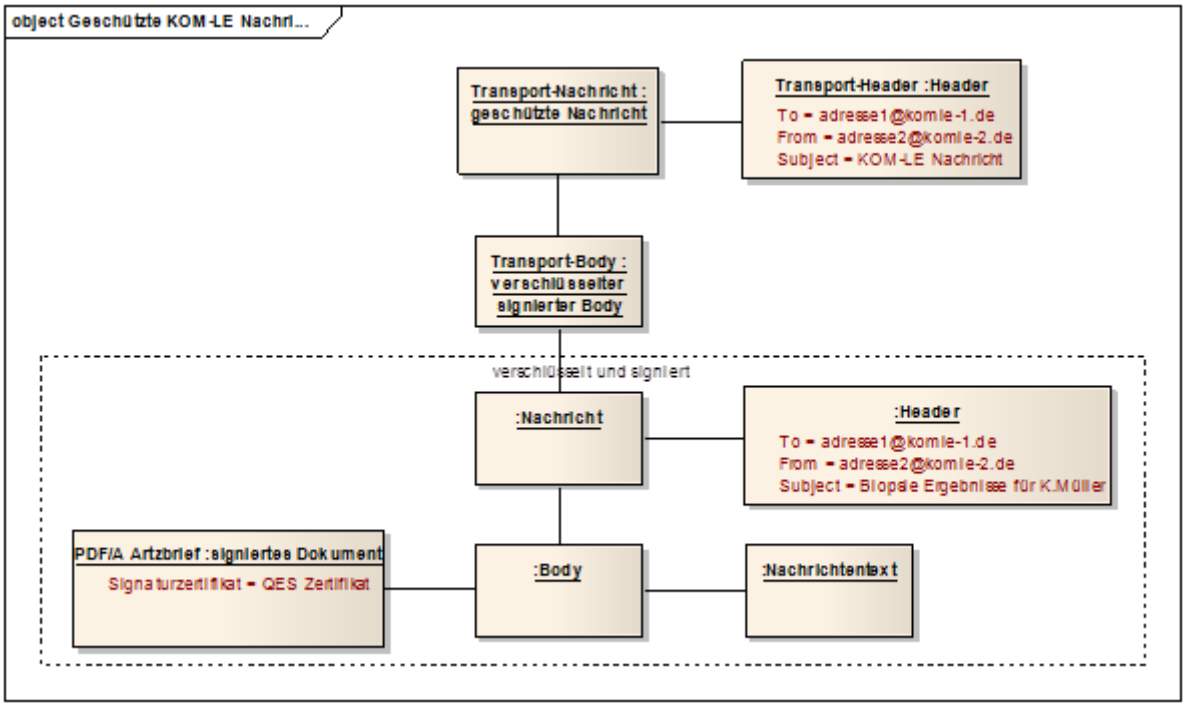

Abbildung 31: Abb_Bsp_prot_Msg Beispiel einer geschützten KOM-LE-Nachricht

Zusätzlich betrachten die KOM-LE-Anwendungsfälle zwei zusätzliche Nachrichtentypen: Zustell- und Lesebestätigung. Eine Zustellbestätigung wird nicht über ein KOM-LE-Clientmodul geschickt und als ungeschützte Nachricht über die TI übertragen. Eine Lesebestätigung wird im Primärsystem oder E-Mail-Client generiert und auch automatisch im KOM-LE-Clientmodul signiert und verschlüsselt.

6.1.1.1 Datenschutz- und Sicherheitsanforderungen

Der für die Informationsobjekte aus dem Infomodell Nachricht geltende Schutzbedarf ist in [gemKPT_Sich_KOM-LE] beschrieben.

6.1.2 Verzeichnis

Das Infomodell Nachricht (Abbildung 32) stellt die Struktur eines Verzeichnisses mit Einträgen zu KOM-LE-Teilnehmern aus fachlicher Sicht dar. Es beschreibt Verzeichniseinträge, die Informationen über einzelne Teilnehmer, ihre KOM-LE-E-Mail-Adressen und Zertifikate zur Herstellung des Vertraulichkeitsschutzes beinhalten. Zusätzlich zeigt es mit einem Verzeichniseintrag assoziierte Daten für die Registrierung und für den Zugang zum KOM-LE-E-Mail-Dienst erforderliche Anmeldedaten.

Die technische Sicht auf den Verzeichnisdienst wird In der Spezifikation Verzeichnisdienst [gemSpec_VZD] beschrieben.

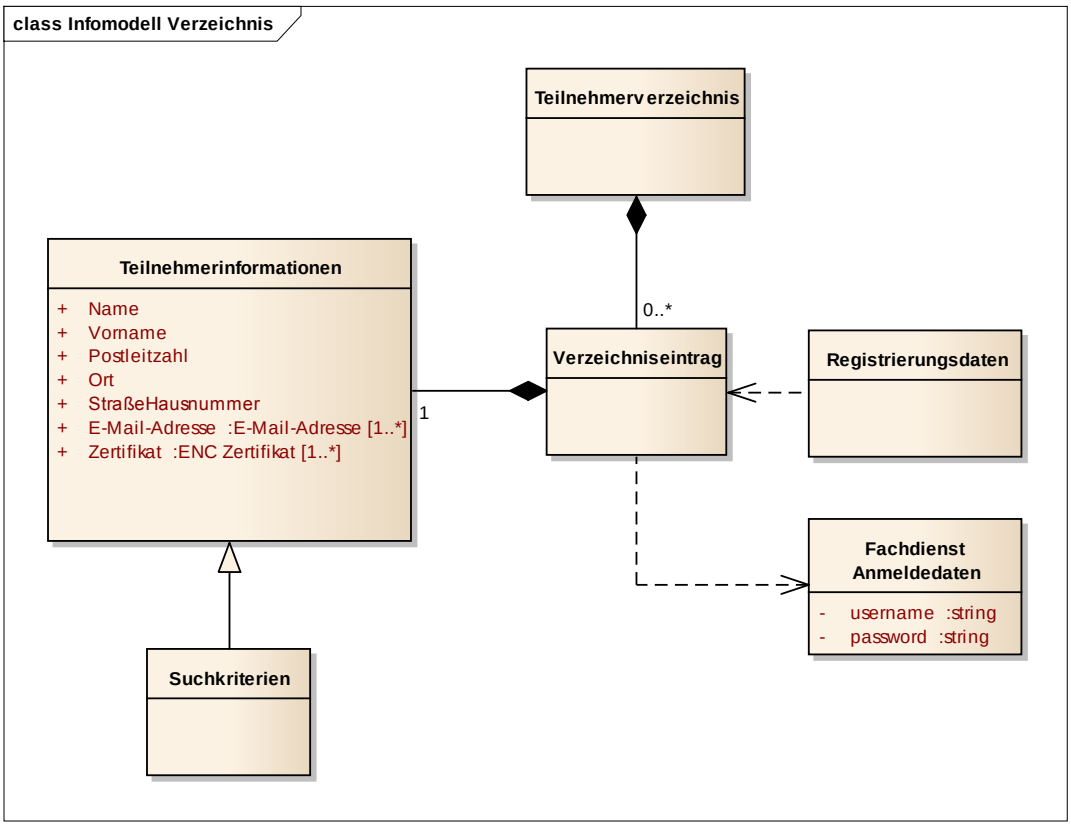

Abbildung 32: Abb_Info_Dir Infomodel Verzeichnis

6.1.2.1 Datenschutz- und Sicherheitsanforderungen

Der für die Informationsobjekte aus dem Infomodell Verzeichnis geltende Schutzbedarf ist in [gemKPT_Sich_KOM-LE] beschrieben.

6.2 Technisches Infomodell

Das technische Infomodell von E-Mail-Nachrichten ist in folgenden normativen Dokumenten beschrieben:

- E-Mail-Nachricht: [RFC5322] „Internet Message Format“
- MIME: [RFC2045], [RFC2046], [RFC2047], [RFC2049], „Multipurpose Internet Mail Extensions“ Parts 1-3,5
- S/MIME : [RFC5751] „Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification“, [RFC5750] „Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling“

Normative Beschreibungen für Zustell- und Lesebestätigung sind in [RFC3464] bzw. [RFC3798] gegeben.

Das technische Infomodell für das Verzeichnis muss gewährleisten, dass marktübliche E-Mail-Clients die Verzeichniseinträge einheitlich interpretieren können. Laut [gemLH_Basis-TI#Basis-TI-A_1060] wird das technische Infomodell in Rahmen des Ba-

sis-TI-Projekts definiert.

7 Anforderungen an externe Partner

7.1 Anforderungen an die KOM-LE Anbieter

AFO-ID	Quelle	Beschreibung
KOM-LE-A_1034	Lastenheft KOM-LE	KOM-LE Anbieter MÜSSEN den Teilnehmer vor Nutzung von KOM-LE ausreichend über die Funktionsweise sowie die Datenschutz- und Sicherheitsmaßnahmen von KOM-LE informieren.

7.2 Anforderungen an die Leistungserbringer

AFO-ID	Quelle	Beschreibung
KOM-LE-A_1027	Lastenheft KOM-LE	Die Teilnehmer MÜSSEN sicherstellen, dass in KOM-LE personenbezogene medizinische Daten von Patienten nur gesendet werden, wenn die Daten für die medizinische Versorgung des Patienten erforderlich sind.
KOM-LE-A_1039	Lastenheft KOM-LE	Die Teilnehmer von KOM-LE KÖNNEN die bereits heute existierenden Verfahren, auf denen die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Patientendaten beruht, auch für KOM-LE nutzen.
KOM-LE-A_1055	Lastenheft KOM-LE	Die Teilnehmer MÜSSEN sicherstellen, dass die Empfänger der durch KOM-LE versandten personenbezogenen Daten der Patienten an dessen medizinischen Versorgung beteiligt sind.

Anhang A

A1– Abkürzungen

Kürzel	Erläuterung
ACT	Aktivitätsdiagramm
AVS	Apothekenverwaltungssystem
Basis-TI	Basis-Telematikinfrastruktur
BCC	Blind Carbon Copy
CC	Carbon Copy
COMP	Komponentendiagramm
DigS	digitale Signatur
DNS	Domain Naming System
E-Mail	elektronische Mail
FQDN	Fully Qualified Domain Name
gematik	Gesellschaft für Telematikanwendungen der Gesundheitskarte
HBA	Heilberufsausweis
KB	Kilobyte
kbps	Kilobit pro Sekunde
KIS	Krankenhausinformationssystem
KOM-LE	adressierte Kommunikation der Leistungserbringer
KOM-LE CM	KOM-LE Clientmodul
LAN	Local Area Network (lokales Netzwerk)
LE	Leistungserbringer
LH	Lastenheft
MB	Megabyte
mbps	Megabit pro Sekunde
MIME	Multipurpose Internet Mail Extensions
PDF	Portable Document Format
PIN	Personal Identification Number
POP3	Post Office Protocol Version 3
PS	Primärsystem
PVS	Praxisverwaltungssystem
QES	qualifizierte elektronische Signatur

Kürzel	Erläuterung
SAK	Signaturanwendungskomponente
SD	Sequenzdiagramm
SMC-B	Security Module Card Typ B, Institutionenkarte
S/MIME	Secure Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
TI	Telematikinfrastruktur
TLS	Transport Layer Security
UC	Use Case
UML	Unified Modeling Language

A2 – Abbildungsverzeichnis

A3– Tabellenverzeichnis

A4– Referenzierte Dokumente

A4.1 – 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 passende jeweils gültige Versionsnummer entnehmen Sie bitte der aktuellsten, auf der Internetseite der gematik veröffentlichten Dokumentenlandkarte, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemKPT_Arch_TIP]	Projektteam Basis-TI: Konzept der Architektur der TI-Plattform
[gemKPT_Sich_KOM-LE]	Projektteam KOM-LE: Sicherheitskonzept Adressierte Kommunikation Leistungserbringer
[gemLH_Basis-TI]	Projektteam Basis-TI: Lastenheft Basis-TI
[gemLH_KOM-LE]	Projektteam KOM-LE: Lastenheft Adressierte Kommunikation Leistungserbringer
[gemMeth_Schutzbed]	Projektteam Basis-TI: Einführung der Gesundheitskarte – Methodik zur Schutzbedarfsfeststellung in der Telematikinfrastruktur
[gem-Meth_SichAnalyse]	Projektteam Basis-TI: Methode der Sicherheitsanalyse in der Telematikinfrastruktur
[gemMeth_Bedr]	Projektteam Basis-TI: Methode Bedrohungs- und Schwachstellenanalyse

A4.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI_GK]	BSI (2005): IT-Grundschutz-Kataloge (11. Ergänzungslieferung 12/2008) https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
[RFC1939]	J. Myers, RFC 1939: Post Office Protocol – Version 3, 1996

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[RFC2045]	N. Freed, N. Borenstein, RFC 2045: Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, 1996
[RFC2046]	N. Freed, N. Borenstein, RFC 2046: Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types, 1996
[RFC2047]	N. Freed, N. Borenstein, RFC 2047: Multipurpose Internet Mail Extensions (MIME) Part Three: Message Header Extensions for Non-ASCII Text, 1996
[RFC2049]	N. Freed, N. Borenstein, RFC 2049: Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples, 1996
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://www.ietf.org/rfc/rfc2119.txt
[RFC3464]	K. Moore, G. Vaudreuil, RFC3464: An Extensible Message Format for Delivery Status Notifications, 2003
[RFC3798]	T. Hansen, G. Vaudreuil, RFC3798: Message Disposition Notification, 2004
[RFC5321]	J. Klensin, RFC 5321: Simple Mail Transfer Protocol, 2008
[RFC5652]	R. Housley, RFC 5652: Cryptographic Message Syntax, 2009
[RFC5322]	P. Resnick, RFC 5322: Internet Message Format, 2008
[RFC5750]	B. Ramsdell, S. Turner, RFC 5750: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling, 2010
[RFC5751]	B. Ramsdell, S. Turner, RFC 5751: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, 2010
[XML-Sig_V1.1_20130411]	W3C Recommendation (11.04.2013): XML Signature Syntax and Processing Version 1.1 http://www.w3.org/TR/2013/REC-xmldsig-core-20130411/
[XMLEnc_V1.1_20130411]	W3C Recommendation (11.04.2013): XML Encryption Syntax and Processing Version 1.1 http://www.w3.org/TR/2013/REC-xmlenc-core1-20130411/

Anhang B – Abweichungen vom LH

Dieser Anhang gibt einen Überblick über die Änderung von Anforderungen aus dem Lastenheft.

B1 - Ersatz der FES durch digitale Signaturen

Änderung: Durch KOM-LE werden keine fortgeschrittenen elektronischen Signaturen (FES) erzeugt oder gefordert.

Zum Schutz der Nachrichten durch S/MIME werden digitale Signaturen verwendet. Hierzu wird ausschließlich die SMC-B verwendet.

Der HBA darf nicht zur Erstellung einer FES eingesetzt werden.

Zum Schutz von Dokumenten können, neben der QES, auch digitale Signaturen eingesetzt werden.

Begründung: FES beziehen sich auf natürliche Personen. Die Zertifikate auf der SMC-B beziehen sich auf Institutionen und können nicht für eine FES genutzt, aber für eine digitale Signatur verwendet werden. Auf dem HBA befinden sich keine Zertifikate, die für eine FES genutzt werden dürfen.

Unter Nutzung der SMC-B werden sowohl für den Schutz der Nachrichten (S/MIME) als auch für den Schutz von Dokumenten digitale Signaturen angeboten.

Betroffene Anforderungen: KOM-LE-A_1111, KOM-LE-A_1112, KOM-LE-A_1118, KOM-LE-A_1121, KOM-LE-A_1123, KOM-LE-A_1125, KOM-LE-A_1126, LE-A_1127, LE-A_1128, LE-A_1129

B2 - Automatischer Schutz der Nachrichten auf Nachrichtenebene

Änderung: Alle über KOM-LE versandten Nachrichten werden automatisch über das Clientmodul vor dem Senden mit der SMC-B signiert und für den oder die Empfänger verschlüsselt. Hierbei wird die gesamte Originalnachricht inklusive Header signiert und verschlüsselt.

Das Clientmodul entschlüsselt automatisch die KOM-LE-Nachrichten mit dem privaten Schlüssel des Empfängers und prüft die Signatur der Originalnachricht. Eine Integration in handelsübliche E-Mail-Clients entfällt. Die diesbezügliche Anforderung wird gestrichen. Das Clientmodul kann sowohl von E-Mail-Clients als auch von Primärsystemen über die E-Mail-Protokolle angesprochen werden.

Eventuelle Fehlermeldungen werden dem Teilnehmer mitgeteilt.

Die für den Integritätsschutz der Nachrichten verwendete digitale Signatur ermöglicht lediglich die Überprüfung, ob der Inhalt der Nachricht auf dem Weg zum Empfänger geändert wurde und erlaubt keinerlei rechtliche Aussage.

Der E-Mail-Server kann keine Maßnahmen zum Schutz der Nutzdaten vor Malware ergreifen, da die Nutzdaten verschlüsselt sind. Die diesbezügliche Anforderung entfällt.

Begründung: Die medizinischen Daten in den ungeschützten Nachrichten haben einen sehr hohen Schutzbedarf. Für die gesamte Transportstrecke ist es deshalb erforderlich, den Schutzbedarf der Nachricht zu reduzieren. Als hierzu geeignete Maßnahmen wurde die Signatur und Verschlüsselung der Nachricht gewählt. Der obligatorische Einsatz des Clientmoduls ermöglicht eine automatische Verschlüsselung und Signierung der Nachrichten. Eine Interaktion des KOM-LE-Teilnehmers oder eine Anpassung existierender E-Mail-Clients ist hierzu nicht notwendig.

Betroffene Anforderungen: KOM-LE-A_1007, KOM-LE-A_1013, KOM-LE-A_1152

B3 - Der KOM-LE-Teilnehmer darf Nachrichten nur über das Clientmodul an KOM-LE-Fachdienste übergeben

Neu: Es muss gewährleistet werden dass der KOM-LE-Fachdienst nur durch das Clientmodul geschützte Nachrichten akzeptieren darf.

B4 - Anwesenheitspflicht der Karten (HBA/SMC-B) für den Abruf von Nachrichten

Neu: Für das Empfangen von Nachrichten durch Institutionen muss die SMC-B der Institution zum Entschlüsseln der Nachricht durch das Clientmodul verfügbar sein.

Für das Empfangen von Nachrichten durch Leistungserbringer muss der HBA des Leistungserbringers zum Entschlüsseln der Nachricht durch das Clientmodul verfügbar sein.

Begründung: Durch die automatische Verschlüsselung muss zum automatischen Entschlüsseln der Nachricht der private Schlüssel des Empfängers auf der entsprechenden Karte genutzt werden.

B5 - Verpflichtender oder freiwilliger Eintrag im Teilnehmerverzeichnis

Änderung: Der öffentliche Schlüssel (Zertifikat) muss im Verzeichnis vorhanden sein.

Alt: Das Clientmodul muss in der Lage sein, die öffentlichen ENC-Zertifikate der Empfänger die nicht im Verzeichnisdienst aufgeführt sind, zur Verschlüsselung der Nachrichten vorhalten zu können.

Begründung: Durch die automatische Verschlüsselung der Nachrichten können keine Nachrichten versandt werden, die nicht für den Empfänger verschlüsselt sind. Hierzu wird der öffentliche Schlüssel des Empfängers benötigt.

Betroffene Anforderungen: KOM-LE-A_1021, KOM-LE-A_1023, KOM-LE-A_1052

B6 - Verschlüsselungsstandard für Dokumente

Neu: PDF/A-Dokumente müssen entsprechend dem Cryptographic-Message-Syntax (CMS) [RFC5652] Standard verschlüsselt werden können. XML-Dokumente müssen entsprechend dem [XMLEnc_V1.1_20130411] Standard verschlüsselt werden können.

B7 - Signaturstandard für Dokumente

Neu: PDF/A-Dokumente müssen entsprechend dem PDF-Standard signiert werden können. XML-Dokumente müssen entsprechend dem [XMLSig_V1.1_20130411] Standard signiert werden können.

B8 - Verschlüsselungsstandard für Nachrichten

Neu: Nachrichten müssen vom Clientmodul nach den Vorgaben der S/MIME Version 3.2 verschlüsselt werden. Hierzu muss die Basis-TI die entsprechenden Schnittstellen anbieten.

Die zum Entschlüsseln notwendigen Informationen müssen aus der zu entschlüsselnden S/MIME-Nachricht entnommen werden. Insbesondere muss die entsprechende Karte (SMC-B/HBA) auf diese Weise ohne Interaktion mit dem KOM-LE-Teilnehmer identifiziert und genutzt werden.

B9 - Signaturstandard für Nachrichten

Neu: Nachrichten müssen vom Clientmodul nach den S/MIME Version 3.2 Vorgaben signiert werden. Hierzu muss die Basis-TI die entsprechenden Schnittstellen anbieten.

B10 - Performanceanforderungen

Neu: In [gemSpec_Perf#4.4] werden für die einzelnen Anwendungsfälle Performanceanforderungen definiert.

B11 - Anforderungen zum Schutzbedarf

Neu: Der Schutzbedarf der Informationsobjekte und Anwendungen von KOM-LE wird in [gemKPT_Sich_KOM-LE] festgestellt.

B12 - Weitere geänderte Anforderungen

Tabelle 16: Tab_chg_Afos Weitere geänderte Anforderungen

KOM-LE-A_1065	KOM-LE MUSS die Maßnahmen zur Gewährleistung der Schutzziele Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit und Nichtabstreitbarkeit angemessen gestalten.	Nichtabstreitbarkeit ist hier nicht im Sinne von BSI Grundschutz gemeint (Keine inhaltliche Änderung)
KOM-LE-A_1067	Für KOM-LE KÖNNEN Maßnahmen, wie Zustell- oder Lesebestätigungen, genutzt werden, um das Schutzziel Nichtabstreitbarkeit des Transports der Nachrichten zu erfüllen.	Nichtabstreitbarkeit ist hier nicht im Sinne von BSI Grundschutz gemeint (Keine inhaltliche Änderung)