Themengebiet: KIM 1.5.3

C_11193

1 KIM 1.5.3

1.1 Änderung in gemSpec_CM_KOMLE

3.1 Allgemeine Anforderungen

[...]

~~**A_20189-02 – Übermittlung der benötigten KOM-LE Version des Clientmoduls**~~
~~Der Anbieter des KOM-LE-Fachdienstes MUSS seinem KOM-LE Teilnehmer bei der Erstellung des Accounts sowie bei einem relevanten Update des Fachdienstes, die nötige KOM-LE-Version des Clientmoduls mitteilen.~~

~~<=~~

~~Die KOM-LE-Version des Clientmodules muss mitgeteilt werden, damit der Nutzer weiß, welche Clientmodul-Version zu verwenden ist. Bei Nutzung eines Clientmodules in der KOM-LE-Version 1.0 ist eine Registrierung durch den Teilnehmer über die KOM-LE-1.5-Schnittstelle am KOM-LE-Fachdienst nicht möglich.~~

~~Die Übermittlung der KOM-LE-Version vom Anbieter kann hierbei in geeigneter Form erfolgen. Die jeweilige Client-Version kann aus dem LDAP-Directory Attribut: `komLeData` vom VZD entnommen werden. Geltende KOM-LE-Versionen sind `1.0` und `1.5` und werden in der Form in das Header-Element `X-KOM-LE-Version` eingetragen.~~

[...]

A_20650-06 - Übermittlung von Fehlernachrichten
Das KOM-LE-Clientmodul MUSS bei der Übertragung von Fehlernachrichten ein Mail-Header-Attribut `X-KIM-Fehlermeldung` mit dem Wert aus der Tabelle "Tab_Fehlercodes_KOMLE-Clientmodule" befüllen. Treten weitere Fehler auf, die nicht in der Tabelle "Tab_Fehlercodes_KOMLE-Clientmodul" definierte sind, MUSS das Clientmodul für diese Fehler das Mail-Header-Attribut`X-KIM-Fehlermeldung` mit einem herstellerspezifischen Fehlercode befüllen, welcher mit "`X`" beginnt.
[<=]

Tabelle 1: Tab_Fehlercodes_KOMLE-Clientmodule

Fehler	Wert
Fehlermeldungen beim Senden einer KOM-LE-Nachricht	
Empfänger entfernt, wegen falscher KIM-Version	`4001`

Verschlüsselte E-Mail-Daten konnten nicht zum KOM-LE-Attachment-Service übertragen werden	4002
keine eindeutige Telematik-ID mit Verschlüsselungszertifikat gefunden	4003
Nachricht nicht für alle Empfänger verschlüsselbar	4004
Für einen Empfänger existieren mehrere Verschlüsselungszertifikate mit unterschiedlichen Telematik-IDs	4005
Fehlermeldungen beim Empfangen einer KOM-LE-Nachricht	
Verschlüsselte E-Mail-Daten konnten nicht vom KOM-LE-Attachment-Service geladen werden	4006
Beim Entschlüsseln der E-Mail-Daten ist ein Fehler aufgetreten	4007
Das verwendete Clientmodul unterstützt die in der Mail verwendete Version nicht	4008
Die Nachricht konnte auf Grund eines nicht verfügbaren Schlüssels nicht entschlüsselt werden	4009
Die Nachricht konnte aufgrund des falschen Formats nicht entschlüsselt werden	4010
Der Konnektor steht für die Entschlüsselung nicht zur Verfügung	4011
Die Prüfsumme der E-Mail-Daten stimmt nicht mit der beigefügten Prüfsumme überein. Die empfangene aufbereitete Client-Mail entspricht eventuell nicht der vom Sender auf dem KAS hinterlegten aufbereiteten Client-Mail.	4012
Verschlüsselte E-Mail-Daten konnten nicht heruntergeladen werden, da durch zu häufigen Zugriff der KOM-LE-Attachment-Service den Abruf verweigert.	4013
Die Prüfung der Nachricht hat ergeben, dass die Nachricht nach dem Verschlüsseln manipuliert wurde. Möglicherweise wurde die verschlüsselte Nachricht auch an einen nicht empfangsberechtigten Personenkreis versendet.	4014

Die Prüfung der Signatur der Nachricht hat ergeben, dass die Nachricht manipuliert wurde, um einem anderen Nutzer das Entschlüsseln der Nachricht mit einem Schlüssel, der nicht in seinem Besitz ist, zu ermöglichen.	4015
Sonstige Fehlermeldungen	
Bei der Aktualisierung der PKCS#12-Datei ist ein Fehler aufgetreten	4016
Die KIM-Version des Clientmoduls ist kleiner als die im Verzeichnisdienst zu seinem Eintrag hinterlegte Version	4017
Eine KIM-Nachricht mit KAS-Content ist für ein KIM 1.0 - Postfach nicht zulässig	4018
Die KIM-Nachricht mit KAS-Content hat nicht die geforderte Body-Struktur	4019

[...]

A_21387-03 - Prüfung der verwendeten Clientmodul-Version beim Senden
Das KOM-LE-Clientmodul MUSS mindestens einmal am Tag, vor dem Versenden einer Nachricht, die KOM-LE-Version des Absenders mittels des LDAP-Directory Attributs ~~`komLeData`~~`kimData` aus dem Verzeichnisdienst [gemSpec_VZD#5] abfragenund in einem Cache für maximal 24h vorhalten.
Ist die KOM-LE-Version des Clientmoduls kleiner als die im Verzeichnisdienst eingetragene, so MUSS das Clientmodul den Absender mit einer E-Mail darüber informieren. Aus dem Inhalt der E-Mail MUSS hervorgehen, dass die verwendete Clientmodul Version veraltet ist. Die E-Mail ist weder zu signieren noch zu verschlüsseln und entspricht der Delivery Status Notification gemäß [RFC3461-3464].
Ist die KOM-LE-Version des Clientmoduls größer als die im Verzeichnisdienst abgefragte Version MUSS das Clientmodul die Aktualisierung ~~das~~des LDAP-Directory Attribut ~~`komLeData`~~ `kimData` für den Absender mit der neuen Version über den Account Manager durch den Aufruf der Operation `setAccount` veranlassen~~überschreiben~~. Handelt es sich bei der Mail-Adresse um einen HBA-Account, dann erfolgt die Aktualisierung der KIM-Version nachdem ein POP3 Nachrichtenabruf erfolgt ist.**[<=]**

Hinweis: Das Attribut kimData ist in [gemSpec_VZD] definiert.

Beispiel: `empfaenger@hrst_domain.kim.telematik,1.5,eArztbrief|LDT-Auftrag`

Hinweis: Wenn die Mail-Adresse zu einem HBA-Account gehört, dann kann die Aktualisierung der KIM-Version im Verzeichnisdienst erst erfolgen, nachdem ein POP3 Nachrichtenabruf erfolgt ist, da für die Aktualisierung im Verzeichnisdienst die UserID benötigt wird (für den Konnektor-Aufrufkontext zur Erzeugung des jwt).

A_22416-01 - Anfragen von technischen Konfigurationsdaten
Das KOM-LE Clientmodul MUSS beim Versenden einer E-Mail die Operation `getLimits` am Account Manager aufrufen, um alle technischen Konfigurationsdaten eines Nutzers (`dataTimeToLive`, `maxMailSize`, `quota`, `remainQuota`) zu erhalten. Das Clientmodul

KANN für jeden Nutzer-Account die abgerufenen Daten ~~24 Stunden~~für eine konfigurierbare Zeitdauer (TTL_AM_DATA) zwischenspeichern (cachen).
[<=]

A_22417-01 - Einfügen des Ablaufdatums in den äußeren Mail-Header
Das Clientmodul MUSS beim Versand-Vorgang der verschlüsselten Mail einen Header "Expires"[RFC 4021] in den Header der äußeren Nachricht aufnehmen. Der Wert ermittelt sich aus Versandzeitpunkt (TI-Zeit) + TTL (dataTimeToLive) als offset.
[<=]

[...]

A_23541 - Servicelokalisierung durch das Clientmodul
Das Clientmodul MUSS den FQDN des Fachdienstes sowie den zu nutzenden Port per DNS Service Discovery bestimmen, wenn diese nicht durch das Clientsystem im jeweiligen Benutzernamen bereitgestellt wurden.**[<=]**

Hinweis: Die für die Service Lokalisierung zu verwendenden Resource Records werden in [gemSpec_FD_KOMLE#Tab_KOMLE_Service Discovery] beschrieben.

[...]

~~**A_21389 - Übermittlung der Clientmodul- und Produkttypversion an die gematik**~~

!! Diese Anforderung wird in der gemSpec_CM_KOMLE Spezifikation gestrichen und in die gemSpec_FD_KOMLE aufgenommen !!

[...]

A_23737 - Clientmodul - Übermittlung von zusätzlichen Header-Informationen
Das Clientmodul MUSS beim Versand einer Nachricht die folgenden X-KIM Header erzeugen.

- X-KIM-Message-ID: Enthält die Message-id der Nachricht
- X-KIM-FromData: Enthält die Daten aus dem VZD-Eintrag des Senders {postalCode,<professionOID>,<specialization>}. Wenn mehrere Attribute vorhanden sind, werden sie durch "|" getrennt.
  Beispiel: urn:oid:1.3.6.1.4.1.19376.3.276.1.5.5|urn:oid:1.3.6.1.4.1.19376.3.276.1.5.4
- X-KIM-ToData: Enthält die Daten aus dem VZD-Eintrag des Empfängers (MAIL TO) {postalCode,<professionOID>,<specialization>}.
- X-KIM-CcData: Enthält die Daten aus dem VZD-Eintrag des Empfängers (MAIL CC) {postalCode,<professionOID>,<specialization>}

Header-	Beschreibung

Element	
X-KIM-Message-ID	Enthält die Message-Id der Nachricht
X-KIM-FromData	Enthält Daten aus dem VZD-Eintrag des Senders. Wenn mehrere professionOID oder specialization Attribute vorhanden sind, werden sie durch "|" getrennt. Format: {<MAIL FROM>,<postalCode>,<professionOID>,<specialization>} Beispiel: {sender@mailsystem.kim.telematik,10117,1.2.276.0.76.4.50,urn:oid:1.3.6.1.4.1.19376.3.276.1.5.5|urn:oid:1.3.6.1.4.1.19376.3.276.1.5.4}
X-KIM-ToData	Enthält Daten aus dem VZD-Eintrag des Empfängers (MAIL TO). Wenn mehrere professionOID oder specialization Attribute vorhanden sind, werden sie durch "|" getrennt. Format: {<MAIL RCPT TO>,<postalCode>,<professionOID>,<specialization>}
X-KIM-CcData	Enthält die Daten aus dem VZD-Eintrag des Empfängers (MAIL CC). Wenn mehrere professionOID oder specialization Attribute vorhanden sind, werden sie durch "|" getrennt. Format: {<MAIL RCPT CC>,<postalCode>,<professionOID>,<specialization>}

Wenn mehrere Empfänger adressiert wurden, MUSS das jeweilige Header-Element mehrfach angegeben werden.**[<=]**

3.2.1 Senden von großen Client-Mails

[...]

A_19356-07 - Prüfen der Version des Empfängers
Das KOM-LE-Clientmodul MUSS die vom Empfänger verwendete KOM-LE-Version prüfen.
Das KOM-LE-Clientmodul MUSS dazu die KOM-LE-Version mittels des LDAP-Directory Attributs: ~~`komLeData`~~ `kimData` aus dem Verzeichnisdienst [gemSpec_VZD#5] abfragen.
~~Ist das LDAP-Directory Attribut `komLeData` für den Empfänger undefiniert, dann muss ein KOM-LE-Clientmodul mit einer Version 1.0 angenommen werden.~~

Wenn eine Client-Mail größer als 15 MiB an einen Empfänger mit KOM-LE-Version < 1.5 versendet werden soll, oder die KOM-LE-Version nicht mit einem + (zum Beispiel Wert: 1.5+) erweitert wurde, MUSS das KOM-LE-Clientmodul diesen Empfänger aus der Mail entfernen. Wird die KOM-LE-Version der beabsichtigten Empfänger durch internes Caching bereitgestellt, MUSS das Clientmodul, wenn die aktuelle KOM-LE-Version nicht die Bereitschaft zum Empfang großer Nachrichten signalisiert, eine Anfrage am VZD durchführen um auf eine eventuelle Aktualisierung des Eintrages zu prüfen. Beim Entfernen eines Empfängers MUSS das KOM-LE-Clientmodul den Absender mit einer E-Mail über den Fehlerfall informieren. Aus dem Inhalt der Fehlernachricht müssen alle aus der Mail entfernten Empfänger hervorgehen. Die Fehlernachricht ist weder zu signieren noch zu verschlüsseln und entspricht der Delivery Status Notification gemäß [RFC3461-3464]. Kann die Mail für keinen der Empfänger versendet werden, wird das Senden der Nachricht abgebrochen. Dabei wird dem MTA das RSET-Kommando gesendet und das Clientsystem wird mit dem SMTP-Antwortcode "451" über den Fehlerfall informiert.
[<=]

[...]

A_22340-01 - Cachen vom KOM-LE-Versionen
Das Clientmodul MUSS das Cachen von KOM-LE-Versionen der Mail-Empfänger nach der Abfrage am VZD für eine ~~maximale Zeitdauer von 24 Stunden~~konfigurierbare Zeitdauer (TTL_VZD_DATA) unterstützen.

[<=]

[...]

A_23467 - Übermittlung der KAS-Datenmenge
Das KOM-LE-Clientmodul MUSS bei der Übertragung der KOM-LE-Nachricht an den Fachdienst, die im Kontext KAS verarbeitet wurde, ein Mail-Header-Attribut `X-KIM-KAS-Size` mit dem Wert befüllen, der dem Attribut `size` in der KIM-Attachment-Datenstruktur entspricht. **[<=]**

[...]

~~**A_19362 - Client-Authentifizierung**~~
~~Das KOM-LE-Clientmodul MUSS eine beidseitige gesicherte TLS-Verbindung zum KAS des Fachdienstes aufbauen.~~

A_19362-01 - Client Authentifizierung für Upload am KAS
Das KOM-LE-Clientmodul MUSS zum Upload eine beidseitige gesicherte TLS-Verbindung zum KAS des Fachdienstes aufbauen.
[<=]

[...]

~~**A_19368 - Client-Authentifizierung**~~
~~Das KOM-LE-Clientmodul MUSS eine beidseitige gesicherte TLS-Verbindung zum KAS des Fachdienstes aufbauen.~~

A_19368-01 - Client Authentifizierung für Download am KAS
Das KOM-LE-Clientmodul MUSS zum Download eine beidseitige gesicherte TLS-Verbindung zum KAS des Fachdienstes aufbauen.
[<=]

[...]

A_23471 - Löschen von E-Mail-Daten vom KAS bei Fehler
Das KOM-LE-Clientmodul MUSS die auf dem KAS abgelegten E-Mail-Daten wieder löschen, wenn beim weiteren Verarbeiten oder beim Versand der KIM-Mail zum KOM-LE-Fachdienst ein Fehler aufgetreten ist und die Nachricht dem Fachdienst nicht zugestellt werden konnte. Für das Löschen der jeweiligen E-Mail-Daten auf dem KAS MUSS vom KOM-LE-Clientmodul die Operation `delete_Maildata` [gemSpec_FD_KOMLE] an der Schnittstelle I_Attachment_Services aufgerufen werden.**[<=]**

[...]

A_19359-08 - Einbetten von Informationen großer Nachrichten
Das KOM-LE-Clientmodul MUSS für die auf dem KAS abgelegten E-Mail-Daten folgende KIM-Attachment-Datenstruktur gemäß [Attachment_Schema] erzeugen ~~im Mail-Body befüllen~~. Die erzeugte Datenstruktur MUSS als einziges Body-Element den Mail-Body der vorverarbeiteten originalen Client-Mail ersetzen. ~~durch den~~ Der MIME-Part MUSS den Header `Content-Disposition: x-kas enthalten` ~~ersetzen~~.

Tabelle 2 KIM-Attachment-Datenstruktur

Attribut in KIM-Attachment-Datenstruktur	Wert
`link`	Freigabelink der verschlüsselten E-Mail-Daten gemäß [A_19364]
`k`	AES-GCM Key der E-Mail-Daten (symmetrischer Schlüssel) im Base64 Format
`hash`	Hashwert der E-Mail-Daten (entsprechend A_19644 [gemSpec_Krypt] zu bilden) im Base64 Format
`size`	Größe der E-Mail-Daten in Byte

Vor der KIM-Attachment-Datenstruktur MUSS ein MIME konformer Content Header mit `Content-Type: text/plain; charset=utf-8` sowie ein `Content-Disposition: x-kas` eingefügt werden.
[<=]

Hinweis: Es wird empfohlen, bei Verwendung von `Content-Transfer-Encoding, base64` zu nutzen.

3.2.2 Empfangen von großen Client-Mails

[...]

A_19370-05 - Download von E-Mail-Daten
Das KOM-LE-Clientmodul MUSS die E-Mail-Daten anhand des entnommenen Freigabelinks via der Operation read_Attachment am KAS des Fachdienstes herunterladen.

Wenn beim Herunterladen der E-Mail-Daten ein persistenter Fehler (403 und 404) auftritt, dann MUSS das KOM-LE-Clientmodul eine neue `multipart/mixed` MIME-Nachricht mit einer `text/plain` MIME-Einheit mit dem Fehlertext [Tab_Fehlertext_Download] dem Clientsystem übermitteln. Die `orig-date`, `from`, `sender`, `reply-to`, `to` und `cc` Header-Elemente der neuen `multipart/mixed` Nachricht werden aus der empfangenen Nachricht übernommen. Das `subject` Header-Element der neuen `multipart/mixed` Nachricht erhält den Wert *„Die E-Mail-Daten konnten nicht abgerufen werden, bitte kontaktieren Sie den Absender*".

Handelt es sich um einen transienten Fehler ~~Fehler auftritt~~, dann MUSS das KOM-LE-Clientmodul die empfangene, dem KOM-LE-S/MIME-Profil entsprechende Nachricht, als eine `message/rfc822` MIME-Einheit in einer neuen `multipart/mixed` MIME-Nachricht dem Clientsystem übermitteln. Zusätzlich muss diese neue `multipart/mixed` MIME-Nachricht eine `text/plain` MIME-Einheit mit dem Fehlertext [Tab_Fehlertext_Download] enthalten. Die `orig-date`, `from`, `sender`, `reply-to`, `to` und `cc` Header-Elemente der neuen `multipart/mixed` Nachricht werden aus der empfangenen Nachricht übernommen. Das `subject` Header-Element der neuen `multipart/mixed` Nachricht erhält den Wert *„Die E-Mail-Daten konnten nicht abgerufen werden*".
[<=]

3.3.2.2 Verbindungsaufbau mit dem MTA

Das Clientmodul kann die Verbindung mit dem MTA nur dann aufbauen, wenn ihm das Clientsystem die Adresse des MTAs und die Portnummer des SMTP-Dienstes während des Authentifizierungsverfahrens als Teil des Benutzernamens mitgeteilt werden. Ist dies nicht der Fall, d.h. ist der im Benutzernamen vorgesehene Teilstring nicht befüllt (#MTA's URI und Port Nummer#), dann ermittelt das Clientmodul diese fehlenden Parameter mit Hilfe des übergebenen Benutzernamens (Domainanteil) und damit ausgelöster DNS Service Discovery [gemSpec_FD_KOMLE#Tab_KOMLE_Service Discovery].
Das Clientmodul führt das Authentifizierungsverfahren mit dem Clientsystem bis zu dem Punkt, an dem es mit dem entsprechenden Antwortcode die Authentifizierung akzeptieren oder ablehnen muss. Das Clientmodul allein kann das Clientsystem nicht authentifizieren. Die Authentizität der Zugangsdaten kann nur vom MTA überprüft werden. Dazu authentifiziert sich das Clientmodul im Auftrag vom Clientsystem gegenüber dem MTA.
Übergibt das Clientsystem d~~D~~ie MTA-Adresse und die Portnummer des SMTP-Dienstes ~~sind~~ als Teil des SMTP-Benutzernamens ~~vom Clientsystem zu übergeben. Sie~~, sind sie vom eigentlichen Benutzernamen durch das Zeichen '#' getrennt und als adresse:port String formatiert.

[...]

3.3.3 Proxy Zustand

[...]

KOM-LE-A_2176-01 - Prüfen auf gültiges ENC-Zertifikat für den Empfänger im RCPT-Kommando
Das Clientmodul MUSS, wenn es vom Clientsystem ein RCPT TO:<recipient-address> Kommando erhält, prüfen, ob für den im Kommando aufgeführten Empfänger mindestens ein gültiges ENC-Zertifikat existiert. Da die Nachricht nur an Empfänger, die ein gültiges ENC-Zertifikat besitzen weitergeleitet werden darf, MUSS das Clientmodul im Negativfall das Kommando verwerfen ~~und dem Clientsystem den Antwortcode „550" senden~~ . Im Positivfall MUSS das Clientmodul das Kommando an den MTA weiterleiten.
[<=]

A_23554 - Weiterleitung MAIL FROM - SIZE-Parameter
Das Clientmodul MUSS, wenn es vom Clientsystem ein MAIL FROM Kommando erhält, prüfen, ob durch das Clientsystem der Parameter `size` befüllt wurde. Ist dies der Fall, MUSS das Clientmodul erst nach Verarbeitung der Nachricht durch das Clientmodul und der Anpassung des Parameters `size` in MAIL FROM das Kommando an den Fachdienst weiterleiten.**[<=]**

3.3.4.1.1 Bearbeitung einer ungeschützten Nachricht

[...]

KOM-LE-A_2299-02 - Vorgehen bei Signatur und Verschlüsselung einer KOM-LE Nachricht
Zur Signatur und Verschlüsselung von KOM-LE Nachrichten MUSS das folgende Vorgehen umgesetzt werden:

1. Zur CMS(CAdES)-Signatur durch den Konnektor übergibt das KOM-LE-CM beim Aufruf der SignDocument-Operation am Konnektor das zu signierende Dokument als MimeType="~~text/plain; charset=utf-8~~application/octet-stream" Dokument. Als Antwort gibt der Konnektors einen binären CMS-Container zurück. Zum Transport sind die binären Objekte in den SOAP-Nachrichten jeweils base64-kodiert.
2. Der binäre CMS-Container mit der signierten Nachricht wird als „application/pkcs7-mime" MIME-Einheit vom smime-type „signed-data" mit dem Content-Transfer-Encoding „binary" (nicht "base64") verpackt.
3. Zur CMS-Verschlüsselung durch den Konnektor übergibt das KOM-LE-CM beim Aufruf der EncryptDocument-Operation am Konnektor die in Schritt zwei erzeugte Nachricht als binär-Dokument. Als Antwort gibt der Konnektors einen binären CMS-Kontainer zurück. Zum Transport sind die binären Objekte in den SOAP-Nachrichten jeweils base64-kodiert.
4. Der aus der Verschlüsselung resultierende CMS-Container wird in eine „application/pkcs7-mime" MIME-Einheit vom smime-type „authenticated-enveloped-data" mit dem Content-Transfer-Encoding „base64" verpackt.

[<=]

[...]

KOM-LE-A_2192-01 - Fehlernachricht bei Empfänger mit unterschiedlichen Telematik-IDs in den Verschlüsselungszertifikaten
Existieren für einen Empfänger mehrere Verschlüsselungszertifikate mit unterschiedlichen Telematik-IDs MUSS das Clientmodul den Absender der Nachricht mit einer Fehlernachricht informieren. Die Fehlernachricht ist weder zu signieren noch zu verschlüsseln und entspricht der Delivery Status Notification gemäß [RFC3461-3464].
[<=]

Hinweis: Entgegen [RFC3464] muss bei der Übermittlung der Fehlernachricht im SMTP Kommando MAIL FROM die Absenderadresse angeben werden. Es geht um die Fehlernachricht-Inhalte. Der [RFC3464] gilt nicht normativ.

[...]

KOM-LE-A_2026-01 - Cachen von Verschlüsselungszertifikaten
Das Clientmodul MUSS das manipulationssichere Cachen von Verschlüsselungszertifikaten für eine konfigurierbare Zeitdauer (TTL_VZD_DATA) unterstützen.
[<=]

[...]

3.3.4.2.1 Bearbeitung einer geschützten KOM-LE-Nachricht

[...]

Beispiel für die oben beschriebene Transformation:

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="unique-boundary-1"
Subject: WG: Signed and encrypted in attachment
Date: Fri, 10 Feb 2012 14:29:21 +0100
From: musterfrau@komle.de
To: musterfrau@komle.de
Message-Id: <II8HEDLEUEU4.EG0B98QUZNPM2@STST-TEST>
X-KIM-Dienstkennung: KIM-Mail;Default;V1.0
X-KIM-Sendersystem: Beispiel-PVS;V2.81
This is a multi-part message in MIME format.
```

[...]

```
X-KOM-LE-Version: 1.0
MIME-Version: 1.0
Content-Type: application/pkcs7-mime;
smime-type=enveloped-data; name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;    filename="smime.p7m"
```

```
Subject: KOM-LE Nachricht
Date: Fri, 9 Feb 2012 12:07:17 +0100
From: mustermann@komle.de
To: musterfrau@komle.de
Message-Id: <II8HEDLEUEU4.EG0B98QUZNPM2@STST-TEST>
Cc: mustermann2@komle.de
```

[...]

3.4.2.2 Verbindungsaufbau mit dem POP3-Server

Das Clientmodul kann die Verbindung mit dem POP3-Server nur dann aufbauen, wenn ihm das Clientsystem die Adresse des POP3-Servers und die Portnummer des POP3-Dienstes übermittelt. Das Clientmodul erwartet, dass der Domain Name oder die IP-Adresse und die Portnummer während des Authentifizierungsverfahrens als Teil des Benutzernamens übergeben werden. Ist dies nicht der Fall, d.h. ist der im Benutzernamen vorgesehene Teilstring nicht befüllt (#POP3 Server und Port Nummer#), dann ermittelt das Clientmodul diese fehlenden Parameter mit Hilfe des übergebenen Benutzernamens (Domainanteil) und damit ausgelöster DNS Service Discovery [gemSpec_FD_KOMLE#Tab_KOMLE_Service Discovery].

Das Clientmodul führt das Authentifizierungsverfahren mit dem Clientsystem bis zu dem Punkt, an dem es mit dem entsprechenden Antwortcode die Authentifizierung akzeptieren oder ablehnen muss. Das Clientmodul allein kann das Clientsystem nicht authentifizieren. Die Authentizität der Zugangsdaten kann nur vom POP3-Server überprüft werden. Dazu authentisiert sich das Clientmodul im Auftrag vom Clientsystem gegenüber dem POP3-Server.

Übergibt das Clientsystem d~~D~~ie Server Adresse und die Portnummer des POP3-Dienstes ~~sind~~ als Teil des POP3-Benutzernamens ~~vom Clientsystem zu übergeben. Sie~~, sind sie vom eigentlichen Benutzernamen durch das Zeichen '#' getrennt und als adresse:port String formatiert.

[...]

3.4.4.2.1 Entschlüsselung

[...]

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="unique-boundary-1"
Subject: Die Nachricht konnte nicht entschl~~ü~~uesselt werden
Date: Fri, 9 Feb 2012 12:07:17 +0100
From: mustermann@komle.de
To: musterfrau@komle.de
Message-Id: <II8HEDLEUEU4.EG0B98QUZNPM2@STST-TEST>
X-KIM-Fehlermeldung: cmgerr_4
X-KIM-DecryptionResult: 01
```

[...]

```
X-KOM-LE-Version: 1.0
MIME-Version: 1.0
Content-Type: application/pkcs7-mime; name="smime.p7m"; name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;    filename="smime.p7m"
Subject: KOM-LE Nachricht
Date: Fri, 9 Feb 2012 12:07:17 +0100
From: mustermann@komle.de
To: musterfrau@komle.de
Message-Id: <II8HEDLEUEU4.EG0B98QUZNPM2@STST-TEST>
```

[...]

KOM-LE-A_2179-02 - Vermerk in der Nachricht bei erfolgreicher Entschlüsselung

Das Clientmodul MUSS bei erfolgreicher Entschlüsselung der KOM-LE-Nachricht den Vermerk „Die KOM-LE Nachricht wurde erfolgreich entschlüsselt.“ als Mail-Header-Attribut `X-KIM-DecryptionResult` (ID 00) in den Header der Nachricht eintragen. ~~an den Text der Nachricht anhängen. Es ist dabei das Format des TextParts zu beachten (mediatype text/html oder text/plain) und der Vermerk diesem Format anzupassen.~~

[<=]

3.4.4.2.2 Integritätsprüfung

[...]

```
Date: Fri, 9 Feb 2012 12:07:17 +0100
MIME-Version: 1.0
From: mustermann@komle.de
To: musterfrau@komle.de
Message-Id: <II8HEDLEUEU4.EG0B98QUZNPM2@STST-TEST>
Subject: Arztbrief
```

[...]

Hinweistext unter der Anforderung KOM-LE-A_2048-01

Hinweis: Für lange Header-Elemente (z. B. bei `reply-to`) muss "folding" gemäß [RFC822] unterstützt werden.

Ein "folding" muss beim Header-Vergleich berücksichtigt werden und muss daher, wenn es vorhanden ist, vor dem Vergleich entfernt werden. Die Integritätsprüfung beinhaltet nur die Werte der Header-Elemente, nicht die Bezeichner der Header-Elemente. Die Werte der Header-Elemente müssen der Addr-Spec Specification genügen (https://datatracker.ietf.org/doc/html/rfc5322#section-3.4).

[...]

3.7 Administrationsmodul

Das Administrationsmodul ist Bestandteil des KOM-LE-Clientmoduls. Das Modul ermöglicht die Verwaltung des Accounts des KOM-LE-Teilnehmers. Dazu kommuniziert das Administrationsmodul über eine TLS-Verbindung mit dem Account Manager des KOM-LE-Fachdienstes. Zum Funktionsumfang des Modules gehören:

- Registrierung des neuen KOM-LE-Teilnehmers,
- Deregistrierung des KOM-LE-Teilnehmers,
- Beantragen und Herunterladen der PKCS#12-Datei,
- Lokalisierung des Account Managers über DNS Service Discovery,
- Meldung der KIM-Version an den Account Manager,
- Meldung der Anwendungskennzeichen an den Account Manager,
- Verwaltung von Abwesenheitsnotizen.

[...]

3. Der Leistungserbringer verwendet das Administrationsmodul, um sich am Account Manager seines Fachdienstes zu registrieren

   a. Es wird eine serverseitig authentisierte TLS-Verbindung zwischen dem Administrationsmodul und dem Account Manager des Fachdienstes aufgebaut.

   b. Im Zuge des Registrierungsprozesses wird die Operation `registerAccount()` am Account Manager aufgerufen und folgende Parameter an den Account Manager übermittelt:

      i. die referenceID,

      ii. das initiale Passwort,

      iii. eine E-Mail-Adresse,

      iv. das neue Passwort (die Operation getServiceInformation der Schnittstelle I_ServiceInformation stellt die Password Policy des Anbieters bereit),

      v. die KIM-Version.

      vi. optional Anwendungskennzeichen

   c. Der Request wird mit dem Auth-Zertifikat der verwendeten Karte (HBA oder SMC-B) signiert

5. Der KOM-LE-Anbieter trägt die angegebene E-Mail-Adresse sowie die KIM-Version in den Verzeichnisdienst ein

4. Optional: Automatisiertes Beantragen des kryptografischen Materials (PKCS#12-Datei)

   a. Das Administrationsmodul generiert optional ein Passwort gemäß [gemSpec_Krypt] zum Sichern der PKCS#12-Datei.

   b. Anschließend ruft das Administrationsmodul die Operation `createCert()` auf, um das kryptografische Material (PKCS#12) anzufordern.

c. Das Administrationsmodul übergibt die PKCS#12-Datei an das Clientmodul. Wenn kein Passwort verwendet wurde, dann darf die heruntergeladene PKCS#12 Datei nicht persistent gespeichert werden.

d. Dieses Zertifikat wird anschließend vom Clientmodul für alle E-Mail-Adressen und KIM-Fachdienste verwendet. ~~Weiterhin wird dieses Zertifikat für die TLS-Client Authentisierung gegenüber dem Konnektor genutzt.~~

[...]

3.7.1 Allgemeine Anforderungen

[...]

A_23713 - Clientmodul, Pflege der Anwendungskennzeichen
Das Clientmodul MUSS ein User Interface zur Pflege der Anwendungskennzeichen pro KIM-Adresse des Nutzers bereitstellen.
Die Änderungen an den Anwendungskennzeichen einer KIM-Adresse MUSS das Clientmodul über die Schnittstelle I_AccountManager_Service an den Account Manager übergeben. Es dürfen nur gültige Anwendungskennzeichen verwendet werden.
[<=]

A_23711 - Clientmodul, gültige Anwendungskennzeichen
Das Clientmodul MUSS die Liste der gültigen Anwendungskennzeichen immer dann auf das Vorhandensein der neuesten Version prüfen und ggf. vom Accountmanager aktualisieren und persistent speichern, wenn der KIM-Teilnehmer oder der Administrator Änderungen an den Anwendungskennzeichen vornehmen möchte. **[<=]**

Hinweis: Das Clientmodul kann das Prüfergebnis für 3 Stunde in einem Cache speichern.
Hinweis: KIM-Teilnehmer können zu ihrer KIM Mail-Adresse ein oder mehrere Anwendungskennzeichen festlegen. Die Zuordnung von KIM-Version zur KIM Mail-Adresse sowie die dazu vergebenen Anwendungskennzeichen werden im Verzeichnisdienst-Eintrag gespeichert. Ein sendendes Clientsystem kann aus dem gefundenen Verzeichnisdienst-Eintrag die KIM Mail-Adresse des Empfängers aussuchen, die das zur X-KIM-Dienstkennung passende Anwendungskennzeichen hat.

Die Anwendungskennzeichen werden von den jeweiligen KIM-Anwendungen festgelegt und der gematik mitgeteilt. Die gematik veröffentlicht alle gültigen Anwendungskennzeichen in der Dienstkennungsliste (https://fachportal.gematik.de/toolkit/dienstkennung-kim-kom-le) und für technische Systeme in einem FHIR CodeSystem (https://simplifier.net/app-transport-framework/GEM-CS-KIM-Dienstkennung/$download?format=json).

Das Anwendungskennzeichen wird im Verzeichnisdienst LDAP-Directory im Attribut kimData gespeichert. Die Pflege des Anwendungskennzeichens erfolgt durch den Nutzer mittels Clientmodul und Accountmanager.

Unterhalb A_19523 wird folgender Text ergänzt.

Die URL wird wie folgt gebildet:

```
https://<FQDN gemäß DNS-SD SRV RR>:<Port gemäß DNS-SD SRV RR><Base-path gemäß TXT RR><path gemäß yaml Datei>
```

A_19457-03 - Client Authentisierung Administrationsmodul

Das Administrationsmodul MUSS bei der initialen Registrierung eine serverseitig gesicherte TLS-Verbindung zum Account Managers des Fachdienstes aufbauen.

Für die Authentisierung am Account Manager MUSS das Administrationsmodul ein JSON-Web-Token gemäß [RFC7519] mit den Elementen aus der folgenden Tabelle erzeugen und zusammen mit dem Passwort des Nutzers an den Account Manager übergeben. Die Gültigkeitsdauer (`exp - iat`) des JSON-Web-Token MUSS 6 Stunden betragen.

JSON Web Token	
Header	
alg	PS256
typ	JWT
x5c	[BASE-64 kodiertes AUT-Cert]
Body	
~~nbf~~	~~[Gültigkeitsbeginn (Unixzeit)]~~
iat	[Ausstellungszeitpunkt (Unixzeit)]
exp	[Ablaufzeitpunkt (Unixzeit)]

[<=]

3.7.3 Deregistrierung KOM-LE-Teilnehmer

[...]

A_19464-04 - Deregistrierungsdialog KOM-LE-Teilnehmer Administrationsmodul
Das Administrationsmodul MUSS die Deregistrierung des KOM-LE-Teilnehmers im Dialog durchführen. Im Verlauf der Deregistrierung MUSS der KOM-LE-Teilnehmer in geeigneter Form informiert werden, dass nach der Deregistrierung diese zunächst nur temporär für einen Zeitraum von mindestens 30 Tage umgesetzt wird. Nach Ablauf dieses Zeitraumes ist kein weiterer Zugriff auf den E-Mail-Account möglich und der gelöschte Account kann nicht wiederhergestellt werden. Innerhalb~~der 30 Tage ist~~des Zeitraums sollte der Zugriff auf das E-Mail-Konto zum Abholen von Nachrichten weiterhin möglichsein. Das Administrationsmodul MUSS die Rücknahme der Deregistrierung innerhalb ~~der 30 Tage~~des Zeitraums ermöglichen, um die E-Mail-Adresse wieder nutzen zu können. Hierfür MUSS das Administrationsmodul die Operation `revokeDeregistration` am Account

Manager aufrufen.
[<=]

[...]

3.7.4 Download PKCS#12 KOM-LE-Teilnehmer

A_19468-03 - Beantragen und Herunterladen der PKCS#12 Datei
Das Administrationsmodul MUSS die PKCS#12-Datei über die Operation `createCert()` am Account Manager beantragen und vom Account Manager herunterladen. ~~Nach dem Herunterladen der PKCS#12-Datei MUSS das Administrationsmodul diese mit dem vom Administrationsmodul erzeugten symmetrischen Schlüssel entschlüsseln~~.
[<=]

~~**A_21382 - Generierung eines symmetrischen Schlüssels für die PKCS#12-Datei**~~

~~Das Administrationsmodul MUSS bei Aufruf der Operation `createCert()` einen symmetrischen Schlüssel gemäß den Kriterien [gemSpec_Kryp] generieren und als Parameter CertPassword übergeben.~~

4.1.1 Allgemeine Festlegungen

[...]

Üblicherweise liegt ein Zertifikat zusammen mit dem zugehörigen geheimen Schlüssel in einem standardisierten und (optional) passwortgeschützten Format (p12) [PKCS#12] vor. Das Clientmodul kann ein Zertifikat und den zugehörigen geheimen Schlüssel auf mindestens zwei Arten nutzen:

1. Das Clientmodul importiert das Zertifikat und den Schlüssel aus der p12-Datei und verwaltet diese anschließend in einem eigenen Schlüsselspeicher. Wenn die p12-Datei passwort-geschützt ist, dann ~~Dazu~~ muss während des Importvorgangs das Passwort der p12-Datei eingegeben werden (Transportsicherung). Danach hat das Clientmodul Zugriff auf den für den TLS-Verbindungsaufbau benötigten privaten Schlüssel.
2. Das Clientmodul nutzt einen Systemschlüsselspeicher, z.B. den Zertifikatsspeicher von Windows oder den des Java JRE. Auch hier ist für den Importvorgang (optional) das Passwort der p12-Datei einzugeben. Anschließend stehen das Zertifikat und der Schlüssel über entsprechende Systemfunktionen/Bibliotheken zur Verfügung. Idealerweise kann der Administrator des Clientmoduls im gewählten Zertifikatsspeicher browsen und das gewünschte Zertifikat für die Verwendung auswählen. Alternativ kann in der Clientmodul-Konfiguration eine eindeutige Referenz auf das Zertifikat (Name oder Index) eingegeben werden.

~~**A_18783 - Import Schlüssel und Zertifikat als PKCS#12 Datei**~~

~~Das Clientmodul KOM-LE MUSS das Schlüsselmaterial und das Zertifikat für die TLS-Verbindungen als passwortgeschützte PKCS#12 Datei importieren können.~~

[...]

3.8.4 Entschlüsselung einer Nachricht mit einer SM-B bzw. einem HBA

[...]

KOM-LE-A_2061-01 - Speichern von Zuordnungen im Cache beim Entschlüsseln
Wird beim Entschlüsseln die erforderliche Karte (SM-B bzw. HBA) unter Verwendung der Operation `ReadCardCertificate` des Konnektors ermittelt, MUSS das Clientmodul die zu dieser Karte korrespondierende Zuordnung von E-Mail-Adresse des Empfängers, Zertifikats-ID und ICCSN im Cache (konfigurierbare Zeitdauer TTL_EMAIL_ICCSN) speichern.
[<=]

[...]

4.1.4 Transportsicherung zwischen Clientmodul und Fachdienst

[...]

A_22348-01 - Caching der Prüfergebnisse der TLS-Server-Zertifikate
Das Clientmodul KANN das Ergebnisse der Zertifikatsprüfung für eine definierte Zeitdauer (Tabelle 15: Tab_Konf_Param Standardkonfiguration allgemeine Parameter) temporär und manipulationssicher speichern. Für die Zuordnung sind eindeutige Identifikatoren, wie bspw. der Zertifikats-Fingerabdruck, zu verwenden. Bei erneuter Prüfung eines gleichen Zertifikats kann das vorangegangene Verifikations-Ergebnis dieses Zertifikats genutzt werden. Die Speicherdauer ist an die zeitliche Gültigkeit ("notAfter") des Zertifikats anzupassen, d.h. darf nicht über die Gültigkeit hinweg reichen.

[<=]

4.3 Protokollierung/Logging

Das Clientmodul soll Protokolldateien schreiben, die eine Analyse technischer Vorgänge erlauben. Diese Protokolldateien sind dafür vorgesehen, aufgetretene Fehler zu identifizieren~~, die Performance zu analysieren~~ und interne Abläufe zu beobachten. Um die Anforderungen an den Datenschutz zu gewährleisten, dürfen keine medizinischen und personenbezogenen Daten protokolliert werden. Geheimes Schlüsselmaterial darf ebenfalls nicht protokolliert werden.

KOM-LE-A_2079-01 - Protokolldateien für Ablauf und Fehler
Das Clientmodul MUSS das Protokollieren von Abläufen~~, Performanceinformationen~~ und Fehlern ermöglichen.**[<=]**

[...]

Der Zugriff auf Protokolldateien muss auf autorisierte Personen durch angemessene technische oder organisatorische Maßnahmen eingeschränkt werden. Die Logdateien können auf ein separates Speichermedium kopiert werden. Zudem soll der Administrator

das Protokollierenfür die Performanceanalyse und der internen Abläufe einzeln deaktivieren und wieder aktivieren können. Für den Produktivbetrieb soll das Protokollieren der internen Abläufe grundsätzlich deaktiviert sein. Damit die Protokolldateien nur begrenzten Speicherplatz belegen, werden sie automatisch nach einem konfigurierbaren Zeitraum gelöscht bzw. überschrieben.

KOM-LE-A_2084 - Aktivierung und Deaktivierung der Protokollierung von Performanceinformationen

Das KOM-LE-Clientmodul MUSS das Aktivieren und Deaktivieren der Protokollierung von Performanceinformationen ermöglichen.

<=

4.3.2 Performance

Die Protokolleinträge im Performanceprotokoll enthalten mindestens die in Tabelle Tab_Felder_Perf_Prot aufgezählten Felder und müssen geeignet sein, um die tatsächlichen Ausführungszeiten des KOM-LE-Clientmoduls mit den Vorgaben in Kapitel 4.6.1 zu vergleichen. Für jeden Aufruf einer Schnittstelle des Clientmoduls KOM-LE werden ein oder mehrere Protokolleinträge geschrieben.

Tabelle 3: Tab_Felder_Perf_Prot Felder im Performance-Protokoll

Feld	Beschreibung
Vorgangsnummer	Pseudozufällige Zeichenkette zur Korrelation der Protokolleinträge
Name der Aktion	Name der Aktion für Protokolleintrag
Startzeitpunk	Startzeitpunkt der Aktion
Endezeitpunkt	Endezeitpunkt der Aktion
Dauer in ms	Dauer in ms

KOM-LE-A_2088 - Felder zur Protokollierung der Performance

Das KOM-LE-Clientmodul MUSS die Protokollierung der Performance mit mindestens folgenden Feldern ermöglichen:

- pseudozufällige Zeichenkette zur Korrelation der Protokolleinträge,
- Name der Aktion für den Protokolleintrag,
- Startzeitpunkt der Aktion,
- Endezeitpunkt der Aktion und
- Dauer in ms.

<=

Jede der in Tabelle Tab_Auslöser_Prot_Entry aufgelisteten Aktionen führt zu einem Eintrag im Performanceprotokoll. Diese Durchlaufzeiten sollen separat protokolliert werden, damit die Ausführungszeit des Clientmoduls ohne Zeiten anderer Komponenten ermittelbar ist.

Tabelle 4: Tab_Auslöser_Prot_Entry Auslöser Protokolleinträge im Performanceprotokoll

Auslöser	Name der Aktion für Protokolleintrag	Beschreibung
Ankommen einer SMTP bzw. POP3-Meldung	SMTP bzw. POP3-Meldung	Wird beim Ankommen einer SMTP bzw. POP3-Meldung ausgelöst und endet mit der Weiterleitung an den Fachdienst oder der Antwort an das Clientsystem.
Aufruf einer Operation des Konnektors	Name der Operation	Wird durch den Aufruf einer Operation des Konnektors ausgelöst und endet mit der Rückkehr der Aktion

KOM-LE-A_2089 - Aktionen zur Protokollierung der Performance

Das KOM-LE-Clientmodul MUSS für die folgenden Aktionen Einträge in das Performanceprotokoll schreiben:

- Ankommen einer SMTP bzw. POP3-Meldung und
- Aufruf einer Schnittstelle des Konnektors.

<=

4.4 Konfiguration

Tabelle 5: Tab_Konf_Param Standardkonfiguration allgemeine Parameter

Parameter	Beschreibung des Parameters	Defaultwert
TLS_AUTH_KONNEKTOR	Authentifizierung des Clientmoduls gegenüber dem Konnektor bei aktivierter TLS-Verbindung (zertifikatsbasiert, Basic-Authentifizierung, ohne)	zertifikats-basiert
KONNEKTOR_TIMEOUT	Timeout für Aufrufe von Schnittstellen des Konnektors	1 Minute

SMTP_TIMEOUT_SERVER	Timeout für Antworten vom SMTP-Server auf SMTP-Kommandos	5 Minuten
SMTP_TIMEOUT_CLIENT	Timeout für das Warten auf neue SMTP-Kommandos vom Clientsystem	5 Minuten
POP3_TIMEOUT_SERVER	Timeout für Antworten vom POP3-Server auf POP3-Kommandos	5 Minuten
POP3_TIMEOUT_CLIENT	Timeout für das Warten auf neue POP3-Kommandos vom Clientsystem	5 Minuten
TTL_~~ENC_CERT~~VZD_DATA	Time to Live für gecachte Daten vom VZD wie Verschlüsselungs-zertifikate und Prüfergebnisse und KOM-LE-Versionen (maximaler Wert 24 Stunden)	12 Stunden
TTL_AM_DATA	Time to Live für gecachte Nutzer-Konfigurationsdaten (Operation getLimits) vom Account-Manager (maximaler Wert 24 Stunden)	12 Stunden
TTL_EMAIL_ICCSN	Time to Live für gecachte Zuordnungen von E-Mail-Adressen der Sender bzw. Empfänger zu ICCSNs von deren HBAs/SM-Bs	30 Tage
TTL_PROTS	Time to Live für Protokolldateien.	30 Tage
PROT_PERF	Protokolldatei für Performance	JA
KONNEKTOR_URI	URI des DVD des Konnektors	-
CM_KAS_TIMEOUT	Timeout bei Inaktivität der Kommunikation zwischen Clientmodul und KAS	30 Sekunden

[...]

KOM-LE-A_2184-01 - Standardwerte der Konfigurationsparameter
Die Konfiguration des Clientmoduls MUSS mit den in Tabelle Tab_Konf_Param Standardkonfiguration allgemeine Parameter definierten Defaultwerten ausgeliefert werden.
[<=]

[...]

5.5.1 Dokumente der gematik

704 [...]

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemLH_KOM-LE]	gematik: Lastenheft Adressierte Kommunikation Leistungserbringer
[gemSpec_FD_KOMLE]	gematik: Spezifikation Fachdienst KOM-LE
[gemSpec_Kon]	gematik: Spezifikation Konnektor
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_PKI]	gematik: Spezifikation PKI
[gemSMIME_KOMLE]	gematik: KOM-LE S/MIME Profil 1.0
[gemSysL_KOMLE]	gematik: Systemspezifisches Konzept KOM-LE
[gemSpec_VZD]	gematik: Spezifikation Verzeichnisdienst
[AccountManager.yaml]	gematik: https://raw.githubusercontent.com/gematik/api-kim/main/src/openapi/AccountManager.yaml
[AccountLimit.yaml]	gematik: https://raw.githubusercontent.com/gematik/api-kim/main/src/openapi/AccountLimit.yaml
[AttachmentService.yaml]	gematik: https://raw.githubusercontent.com/gematik/api-kim/main/src/openapi/AttachmentService.yaml
[Attachment_Schema]	gematik: https://raw.githubusercontent.com/gematik/api-kim/main/src/schema/Attachment_schema.json

705

706

707 1.2 Änderung in gemSpec_FD_KOMLE

708

709 3.2 Funktionen des Account Managers

710 [...]

711

712 **A_19591-01 - Eintrag Clientmodul-Version in VZD, Account Manager**

Der Account Manager MUSS die vom Clientmodul übermittelte KIM-Version im Verzeichnisdienst in den KOM-LE-Fachdaten und in seiner lokalen Datenbank für die betroffene "mail"-Adresse eintragen.**[**<=**]**

Es gelten die Festlegungen aus Kap. 4.~~4~~5., da der Verzeichnisdienst zur TI-Plattform gehört.

[...]

A_21376-01 - Eintrag der KOM-LE-Fachdaten in den VZD
Der Account Manager MUSS die vom Clientmodul übermittelten KOM-LE-Fachdaten (gemäß gemSpec_VZD#Datenmodell) während der Registrierung eines neuen KOM-LE-Teilnehmers in den Verzeichnisdienst und in seiner lokale Datenbank für die betroffene "mail"-Adresse eintragen.

Bei Eintragung der KIM-Version in den Verzeichnisdienst ist folgendes Schema zu verwenden: <Hauptversionsnummer.Nebenversionsnummer>
[<=**]**

Hinweis: Die lokale, beim Fachdienst existierende, Datenbank kann für die Bestimmung der aktuell im Verzeichnisdienst hinterlegten KIM Version eines Empfängers verwendet werden und ermöglich dann auch die Bestimmung der hinterlegten KIM Version, wenn durch den Nutzer eine Deregistrierung ausgelöst wurde.

[...]

A_23718 - Account Manager, Eintragung von Anwendungskennzeichen in den VZD
Der Account Manager MUSS die vom Clientmodul mittels der Operationen `registerAccount()` oder `setAccount()` übermittelten Anwendungskennzeichen a) auf Gültigkeit gegenüber dem FHIR Codesystem (https://simplifier.net/app-transport-framework/GEM-CS-KIM-Dienstkennung/$download?format=json) prüfen und b) wenn gültig, im Verzeichnisdienst in den KOM-LE-Fachdaten für die betroffene Mail-Adresse eintragen (Schnittstelle: I_Directory_Application_Maintenance, Operationen: add_Directory_FA-Attributes und modify_Directory_FA-Attributes).**[**<=**]**

A_23722 - Account Manager, regelmäßige Aktualisierung der Liste der Anwendungskennzeichen
Der Account Manager MUSS jede Stunde prüfen, ob eine neuere Version des FHIR CodeSystems (https://simplifier.net/app-transport-framework/GEM-CS-KIM-Dienstkennung/$download?format=json) mit den Anwendungskennzeichen vorhanden ist und ggf. diese herunterladen und persistent speichern.**[**<=**]**

Hinweis: Ob eine neuere Version des CodeSystems vorhanden ist kann mit der HTTP HEAD Operation geprüft werden. Die Dateigröße der heruntergeladenen JSON-Datei kann man als Hashfunktion verwenden. Mit Hilfe des Tools curl kann man die HTTP-Methode HEAD verwenden und damit erfahren ob die lokale Kopie der JSON-Datei noch aktuell ist.

[...]

3.4 Service Lokalisierung

[...]

A_19524-02 - Verwaltung Resource Records Typs für Service Discovery, KIM
Der KOM-LE-Fachdienst MUSS die aufgeführten Resource Records Types im Namensraum der TI gemäß folgender Tabelle verwalten. Zwischen den jeweiligen Fachdiensten MUSS folgender Port benutzt werden:

- SMTPS: 465 und
- POP3S: 995.

Tabelle 6: Tab_KOMLE_Service Discovery

Resource Record Bezeichner	Resource Record Type	Beschreibung
_fdkimsmtp._tcp.kim.telematik	PTR	Ermittlung aller KOM-LE-Anbieter (SMTP)
<fdkimsmtp>.<hrst_domain>.kim.telematik	SRV	SRV Resource Record zur Ermittlung der Ports und des FQDN des KOMLE-LE Fachdienstes
_fdkimpop._tcp.kim.telematik	PTR	Ermittlung aller KOM-LE-Anbieter (POP3)
<fdkimpop>.<hrst_domain>.kim.telematik	SRV	SRV Resource Record zur Ermittlung der Ports und des FQDN des KOMLE-LE Fachdienstes
_accmgr._tcp.kim.telematik	PTR	Ermittlung aller Account Manager Dienste aller KOM-LE-Anbieter.

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

[<=]

Die URL wird wie folgt gebildet:

```
https://<FQDN gemäß DNS-SD SRV RR>:<Port gemäß DNS-SD SRV RR><Base-path
gemäß TXT RR><path gemäß yaml Datei>
```

3.6 Protokollierung

[...]

Die folgende Anforderung wird aus der gemSpec_CM_KOMLE in die gemSpec_FD_KOMLE verschoben

A_21389 - Übermittlung der Clientmodul- und Produkttypversion an die gematik
Der KIM-Anbieter MUSS der gematik auf Anfrage eine nicht-personenbezogene Gesamtübersicht, der sich im Feld befindenden aktiven KIM-Clientmodule, zur Verfügung stellen. **[<=]**

3.8 Konfiguration

KOM-LE-A_2139-03 - Konfiguration Fachdienst
Der Fachdienst KOM-LE MUSS dem Anbieter mindestens die in der Tabelle Tab_Konfig_Parameter dargestellten Parameter zur Konfiguration zur Verfügung stellen.
[<=]

797 **Tabelle 7: Tab_Konfig_Parameter Konfigurationsparameter Fachdienst KOM-LE**

Parameter	Standardwert	Beschreibung
Maximale Nachrichtengröße	700 MB	Dieser Standardwert darf 700 MB nicht unterschreiten, da in KIM 1.5 mindestens 500 MB (netto) unterstützt werden müssen. 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 (brutto ca. 700 MB). Der KIM Teilnehmer kann den Wert auslesen über die Operation `getLimits`, Parameter `maxMailSize`.
Zeitraum für erneute Weiterleitungsversuche	15 Minuten	Dieser Wert gibt an, in welchem Intervall ein Weiterleitungsversuch durch den Mail Server unternommen werden soll.
Zeitraum für Weiterleitungsversuche	~~2~~ 8 Stunden	Nach Ablauf des konfigurierten Wertes werden keine weiteren Weiterleitungsversuche unternommen und es wird eine Fehlermeldung an den Sender übermittelt.
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 Nachrichten nach der endgültigen Deregistrierung	30 Tage	Nachrichten, die vom Fachdienst nach der endgültigen Deregistrierung eines Nutzers nicht abgeholt wurden, müssen nach der angegebenen Frist gelöscht werden.
Löschfrist für automatisch generierte Mails	90 Tage	Diese Löschfrist gilt für Mails, die vom Server automatisch generiert werden, insbesondere Zustellbestätigungen (DSN) und Abwesenheitsnotizen (vacation)
Löschfrist von Logfiles	90 Tage	Die im Rahmen der Nachrichtenverarbeitung erzeugten Logfiles müssen nach der angegebenen Frist gelöscht werden.
Ablaufzeitspanne	5 Minuten	Ablaufzeitspanne für die Requests zum Account Manager. Nach Ablauf der

		Zeitspanne müssen die Requests abgelehnt 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

4.2 Schnittstelle I_Attachment_Services

[...]

Tabelle 8: Operationen vom KAS

Operation	URI	Methode	Request	Response	Beschreibung
add_Attachment	/attachment/	POST	recipients messageID expires binary <File>	string <Freigabelink>	Fügt verschlüsselte E-Mail-Daten im KAS hinzu
delete_Maildata	/attachment/{attachmentId}	POST		200	Löschen von auf dem KAS abgelegten E-Mail-Daten
read_Attachment	/attachment/{attachmentId}	GET	recipient	binary <File>	Lädt die unter einem Freigabelink erreichbaren verschlüsselten E-Mail-Daten herunter

A_19375-05 - KAS – Implementierung der Schnittstelle
Der KAS MUSS die Schnittstelle I_Attachment_Services als REST-Webservices über HTTPS gemäß [AttachmentServices.yaml] in der Version 2.3.~~0~~2 implementieren. Des Weiteren MUSS der KAS für alle in der [AttachmentServices.yaml] definierten Operationen den Zeichensatz UTF-8 unterstützen.
[<=]

[...]

A_21386-01 - KAS - HTTP-Basic-Authentifizierung
Der KAS MUSS bei Aufruf der Operationen `add_attachment` und `delete_Maildata` eine HTTP-Basic-Authentifizierung durchführen.
[<=]

[...]

A_19378-02 - KAS - prüfen der Größe der verschlüsselten E-Mail-Daten
Der KAS MUSS die Dateigröße der verschlüsselten E-Mail-Daten ermitteln, bevor diese gespeichert werden. Der KAS MUSS die Verarbeitung ablehnen, wenn die Gesamtgröße der verschlüsselten E-Mail-Daten den Konfigurationswert (Quota - zwischen Anbieter und Nutzer vereinbart) des KAS übersteigt.
[<=]

[...]

A_19385-03 - KAS – Löschen von Ressource
Der Anbieter des KAS MUSS sicherstellen, dass alle gespeicherten E-Mail-Daten, mit abgelaufener Gültigkeit (`Expires`) zuzüglich einer Karenzzeit von einer Stunde gelöscht werden.
[<=]

Der Wert `Expires` (RFC822 date-time) entspricht dem Ablaufdatum der E-Mail-Daten, der beim Aufruf der Operation add_Attachement() vom Clientmodul übergeben wird. Die Berücksichtigung einer Karenzzeit soll das vorzeitige Löschen der E-Mail-Daten vom KAS verhindern, wenn die Nachricht mit der KIM-Attachment-Datenstruktur erst kurz vor dem Expires-Zeitpunkt heruntergeladen wird.

4.3 Schnittstelle I_AccountManager_Service

[...]

Tabelle 9: Operationen vom Account Manager

Operation	URI	Methode	Request	Response	Beschreibung
`registerAccount`	/account	POST	username password referenc	<Status>	Registrierung des Teilnehmers am KOM-LE-Fachdienst.

			eID iniPassword kimVersion appTags <JWT>		
createCert	/account/{username}/cert	POST	username password certPassword commonName <JWT>	<Status> <PKCS#12-Datei>	Anforderung und Herunterladen der PKCS#12-Datei
setAccount	/account/{username}	PUT	username password(alt) password(neu) kimVersion dataTimeToLive appTags <JWT>	<Status>	Aktualisierung des Accounts: - Passwort - kimVersion - dataTimeToLive - Anwendungskennzeichen (appTags)
getAccount	/account/{username}	GET	username password <JWT>	<Status> username kimVersion regStat deregDate	Lesen der Account Attribute.
revokeDeregistration	/account/{username}/revokeDeregistration	PUT	username password <JWT>	<Status>	Rücknahme der Deregistrierung eines Accounts

getOTP	/account/{username}/OTP	GET	username password <JWT>	<Status> OTP	Liest für den KIM Account/E-Mail Adresse ein One-Time-Passwort (OTP) aus, mit dem die E-Mail-Adresse zu einer Telematik-ID (Karte) portiert werden kann.
setTID	/account/{username}/telematikID	POST	username password <JWT> OTP	<Status>	Entfernt die E-Mail-Adresse vom bisherigen VZD-Eintrag und trägt die für den aktuellen VZD-Eintrag (der den Authentisierungsdaten dieser Operation setTID entspricht) ein.
updateOutOfOffice	/account/{username}/outofoffice	PUT	username password startDate endDate message active <JWT>	<Status>	Einstellung der Abwesenheitsnotiz für den Account aktualisieren
getOutOfOffice	/account/{username}/outofoffice	GET	username password <JWT>	<Status> startDate endDate message active	Einstellung der Abwesenheitsnotiz für den Account lesen
deregisterAccount	/account/{username}	DELETE	username password <JWT>	<Status>	Deregistrierung des Teilnehmers am KOM-LE-Fachdienst.

A_20063-04 - Account Manager - Implementierung der Schnittstelle
Die Teilkomponente Account Manager des Fachdienstes MUSS die Schnittstelle I_AccountManager_Service als REST-Webservice über HTTPS gemäß [AccountManager.yaml] in der Version 2.3.~~0~~1 implementieren. Des Weiteren MUSS der Account Manager für alle in der [AccountManager.yaml] definierten Operationen den Zeichensatz UTF-8 unterstützen.
[<=]

[...]

A_23732 - Account Manager - Aktionen bei Deregistrierung
Der Account Manager MUSS bei einer Deregistrierung eines Accounts folgende Aktionen ausführen:

- Speichern der im VZD für den Account existierenden Fachdaten
- Löschen der im VZD für den Account existierenden Fachdaten (Schnittstelle I_Directory_Application_Maintenance, Operation delete_Directory_FA-Attributes)

[<=]

Hinweis: Weitere für den Account konfigurierte Daten (wie maxMailSize oder dataTimeToLive) bleiben erhalten.

A_23733 - Account Manager - Aktionen bei Rücknahme einer Deregistrierung
Der Account Manager MUSS bei Rücknahme einer Deregistrierung eines Accounts folgende Aktionen ausführen:

- Wiederherstellen der bei der Deregistrierung des Accounts gespeicherten Fachdaten im VZD.

[<=]

[...]

KOM-LE-A_2167-05 - Sperrung des Accounts
Der Fachdienst KOM-LE MUSS den Account eines Teilnehmers nach spätestens drei aufeinanderfolgenden Fehleingaben des Passwortes temporär gegen Brute-Force Angriffe schützen. Hierzu wird spätestens nach der dritten Falscheingabe eine Wartezeit für den nächsten Log-In Versuch vorgegeben, für die weitere Log-in Versuche nicht möglich sind. Die Wartezeit MUSS geeignet gewählt werden, um Brute-Force-Angriffe zu erschweren und gleichzeitig eine akzeptable User-Experience zu erhalten. Im Fall einer Falscheingabe wird dem KOM-LE-Client der Fehlercode 535 (*Authentication credentials invalid*) gemäß [RFC3463] zurückgegeben.
[<=]

A_18784-04 - Bereitstellung Schlüssel und Zertifikat für Clientmodul als passwortgeschützte PKCS#12 Datei
Der Account Manager ~~KOM-LE-Anbieter~~ MUSS dem KOM-LE-Clientmodul ~~Teilnehmer~~ das Schlüsselmaterial und das Zertifikat für die Authentifizierung an den KOM-LE-Fachdienst-Schnittstellen ~~das KOM-LE-Clientmodul~~ über die Schnittstelle I_AccountManager_Service als (optional passwortgeschützte) PKCS#12-Datei zur Verfügung stellen. Die Übermittlung der PKCS#12-Datei muss über eine verschlüsselte, authentifizierte und integritätsgeschützte Verbindung erfolgen. Das KOM-LE-Clientmodul generiert ~~MUSS~~ das Passwort für die PKCS#12-Datei ~~generieren~~ und übermittelt es ~~dem KOM-LE-Fachdienst~~ im Request der Operation ~~übermitteln~~. Im Response übergibt der KOM-LE Fachdienst die – mit dem übermittelten Passwort geschützte – PKCS#12-Datei.
[<=]

A_19542-02 - Schnittstelle für den Download
~~Die Teilkomponente~~ Der Account Manager ~~des Fachdienstes KOM-LE~~ MUSS dem Administrationsmodul eine Operation für die Beantragung und das Herunterladen der PKCS#12-Datei bereitstellen. Wenn vom Clientmodul ein Passwort für die PKCS#12 Datei übergeben wurde, dann MUSS der Account Manager ~~MUSS~~ die PKCS#12-Datei vor der Bereitstellung mit einem vom Passwort abgeleiteten ~~dem vom Administrationsmodul~~

übergebenen symmetrischen Schlüssel verschlüsseln. Für die Verschlüsselung MÜSSEN die Vorgaben aus [gemSpec_Krypt] eingehalten werden.**[<=]**

KOM-LE-A_2187-05 - Authentifizierung des KOM-LE-Teilnehmers über AUT-Zertifikat am AccountManager
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 über das vom Clientmodul übergebene Json-Web-Token prüfen. Hierzu MUSS der Fachdienst folgende Prüfschritte durchführen:

- ist das Token korrekt (mit Validierung der erzeugten Signatur),
- ist das Token zeitlich gültig (also die Verarbeitung erfolgt zwischen `iat` und `exp` ~~`nbf` und `nbf` + konfigurierter Ablaufzeitspanne erfolgt~~),
- sind Username und Passwort korrekt

Für die Operationen gilt:

- bei Aufruf der Operation `registerAccount` und `revokeDeregistration`:
  Die Fachdaten des KOM-LE-Teilnehmers müssen während der Registrierung bzw. bei der Rücknahme einer Deregistrierung in den VZD-Datensatz mit der Telematik-ID des AUT-Zertifikats aus dem Token eingetragen werden.
- bei Aufruf ~~aller anderen~~ der Operationen `setAccount` und `deregisterAccount`:
  Der - in der Operation angegebene - Parameter *username* (E-Mail Adresse) muss in dem VZD-Datensatz mit der Telematik-ID des AUT-Zertifikats aus dem Token im *mail* Attribut der Fachdaten vorhanden sein.

Ist einer dieser Prüfschritte nicht erfolgreich MUSS die Nachricht zurückgewiesen werden. Sind alle Prüfungen erfolgreich, ist die Nachricht valide und MUSS vom Account Manager verarbeitet werden.
[<=]

4.4 Schnittstelle I_AccountLimit_Services

[..]

A_22420-01 - I_AccountLimit_Services – TLS-gesicherte Verbindung
Die Teilkomponente Account Manager des Fachdienstes MUSS die Schnittstelle I_AccountLimit_Service durch Verwendung von TLS mit ~~beid~~serverseitiger Authentisierung sichern. Die Teilkomponente Account Manager des Fachdienstes MUSS für diese TLS-Verbindungen TI-Zertifikate (analog zu Schnittstelle I_Message_Service) nutzen. Die Teilkomponente Account Manager des Fachdienstes MUSS sich mit der Server-Identität von Schnittstelle I_AccountLimit_Service authentisieren.

[<=]

4.5 Schnittstelle I_ServiceInformation

Der KOM-LE-Fachdienst stellt einen Webservice zur Abfrage von Informationen über den KIM Fachdienst bereit. Die Schnittstellenbeschreibung I_ServiceInformation ist in

[ServiceInformation.yaml] definiert. Der Aufruf der REST-Schnittstelle ist ausschließlich vom Clientmodul zulässig.

In der folgenden Tabelle ist die Operation getServiceInformation mit der entsprechenden HTTP-Methode dargestellt. Die Operation ist eine Abstraktion auf den Webservice Endpunkt /ServiceInformation.

Tabelle 10 Operation der Schnittstelle - I_ServiceInformation

Operation	URI	Methode	Request	Response	Beschreibung
getServiceInformation	/ServiceInformation/	GET	-	<Status> - ServiceInformation	Abfragen der Informationen über den KIM Fachdienst

A_23753 - Implementierung der Schnittstelle I_ServiceInformation
Der KOM-LE-Fachdienst MUSS die Schnittstelle I_ServiceInformation als REST-Webservice über HTTPS gemäß [ServiceInformation.yaml] in der Version 1.0.0 implementieren. Des Weiteren MUSS der KOM-LE-Fachdienst für alle in der [ServiceInformation.yaml] definierten Operationen den Zeichensatz UTF-8 unterstützen.
[<=]

A_23754 - I_ServiceInformation – TLS-gesicherte Verbindung
Der KOM-LE-Fachdienst MUSS die Schnittstelle I_ServiceInformation durch Verwendung von TLS mit serverseitiger Authentisierung sichern. Der KOM-LE-Fachdienst MUSS für diese TLS-Verbindungen TI-Zertifikate (analog zu Schnittstelle I_Message_Service) nutzen. Der KOM-LE-Fachdienst MUSS sich mit der Server-Identität von Schnittstelle I_ServiceInformation authentisieren.**[<=]**

4.~~56~~ Genutzte Schnittstellen der TI-Plattform

[...]

KOM-LE-A_2231-01 - Schnittstellen der TI-Plattform
Der Fachdienst KOM-LE MUSS die in der Tabelle Tab_Interface_TIP aufgeführten Schnittstellen der TI-Plattform benutzen.
[<=]

Tabelle 11: Tab_Interface_TIP Schnittstellen zur TI-Plattform des Fachdienstes KOM-LE

Schnittstelle	Operation	benutzt durch

I_Directory_Application_Maintenance	get_Directory_FA-Attributes 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_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

A_20189-02 - Übermittlung der benötigten KOM-LE Version des Clientmoduls
Der Anbieter des KOM-LE-Fachdienstes MUSS seinem KOM-LE Teilnehmer bei der Erstellung des Accounts sowie bei einem relevanten Update des Fachdienstes, die nötige KOM-LE-Version des Clientmoduls mitteilen.
[<=]

Die KOM-LE-Version des Clientmodules muss mitgeteilt werden, damit der Nutzer weiß, welche Clientmodul-Version zu verwenden ist. Bei Nutzung eines Clientmodules in der KOM-LE-Version 1.0 ist eine Registrierung durch den Teilnehmer über die KOM-LE-1.5-Schnittstelle am KOM-LE-Fachdienst nicht möglich.

Die Übermittlung der KOM-LE-Version vom Anbieter kann hierbei in geeigneter Form erfolgen. ~~Die jeweilige Client-Version kann aus dem LDAP-Directory-Attribut: `komLeData` vom VZD entnommen werden.~~ Geltende KOM-LE-Versionen sind `1.0` und `1.5` und werden in der Form in das Header-Element `X-KOM-LE-Version` eingetragen.

[...]

5.4 Betriebsdatenerfassung

Um die Kommunikation über KIM besser zu verstehen und um im Fehlerfall die Ursache einfacher ermitteln zu können, werden Metadaten der Kommunikationsbeziehungen zentral erfasst und analysiert. Die Daten werden pseudonymisiert und es ist nicht möglich die Kommunikationsbeziehungen konkreter KIM-Teilnehmer zu überwachen.

A_23746 - KIM Fachdienst, Betriebsdatenerfassung Senderichtung
Der KIM Fachdienst MUSS für jede von den Clientmodulen eingehende KIM-Nachricht einen Reporting Datensatz erzeugen und per Schnittstelle I_OpsData_Update an die gematik übertragen.
Der Reporting Datensatz MUSS alle X-KIM-* Header-Elemente beinhalten.

Der Datensatz MUSS dem Format des Rohdaten-Performance-Berichts gemäß [gemSpec_Perf] entsprechen. Die Felder `<duration>` und `<status>` bleiben frei. Der Wert für das Feld `<operation>` MUSS `"mailFromCm"` sein. Die X-KIM-* Header werden aus dem Mail-Header übernommen und durch das Zeichen `"|"` getrennt.

Im Header-Element `X-KIM-FromData` MUSS die enthaltene Absender-Mail-Adresse durch den sha256 hash der Absender-Mail-Adresse ersetzt werden. Die weiteren Bestandteile dieses Header Elements werden übernommen. Bei der Erzeugung des Hash-Wertes MUSS ein nur dem KIM Fachdienst bekanntes SALT verwendet werden.
[<=]

Beispiel für X-KIM-FromData:

```
X-KIM-FromData:
{sha256(sender@sender.kim+salt),10117,1.2.276.0.76.4.50,urn:oid:1.3.6.1.4.1
.19376.3.276.1.5.5|urn:oid:1.3.6.1.4.1.19376.3.276.1.5.4}
```

Beispiel für Reporting Datensatz (unvollständig):

```
2023-03-30T10:02:16+01:00;;mailFromCm;;X-KIM-Message-ID:
II8HEDLEUEU4.EG0B98QUZNPM2@STST-TEST|X-KIM-Sendersystem: ps1|...
```

A_23748 - KIM Fachdienst, Betriebsdatenerfassung Empfangsrichtung
Der KIM Fachdienst MUSS für jede von einem KIM Fachdienst eingehende KIM-Nachricht einen Reporting Datensatz erzeugen und per Schnittstelle I_OpsData_Update an die gematik übertragen.
Der Reporting Datensatz MUSS alle X-KIM-* Header-Elemente beinhalten.

Der Datensatz MUSS dem Format des Rohdaten-Performance-Berichts gemäß [gemSpec_Perf] entsprechen. Die Felder `<duration>` und `<status>` bleiben frei. Der Wert für das Feld `<operation>` MUSS `"mailFromFd"` sein. Die X-KIM-* Header werden aus dem Mail-Header übernommen und durch das Zeichen `"|"` getrennt.

Im Header-Element `X-KIM-ToData` und `X-KIM-CcData` MÜSSEN die enthaltenen Absender-Mail-Adressen durch den sha256 hash der jeweiligen Absender-Mail-Adresse ersetzt werden. Die weiteren Bestandteile dieses Header Elements werden übernommen. Bei der Erzeugung des Hash-Wertes MUSS ein nur dem KIM Fachdienst bekanntes SALT verwendet werden.**[<=]**

6.5.1 Dokumente der Gematik

[DirectoryApplicationMaintenance.yaml]

~~gematik: https://github.com/gematik/api-kim/blob/master/src/openapi/DirectoryApplicationMaintenance.yaml~~

gematik: api-vzd/DirectoryApplicationMaintenance.yaml at main · gematik/api-vzd (github.com)

1.3 Änderung in AttachmentService.yaml

siehe akquinet Pull request https://github.com/gematik/api-kim/pull/18

siehe Pull request https://github.com/gematik/api-kim/pull/23

1.4 Änderung in AccountManager.yaml

- Parameter der `setAccount` Operation überarbeitet,

- `dataTimeToLive` Maximalwert (maximum) auf 90 reduziert,

siehe Pull request https://github.com/gematik/api-kim/pull/23

1.5 Änderung in AccountLimit.yaml

siehe Pull request https://github.com/gematik/api-kim/pull/23

1.6 Änderung in gemSpec_Perf

2.5.2 Rohdaten-Performance-Reporting (Rohdatenerfassung v.02)

Tab_gemSpec_Perf_Produkte_Rohdatenerfassung_Version_v02

PDT	Produkttyp
PDT02	Trust Service Provider X.509 QES
PDT03	Trust Service Provider X.509 nonQES - eGK
PDT24	Fachdienst KOM-LE

PDT36	Trust Service Provider X.509 nonQES - HBA
PDT38	Trust Service Provider X.509 nonQES – SMC-B
PDT52	Identity Provider Dienst
PDT64	TI-Messenger Fachdienst
PDT68	sektoraler Identity Provider

Neue Kapitel / Struktur:

3.x Kommunikation im Medizinwesen KOM-LE

Im folgenden Kapitel werden die spezifischen, performancerelevanten Anforderungen an die KIM-Anwendung und ihre Komponenten ausgeführt.

3.x.1 Leistungsanforderungen KOM-LE

Übernahme der Inhalte aus dem bisherigen Kapitel 4.1.3 Kommunikation Leistungserbringer (KOM-LE)

[...]

Hinweis: In der Version KOM-LE 1.0 ist die Nachrichtengröße auf ~~25 MB~~ 15 MiB begrenzt. Ab KOM-LE 1.5 ist es auch möglich E-Mail-Nachrichten mit Anhängen größer ~~25 MB~~ 15 MiB zu versenden bzw. zu empfangen. Der Mail-Body ohne Anhänge darf aber weiterhin die Größe von ~~25 MB~~ 15 MiB nicht übersteigen und muss durch das KOM-LE-Clientmodul und den KOM-LE-Fachdienst verarbeitet werden.

[...]

3.x.1.1 Lastmodell KOM-LE

Übernahme der Inhalte aus dem bisherigen Kapitel *4.1.8 Lastmodell auf Ebene der Anwendungsfälle*

3.x.1.2 Bearbeitungszeiten KOM-LE

Übernahme der Inhalte aus dem bisherigen Kapitel *4.2.1 Bearbeitungszeiten KOM-LE*

3.x.1.3 Performancevorgaben KOM-LE

Übernahme der Inhalte aus dem bisherigen Kapitel *"5.4.2 Produkttyp KOM-LE Fachdienst" mit folgenden Änderungen:*

[...]

GS-A_5138-02 - Performance – KOM-LE-Fachdienst – TLS-Verbindungsaufbau unter Last

Der Produkttyp KOM-LE-Fachdienst MUSS ~~die Bearbeitungszeitvorgabe aus Tab_gemSpec_Perf_KOMLE_Clientmodul für den „Aufbau TLS-Kanal zwischen KOM-LE-Clientmodul und KOM-LE-Fachdienst“~~ erreichen, dass der TLS-Verbindungsaufbau, unter der für diesen Anwendungsfall gemäß Tabelle Tab_gemSpec_Perf_KOMLE_Fachdienst anliegenden Spitzenlast, ~~für seine KOM-LE-Teilnehmer~~ im Mittel innerhalb von 3,9 Sekunden abgeschlossen wird ~~erfüllen~~. ~~Der KOM-LE-Fachdienst muss diese Zeiten unter der Nebenbedingung erbringen, dass die anderen Produkttypen die Zeiten gemäß der Zerlegung der Bearbeitungszeiten in Tabelle Tab_gemSpec_Perf_KOMLE_Bearbeitungszeitbeiträge einhalten. Bei gecachten OCSP-Responses reduziert sich die Zeit um den dort angegebenen Betrag.~~
[<=]

Zur Erläuterung der Afo [GS-A_5138-0~~1~~2]:

Der Anbieter muss die Anzahl seiner KOM-LE-Teilnehmer kennen und sein System mindestens so dimensionieren, dass die Lastvorgaben eingehalten werden. Beispielrechnung: Für 210.000 KOM-LE-Teilnehmer (siehe Tabelle "Tab_Mengengerüst: Annahmen für Modellierung") ergibt sich auf Basis von 10.000 Teilnehmern eines Anbieters eine Spitzenlast von 41 Anfragen pro Sekunde mit einer mittleren Bearbeitungszeit von 3,9 Sekunden für den Aufbau des TLS-Kanals zwischen KOM-LE-Clientmodul und KOM-LE-Fachdienst. (5% von 820 Anfragen pro Sekunde).

Die Anforderung gilt für alle Server-Komponenten des KOM-LE-Fachdienstes (Mailserver, Account Manager und KAS).

[...]

A_20127-01 - Performance - KOM-LE-Fachdienst – Spitzenlastvorgaben für den KAS
Der Anbieter KOM-LE-Fachdienst MUSS den KAS und die Anbindung an das zentrale Netz der TI mindestens so dimensionieren, dass ~~für seine Nutzer~~ die erwartete Spitzenlast gemäß Tabelle "Tab_gemSpec_Perf_KOMLE_Fachdienst: Lastvorgaben des KAS" erfüllt wird.

Die Lastvorgaben sind für ~~die vom Anbieter definierte maximale Größe der Zulässigen~~ 20 MiB Anhänge zu erfüllen.

Tabelle 12 Tab_gemSpec_Perf_KOMLE_Fachdienst: Lastvorgaben des KAS

Schnittstellenoperationen	Spitzenlast [1/sec]
I_Attachment_Service::add_Attachment	~~22~~ 5
I_Attachment_Service::read_Attachment	~~30~~ 5
~~I_Attachment_Service::MaxMailSize~~	~~22~~

[<=]

~~Zur Erläuterung der Afo [A_20127]:~~

~~*Der Anbieter muss die Anzahl seiner KOM-LE-Teilnehmer kennen und sein System mindestens so dimensionieren, dass die Lastvorgaben eingehalten werden. Beispielrechnung: Für 210.000 KOM-LE-Teilnhmer (siehe Tabelle "Tab_Mengengerüst: Annahmen für Modellierung") ergibt sich auf Basis von 10.000 Teilnehmern eines*~~

~~*Anbieters eine Lastvorgabe von mindestens 1 Anfrage pro Sekunde für das Hochladen von Anhängen (I_Attachment_Service::add_Attachment) mit einer vom Anbieter definierten maximal zulässigen Größe von z. B. 250 MB. (5% von 22 Anfragen pro Sekunde).*~~

~~**A_20130 - Performance - KOM-LE-Fachdienst - TLS Kanal KAS**~~

~~Der Anbieter KOM-LE-Fachdienst MUSS den KAS so dimensionieren, dass für seine Nutzer die erwartete Spitzenlast gemäß "Tab_gemSpec_Perf_KOMLE_Fachdienst: Lastvorgaben des KAS" für den Aufbau des TLS-Kanal zwischen KOM-LE-Clientmodul und KOM-LE-Fachdienst erfüllt wird.~~

~~<=~~

[...]

3.x.2 Rohdaten-Performance-Reporting Spezifika KOM-LE

In Ergänzung an die allgemeinen Anforderungen an das Performance-Rohdaten-Reporting befinden sich nachfolgend die produktspezifischen Anforderungen.

3.x.2.1 Umfang KOM-LE

keine Spezifischen Anforderungen zum Umfang

3.x.2.2 Format KOM-LE

A_23823 - Performance - Rohdaten - Spezifika Fachdienst KOM-LE Status (Rohdatenerfassung v.02)
In Ergänzung zu A_21981 MUSS im Feld "status" der Rückgabewert desjeweiligen Protokolls eingetragen werden. Also bei send_Message und receive_Message der jeweilige SMTP bzw. POP3 Statuscode und bei add_Attachement und read_Attachement der Status des jeweils genutzten Protokolls. **[**<=**]**

A_23170 - Performance - Rohdaten - Spezifika Fachdienst KOM-LE Format (Rohdatenerfassung v.02)
Der KOM-LE-Fachdienst MUSS für jede Nachricht bzw. jedes Attachement innerhalb einer Operation (send_Message, receive_Message, add_Attachment, read_Attachment) eine neue Zeile schreiben.**[**<=**]**

A_23168 - Performance - Rohdaten - Spezifika KIM-FD - Operation (Rohdatenerfassung v.02)
Das Produkt MUSS bei Rohdaten-Performance-Berichten bzgl. der "operation"- und "duration_in_ms"-Felder, in Ergänzung zu A_21981, die Vorgaben aus der Tabelle Tab_gemSpec_Perf_Berichtsformat_KIM-FD berücksichtigen.**[**<=**]**

Tab_gemSpec_Perf_Berichtsformat_KIM-FD

$operation	Produkttyp-Komponente	Operation	Beschreibung und Definition duration

I_Message_Service::send_Message	FD-KIM-Mail-Server	send_Message	Bei Aufruf der Operation send_Message beginnt die Messung mit dem Zeitpunkt der quittierten Übergabe der Nachricht vom KIM Clientmodul an den KIM Fachdienst des E-Mail-Senders und endet mit dem Zeitpunkt der quittierten Übergabe an den KIM Fachdienst des E-Mail-Empfängers.
I_Message_Service::receive_Message	FD-KIM-Mail-Server	receive_Message	Bei Aufruf der Operation receive_Message beginnt die Messung mit dem Zeitpunkt der Annahme der Operation an der Außenschnittstelle des Produkttyps und endet mit dem Zeitpunkt der quittierten Übergabe der Nachricht an das KIM Clientmodul des E-Mail-Empfängers.
I_Attachment_Service::add_Attachment	FD-KIM-KAS	add_Attachment	Bei Aufruf der Operation add_Attachment beginnt die Messung mit Annahme des Anhangs an der Außenschnittstelle des Produkttyps und endet mit dem quittierten Versand der Antwort an der

			Außenschnittstelle zum KIM-Client.
I_Attachment_Service::read_Attachment	FD-KIM-KAS	read_Attachment	Bei Aufruf der Operation read_Attachment beginnt die Messung mit der Anfrage des KIM-Clients an der Außenschnittstelle des Produkttyps und endet mit dem quittierten Ende des Versands des Anhangs bzw. der Anhänge.

A_23167 - Performance - Rohdaten - Spezifika KIM message-Block (Rohdatenerfassung v.02)
Das Produkt MUSS - bei Rohdaten-Performance-Berichten im "message"-Feld – folgende Informationen im JSON-Format übermitteln:

```
{
"Message-ID": "$Message-ID",
"X-KIM-Header": "$Wert",
"size": $size,
"Richtung": "$Richtung"
}
```

Für $Message-ID ist die entsprechende Message-ID einzutragen.
Für "X-KIM-Header" sind alle X-KIM-Header der jeweiligen äußeren Nachricht und die dazugehörigen Werte ($Wert) einzutragen.
Für $size ist das übertragene Datenvolumen in Byte als Integer einzutragen.
Für $Richtung ist entweder "CM-FD" einzutragen falls die Operation zwischen Clientmodul und Fachdienst durchgeführt wird oder "FD-FD" falls die Operation zwischen Fachdiensten durchgeführt wird.**[**<=**]**

~~5.4.1 Produkttyp KOM-LE-Clientmodul~~

~~GS-A_5136 - Performance – KOM-LE-Clientmodul – Bearbeitungszeit unter Last~~

~~Der Produkttyp KOM-LE-Clientmodul MUSS die Bearbeitungszeitvorgaben unter Last aus Tab_gemSpec_Perf_KOMLE_Clientmodul unter der für die Anwendungsfälle parallel anliegenden Spitzenlast erfüllen. Die Lastanforderungen müssen von den Clientmodulen für die jeweilige Leistungserbringerumgebung LE-U1, LE-U2, LE-U3 oder LE-U4 erbracht~~

werden. Das KOM-LE-Clientmodul muss diese Zeiten unter der Nebenbedingung erbringen, dass die anderen Produkttypen die Zeiten gemäß der Zerlegung der Bearbeitungszeiten in Tabelle Tab_gemSpec_Perf_KOMLE_Bearbeitungszeitbeiträge einhalten und dass die Ausführung auf einem durchschnittlichen PC erfolgt.

<=

Tabelle 13: Tab_gemSpec_Perf_KOMLE_Clientmodul: Last- und Bearbeitungszeitvorgaben

Anwendungsfall	Datenmenge in KB	Spitzenlast [1/h]				Bearbeitungszeit
		LE-U1	LE-U2	LE-U3	LE-U4	Mittelwert [sec]
Empfängerdaten ermitteln	10	10	37	94	237	1,2
Nachricht schützen und an KOM-LE-Fachdienst senden	50	200	200	200	200	8,9
	100	10	35	90	224	12,5
	25600	13	13	13	13	260 (*)
Nachricht vom KOM-LE Fachdienst holen und aufbereiten	50	200	200	200	200	4,3
	100	10	35	90	224	4,8
	25600	13	13	13	13	38,5 (*)
Aufbau sicherer Kanal vom Clientmodul zum Fachdienst	-	34	34	70	70	3,9

(*) In diesem besonderen Nutzungsbedarf wird von einer Transportnetzanbindung von 16 Mbit/sec in Download-Richtung und 1024 Kbit/sec in Upload-Richtung ausgegangen.

Tabelle 14: Tab_gemSpec_Perf_KOMLE_Bearbeitungszeitbeiträge: Zerlegung Bearbeitungszeiten

Anwendungsfall	Datenmenge in KB	Bearbeitungszeitbeiträge [sec]					
		Konnektor, Anzeige am Arbeitsplatz, Kartenterminal, Karten, Verzeichnisdienst	LE-LAN	Zugangsnetz	KOM-LE Clientmodul	KOM-LE Fachdienst	OCSP-Responder
Empfängerdaten ermitteln	10	1,0	0,0	0,1	0,0	0,0	0,0
	50	3,3	0,1	3,9	0,5	0,0	1,0

Nachricht schützen und an KOM-LE Fachdienst senden	100	3,3	0,1	7,5	0,5	0,0	1,0
	25600	4,6	23,5	229,3 *	1,0	0,0	1,0
Nachricht vom KOM-LE Fachdienst holen und aufbereiten	50	1,2	0,1	0,6	0,5	0,0	1,0
	100	1,2	0,1	1,1	0,5	0,0	1,0
	25600	2,3	18,8	14,4 *	1,0	0,0	1,0
Aufbau TLS-Kanal zwischen KOM-LE-Clientmodul und KOM-LE-Fachdienst	-	1,3	0	0,4	0,1	0,1	2,0

(*) In diesem besonderen Nutzungsbedarf wird von einer Transportnetzanbindung von 16 Mbit/sec in Download-Richtung und 1024 Kbit/sec in Upload-Richtung ausgegangen.

1.7 Änderungen in gemSpec_VZD

4.3 Schnittstelle I_Directory_Application_Maintenance

Am Ende vom Kapitel wird eingefügt:

A_23728 - VZD, I_Directory_Application_Maintenance, Aktualisierung zulässiger Anwendungskennzeichen

Der VZD MUSS jede Stunde prüfen, ob eine neuere Version des FHIR CodeSystems (https://simplifier.net/app-transport-framework/GEM-CS-KIM-Dienstkennung/$download?format=json) mit den Anwendungskennzeichen vorhanden ist und ggf. diese herunterladen und persistent speichern.**[<=]**

Hinweis: Ob eine neuere Version des CodeSystems vorhanden ist kann mit der HTTP HEAD Operation geprüft werden. Die Dateigröße der heruntergeladenen JSON-Datei kann man als Hashfunktion verwenden. Mit Hilfe des Tools curl kann man die HTTP-Methode HEAD verwenden und damit erfahren ob die lokale Kopie der JSON-Datei noch aktuell ist.

4.3.2.4 Nutzung LDAPv3

Am Ende vom Kapitel wird eingefügt:

A_23729 - VZD, I_Directory_Application_Maintenance, Anwendungskennzeichen Prüfung LDAP

Der VZD MUSS bei Änderungen an KOM-LE-Fachdaten mit den Operationen "add_Directory_FA-Attributes (LDAPv3)" und "modify_Directory_FA-Attributes (LDAPv3)" den Inhalt von Parameter Anwendungskennzeichen (appTags) des Operation Requests gegen die Liste der gültigen Werte prüfen. Im Falle von ungültigen Werten MUSS der VZD mit LDAP Result Code constraintViolation (19) antworten und darf die Operation nicht ausführen.**[<=]**

4.3.2.5 Umsetzung REST

Am Ende vom Kapitel wird eingefügt:

A_23730 - VZD, I_Directory_Application_Maintenance, Anwendungskennzeichen Prüfung REST

Der VZD MUSS bei Änderungen an KOM-LE-Fachdaten mit den Operationen „add_Directory_FA-Attributes" und "modify_Directory_FA-Attributes" den Inhalt von Parameter Anwendungskennzeichen (appTags) des Operation Requests gegen die Liste der gültigen Werte prüfen. Im Falle von ungültigen Werten MUSS der VZD mit HTTP-Statuscode 400 (attributeName="appTags" , attributeError="erläuternder Fehlertext") antworten und darf die Operation nicht ausführen.**[<=]**

A_23819 - VZD, I_Directory_Application_Maintenance, Behandlung komLeData & kimData REST

Der VZD MUSS bei Änderungen an KOM-LE-Fachdaten mit den Operationen „add_Directory_FA-Attributes" und "modify_Directory_FA-Attributes" den Inhalt von Parameter komLeData wie folgendermassen in die LDAP Datenstruktur eintragen:

- komLeData.mail der REST Operation wird in die LDAP Attribute komLeData.mail und kimData.mail eingetragen.
- komLeData.version der REST Operation wird in die LDAP Attribute komLeData.version und kimData.version eingetragen.
- komLeData.appTags der REST Operation wird in die LDAP Attribut kimData.appTags eingetragen.

Dabei MUSS die Reihenfolge der Attribute im LDAP String gewährleistet werden:

komLeData: version,mail
kimData: mail,version,appTags

Als Trennzeichen der Attribute MUSS ein Komma ',' verwendet werden.
Wenn Attribut appTags mehrere Werte enthält, MUSS als Trennzeichen eine Pipe '|' verwendet werden.
[<=]

Hinweis: Das LDAP Attribut "komLeData" ist aus Performancegründen nicht für die Suche nach der Mail Adresse geeignet. Falls das LDAP Attribut "mail" nicht für die Suche geeignet ist, muss LDAP Attribut "kimData" genutzt werden.

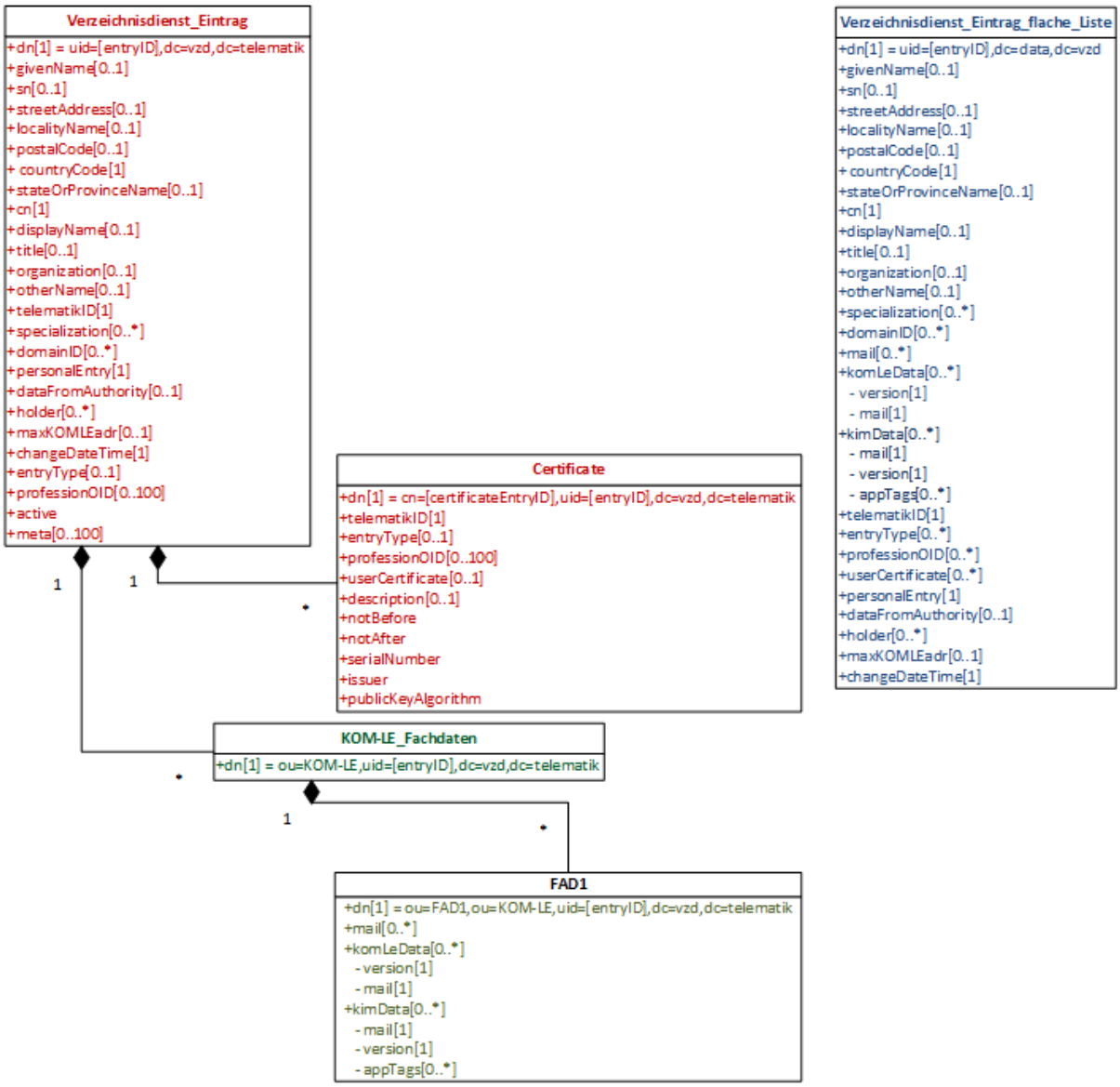
5 Datenmodell

Anforderung TIP1-A_5607 wird aktualisiert:

TIP1-A_5607-10 - VZD, logisches Datenmodell

Der VZD MUSS das logische Datenmodell nach Abb_VZD_logisches_Datenmodell und Tab_VZD_Datenbeschreibung implementieren. Es wird keine Vorgabe an die technische Ausprägung des Datenmodells gemacht.
Der VZD MUSS sicherstellen, dass ein Eintrag nur Zertifikate aus dem Vertrauensraum der TI mit gleicher Telematik-ID enthält.

1283



1284

1285 **Abbildung 1: Abb_VZD_logisches_Datenmodell**

1286 **Tabelle 15: Tab_VZD_Datenbeschreibung**

LDAP-Directory Attribut	Pflichtfeld?	Erläuterung
givenName	optional	HBA-Eintrag: Bezeichner: Vorname, Wird vom VZD aus dem Zertifikatsattribut givenName übernommen, wenn der Client von Schnittstelle I_Directory_Administration keinen Wert angibt. Wird über die Schreiboperationen von Schnittstelle I_Directory_Administration für givenName ein Inhalt geliefert, so wird dieser Wert für das Attribut gesetzt. Wird dem Verzeichniseintrag ein neues Zertifikat hinzu gefügt, wird der aktuelle Wert des Attributs durch der Wert aus Zertifikatsattribut givenName überschrieben.

		SMC-B-Eintrag: wird nicht verwendet

sn	optional	Wird von E-Mail-Clients für die Suche nach Einträgen und die Anzeige von gefundenen Einträgen verwendet.
		
		HBA-Eintrag: Bezeichner: Nachname
		Verhalten der Befüllung des Attributs bei Nutzung der Operationen
		
		• add_Directory_Entry:
		  • Wird sn als Parameter übergeben, wird der angegebene Wert übernommen.
		  • Wird sn nicht als Parameter übergeben, wird sn als Kopie von Parameter displayName gesetzt.
		  • Wird sn und displayName nicht als Parameter übergeben und ein Zertifikat übergeben, wird sn mit dem Inhalt von Attribut surName aus dem Zertifikat gefüllt.
		• modify_Directory_Entry:
		  • Wird sn als Parameter übergeben, wird der angegebene Wert übernommen.
		  • Wird sn nicht als Parameter übergeben, wird sn als Kopie von Parameter displayName gesetzt.
		• add_Directory_Entry_Certificate
		  • Bei dem Hinzufügen eines Zertifikats wird sn mit dem Inhalt von Attribut surName aus dem Zertifikat gefüllt/überschrieben.
		SMC-B Eintrag:
		Verhalten der Befüllung des Attributs bei Nutzung der Operationen
		• add_Directory_Entry:
		  • Wird sn als Parameter übergeben, wird der angegebene Wert übernommen.
		  • Wird sn nicht als Parameter übergeben, wird sn als Kopie von Parameter displayName gesetzt.
		  • Wird sn und displayName nicht als Parameter übergeben, wird sn auf einen leeren Wert gesetzt ("-" im LDAP-View).
		• modify_Directory_Entry:
		  • Wird sn als Parameter übergeben, wird der angegebene Wert übernommen.
		  • Wird sn nicht als Parameter übergeben, wird sn gelöscht ("-" im LDAP-View).
		• add_Directory_Entry_Certificate
		  • Hat keine Auswirkungen auf das sn Attribut.

cn	obligatorisch	Wird von E-Mail Clients für die Suche nach Einträgen und die Anzeige von gefundenen Einträgen verwendet HBA: Eintrag: Bezeichner: Nachname, Vorname SMC-B Eintrag: Bezeichner: Name Unabhängig vom Kartentyp wird bei Nutzung der Schreiboperationen von Schnittstelle I_Directory_Administration cn als Kopie von Attribut displayName gesetzt, wenn cn nicht als Parameter übergeben wird. Wird cn als Parameter übergeben, wird der angegebene Wert übernommen.
displayName	optional	Bezeichner: Anzeigename, Name, nach dem der Eintrag von Nutzern gesucht wird, und unter dem gefundene Einträge angezeigt werden. HBA: Konvention für HBA Einträge: Name, Vorname Dieses Attribut wird genutzt, um den Namen der Person gegenüber dem Anwender darzustellen (Verwendung als Filter-Attribut, um die Suche einzuschränken, und bei der Darstellung des Ergebnisses). SMC-B: Dieses Attribut wird genutzt, um den Namen der Betriebsstätte gegenüber dem Anwender darzustellen (Verwendung als Filter-Attribut, um die Suche einzuschränken, und bei der Darstellung des Ergebnisses). Unabhängig vom Kartentyp: Dieses Attribut wird durch den VZD nicht automatisch aus dem Zertifikat ermittelt. Es kann über die Schreiboperationen von Schnittstelle I_Directory_Administration gesetzt werden. Wird über die Operation add_Directory_Entry von Schnittstelle I_Directory_Administration für displayName kein Inhalt geliefert, so wird in displayName der Wert "-" gesetzt.
streetAddress	optional	Bezeichner: Straße und Hausnummer Alias: street (wird vom VZD in der Response zu einer LDAP Query verwendet)
postalCode	optional	Bezeichner: Postleitzahl
countryCode	obligatorisch	Kann beim Anlegen des Datensatzes und beim Ändern gesetzt werden (falls nicht gesetzt, ergänzt der VZD den Defaultwert für Deutschland).
localityName	optional	Bezeichner: Ort Alias: l (wird vom VZD in der Response zu einer LDAP Query verwendet)
stateOrProvinceName	optional	Bezeichner: Bundesland oder Region Alias: st (wird vom VZD in der Response zu einer LDAP Query verwendet)

title	optional	HBA: Bezeichner: Titel SMC-B: nicht verwendet
organization	optional	HBA: Bezeichner: Name der Organisation oder Name der Betriebsstätte SMC-B: Alternativer Name, nach dem der Eintrag von Nutzern gesucht wird, und unter dem gefundene Einträge angezeigt werden
otherName	optional	Bezeichner: Anderer Name Veraltet: Wird für die Suche nach Einträgen und die Anzeige von gefundenen Einträgen nicht benötigt (siehe displayName und organization)
specialization	optional	Bezeichner: Fachgebiet Kann mehrfach vorkommen (1..100). **Für Einträge der Leistungserbringerorganisationen (SMC-B Eintrag)** Der Wertebereich entspricht den in hl7 definierten und für ePA festgelegten Werten (https://wiki.hl7.de/index.php?title=IG:Value_Sets_f%C3%BCr_XDS#DocumentEntry.practiceSettingCode). urn:psc:<OID Codesystem:Code> Beispiel für Allgemeinmedizin: urn:psc:1.3.6.1.4.1.19376.3.276.1.5.4:ALLG Beispiel für Zahnmedizin: urn:psc:1.3.6.1.4.1.19376.3.276.1.5.4:MKZH Beispiel für Apotheke: urn:psc:1.3.6.1.4.1.19376.3.276.1.5.5:PHZ Beispiel für Krankenhaus: urn:psc:1.3.6.1.4.1.19376.3.276.1.5.4:GESU **Für Einträge der Leistungserbringer (HBA-Eintrag)** Der Wertebereich entspricht den in hl7 definierten Werten (https://wiki.hl7.de/index.php?title=IG:Value_Sets_f%C3%BCr_XDS#DocumentEntry.authorSpecialty). urn:as:<OID Codesystem:Code> Psychologischer Psychotherapeut: urn:as:1.3.6.1.4.1.19376.3.276.1.5.11:82 Psychotherapeut: urn:as:1.3.6.1.4.1.19376.3.276.1.5.11:183 Fachpsychotherapeut für Kinder und Jugendliche: urn:as:1.3.6.1.4.1.19376.3.276.1.5.11:184 Fachpsychotherapeut für Erwachsene: urn:as:1.3.6.1.4.1.19376.3.276.1.5.11:185 Beispiel für FA Allgemeinmedizin: urn:as:1.2.276.0.76.5.514:011001 Beispiel für Zahnarzt: urn:as:1.2.276.0.76.5.492:1
domainID	optional	Bezeichner: domänenspezifisches Kennzeichen des Eintrags. kann mehrfach vorkommen (0..100)
holder	optional	Legt fest, wer Änderungen an den Basisdaten des Eintrags vornehmen darf. Hat keinen Einfluss auf Fachdaten und Zertifikatsdaten.
maxKOMLEadr	optional	Maximale Anzahl von mail Adressen in den KOM-LE-Fachdaten. Falls kein Wert eingetragen wurde, können beliebig viele mail Adressen in den KOM-LE Fachdaten eingetragen werden. Falls ein Wert eingetragen wurde, können maximal so viele mail Adressen in den KOM-LE Fachdaten eingetragen werden.

personalEntry	obligatorisch	Wird vom VZD eingetragen Wert == TRUE, wenn baseDirectoryEntry.entryType 1 hat (Berufsgruppe), Wert == FALSE sonst. Nach Löschung aller Zertifikate bleibt der Wert dieses Attributs `personalEntry` erhalten.
dataFromAuthority	optional	Wird vom VZD eingetragen Wert == TRUE, wenn der Verzeichnisdienst_Eintrag von dem Kartenherausgeber geschrieben wurde, Wert == FALSE sonst
active	obligatorisch	Mit diesem Attribut im Basiseintrag (Verzeichnisdienst_Eintrag in Abb_VZD_logisches_Datenmodell) kann der Client (Kartenherausgeber, TSP) die Aufnahme des VZD-Eintrags in die flache Liste steuern. Wenn das Attribut beim Anlegen eines VZD-Eintrags mit Zertifikat nicht angegeben wird, setzt der VZD das Attribut active auf TRUE (Default-Wert). Bei FALSE wird der Eintrag vom VZD aus der flachen Liste entfernt bzw. nicht übertragen. Dieses Attribut ist nicht in der flachen Liste enthalten. Wenn der VZD beim zeitlichen Ablauf des letzten Zertifikats einen VZD-Eintrag aus der flachen Liste entfernt, bleibt das Attribut active unverändert. Beim erneuten Hinzufügen eines Zertifikats wird der VZD-Eintrag also wieder in die flache Liste übernommen, wenn dieses Attribut den Wert "true" enthält.
meta	optional	Kann von den pflegenden Clients zur Abstimmung der Prozesse zwischen z. B. Kartenherausgeber und TSP genutzt werden. Dieses Attribut wird durch den VZD nicht ausgewertet. Die Werte für dieses Attribut müssen von den pflegenden Organisationen festgelegt und abgestimmt werden. Array von Strings (wird in LDAP auf <String, String> gemappt). Dieses Attribut ist nicht in der flachen Liste enthalten. Kann mehrfach vorkommen (0..100).
userCertificate	optional	Bezeichner: Enc-Zertifikat kann mehrfach vorkommen (0..50) Das Zertifikat wird gelöscht, wenn es ungültig geworden ist. Wenn kein Zertifikat vorliegt, dann kann der Eintrag nicht mittels LDAP-Abfrage gefunden werden. Format: DER, Base64-kodiert
notBefore	obligatorisch	Wird vom VZD bei Eintrag eines Zertifikats aus dem Zertifikat entnommen und ist nicht änderbar. Wird vom VZD zur Ermittlung der zeitlich gültigen Zertifikate genutzt. Dieses Attribut ist nicht in der flachen Liste enthalten.
notAfter	obligatorisch	Wird vom VZD bei Eintrag eines Zertifikats aus dem Zertifikat entnommen und ist nicht änderbar. Wird vom VZD zur Ermittlung der zeitlich gültigen Zertifikate genutzt. Dieses Attribut ist nicht in der flachen Liste enthalten.
serialNumber	obligatorisch	Wird vom VZD bei Eintrag eines Zertifikats aus dem Zertifikat entnommen und ist nicht änderbar. Kann zur Suche nach Zertifikaten genutzt werden. Dieses Attribut ist nicht in der flachen Liste enthalten.

issuer	obligatorisch	Wird vom VZD bei Eintrag eines Zertifikats aus dem Zertifikat entnommen und ist nicht änderbar. Kann zur Suche nach Zertifikaten genutzt werden. Dieses Attribut ist nicht in der flachen Liste enthalten.
publicKeyAlgorithm	obligatorisch	Wird vom VZD bei Eintrag eines Zertifikats aus dem Zertifikat entnommen und ist nicht änderbar. Kann zur Suche nach Zertifikaten genutzt werden. Dieses Attribut ist nicht in der flachen Liste enthalten.
entryType	optional	Bezeichner: Eintragstyp Wird vom VZD anhand der im Zertifikat enthaltenen OID (Extension Admission, Attribut ProfessionOID) und der Spalte Eintragstyp in Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID automatisch eingetragen. Siehe auch [gemSpecOID]# Tab_PKI_402 und Tab_PKI_403. entryType kann über Operationen add_Directory_Entry und modify_Directory_Entry gesetzt werden. Wird in Operation add_Directory_Entry ein Zertifikat angegeben wird, muss ein eventuell angegebener Parameter entryType mit dem Wert aus dem Zertifikat übereinstimmen. Bei nicht angegebenem Parameter entryType wird das Attribut entryType entsprechend dem Zertifikat gesetzt. Mit Operation modify_Directory_Entry kann über Request Parameter entryType das Attribut im VZD geändert werden, solange kein Zertifikat im VZD enthalten ist (welches dann einen abweichenden Wert gegenüber dem Request Parameter entryType enthalten würde). Wenn mit Operation add_Directory_Entry_Certificate ein neues Zertifikat hinzugefügt wird - welches in Bezug auf Attribut entryType vom Basisdatensatz abweicht - dann führt das zum Abbruch der Operation mit einem Fehler.
telematikID	obligatorisch	Bezeichner: TelematikID Wird vom VZD anhand der im jeweiligen Zertifikat enthaltenen Telematik-ID (Feld registrationNumber der Extension Admission) übernommen. Ist in den Basisdaten und in den Zertifikatsdaten enthalten.
professionOID	optional	Bezeichner: Profession OID Wird vom VZD anhand der im Zertifikat enthaltenen OID (Extension Admission, Attribut ProfessionOID) und dem Mapping in Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID automatisch eingetragen. Siehe [gemSpecOID#Tab_PKI_402 und Tab_PKI_403]. kann mehrfach vorkommen (0..100)
usage	optional	Bezeichner: Nutzungskennzeichnung kann pro Zertifikat mehrfach (0..100) vergeben werden Hinweis: wird nicht verwendet.
description	optional	Bezeichner: Beschreibung Dieses Attribut ermöglicht das Zertifikat zu beschreiben, um die Administration des VZD-Eintrags zu vereinfachen. Hinweis: wird aktuell nicht verwendet.

mail	optional	Bezeichner: KOM-LE-Mail-Adresse kann mehrfach vorkommen (0..1000) Wird vom KOM-LE-Fachdienst-Anbieter eingetragen.
komLeData	optional	Bezeichner: komLeData kann mehrfach vorkommen (0..1000) Enthält die KOM-LE-Version des Clientmoduls der angegebenen "mail" Adresse im Attribut "version". Anhand dieser Version erkennt das sendende Clientmodul, welche KOM-LE-Version vom Empfänger-Clientmodul unterstützt wird und in welchem Format die Mail an diesen Empfänger versandt wird. Wenn zu einer KOM-LE-Mail-Adresse aus Attribut Mail kein korrespondierender Eintrag (mit gleicher KOM-LE-Mail-Adresse) im komLeData Attribut enthalten ist, muss KOM-LE-Version 1.0 angenommen werden. Jeder Datensatz - bestehend aus Version und KOM-LE-Mail-Adresse - muss vollständig sein (beide Attribute sind obligatorisch). Zu beachten ist bei der Auswertung bzw. Pflege dieser Daten: • Ein komLeData Eintrag setzt sich zusammen aus der Mail Adresse (Attribut "mail") und der zugehörigen KOM-LE Version (Attribut "version"). • Für jede Mail Adresse aus dem "mail" Attribut darf es nur einen Eintrag in Datenstruktur komLeData geben. Es dürfen in komLeData keine Mail Adressen referenziert werden, die nicht im übergeordneten "mail" Attribut enthalten sind. • Wenn eine Mail Adresse gelöscht wird, muss auch ihr komLeData Eintrag gelöscht werden. Geschrieben wird immer die gesamte Liste. Für Änderungen muss erst der aktuelle Eintrag gelesen werden und nach Änderung in der Liste der gesamte Eintrag wieder geschrieben werden. • Beispiel für den Wert eines komLeData Eintrags in der flachen Liste (Ausgabe einer LDAP Suche): komLeData: 1.0,mc_smcb_za@dom1.komle.telematik-test komLeData: 1.0,mz_smcb_za@dom2.kim.telematik-test komLeData: 1.0,mz_smcb_za@dom1.kim.telematik-test komLeData: 1.0,mb_secu_sm@dom3.kim.telematik-test komLeData: 1.0,mb_secu_sm@dom4.kim.telematik-test komLeData: 1.5,ak_secu_102@dom5.kim.telematik-test
kimData	optional	Bezeichner: kimData kann mehrfach vorkommen (0..1000) Enthält die KOM-LE-Version des Clientmoduls der angegebenen "mail" Adresse im Attribut "version". Zusätzlich kann zur KOM-LE-Version ein "+" angegeben sein. Anhand dieser Version erkennt das sendende Clientmodul, welche KOM-LE-Version vom Empfänger-Clientmodul unterstützt wird und in welchem Format die Mail an diesen Empfänger versandt wird. Wenn ein zusätzliches "+" angegeben ist, dann können mit dieser "mail" Adresse Nachrichten größer 15MiB verarbeitet werden. Jeder Datensatz MUSS die Attribute KOM-LE-Mail-Adresse und Version enthalten (beide Attribute sind obligatorisch). Wenn noch keine Version zu einer KOM-LE-Mail-Adresse angegeben wurde, dann wird vom VZD die Version 1.0 eingetragen.

		Jeder Datensatz kann zusätzlich ein oder mehrere Anwendungskennzeichen der angegebenen "mail" Adresse im Attribut "appTags" enthalten. Anhand dieser Anwendungskennzeichen erkennt das sendende Clientmodul, welche KIM Anwendungen vom Empfänger verarbeitet werden können. Das Attribut Anwendungskennzeichen (appTags) ist optional. Wenn zu einer KOM-LE-Mail-Adresse kein Anwendungskennzeichen enthalten ist, können alle KIM Anwendungen an diesen Empfänger versendet werden. Die Bestandteile KOM-LE-Mail-Adresse, KOM-LE-Version und Anwendungskennzeichen sind jeweils durch das Zeichen "," getrennt. Wenn mehrere Anwendungskennzeichen angegeben sind, dann sind diese durch das Zeichen "|" getrennt. Zu beachten ist bei der Auswertung bzw. Pflege dieser Daten: • Ein kimData Eintrag setzt sich zusammen aus der Mail Adresse (Attribut "mail"), der zugehörigen KOM-LE Version (Attribut "version") inklusive dem optionalen "+" und optional einem oder mehreren Anwendungskennzeichen (Attribut "appTags"). • Bei Angabe von mehreren Anwendungskennzeichen werden sie im LDAP Attribut durch das '|' Zeichen getrennt (siehe Beispiel unten). • Für jede Mail Adresse darf es nur einen Eintrag in der Datenstruktur kimData geben. • Wenn eine Mail Adresse gelöscht wird, muss auch ihr kimData Eintrag gelöscht werden. Geschrieben wird immer der gesamte kimData Eintrag inklusive aller enthaltenen Attribute mit ihren Werten (für alle Mail Adressen) . Für Änderungen muss erst der aktuelle Eintrag gelesen werden und nach Änderung der gesamte Eintrag wieder geschrieben werden. • Beispiel für den Wert eines kimData Eintrags in der flachen Liste (Ausgabe einer LDAP Suche): kimData: mc_smcb_za@dom1.komle.telematik-test,1.0,eEB;V1.0 kimData: mz_smcb_za@dom2.kim.telematik-test,1.0,DALE-UV;Einsendung;V1.0|eEB;V1.0 kimData: mz_smcb_za@dom1.kim.telematik-test,1.0 kimData: mb_secu_sm@dom3.kim.telematik-test,1.0 kimData: mb_secu_sm@dom4.kim.telematik-test,1.0 kimData: ak_secu_102@dom5.kim.telematik-test,1.5
changeDateTime	obligatorisch	Der VZD setzt dieses Attribut bei jeder Schreiboperation für den Datensatz (Basisdaten und Zertifikate) auf die aktuelle Zeit. Format entsprechend RFC 3339, section 5.6.

[<=]

1.8 Änderungen in DirectoryApplicationMaintenance.yaml

Anwendungskennzeichen in Attribut komLeData aufgenommen:

https://github.com/gematik/api-vzd/blob/feature/AWK_Yaml/src/openapi/DirectoryApplicationMaintenance.yaml

1.9 Änderungen in DirectoryAdministration.yaml

Anwendungskennzeichen in Attribut komLeData aufgenommen:

https://github.com/gematik/api-vzd/blob/feature/AWK_Yaml/src/openapi/DirectoryAdministration.yaml

1.10 Änderungen in Steckbriefen

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_...]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Änderungen in gemProdT_CM_KOMLE und gemProdT_Basis-Consumer

Tabelle 16 Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_20650-06	Übermittlung von Fehlernachrichten	gemSpec_CM
A_21387-03	Prüfung der verwendeten Clientmodul-Version beim Senden	gemSpec_CM
A_22416-01	Anfragen von technischen Konfigurationsdaten	gemSpec_CM
A_22417-01	Einfügen des Ablaufdatums in den äußeren Mail-Header	gemSpec_CM
A_23541	Servicelokalisierung durch das Clientmodul	gemSpec_CM
~~A_21389~~	~~Übermittlung der Clientmodul- und Produkttypversion an die gematik~~	gemSpec_CM
A_23737	Clientmodul - Übermittlung von zusätzlichen Header-Informationen	gemSpec_CM
A_19356-07	Prüfen der Version des Empfängers	gemSpec_CM

A_22340-01	Cachen vom KOM-LE-Versionen	gemSpec_CM
A_23467	Übermittlung der KAS-Datenmenge	gemSpec_CM
~~A_19362~~	~~Client-Authentifizierung~~	gemSpec_CM
A_19362-01	Client Authentifizierung für Upload am KAS	gemSpec_CM
~~A_19368~~	~~Client-Authentifizierung~~	gemSpec_CM
A_19368-01	Client Authentifizierung für Download am KAS	gemSpec_CM
A_23471	Löschen von E-Mail-Daten vom KAS bei Fehler	gemSpec_CM
A_19359-08	Einbetten von Informationen großer Nachrichten	gemSpec_CM
A_19370-05	Download von E-Mail-Daten	gemSpec_CM
KOM-LE-A_2176-01	Prüfen auf gültiges ENC-Zertifikat für den Empfänger im RCPT-Kommando	gemSpec_CM
A_23554	Weiterleitung MAIL FROM - SIZE-Parameter	gemSpec_CM
KOM-LE-A_2179-02	Vermerk in der Nachricht bei erfolgreicher Entschlüsselung	gemSpec_CM
A_23713	Clientmodul, Pflege der Anwendungskennzeichen	gemSpec_CM
A_23711	Clientmodul, gültige Anwendungskennzeichen	gemSpec_CM
A_19457-03	Client Authentisierung Administrationsmodul	gemSpec_CM
A_19464-04	Deregistrierungsdialog KOM-LE-Teilnehmer Administrationsmodul	gemSpec_CM
A_19468-03	Beantragen und Herunterladen der PKCS#12 Datei	gemSpec_CM
~~A_21382~~	~~Generierung eines symmetrischen Schlüssels für die PKCS#12-Datei~~	gemSpec_CM
~~A_18783~~	~~Import Schlüssel und Zertifikat als PKCS#12 Datei~~	gemSpec_CM
KOM-LE-A_2061-01	Speichern von Zuordnungen im Cache beim Entschlüsseln	gemSpec_CM
A_22348-01	Caching der Prüfergebnisse der TLS-Server-Zertifikate	gemSpec_CM

KOM-LE-A_2079-01	Protokolldateien für Ablauf und Fehler	gemSpec_CM
~~KOM-LE-A_2084~~	~~Aktivierung und Deaktivierung der Protokollierung von Performanceinformationen~~	gemSpec_CM
~~KOM-LE-A_2088~~	~~Felder zur Protokollierung der Performance~~	gemSpec_CM
~~KOM-LE-A_2089~~	~~Aktionen zur Protokollierung der Performance~~	gemSpec_CM
~~GS-A_5136~~	~~Performance – KOM-LE-Clientmodul – Bearbeitungszeit unter Last~~	gemSpec_Perf

Tabelle 17 Anforderungen zur organ/betriebl. Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_20189-02~~	~~Übermittlung der benötigten KOM-LE Version des Clientmoduls~~	gemSpec_CM

Tabelle 18 Anforderungen zur Sich.techn. Eignung: Herstellererklärung

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
KOM-LE-A_2299-02	Übermittlung der benötigten KOM-LE Version des Clientmoduls	gemSpec_CM

Tabelle 19 Anforderungen zur funkt. Eignung: Herstellererklärung

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
KOM-LE-A_2026-01	Cachen von Verschlüsselungszertifikaten	gemSpec_CM
A_22348-01	Caching der Prüfergebnisse der TLS-Server-Zertifikate	gemSpec_CM
KOM-LE-A_2184-01	Standardwerte der Konfigurationsparameter	gemSpec_CM

Änderungen in gemProdT_FD_KOMLE

1316 **Tabelle 20 Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender**
1317 **Test"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_19591-01	Eintrag Clientmodul-Version in VZD, Account Manager	gemSpec_FD
A_21376-01	Eintrag der KOM-LE-Fachdaten in den VZD	gemSpec_FD
A_23718	Account Manager, Eintragung von Anwendungskennzeichen in den VZD	gemSpec_FD
A_23722	Account Manager, regelmäßige Aktualisierung der Liste der Anwendungskennzeichen	gemSpec_FD
A_19524-02	Verwaltung Resource Records Typs für Service Discovery, KIM	gemSpec_FD
KOM-LE-A_2139-03	Konfiguration Fachdienst	gemSpec_FD
A_19375-05	KAS – Implementierung der Schnittstelle	gemSpec_FD
A_21386-01	KAS - HTTP-Basic-Authentifizierung	gemSpec_FD
A_19378-02	KAS - prüfen der Größe der verschlüsselten E-Mail-Daten	gemSpec_FD
A_20063-04	Account Manager - Implementierung der Schnittstelle	gemSpec_FD
A_23732	Account Manager - Aktionen bei Deregistrierung	gemSpec_FD
A_23733	Account Manager - Aktionen bei Rücknahme einer Deregistrierung	gemSpec_FD
KOM-LE-A_2167-05	Sperrung des Accounts	gemSpec_FD
A_19542-02	Schnittstelle für den Download	gemSpec_FD
KOM-LE-A_2187-05	Authentifizierung des KOM-LE-Teilnehmers über AUT-Zertifikat am AccountManager	gemSpec_FD
A_22420-01	I_AccountLimit_Services – TLS-gesicherte Verbindung	gemSpec_FD
A_23753	Implementierung der Schnittstelle I_ServiceInformation	gemSpec_FD

A_23754	I_ServiceInformation – TLS-gesicherte Verbindung	gemSpec_FD
KOM-LE-A_2231-01	Schnittstellen der TI-Plattform	gemSpec_FD
A_23746	KIM Fachdienst, Betriebsdatenerfassung Senderichtung	gemSpec_FD
A_23748	KIM Fachdienst, Betriebsdatenerfassung Empfangsrichtung	gemSpec_FD
~~A_17671~~	~~Performance - Rohdaten-Performance-Berichte - Format des Performance-Berichts~~	gemSpec_Perf
~~A_17678~~	~~Performance - Rohdaten-Performance-Berichte - Übermittlung~~	gemSpec_Perf
~~A_17679~~	~~Performance - Rohdaten-Performance-Berichte - Berichtsintervall~~	gemSpec_Perf
~~A_17755~~	~~Performance - Rohdaten-Performance-Berichte - Name der Berichte~~	gemSpec_Perf
~~A_17756~~	~~Performance - Rohdaten-Performance-Berichte - Korrektheit~~	gemSpec_Perf
~~A_17757-01~~	~~Performance - Rohdaten-Performance-Lieferung - zu liefernde Dateien~~	gemSpec_Perf
~~A_17758~~	~~Performance - Rohdaten-Performance-Berichte - Frist für Nachlieferung~~	gemSpec_Perf
~~A_20136~~	~~Performance - Erfassung von Rohdaten - KOM-LE-Fachdienst~~	gemSpec_Perf
A_22482	Performance - Rohdaten - Erfassung von Rohdaten (Rohdatenerfassung v.02)	gemSpec_Perf
A_22002	Performance - Rohdaten - Übermittlung (Rohdatenerfassung v.02)	gemSpec_Perf
A_22000	Performance - Rohdaten - zu liefernde Dateien (Rohdatenerfassung v.02)	gemSpec_Perf
A_22429	Performance - Rohdaten - Inhalt der Selbstauskunft (Rohdatenerfassung v.02)	gemSpec_Perf
A_22004	Performance - Rohdaten - Korrektheit (Rohdatenerfassung v.02)	gemSpec_Perf

A_21975	Performance - Rohdaten - Default-Werte für Lieferintervalle (Rohdatenerfassung v.02)	gemSpec_Perf
A_21980	Performance - Rohdaten - Leerlieferung (Rohdatenerfassung v.02)	gemSpec_Perf
A_22001-01	Performance - Rohdaten - Name der Berichte (Rohdatenerfassung v.02)	gemSpec_Perf
A_21981-02	Performance - Rohdaten - Format des Rohdaten-Performance-Berichtes (Rohdatenerfassung v.02)	gemSpec_Perf
A_22500-01	Performance - Rohdaten - Status-Block (Rohdatenerfassung v.02)	gemSpec_Perf
A_21982-01	Performance - Rohdaten - Message-Block (Rohdatenerfassung v.02)	gemSpec_Perf
A_22513-01	Performance - Rohdaten - Message-Block im Fehlerfall (Rohdatenerfassung v.02)	gemSpec_Perf
A_23170	Performance - Rohdaten - Spezifika KIM-FD Format (Rohdatenerfassung v.02)	gemSpec_Perf
A_23168	Performance - Rohdaten - Spezifika KIM-FD - Operation (Rohdatenerfassung v.02)	gemSpec_Perf
A_23167	Performance - Rohdaten - Spezifika KIM message-Block (Rohdatenerfassung v.02)	gemSpec_Perf
GS-A_5138-02	Performance – KOM-LE-Fachdienst – TLS-Verbindungsaufbau unter Last	gemSpec_Perf
A_20127-01	Performance - KOM-LE-Fachdienst – Spitzenlastvorgaben für den KAS	gemSpec_Perf
~~A_20130~~	~~Performance - KOM-LE-Fachdienst - TLS Kanal KAS~~	gemSpec_Perf
A_21459	FAD, VZD, TUC_VZD_0012 "add_Directory_FA-Attributes (REST)"	gemSpec_VZD
A_21461	FAD, TUC_VZD_0013 "delete_Directory_FA-Attributes (REST)"	gemSpec_VZD
A_21463	FAD, TUC_VZD_0014 "modify_Directory_FA-Attributes (REST)"	gemSpec_VZD

A_23823	Performance - Rohdaten - Spezifika Fachdienst KOM-LE Status (Rohdatenerfassung v.02)	gemSpec_Perf

Tabelle 21 Festlegungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_19385-03	KAS – Löschen von Ressource	gemSpec_FD
A_22005	Performance - Rohdaten - Frist für Nachlieferung (Rohdatenerfassung v.02)	gemSpec_Perf
A_21976	Performance - Rohdaten - Konfigurierbarkeit der Lieferintervalle (Rohdatenerfassung v.02)	gemSpec_Perf
A_22047	Performance - Rohdaten - Änderung der Konfiguration der Lieferintervalle (Rohdatenerfassung v.02)	gemSpec_Perf
A_21978	Performance - Rohdaten - Trennung der Lieferintervalle (Rohdatenerfassung v.02)	gemSpec_Perf
A_21979	Performance - Rohdaten - Bezug der Lieferverpflichtung (Rohdatenerfassung v.02)	gemSpec_Perf

Tabelle 22 *Anforderungen zur organ/betriebl. Eignung "Anbietererklärung"*

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_20189-02	Übermittlung der benötigten KOM-LE Version des Clientmoduls	gemSpec_FD
A_21389	Übermittlung der Clientmodul- und Produkttypversion an die gematik	gemSpec_FD

Änderungen in gemAnbT_FD_KOMLE

Tabelle 23 Anforderungen zur Sich.techn. Eignung: Gutachten (Anbieter)

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_18784-04	Bereitstellung Schlüssel und Zertifikat für Clientmodul als passwortgeschützte PKCS#12 Datei	gemSpec_FD

Tabelle 24 Festlegungen zur betrieblichen Eignung "Prozessprüfung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_22057	Performance - Rohdaten - Verpflichtung des Anbieters (Rohdatenerfassung v.02)	gemSpec_Perf

Tabelle 25 Festlegungen zur betrieblichen Eignung "Anbietererklärung"

ID	Afo-Bezeichnung	Quelle (Referenz)
A_20127-01	Performance - KOM-LE-Fachdienst – Spitzenlastvorgaben für den KAS	gemSpec_Perf
~~A_20130~~	~~Performance - KOM-LE-Fachdienst - TLS Kanal KAS~~	gemSpec_Perf
A_22003-01	Performance - Rohdaten - Nachlieferung auf Anforderung (Rohdatenerfassung v.02)	gemSpec_Perf
A_22620	Rohdaten - Umsetzungszeit für Änderung der Lieferintervalle	gemSpec_Perf

Änderungen in gemProdT_VZD

Tabelle 26 Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23728	VZD, I_Directory_Application_Maintenance, Aktualisierung zulässiger Anwendungskennzeichen	gemSpec_VZD
A_23729	VZD, I_Directory_Application_Maintenance, Anwendungskennzeichen Prüfung LDAP	gemSpec_VZD
A_23730	VZD, I_Directory_Application_Maintenance, Anwendungskennzeichen Prüfung REST	gemSpec_VZD
A_23819	VZD, I_Directory_Application_Maintenance, Behandlung komLeData & kimData REST	gemSpec_VZD
TIP1-A_5607-10	VZD, logisches Datenmodell	gemSpec_VZD

1334

1335