Themengebiet:

Notwendiges Hotfix für KIM 1.5.2-1 und R3.1.3-12

Änderungen:

- Änderung bei der Integritätsprüfung und der Wegfall vom Vermerk bei einer fehlgeschlagenen Signaturprüfung
- Prüfung auf korrekte Befüllung der Mail Header FROM und RCPT vor dem versenden einer KOM-LE-Nachricht
- Ändern des Ablaufs zum Versand von großen E-Mails
- Korrektur des Architekturbildes für KIM 1.5
- Aufnahme eines Hinweises für die Verwendung des Initialisierungsvektors bei der Erzeugung des symmetrischen Schlüssels
- Korrektur bei der Deregistrierung von Nutzer-Accounts
- Aufnahme von herstellerspezifischen Fehlercodes bei der Entschlüsselung einer KOM-LE-Nachricht

Inhaltsverzeichnis

1 KIM 1.0 (R3.1.3-12)

1.1 Änderung in gemSpec_CM_KOMLE

2 Systemüberblick

[...]

Die im Clientmodul zu bearbeitenden originalen MIME-Nachrichten von einem Clientsystem~~E-Mail-Nachrichten~~ werden beim Senden entsprechend dem KOM-LE-S/MIME-Profil gemäß [gemSMIME_KOMLE] digital signiert und verschlüsselt und ~~beim~~ im ~~Empfangen~~ empfangenden Clientmodul entschlüsselt und deren Signatur geprüft. Die originale MIME-Nachrichten die von einem Clientsystem an das Clientmodul übergeben wird, wird im KIM-Kontext als Client-Mail bezeichnet. Das KOM-LE-S/MIME-Profil konkretisiert die S/MIME-Spezifikation und stellt sicher, dass die Interoperabilität zwischen den verschiedenen KOM-LE-Komponenten sowie der Schutz von Integrität und Vertraulichkeit für alle personenbezogenen medizinischen Daten gewährleistet werden.

Jede dem KOM-LE-S/MIME-Profil entsprechende Nachricht hat die in Abbildung 3 dargestellte Struktur. Die äußere

Nachricht ist eine entsprechend dem S/MIME-Standard signierte und verschlüsselte E-Mail-Nachricht. Die innere Nachricht ist die vom Clientmodul verarbeitete Client-Mail (signiert und verschlüsselt) die ~~eine im Clientsystem erzeugte E-Mail-Nachricht, die Nutzdaten enthält und als~~ gemäß `message/rfc822` als Anhang in die äußere Nachricht ~~verpackt ist~~ angehangen wird. Die so erzeugte Mail wird im KIM-Kontext als KOM-LE-Nachricht bezeichnet.

3.1 Allgemeine Anforderungen

[...]

KOM-LE-A_2004-01 - Verarbeitung einer Client-Mail bis zu 15 MiB
Das KOM-LE-Clientmodul MUSS eine decodierte MIME-Message (Client-Mail)~~Nachrichten~~ mit einer ~~Netto~~Größe von bis zu ~~25~~ 15 MiB verarbeiten können. ~~Dabei ist zu beachten, dass sich durch die base64-Kodierung der übersendeten Client-MailNachrichtent die empfangene Mailgröße am Clientmodul um den Faktor 1,37 erhöht istin etwzu verarbeitende Bruttogröße um den Faktor 1,37 erhöht.~~

<=

Hinweis:

- *Durch die Limitierung des Konnektors ist die Client-Mail Verarbeitung nur bis zu einer Größe von 15 MiB sinnvoll möglich.*
- *Es ist zu beachten, dass durch die base64-Kodierung der übersendeten Client-Mail die empfangene Mailgröße am Clientmodul durch die Transportkodierung um den Faktor 1,37 erhöht ist.*

A_23171 - Verarbeitung einer Client-Mail größer 15 MiB
Das KOM-LE-Clientmodul MUSS eine Client-Mail von bis zu 15 MiB verarbeiten können. Ist die Client-Mail größer gleich 15 MiB, dann MUSS das KOM-LE-Clientmodul an den Mail-Client den Fehlercode 552 5.3.4 (*Message too big for system*) gemäß [RFC3463] zurückgeben.
[<=]

3.2.4.1.1 Bearbeitung einer ungeschützten Nachricht

[...]

A_23169 - Sicherstellung der Absenderintegrität
Das Clientmodul MUSS sicherstellen, dass nur die vom Clientsystem zuvor im SMTP-Kommando `MAIL FROM` an das Clientmodul übergebene E-Mail-Adresse in der KOM-LE-Nachricht als einzige Adresse (wenn vorhanden inkl. display name) im Mail Header `from` enthalten ist und prüfen ob für diese E-Mail-Adresse mindestens ein ENC-Zertifikat im VZD existiert. Existiert ein `reply-to` Header-Element in der originalen Nachricht so MUSS dieses ebenfalls durch die zuvor geprüfte E-Mail-Adresse aus dem SMTP-Kommando `MAIL FROM` befüllt werden.
[<=]

A_23174 - Sicherstellung der Empfängeradressen
Das Clientmodul MUSS sicherstellen, dass nur die vom Clientsystem an das Clientmodul übergebenen E-Mail-Adressen die zuvor im SMTP-Kommando `RCPT TO` gemäß [KOM-LE-A_2176] geprüft wurden im Mail Header `to`, `cc` und `bcc` in der KOM-LE-Nachricht verbleiben.
[<=]

3.3.1 Übersicht

[...]

Beim Abholen von Nachrichten findet die Kommunikation zwischen dem Clientsystem, dem Clientmodul und dem POP3-Server über POP3 statt. Das Clientmodul fungiert als POP3-Proxy, der das Clientsystem mit dem POP3-Server verbindet, die Entschlüsselung und Signaturprüfung für die abgeholten KOM-LE-Nachrichten durchführt und die entschlüsselten Nachrichten an das Clientsystem liefert. ~~Die Ergebnisse der Signaturprüfung werden dem Nutzer als Vermerk, der in den Inhalt der Nachricht integriert wird sowie als ein detaillierter Bericht in Form einer angehängten PDF-Datei mitgeteilt.~~ Bei einer fehlgeschlagenen Integritätsprüfung wird der Empfänger der KOM-LE-Nachricht mit einer Fehlernachricht informiert. Die Weiterleitung der Client-Mail an das Clientsystem des Empfängers wird in diesem Fall durch das Clientmodul unterbunden.

[...]

Fehler, die bei der Entschlüsselung oder ~~Signaturprüfung~~ Integritätsprüfung einer Nachricht auftreten, werden anders behandelt:

- Kann die Nachricht nicht entschlüsselt werden (z.B. weil der entsprechende HBA nicht zu Verfügung steht), wird durch das Clientmodul eine Fehlernachricht generiert, die die verschlüsselte Nachricht als Anhang enthält. Um die Nachricht nachträglich zu entschlüsseln und ihre Signatur zu prüfen, kann der Nutzer die Nachricht an seine eigene E-Mail-Adresse senden, Maßnahmen treffen damit beim nächsten Abholen der entsprechende Schlüssel gefunden wird und den Abholvorgang wiederholen.
- Wenn die ~~Signaturprüfung~~ Integritätsprüfung der entschlüsselten KOM-LE-Nachricht fehlschlägt (z. B. weil die Integrität der KOM-LE-Nachricht verletzt wurde) wird die entschlüsselte Nachricht ~~dem Clientsystem mit dem entsprechenden Vermerk übergeben~~ verworfen und eine Fehlernachricht an den Sender sowie den Empfänger der KOM-LE-Nachricht gesendet.

3.3.4 PROCESS-Zustand

[...]

Im PROZESS-Zustand nimmt das Clientmodul die Inhalte der vom POP3-Server abgerufenen KOM-LE-Nachricht entgegen, entschlüsselt die Nachricht, prüft deren Integrität~~, fügt einen Vermerk sowie einen PDF-Anhang mit dem Ergebnis der Signaturprüfung in die Nachricht ein~~ und leitet die aufbereitete Client-Mail ~~Nachricht~~ dem Clientsystem weiter. Im Erfolgsfall wird in die aufbereitete Client-Mail ein Vermerk hinzugefügt und das Clientsystem über das erfolgreiche Abholen der Nachricht in Kenntnis gesetzt. Im Fehlerfall wird das Clientsystem mit dem entsprechenden Antwortcode bzw. Fehlernachricht über den Fehler informiert.

3.3.4.2.1 Entschlüsselung

[...]

KOM-LE-A_2047-02 - Fehlertexte bei fehlgeschlagener Entschlüsselung

Das Clientmodul MUSS bei fehlgeschlagener Entschlüsselung entsprechend der jeweiligen Bedingung ~~die~~den in Tabelle Tab_Fehlertext_Entschl definierten Fehlertexte in die `text/plain` MIME-Einheit der multipart/mixed MIME-Fehlernachricht aufnehmen. Zusätzlich MUSS das Clientmodul ein Mail-Header-Attribut `X-KIM-DecryptionResult` mi

t der dazugehörigen ID aus der Tabelle "Tab_Fehlertext_Entschl" Fehlercode befüllen. Treten im Entschlüsselungsprozess Fehler auf, die nicht in der Tabelle "Tab_Fehlertext_Entschl" definierte sind, MUSS das Clientmodul für diese Fehler das Mail-Header-Attribut `X-KIM-DecryptionResult` mit einem herstellerspezifischen Fehlercode befüllen, welcher mit "X" beginnt. **[<=]**

Hinweis: Sollten mehrere negative Ergebnisse bei der Entschlüsselung einer KOM-LE Nachricht hervorgehen KANN das Mail-Header-Attribut `X-KIM-DecryptionResult` mehrmals verwendet werden.

Beispiel:

```
X-KIM-DecryptionResult: 01
X-KIM-DecryptionResult: 02
X-KIM-DecryptionResult: X99
```

3.3.4.2.2 Integritätsprüfung

[...]

~~Das Ergebnis der Signaturprüfung und des Abgleichs des `recipient-emails` Attributs wird als Vermerk, der den Text der Nachricht ergänzt, dem Empfänger mitgeteilt.~~

~~Falls der Zertifikatstatus des Signaturzertifikates nicht geprüft werden kann (z.B. der OCSP-Responder ist unerreichbar), die mathematische Prüfung der Signatur aber erfolgreich durchgeführt wurde, wird ein entsprechender Vermerk in den Body der Nachricht eingetragen.~~

Wenn die Integritätsprüfung der entschlüsselten KOM-LE-Nachricht fehlschlägt, dann wird eine Fehlernachricht gemäß [A_23165] generiert und das `X-KIM-IntegrityCheckResult` Header-Element mit der jeweiligen ID gemäß der Tabelle "Tab_Verm_Sig_Prüf" befüllt.

~~Tabelle Tab_Verm_Sig_Prüf stellt die Vermerke entsprechend den Ergebnissen der Signaturprüfung dar.~~

Tabelle 1: Tab_Verm_Sig_Prüf Vermerke mit Ergebnissen der Signaturprüfung

ID*	Prüfergebnis	Fehlercode	Ergebnis	Vermerk
01	~~VALID~~ true	-	Die Signatur der Nachricht wurde erfolgreich geprüft.	Die Signatur wurde erfolgreich geprüft.
02	~~INVALID~~ false	4115	Die Integrität der Nachricht wurde verletzt.	~~Die Prüfung der Signatur hat ergeben, dass die Nachricht manipuliert wurde.~~
03	~~INVALID~~ false	4253	Die digitale Signatur ist nicht vorhanden.	~~Die Nachricht ist nicht signiert. Die Nachricht ist deshalb eventuell manipuliert worden.~~
04	~~INVALID~~ false	4112	Die digitale Signatur konnte aufgrund des falschen Formats nicht geprüft werden.	~~Die Signatur der Nachricht konnte aufgrund eines falschen Formats nicht geprüft werden. Die Nachricht ist deshalb eventuell manipuliert worden.~~
			Der Zertifizierungspfad des Signaturzertifikats kann nicht	~~Die Signatur der Nachricht wurde geprüft. Die dabei durchgeführte Integritätsprüfung der Nachricht war erfolgreich. Der Status des zur~~

05	~~INVALID~~ false	4206	validiert werden ~~(abgelaufenes Zertifikat, der Zertifizierungspfad konnte nicht aufgebaut werden usw.)~~.	~~Signatur verwendeten Zertifikats konnte nicht vollständig durchgeführt werden, weil nicht alle am Signaturprozess beteiligten Zertifikate validiert werden konnten.~~ -
06	~~INVALID~~ false	[Fehlercode]	Die digitale Signatur konnte aufgrund eines nicht zuordenbaren Fehlercodes des Konnektors nicht geprüft werden.	~~Bei der Prüfung der digitalen Signatur ist ein unerwarteter Fehler aufgetreten.~~ -
07	~~INCONCLUSIVE~~ true	4264	Die digitale Signatur ist mathematisch korrekt, der Zertifikatsstatus des Signaturzertifikats konnte aber nicht geprüft werden.	~~Die Signatur der Nachricht wurde geprüft. Die dabei durchgeführte Integritätsprüfung der Nachricht war erfolgreich. Der Status des zur Signatur verwendeten Zertifikats konnte nicht vollständig geprüft werden, weil zum Prüfungszeitpunkt nicht alle erforderlichen technischen Ressourcen verfügbar waren.~~ Die Signatur wurde erfolgreich geprüft.
08	~~VALID~~ false	-	Die digitale Signatur ist mathematisch korrekt und der Zertifikatsstatus des Signaturzertifikats konnte erfolgreich geprüft werden, aber beim Vergleich der Header-Elemente from, sender, reply-to, to und cc der äußeren Nachricht mit denen der inneren Nachricht wurden Abweichungen festgestellt.	~~Die Signatur der Nachricht wurde geprüft. Die Prüfung hat ergeben, dass die Nachricht nach dem Verschlüsseln manipuliert wurde. Möglicherweise wurde die verschlüsselte Nachricht auch an einen nicht empfangsberechtigten Personenkreis versendet.~~ -
09	~~VALID~~ false	-	Die digitale Signatur ist mathematisch korrekt und der Zertifikatsstatus des Signaturzertifikats konnte erfolgreich geprüft werden, aber das recipient-emails-Attribut aus signerInfos enthält nicht die gleichen Werte wie das recipient-emails-Attribut aus dem enveloped-data CMS-Objekt.	~~Die Signatur der Nachricht wurde geprüft. Die Prüfung 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.~~ -

~~*) Hinweis: Die in der Tabelle enthaltene ID des jeweiligen Prüfvermerks kann gemäß [KOM-LE-A_2050] als ID dem Vermerk hinzugefügt werden und muss in das `X-KIM-IntegrityCheckResult` Header-Element aufgenommen werden, um damit eine spätere automatische Auswertung zu ermöglichen.~~

[...]

KOM-LE-A_2050-05 - Verhalten bei positiver Integritätsprüfung

Das Clientmodul MUSS nach einer ~~validen~~ ~~abhängig vom Ergebnis der~~ ~~Signaturprüfung~~ Integritätsprüfung einer KOM-LE-Nachricht mit positivem Prüfergebnis (true) ~~die~~ den in Tabelle "Tab_Verm_Sig_Prüf" definierten Vermerke~~n~~ an den Nachrichtentext der KOM-LE-Nachricht anfügen. Es ist dabei das Format des TextParts zu beachten (`mediatype text/html` oder `text/plain`) und der Vermerk diesem Format anzupassen. Zusätzlich MUSS das Clientmodul ein

Mail-Header-Attribut `X-KIM-IntegrityCheckResult` mit der dazugehörigen ID~~=01~~ aus der Tabelle "Tab_Verm_Sig_Prüf" ~~Fehlercode~~ befüllen.
[<=]

A_23165 - Verhalten bei fehlgeschlagener Integritätsprüfung

Das Clientmodul MUSS nach einer fehlgeschlagenen Integritätsprüfung den Mail-Body ~~die~~ der entschlüsselten originalen Nachricht ~~KOM-LE-Nachricht~~ mit dem folgenden ~~Text~~ Inhalt als `text/plain` MIME-Einheit ersetzen und an den Empfänger weiterleiten:
"*Beim Empfang dieser KIM-Nachricht wurde eine Sicherheitsverletzung erkannt. Dies kann eine technisches Ursache haben oder auf eine missbräuchliche Nutzung des KIM-Dienstes hinweisen. Zu Ihrem Schutz wurde der Inhalt dieser Nachricht durch diesen Text ausgetauscht. ~~Zusätzlich wurde der Absender der ursprünglichen Nachricht automatisch über diesen Vorfall informiert~~*".

~~Darüber hinaus MUSS das KOM-LE-Clientmodul den Absender über die fehlgeschlagene Integritätsprüfung informieren. Aus dem Inhalt der Fehlernachricht MUSS hervorgehen, dass bei der Integritätsprüfung der gesendeten Nachricht beim Empfänger ein Fehler festgestellt wurde. Die Fehlernachricht ist weder zu signieren noch zu verschlüsseln und entspricht der Delivery Status Notification gemäß [RFC3461-3464].~~

~~In beiden Nachrichten~~ Zusätzlich MUSS das Clientmodul das Mail-Header-Attribut `X-KIM-IntegrityCheckResult` mi t der dazugehörigen ID aus der Tabelle "Tab_Verm_Sig_Prüf" ~~Fehlercode~~ befüllen. Kommt es bei der Integritätsprüfung zu Fehlern, die nicht in der Tabelle "Tab_Verm_Sig_Prüf" definierte sind, MUSS das Clientmodul für diese Fehler das Mail-Header-Attribut `X-KIM-IntegrityCheckResult` mit einem herstellerspezifischen Fehlercode befüllen, welcher mit "X" beginnt.
[<=]

Hinweis: Sollten mehrere negative Ergebnisse aus der Integritätsprüfung hervorgehen KANN das Mail-Header-Attribut X-KIM-IntegrityCheckResult mehrmals verwendet werden.

Beispiel:
```
X-KIM-IntegrityCheckResult: 08
X-KIM-IntegrityCheckResult: X99
```

1.2 Änderung in gemSpec_FD_KOMLE

Keine Anpassung notwendig

1.3 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

Table *1* Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23169	Sicherstellung der Absenderintegrität	gemSpec_CM

A_23174	Sicherstellung der Empfängeradressen	gemSpec_CM
KOM-LE-A_2047-02	Fehlertexte bei fehlgeschlagener Entschlüsselung	gemSpec_CM
~~KOM-LE-A_2050-04~~	~~Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht~~	~~gemSpec_CM~~
KOM-LE-A_2050-05	Verhalten bei positiver Integritätsprüfung	gemSpec_CM
A_23165	Verhalten bei fehlerhafter Integritätsprüfung	gemSpec_CM
~~KOM-LE-A_2004~~	~~Größe einer E-Mail-Nachricht bis zu 25 MB~~	~~gemSpec_CM~~
KOM-LE-A_2004-01	Verarbeitung einer Client-Mail bis zu 15 MiB	gemSpec_CM
A_23171	Client-Mail größer 15 MiB	gemSpec_CM

Änderungen in gemProdT_FD_KOMLE

Table 2 Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
-	-	-

2 KIM 1.5.2-1

2.1 Änderung in gemSpec_CM_KOMLE

2. Systemüberblick

[...]

Die im Clientmodul zu bearbeitenden originalen MIME-Nachrichten von einem Clientsystem, die ~~von~~ kleiner oder gleich ~~25~~ 15 MiB sind, werden beim Senden entsprechend dem KOM-LE-S/MIME-Profil gemäß [gemSMIME_KOMLE] digital signiert und verschlüsselt und ~~beim~~ im ~~Empfangen~~ empfangenden Clientmodul entschlüsselt und deren Signatur geprüft. Die originale MIME-Nachrichten die von einem Clientsystem an das Clientmodul übergeben wird, wird im KIM-Kontext als Client-Mail bezeichnet. Bei ~~E-Mail-Nachrichten~~ Client-Mails größer ~~als 25~~ 15 MiB ~~wird der Anhang aus der E-Mail extrahiert und~~ wird die gesamte Client-Mail auf einem separaten Speicherort (Fachdienst) verschlüsselt abgelegt (E-Mail-Daten). Das KOM-LE-S/MIME-Profil konkretisiert die S/MIME-Spezifikation und stellt sicher, dass die Interoperabilität zwischen den verschiedenen KOM-LE-Komponenten sowie der Schutz von Integrität und Vertraulichkeit für alle personenbezogenen medizinischen Daten gewährleistet werden.

Jede dem KOM-LE-S/MIME-Profil entsprechende Nachricht hat die in Abbildung 3 dargestellte Struktur. Die äußere Nachricht ist eine entsprechend dem S/MIME-Standard signierte und verschlüsselte E-Mail-Nachricht. Die innere Nachricht ist die vom Clientmodul verarbeitete Client-Mail (signiert und verschlüsselt) die ~~eine im Clientsystem erzeugte E-Mail-Nachricht, die Nutzdaten enthält und als~~ gemäß `message/rfc822` als Anhang in die äußere Nachricht ~~verpackt ist~~ angehangen wird. Die so erzeugte Mail wird im KIM-Kontext als KOM-LE-Nachricht bezeichnet.

[...]

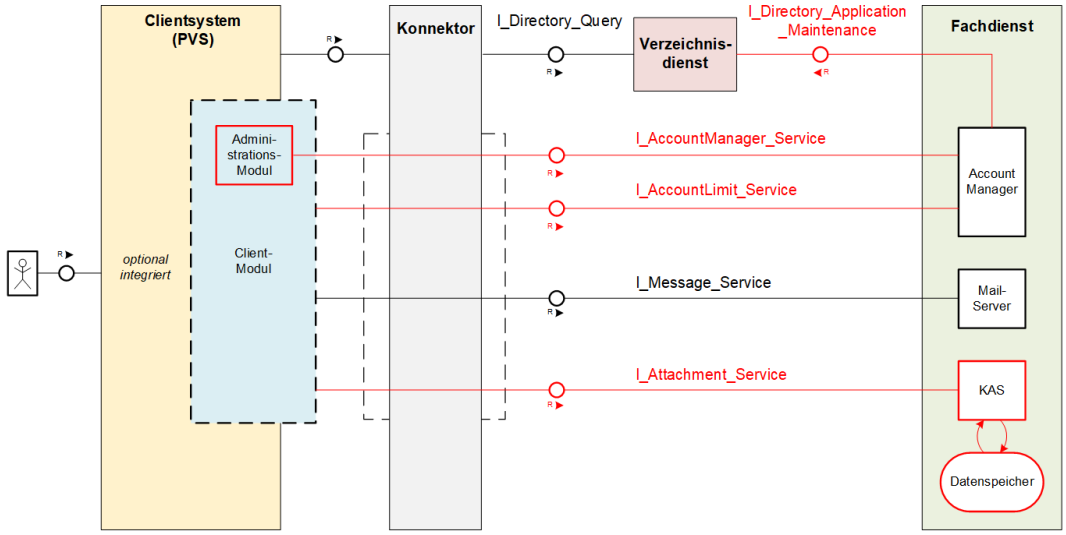

Abbildung 1: Administrationsmodul für die Kommunikation mit dem Account Manager

3.1 Allgemeine Anforderungen

[...]

KOM-LE-A_2004-01 - Verarbeitung einer Client-Mail bis zu 15 MiB

Das KOM-LE-Clientmodul MUSS eine decodierte MIME-Message (Client-Mail)~~Nachrichten~~ mit einer ~~Netto~~Größe von bis zu ~~25~~ 15 MiB verarbeiten können. ~~Dabei ist zu beachten, dass sich durch die base64-Kodierung der übersendeten Client-MailNachrichtent die empfangene Mailgröße am Clientmodul um den Faktor 1,37 erhöht ist in etwzu verarbeitende Bruttogröße um den Faktor 1,37 erhöht.~~

[<=]

Hinweis:

- *Durch die Limitierung des Konnektors ist die Client-Mail Verarbeitung nur bis zu einer Größe von 15 MiB sinnvoll möglich.*
- *Es ist zu beachten dass durch die base64-Kodierung der übersendeten Client-Mail die empfangene Mailgröße am Clientmodul durch die Transportkodierung um den Faktor 1,37 erhöht ist.*
- *Wenn der Empfänger ein Clientmodul ab Version 1.5 nutzt, können mit der in Kap. 3.2 beschriebenen Vorgehensweise auch große Client-Mails über 15 MiB versendet werden.*

A_19366-02 - Größe einer E-Mail-Nachricht größer 25 MB

~~Das KOM-LE-Clientmodul MUSS Nachrichten (ohne oder nach dem entfernen aller Anhänge), die eine Nettogröße von bis zu 25 MB haben, verarbeiten können.~~
~~Ist der E-Mail-Body (ohne Anhänge) größer als 25 MB (netto), dann MUSS das KOM-LE-Clientmodul an den Mail-Client den Fehlercode X.3.4 (*Message too big for system*) gemäß [RFC3463] zurückgeben.~~

<=

~~Durch die Limitierung des Konnektors sind E-Mail-Nachrichten bis zu einer Größe von 25 MB möglich. Wenn der Empfänger einen KOM-LE-Client ab Version 1.5 nutzt, können mit der in Kap. 3.2 beschriebenen Vorgehensweise auch große Mails mit Anhängen von über 25 MB versendet werden. Die Nachricht darf, nach Extraktion der Anhänge, weiterhin die Größe von 25 MB nicht übersteigen und muss durch das KOM-LE-Clientmodul und den KOM-LE-~~

~~Fachdienst verarbeitet werden.~~

[...]

A_20650-05 - 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-Clientmodul

Fehler	Wert
Fehlermeldungen beim Senden einer ~~KIM-Nachricht~~ KOM-LE-Nachricht	
Empfänger entfernt, wegen falscher KIM-Version	`4001`
~~Anhang~~ 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 ~~KIM-Nachricht~~ KOM-LE-Nachricht	
~~Anhang~~ Verschlüsselte E-Mail-Daten konnten nicht vom KOM-LE-Attachment-Service geladen werden	`4006`
Beim Entschlüsseln ~~eines Anhangs~~ der E-Mail-Daten ist ein Fehler aufgetreten	`4007`
Das verwendete Clientmodul unterstützt die in der Mail verwendete Version nicht	`4008`
Die ~~KIM~~ ~~KOM-LE~~ Nachricht konnte auf Grund eines nicht verfügbaren Schlüssels nicht entschlüsselt werden	`4009`
Die ~~KIM~~ ~~KOM-LE~~ Nachricht konnte aufgrund des falschen Formats nicht entschlüsselt werden	`4010`
Der Konnektor steht für die Entschlüsselung nicht zur Verfügung	`4011`
Die Prüfsumme ~~des Anhangs~~ der E-Mail-Daten stimmt nicht mit der ~~dem Anhang~~ beig efügten Prüfsumme überein. ~~Der~~ Die empfangene ~~Anhang~~ aufbereitete Client-Mail ent spricht eventuell nicht ~~dem~~ der ~~originalen Anhang~~ vom Sender auf dem KAS hinterlegten aufbereiteten Client-Mail.	`4012`
~~Anhang~~ 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	`4014`

empfangsberechtigten Personenkreis versendet.	
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
~~Übernahme der Fehlercodes und Vermerke aus der Tabelle~~ Tab_Verm_Sig_Prüf	~~[Fehlercode]~~

Hinweis: Sollten mehrere negative Ergebnisse auftreten KANN das Mail-Header-Attribut X-KIM-Fehlermeldung mehrmals verwendet werden.

Beispiel:
```
X-KIM-Fehlermeldung: 4001
X-KIM-Fehlermeldung: 4004
X-KIM-Fehlermeldung: X99
```

[...]

Die Anforderung A_22412-01 wird in das Kapitel 3.2.2 Empfang von Nachrichten mit großen Anhängen verschoben

A_22412-01 - Behandlung von Zugriffs-Limitierung

Das Clientmodul MUSS bei Aufruf der Operation read_Attachment bei der Rückgabe des HTTP-Fehlercodes 429, das Mail-Header-Attribut `X-KIM-Fehlermeldung` mit dem Wert gemäß Tabelle „Tab_Fehlercodes_KOMLE-Clientmodule“ ~~4017~~ 4013 in die empfangene KOM-LE-Nachricht befüllen ~~und an der Position des Anhangs ein MIME-Element mit `Content-Type: text/plain; charset=utf-8` und `Content-Disposition: attachment; filename=<Original-Filename>_Fehlermeldung.txt` sowie folgende Informationen als Inhalt des Anhangs einfügen: Der Anhang { "`name`": "Dateiname des Anhangs", "`size`": Größe des Anhangs in Byte, "`type`": "MIME-Type des Anhangs" } konnte nicht abgerufen werden. Als Betreff ist Folgendes zu verwenden: `Subject:[Fehler beim Abruf eines Anhangs *_Fehlermeldung.txt] <Original-Subject>`. die zugehörige Fehlermeldung gemäß der Tabelle „Tab_Fehlercodes_KOMLE-Clientmodule“ in den Mail-Body aufnehmen~~.

Ebenfalls 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_Fehlercodes_KOMLE-Clientmodule] 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“.

[<=]

Bei einer solchen Fehlernachricht gibt es folgende Optionen:

- Wenn die empfangene Nachricht vom Server gelöscht wurde, hat der Nutzer die Möglichkeit, durch das Senden

an die eigene E-Mail-Adresse und das anschließende Abholen die ~~Aufbereitung~~ Verarbeitung zu wiederholen.
- Wenn die empfangene Nachricht nicht vom Server gelöscht wurde, wird beim nächsten Abholen die Verarbeitung wiederholt.

Tabelle "Tab_Fehlercodes_KOMLE-Clientmodule" enthält den Fehlertext, der in die Nachricht eingefügt wird, wenn der Abruf von E-Mail-Daten zu häufig ausgeführt wurde.

3.2 Umgang mit großen ~~Anhängen~~ Client-Mails

Dieses Kapitel beschreibt die Verarbeitung von Client-Mails, welche die ~~Netto~~Größe von ~~25~~ 15 MiB überschreiten. Die Größenbeschränkung auf ~~25~~ 15 MiB basiert auf ~~den~~ Limitierungen der Konnektoroperationen zum Signieren und Verschlüsseln. ~~Für diese Operationen existiert eine Größenbeschränkung auf 25 MB (netto).~~

Client-Mails ~~E-Mails~~ mit einer Gesamtgröße bis zu ~~25~~ 15 MiB werden entsprechend den Festlegungen im KOM-LE 1.0 behandelt. Übersteigt die Größe einer Client-Mail die ~~25~~ 15-MiB-Grenze, wird die gesamte Client-Mail (E-Mail-Daten) ~~E-Mail werden alle Anhänge~~ durch das KOM-LE-Clientmodul ~~aus der Mail entnommen und~~ auf einem Speicher des KOM-LE-Fachdienstes (KAS) abgelegt. Das KOM-LE-Clientmodul ~~ergänzt~~ ersetzt die KOM-LE-Nachricht~~Mail um~~ mit den Metadaten der auf dem KAS abgelegten E-Mail-Daten ~~die Links auf die Anhänge~~ und versendet sie als ~~die~~ signierte und verschlüsselte KOM-LE-~~Mail~~Nachricht. Das KOM-LE-Clientmodul des Empfängers erkennt anhand der im Mail Header übergebenen `X-KOM-LE-Version`, dass es sich um eine KOM-LE 1.5 Nachricht handelt. Es nutzt die im Mail Body enthaltene Information, um die verschlüsselten E-Mail-Daten vom ~~die Links der entfernten Anhänge in der Mail, lädt die Anhänge vom~~ KOM-LE-Fachdienst (KAS) abzurufen ~~setzt sie wieder in die Mail ein~~, zu entschlüsseln und zu einer Client-Mail zusammenzufügen.

In [gemSpec_FD_KOMLE] Kapitel "Schnittstelle I_Attachment_Services" wird der Umgang mit großen ~~Anhängen~~ Client-Mails in einem Sequenzdiagramm erläutert.

3.2.1 Senden von großen ~~Nachrichten~~ Client-Mails~~mit großen Anhängen~~

In diesem Kapitel werden Anforderungen an das Clientmodul formuliert, die es erlauben, ~~Nachrichten~~Client-Mails von über ~~25~~ 15 MiB ~~inklusiver Anhänge~~ zu versenden.

[...]

A_19356-05 - 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` 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 ~~25~~ 15 MiB an einen Empfänger mit KOM-LE-Version < 1.5 versendet werden soll, MUSS das KOM-LE-Clientmodul diesen Empfänger aus der Mail entfernen. 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_19357-02 - Verarbeitung einer Client-Mail größer 15 MiB

Das KOM-LE-Clientmodul MUSS gewährleisten, dass die von einem Clientsystem übergebene Client-Mail~~Nachrichtengröße~~ vor der Übergabe an den Konnektor ~~nicht 25~~ 15 MiB nicht überschreitet. ~~Hierzu MUSS das KOM-LE-Clientmodul alle Anhänge aus der Mail extrahieren. Die Anhänge müssen inklusive ihrer Content-Header aus dem Mail-Body extrahiert werden~~. Übersteigt die Größe einer Client-Mail die 15 MiB-Grenze MUSS das Clientmodul die gesamte Client-Mail verschlüsselt auf einem Speicher des KOM-LE-Fachdienstes (KAS) abgelegen und die Metadaten der auf dem KAS abgelegten Client-Mail in die zu versendende KOM-LE-Mail einbetten.

[<=]

A_19358-01 - Erzeugung symmetrischer Schlüssel

Das KOM-LE-Clientmodul MUSS für die Verschlüsselung ~~der Anhänge~~ der auf dem KAS abzulegenden E-Mail-Daten ein en symmetrischen Schlüssel generieren. Hierbei MUSS das KOM-LE-Clientmodul die Kriterien gemäß [gemSpec_Krypt] einhalten.

[<=]

Hinweis: Der Initialisierungsvektor muss vom Sender pro Nachricht zufällig erzeugt werden. Dieser wird nach Konvention dem Chiffrat (=> ersten 12 Byte) vorangestellt: [IV + Chiffrat].

A_19364-02 - Freigabelink in die Mail aufnehmen

Das KOM-LE-Clientmodul MUSS das Ergebnis der Operation add_Attachment [gemSpec_FD_KOMLE] prüfen. Bei einem HTTP-Status 201 MUSS das KOM-LE-Clientmodul den zurückgelieferten Freigabelink in die KIM-Attachment-Datenstruktur ~~des Anhangs~~ im Mail-Body der zu versendenden KOM-LE-Nachricht aufnehmen.

[<=]

[...]

A_19359-07 - Einbetten von Informationen großer Nachrichten

Das KOM-LE-Clientmodul MUSS für ~~jeden~~ die auf dem KAS abgelegten ~~Anhang die~~ E-Mail-Daten folgende KIM-Attachment-Datenstruktur gemäß [Attachment_Schema] ~~an der Position des extrahierten Anhanges~~ im Mail-Body bef üllen ~~einfügen:~~ und als einziges Body-Element in den Mail-Body der vorverarbeiteten originalen Client-Mail durch den MIME-Part Content-Disposition: x-kas ersetzen. ~~in die zu versendende KOM-LE-Nachricht einfügen:~~

Tabelle 2 KIM-Attachment-Datenstruktur

Attribut in KIM-Attachment-Datenstruktur	Wert
~~name~~	~~Dateiname des Anhangs~~
link	Freigabelink ~~des Anhangs~~ der verschlüsselten E-Mail-Daten gemäß [A_19364]
k	AES-GCM Key ~~des Anhangs~~ der E-Mail-Daten (symmetrischer Schlüssel) im Base64 Format
hash	Hashwert ~~des Anhangs~~ der E-Mail-Daten (entsprechend A_19644 [gemSpec_Krypt] zu bilden) im Base64 Format
~~type~~	~~MIME-Type des Anhanges~~
size	Größe ~~des Anhangs~~ 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: Bei den E-Mail-Daten handet es sich um die verschlüsselte Client-Mail die auf dem KAS abgelegt wurde und über den Freigabelink eindeutig zuordbar ist. In der zu erzeugenden KOM-LE-Nachricht wird der Mail-Header der Client-Mail übernommen und der Mail-Body mit der KIM-Attachment-Datenstruktur ersetzt. Das folgende Beispiel soll die Verarbeitung verdeutlichen:

Beispiel für eine Client-Mail mit zwei Anhängen die 15 MiB überschreitet ~~vor der Entnahme der Anhänge~~:

```
From: "Sender" <sender@maildomain.de>
To: <empfaenger@maildomain.de>
Message-Id: <II8HEDLEUEU4.EG0B98QUZNPM2@STST-TEST>
Subject: Mail mit zwei Anhängen
Mime-Version: 1.0
```

[...]

~~**Die gleiche Client-Mail nach Entnahme** der Anhänge:~~

Die zu erzeugende KOM-LE-Nachricht mit der KIM-Atachment-Datenstruktur:

```
From: "Sender" <sender@maildomain.de>
To: <empfaenger@maildomain.de>
Message-Id: <II8HEDLEUEU4.EG0B98QUZNPM2@STST-TEST>
Subject: Mail mit zwei Anhängen
Mime-Version: 1.0

X-KIM-Dienstkennung: KIM-Mail;Default;V1.0
X-KIM-CMVersion: [VendorID]_2.1.2-8
X-KIM-PTVersion: 1.5.0-2
X-KIM-KONVersion: <secunet konnektor 2.0.0><Konnektor PTV4Plus><4.80.3><2.0.0><4.10.1>
X-KIM-Sendersystem: Beispiel-PVS;V2.81

Content-Type: ~~multipart/mixed; boundary="body_part_boundary"~~ text/plain; charset=utf-8

~~--body_part_boundary~~
~~Content-Type: text/plain; charset=utf-8~~
~~Content-Transfer-Encoding: quoted-printable~~
~~Content-Disposition: inline~~

~~Ein Dokument und eine Aufnahme im Anhang.~~

~~--body_part_boundary~~
~~Content-Type: text/plain; charset=utf-8~~
Content-Disposition: x-kas

  {
    ~~"name":     "MR-2020-04-01-xyz.doc",~~
    "link":     "HTTPS://KIM-FD1.telematik.de/CXFDTE82346dfzwr7634dfs76sd76sdtzq376e3tzsd",
    "k":        "RzVEY3M0MzkmNGZkc2RneCVoX2tkdFQlNXczZnZDdDM2ZGZ2eGZzJDYxITJndmR1VWpzKGk=",
    "hash":     "Z6A65Z2dasI2I00mM7uxtQjLsEwwl+WLMnDw8eLntaA=",
    "size":     ~~143271~~ 25525700,
    ~~"type":     "application/msword"~~
  }
~~--body_part_boundary~~
```

~~Content-Type: text/plain; charset=utf-8~~
~~Content-Disposition: x-kas~~

~~{~~
~~"name": "Roentgenbild 375632378.jpg",~~
~~"link": "HTTPS://KIM-FD1.telematik.de/Cduiz763478dfjkdfjhgow4784JHKZsdtq376e3t478d",~~
~~"k": "Ry80ZmRpdWhjczQzOSY0ZmRzZGd4JWhfa2R0VCU1dzNmdkzZkYXNlcmZnODkzNDV1aXNyZg==",~~
~~"hash": "Hp30Rx6T9aX0PUmyuASDDIAJ2lPAwbPdc5OSAMK49I=",~~
~~"size": 32573,~~
~~"type": "image/jpeg"~~
~~}~~
~~--body_part_boundary--~~

A_19360-02 - Verschlüsselung der E-Mail-Daten

Das KOM-LE-Clientmodul MUSS ~~den Anhang~~ die E-Mail-Daten, welche auf dem KAS abgelegt werden, mit dem erzeugten symmetrischen Schlüssel gemäß GS-A_5016 [gemSpec_Krypt] verschlüsseln.

[<=]

[...]

A_19363-03 - Übertragung von E-Mail-Daten

Das KOM-LE-Clientmodul MUSS für die Übertragung ~~des Anhanges~~ von E-Mail-Daten, die vom KAS des Fachdienstes bereitgestellte Operation add_Attachment aufrufen.

~~Im Fehlerfall MUSS das KOM-LE-Clientmodul den Absender mit einer E-Mail über den Fehlerfall informieren. Aus dem Inhalt der Fehlernachricht MUSS hervorgehen, welcher Anhang nicht an den KAS übermittelt werden konnte. Die Fehlernachricht ist weder zu signieren noch zu verschlüsseln und entspricht der Delivery Status Notification gemäß [RFC3461-3464]. Zusätzlich muss der vom KAS gemeldete Fehlertext wie folgt eingefügt werden: Fehlertext: <message>. Die ursprüngliche KOM-LE-Nachricht darf im Fehlerfall nicht versendet werden.~~

Im Fehlerfall MUSS das Clientmodul das Clientsystem mit dem SMTP-Antwortcode „451“ (gemäß [RFC3463]) benachrichtigen und den Versandt zum MTA mit dem RSET-Kommando abbrechen, da die Nachricht nicht übertragen werden konnte. Verarbeitungschritte des Clientmoduls, welche die originale Nachricht betreffen (z. B. Anpassung Headerinformationen) MÜSSEN vor der Übertragung der originalen E-Mail-Daten zum KAS erfolgen.

[<=]

A_19365-02 - Senden der KOM-LE-Nachricht

Das KOM-LE-Clientmodul MUSS die ~~– um die großen Anhänge reduzierte –~~ ~~E~~KOM-LE-~~Mail~~ Nachricht, welche das Body-Element der KIM-Attachment-Datenstruktur beinhaltet, entsprechend den Festlegungen für Mails kleiner oder gleich ~~25~~ 15 MiB senden. **[<=]**

A_22419-01 - Behandlung von Quota-Überschreitung

Wenn das Clientmodul ~~beim Versand eines E-Mail-Anhanges~~ bei der Übertragung von E-Mail-Daten ~~vom KAS~~ einen Fehlercode 507 vom KAS erhält, MUSS es den Mailversand abbrechen und dem KOM-LE-Client den SMTP-Fehlercode 521 gemäß [RFC3463] zurückgeben und ~~die existierende SMTP-Verbindung zum Mail-Server abbauen~~ den Versandt zum MTA mit dem RSET-Kommando abbrechen.

[<=]

A_22427-01 - I_Attachment_Services - Content-Length

Das KOM-LE-Clientmodul MUSS bei der Übertragung ~~des Anhanges~~ der E-Mail-Daten das HTTP-Header-Element "`Content-Length`" immer mit der Gesamt-Länge des Request-Bodys befüllen.

[<=]

3.2.2 Empfangen von großen Client-Mails ~~Nachrichten mit großen Anhängen~~

In diesem Kapitel werden Anforderungen an das Clientmodul formuliert, die es erlauben, große ~~Anhänge~~ Client-Mails zu empfangen.

[...]

~~*Eine KOM-LE 1.0 E-Mail ist maximal 25 MB groß (netto). Hierbei ist zu beachten, dass durch die Base64-Kodierung der Nachricht die zu verarbeitende Bruttogröße um den Faktor 1,37 erhöht wird (brutto).*~~

[...]

A_19369-02 - Ermittlung von Informationen der auf dem KAS abgelegten E-Mail-Daten

~~Das KOM-LE-Clientmodul MUSS die Dateinamen, Hash-Werte und die Freigabelinks der extrahierten Anhänge sowie den symmetrischen Schlüssel aus der KIM-Attachment-Datenstruktur der Anhänge im Mail-Body entnehmen.~~

Das KOM-LE-Clientmodul MUSS den Hash-Wert, den Freigabelink sowie den symmetrischen Schlüssel aus der KIM-Attachment-Datenstruktur, aus dem Body-Element der abgerufenen KOM-LE-Nachricht entnehmen. Das KOM-LE-Clientmodul DARF KOM-LE-Nachrichten NICHT verarbeiten, die mehr als eine KIM-Attachment-Datenstruktur gemäß [A_19359] beinhalten.

Ist mehr als eine KIM-Attachment-Datenstruktur in der abgerufenen KOM-LE-Nachrichten enthalten, MUSS das Clientmodul den Nutzer ~~mit einer E-Mail~~ über den Fehlerfall informieren. ~~Die Fehlernachricht entspricht einer multipart/mixed MIME-Nachricht. Die Originalnachricht MUSS als message/rfc822 MIME-Einheit in die Fehlernachricht eingepackt werden. Zusätzlich muss diese neue multipart/mixed MIME-Nachricht eine text/plain MIME-Einheit mit dem Fehlertext, "*Nachricht konnte aufgrund uneindeutiger Informationen nicht abgerufen werden*." 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 „*Nachricht konnte aufgrund uneindeutiger Informationen nicht abgerufen werden*“.~~ Hierfür MUSS das Clientmodul den Mail-Body der entschlüsselten originalen Nachricht durch den folgenden Inhalt "*Nachricht konnte aufgrund uneindeutiger Informationen nicht abgerufen werden*" als `text/plain` MIME-Einheit ersetzen.

[<=]

A_19370-04 - Download von E-Mail-Daten

Das KOM-LE-Clientmodul MUSS die ~~Anhänge~~ E-Mail-Daten anhand des ~~zu den~~ entnommenen Freigabelinks via der Operation read_Attachment am KAS des Fachdienstes herunterladen.

Wenn beim Herunterladen ~~eines Anhangs~~ der E-Mail-Daten ein 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 „~~Mindestens ein Anhang der Nachricht~~ Die E-Mail-Daten konnten nicht ~~heruntergeladen~~ abgerufen werden“.

[<=]

~~Bei einer Nachricht mit dem Subject „Mindestens ein Anhang der Nachricht konnte nicht heruntergeladen werden“ gibt es folgende Optionen:~~ Bei einer solchen Fehlernachricht gibt es folgende Optionen:

- Wenn die empfangene Nachricht vom Server gelöscht wurde, hat der Nutzer die Möglichkeit, durch das Senden an die eigene E-Mail-Adresse und das anschließende Abholen die ~~Aufbereitung~~ Verarbeitung zu wiederholen.
- Wenn die empfangene Nachricht nicht vom Server gelöscht wurde, wird beim nächsten Abholen die ~~Aufbereitung~~ Verarbeitung wiederholt.

Tabelle "Tab_Fehlertext_Download Fehlertext beim Download von ~~Anhängen~~ E-Mail-Daten" enthält den Fehlertext, der in die Nachricht eingeführt wird, wenn der Download von ~~Anhängen~~ E-Mail-Daten nicht durchgeführt werden konnte.

Tabelle 3 Tab_Fehlertext_Download Fehlertext beim Download von E-Mail-Daten

Bedingung	Fehlertext
~~Mindestens ein Anhang der Nachricht konnte nicht heruntergeladen werden.~~ E-Mail-Daten konnten nicht heruntergeladen werden.	~~Nicht alle Anhänge~~ E-Mail-Daten dieser Nachricht konnten nicht heruntergeladen werden. Bitte leiten Sie diese Nachricht nach einer angemessenen Zeit an Ihre eigene E-Mail-Adresse (<Email Adresse>) weiter. Beim nächsten Abholen wird der Download wiederholt.
E-Mail-Daten konnten nicht entschlüsselt werden.	E-Mail-Daten dieser Nachricht konnten nicht entschlüsselt werden. Bitte leiten Sie diese Nachricht nach einer angemessenen Zeit an Ihre eigene E-Mail-Adresse (<Email Adresse>) weiter. Beim nächsten Abholen wird der Download wiederholt und ein erneuter Entschlüsselungsversuch unternommen.

A_19371-04 - Entschlüsselung vom KAS abgerufener E-Mail-Daten

Das KOM-LE-Clientmodul MUSS die heruntergeladenen ~~Anhänge~~ E-Mail-Daten mit dem symmetrischen Schlüssel entschlüsseln.

~~Wenn beim Entschlüsseln eines Anhangs der E-Mail ein Fehler auftritt, dann MUSS das KOM-LE-Clientmodul an der Position des Anhangs ein MIME-Element mit `Content-Type: text/plain; charset=utf-8`, `Content-Transfer-Encoding: quoted-printable` und `Content-Disposition: attachment; filename=<Original-Filename>_Fehlermeldung.txt` sowie folgende Informationen als Inhalt des Anhangs einfügen: Der Anhang { "`name`": "Dateiname des Anhangs", "`size`": Größe des Anhangs in Byte, "`type`": "MIME-Type des Anhangs" } konnte nicht entschlüsselt werden. Im Betreff der entschlüsselten Nachricht ist Folgendes anzugeben: `[Fehler beim Entschlüsseln eines Anhangs *_Fehlermeldung.txt]` <Original-Subject>.~~

Wenn beim Entschlüsseln der E-Mail-Daten ein Fehler auftritt, MUSS das KOM-LE-Clientmodul den Mail-Body der entschlüsselten originalen Nachricht durch den folgenden Inhalt "Abgerufene E-Mail-Daten konnten nicht entschlüsselt werden" als `text/plain` MIME-Einheit ersetzen.~~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 „*Abgerufene E-Mail-Daten konnten nicht entschlüsselt werden*“.~~ Zusätzlich MUSS das Clientmodul das Mail-Header-Attribut `X-KIM-Fehlermeldung` mit dem Wert 4007 gemäß Tabelle „Tab_Fehlercodes_KOMLE-Clientmodule“ befüllen.

[<=]

~~Bei einer solchen Fehlernachricht gibt es folgende Optionen:~~

- ~~Wenn die empfangene Nachricht vom Server gelöscht wurde, hat der Nutzer die Möglichkeit, durch das Senden an die eigene E-Mail-Adresse und das anschließende Abholen die Aufbereitung zu wiederholen.~~
- ~~Wenn die empfangene Nachricht nicht vom Server gelöscht wurde, wird beim nächsten Abholen die Aufbereitung wiederholt.~~

~~Tabelle "Tab_Fehlertext_Download" enthält den Fehlertext, der in die Nachricht eingefügt wird, wenn die Entschlüsselung von E-Mail-Daten nicht erfolgreich durchgeführt werden konnte.~~

A_19372-03 - Prüfen der E-Mail-Daten

Das KOM-LE-Clientmodul MUSS den Hash-Wert ~~des~~ der entschlüsselten ~~Anhanges~~ E-Mail-Daten entsprechend [A_19644] bilden und mit dem ~~aus dem Content-Header des Anhangs im Mail-Body entnommenen~~ Hash-Wert aus der abgerufenene KIM-Attachment-Datenstruktur vergleichen. Bei einer Nichtübereinstimmung MUSS das KOM-LE-Clientmodul den Mail-Body der entschlüsselten originalen Nachricht durch den folgenden Inhalt als `text/plain` MIME-Einheit ~~die Nachricht dem Clientsystem und einem entsprechenden Vermerk übergeben. die KOM-LE-Nachricht mit der folgenden Nachricht~~ ersetzen und an den Empfänger weiterleiten:
"*Beim Empfang dieser KIM-Nachricht wurde eine Sicherheitsverletzung erkannt. Dies kann eine technisches Ursache haben oder auf eine missbräuchliche Nutzung des KIM-Dienstes hinweisen. Zu Ihrem Schutz wurde der Inhalt dieser Nachricht durch diesen Text ausgetauscht. ~~Der Absender wurde über diesen Vorfall informiert.~~ Bitte antworten Sie nicht auf diese Nachricht. Sie können diese Nachricht löschen. [+ optionaler Freitext der Anbieter]*".

~~Darüber hinaus MUSS das KOM-LE-Clientmodul den Absender über die Nichtübereinstimmung informieren. Aus dem Inhalt der Fehlernachricht MUSS hervorgehen, dass bei der Prüfung der gesendeten Nachricht beim Empfänger ein Fehler festgestellt wurde. Die Fehlernachricht ist weder zu signieren noch zu verschlüsseln und entspricht der Delivery Status Notification gemäß [RFC3461-3464].~~

~~Das KOM-LE-Clientmodul MUSS den Vermerk mit der folgenden Bildungsregel an den Text der Nachricht anhängen: "Die Prüfsumme des `name` (gemäß [A_19359]) stimmt nicht überein. Der empfangene Anhang entspricht eventuell nicht dem originalen Anhang." Es ist dabei das Format des TextParts zu beachten (mediatype text/html oder text/plain) und der Vermerk diesem Format anzupassen.~~

~~In beiden Fällen MUSS das Clientmodul das Mail-Header-Attribut `X-KIM-IntegrityCheckResult` mit der ID=4012 gemäß der Tabelle "Tab_Fehlercodes_KOMLE-Clientmodule" Fehlercode befüllen.~~ Zusätzlich MUSS das Clientmodul das Mail-Header-Attribut `X-KIM-Fehlermeldung` mit dem Wert 4012 gemäß Tabelle „Tab_Fehlercodes_KOMLE-Clientmodule“ befüllen.

[<=]

A_19374-03 - Zusammensetzen der Mail

~~Das KOM-LE-Clientmodul MUSS alle entschlüsselten Anhänge in die Mail an ihrer ursprünglichen Position integrieren, welche den MIME-Part mit den Informationen zu diesem Anhang enthält und die eingefügten KIM-Attachment-Datenstrukturen - inklusive der eingefügten MIME-Content-Header - entfernen.~~

Das KOM-LE-Clientmodul MUSS die vom KAS abgerufenen und entschlüsselten E-Mail-Daten, als originale Nachricht (Client-Mail) ~~weiterverarbeiten~~ wiederherstellen und ergänzt um ~~Informationen aus den umliegenden Verarbeitungsschritten (u. a. Vermerke, Headerdaten, ...)~~ den Vermerk der erfolgreichen Verarbeitung (Entschlüsselung und Integritätsprüfung)

an das Clientsystem übermitteln.

[<=]

3.3.1 Überblick

Beim Senden von KOM-LE-Nachrichten sorgt das Clientmodul dafür, dass die gesendeten ~~E-Mail-~~KOM-LE-Nachrichten digital signiert und verschlüsselt dem MailTransfer Agent des KOM-LE-Fachdienstes (weiter im Text als MTA bezeichnet), bei dem der Sender registriert ist, übermittelt werden. Bei ~~E-Mail-Nachrichten~~ Client-Mails größer ~~25~~ 15 MiB ~~werden alle zur E-Mail-Nachricht gehörenden Anhänge vor der Durchführung der kryptographischen Operationen extrahiert und symmetrisch verschlüsselt auf dem Fachdienst abgespeichert.~~ wird die Client-Mail symmetrisch verschlüsselt und auf dem KAS des Fachdienstes abgespeichert.

3.3.4.1.1 Bearbeiten einer ungeschützten Nachricht

Um die Vertraulichkeit und die Integrität einer ~~Nachricht~~ Client-Mail zu schützen wird die ~~Nachricht~~ diese entsprechend dem KOM-LE-S/MIME-Profil signiert und verschlüsselt. Für das Signieren und die Verschlüsselung nutzt das Clientmodul die Dienste der TI-Plattform. Die folgende Abbildung stellt den prinzipiellen Ablauf und die Aktivitäten des Clientmoduls beim Erzeugen einer dem KOM-LE-S/MIME-Profil entsprechenden KOM-LE-Nachricht dar. Hierbei wird von einer ~~E-Mail-Nachricht~~ Client-Mail Größe ~~von~~ kleiner oder gleich ~~25~~ 15 MiB ausgegangen.

[...]

A_23169 - Sicherstellung der Absenderintegrität

Das Clientmodul MUSS sicherstellen, dass nur die vom Clientsystem zuvor im SMTP-Kommando `MAIL FROM` an das Clientmodul übergebene E-Mail-Adresse in der KOM-LE-Nachricht als einzige Adresse (wenn vorhanden inkl. display name) im Mail header `from` enthalten ist und prüfen ob für diese E-Mail-Adresse mindestens ein ENC-Zertifikat im VZD existiert. Existiert ein `reply-to` Header-Element in der originalen Nachricht so MUSS dieses ebenfalls durch die zuvor geprüfte E-Mail-Adresse aus dem SMTP-Kommando `MAIL FROM` befüllt werden.

<=

A_23174 - Sicherstellung der Empfängeradressen

Das Clientmodul MUSS sicherstellen, dass nur die vom Clientsystem an das Clientmodul übergebenen E-Mail-Adressen die zuvor im SMTP-Kommando `RCPT TO` gemäß [KOM-LE-A_2176] geprüft wurden im Mail Header `to`, `cc` und `bcc` in der KOM-LE-Nachricht verbleiben.

<=

3.4.1 Übersicht

[...]

Beim Abholen von Nachrichten findet die Kommunikation zwischen dem Clientsystem, dem Clientmodul und dem POP3-Server über POP3 statt. Das Clientmodul fungiert als POP3-Proxy, der das Clientsystem mit dem POP3-Server verbindet, die Entschlüsselung und Signaturprüfung für die abgeholten KOM-LE-Nachrichten durchführt und die entschlüsselten Nachrichten an das Clientsystem liefert. ~~Die Ergebnisse der Signaturprüfung werden dem Nutzer als Vermerk, der in den Inhalt der Nachricht integriert wird sowie als ein detaillierter Bericht in Form einer angehängten PDF-Datei mitgeteilt.~~ Bei einer fehlgeschlagenen Integritätsprüfung wird der Empfänger der KOM-LE-Nachricht mit einer Fehlernachricht informiert. Die Weiterleitung der Client-Mail an das Clientsystem des Empfängers wird in diesem Fall durch das Clientmodul unterbunden.

[...]

Fehler, die bei der Entschlüsselung oder ~~Signaturprüfung~~ Integritätspüfung einer Nachricht auftreten, werden anders behandelt:

- Kann die Nachricht nicht entschlüsselt werden (z.B. weil der entsprechende HBA nicht zu Verfügung steht), wird durch das Clientmodul eine Fehlernachricht generiert, die die verschlüsselte Nachricht als Anhang enthält. Um die Nachricht nachträglich zu entschlüsseln und ihre Signatur zu prüfen, kann der Nutzer die Nachricht an seine eigene E-Mail-Adresse senden, Maßnahmen treffen damit beim nächsten Abholen der entsprechende Schlüssel gefunden wird und den Abholvorgang wiederholen.
- Wenn die ~~Signaturprüfung~~ Integritätspüfung der entschlüsselten KOM-LE-Nachricht fehlschlägt (z. B. weil die Integrität der Nachricht verletzt wurde) wird die entschlüsselte Nachricht ~~dem Clientsystem mit dem entsprechenden Vermerk übergeben~~ verworfen und eine Fehlernachricht an den Sender sowie den Empfänger der KOM-LE-Nachricht gesendet.

3.4.4 PROCESS-Zustand

[...]

Im PROZESS-Zustand nimmt das Clientmodul die Inhalte der vom POP3-Server abgerufenen KOM-LE-Nachricht entgegen, entschlüsselt die Nachricht, prüft deren Integrität~~, fügt einen Vermerk sowie einen PDF-Anhang mit dem Ergebnis der Signaturprüfung in die Nachricht ein~~ und leitet die aufbereitete ~~Nachricht~~ Client-Mail dem Clientsystem weiter. Im Erfolgsfall wird in die aufbereitete Client-Mail ein Vermerk hinzugefügt und das Clientsystem über das erfolgreiche Abholen der Nachricht informiert. Im Fehlerfall wird das Clientsystem mit dem entsprechenden Antwortcode bzw. Fehlernachricht über den Fehler informiert.

3.4.4.2.1 Entschlüsselung

[...]

KOM-LE-A_2047-02 - Fehlertexte bei fehlgeschlagener Entschlüsselung

Das Clientmodul MUSS bei fehlgeschlagener Entschlüsselung entsprechend der jeweiligen Bedingung ~~die~~ den in Tabelle Tab_Fehlertext_Entschl definierten Fehlertexte in die `text/plain` MIME-Einheit der multipart/mixed MIME-Fehlernachricht aufnehmen. Zusätzlich MUSS das Clientmodul ein Mail-Header-Attribut `X-KIM-DecryptionResult` mi t der dazugehörigen ID aus der Tabelle "Tab_Fehlertext_Entschl" Fehlercode befüllen. Treten im Entschlüsselungsprozess Fehler auf, die nicht in der Tabelle "Tab_Fehlertext_Entschl" definierte sind, MUSS das Clientmodul für diese Fehler das Mail-Header-Attribut X-KIM-DecryptionResult mit einem herstellerspezifischen Fehlercode befüllen, welcher mit "X" beginnt.

<=

Hinweis: Sollten mehrere negative Ergebnisse bei der Entschlüsselung einer KOM-LE Nachricht hervorgehen KANN das Mail-Header-Attribut `X-KIM-DecryptionResult` mehrmals verwendet werden.

Beispiel:

```
X-KIM-DecryptionResult: 01
X-KIM-DecryptionResult: 02
```

`X-KIM-DecryptionResult: X99`

3.4.4.2.2 Integritätsprüfung

[...]

~~Das Ergebnis der Signaturprüfung und des Abgleichs des `recipient-emails` Attributs wird als Vermerk, der den Text der Nachricht ergänzt, dem Empfänger mitgeteilt.~~

~~Falls der Zertifikatstatus des Signaturzertifikates nicht geprüft werden kann (z.B. der OCSP-Responder ist unerreichbar), die mathematische Prüfung der Signatur aber erfolgreich durchgeführt wurde, wird ein entsprechender Vermerk in den Body der Nachricht eingetragen.~~

Wenn die Integritätsprüfung der entschlüsselten KOM-LE-Nachricht fehlschlägt, dann wird eine Fehlernachricht gemäß [A_23165] generiert und das `X-KIM-IntegrityCheckResult` Header-Element mit der jeweiligen ID gemäß der Tabelle "Tab_Verm_Sig_Prüf" befüllt.

~~Tabelle Tab_Verm_Sig_Prüf stellt die Vermerke entsprechend den Ergebnissen der Signaturprüfung dar.~~

Tabelle 4: Tab_Verm_Sig_Prüf Vermerke mit Ergebnissen der Signaturprüfung

ID*	Prüfergebnis	Fehlercode	Ergebnis	Vermerk
01	~~VALID~~ true	-	Die Signatur der Nachricht wurde erfolgreich geprüft.	Die Signatur wurde erfolgreich geprüft.
02	~~INVALID~~ false	4115	Die Integrität der Nachricht wurde verletzt.	~~Die Prüfung der Signatur hat ergeben, dass die Nachricht manipuliert wurde.~~ -
03	~~INVALID~~ false	4253	Die digitale Signatur ist nicht vorhanden.	~~Die Nachricht ist nicht signiert. Die Nachricht ist deshalb eventuell manipuliert worden.~~ -
04	~~INVALID~~ false	4112	Die digitale Signatur konnte aufgrund des falschen Formats nicht geprüft werden.	~~Die Signatur der Nachricht konnte aufgrund eines falschen Formats nicht geprüft werden. Die Nachricht ist deshalb eventuell manipuliert worden.~~ -
05	~~INVALID~~ false	4206	Der Zertifizierungspfad des Signaturzertifikats kann nicht validiert werden ~~(abgelaufenes Zertifikat, der Zertifizierungspfad konnte nicht aufgebaut werden usw.)~~.	~~Die Signatur der Nachricht wurde geprüft. Die dabei durchgeführte Integritätsprüfung der Nachricht war erfolgreich. Der Status des zur Signatur verwendeten Zertifikats konnte nicht vollständig durchgeführt werden, weil nicht alle am Signaturprozess beteiligten Zertifikate validiert werden konnten.~~ -
06	~~INVALID~~ false	[Fehlercode]	Die digitale Signatur konnte aufgrund eines nicht zuordenbaren Fehlercodes des Konnektors nicht geprüft werden.	~~Bei der Prüfung der digitalen Signatur ist ein unerwarteter Fehler aufgetreten.~~ -
				~~Die Signatur der Nachricht wurde geprüft. Die~~

07	~~INCONCLUSIVE~~ true	4264	Die digitale Signatur ist mathematisch korrekt, der Zertifikatsstatus des Signaturzertifikats konnte aber nicht geprüft werden.	~~dabei durchgeführte Integritätsprüfung der Nachricht war erfolgreich. Der Status des zur Signatur verwendeten Zertifikats konnte nicht vollständig geprüft werden, weil zum Prüfungszeitpunkt nicht alle erforderlichen technischen Ressourcen verfügbar waren.~~ Die Signatur wurde erfolgreich geprüft.
08	~~VALID~~ false	-	Die digitale Signatur ist mathematisch korrekt und der Zertifikatsstatus des Signaturzertifikats konnte erfolgreich geprüft werden, aber beim Vergleich der Header-Elemente from, sender, reply-to, to und cc der äußeren Nachricht mit denen der inneren Nachricht wurden Abweichungen festgestellt.	~~Die Signatur der Nachricht wurde geprüft. Die Prüfung hat ergeben, dass die Nachricht nach dem Verschlüsseln manipuliert wurde. Möglicherweise wurde die verschlüsselte Nachricht auch an einen nicht empfangsberechtigten Personenkreis versendet.~~ ~~-~~
09	~~VALID~~ false	-	Die digitale Signatur ist mathematisch korrekt und der Zertifikatsstatus des Signaturzertifikats konnte erfolgreich geprüft werden, aber das recipient-emails-Attribut aus signerInfos enthält nicht die gleichen Werte wie das recipient-emails-Attribut aus dem enveloped-data CMS-Objekt.	~~Die Signatur der Nachricht wurde geprüft. Die Prüfung 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.~~ ~~-~~

~~*) Hinweis: Die in der Tabelle enthaltene ID des jeweiligen Prüfvermerks kann gemäß [KOM-LE-A_2050] als ID dem Vermerk hinzugefügt werden und muss in das `X-KIM-IntegrityCheckResult` Header-Element aufgenommen werden, um damit eine spätere automatische Auswertung zu ermöglichen.~~

[...]

KOM-LE-A_2050-05 - Verhalten bei positiver Integritätsprüfung

Das Clientmodul MUSS nach einer ~~validen~~ ~~abhängig vom Ergebnis der~~ ~~Signaturprüfung~~ Integritätsprüfung einer KOM-LE-Nachricht mit positivem Prüfergebnis (true) ~~die~~ den in Tabelle "Tab_Verm_Sig_Prüf" definierten Vermerke~~n~~ an den Nachrichtentext der KOM-LE-Nachricht anfügen. Es ist dabei das Format des TextParts zu beachten (mediatype text/html oder `text/plain`) und der Vermerk diesem Format anzupassen. Zusätzlich MUSS das Clientmodul ein Mail-Header-Attribut `X-KIM-IntegrityCheckResult` mit der dazugehörigen ID~~=01~~ aus der Tabelle "Tab_Verm_Sig_Prüf" ~~Fehlercode~~ befüllen.

<=

A_23165 - Verhalten bei fehlgeschlagener Integritätsprüfung

Das Clientmodul MUSS nach einer fehlgeschlagenen Integritätsprüfung den Mail-Body ~~die~~ der entschlüsselten originalen Nachricht ~~KOM-LE-Nachricht~~ mit dem folgenden ~~Text~~ Inhalt als `text/plain` MIME-Einheit ersetzen und an den Empfänger weiterleiten:
"*Beim Empfang dieser KIM Nachricht wurde eine Sicherheitsverletzung erkannt. Dies kann eine technisches Ursache*

haben oder auf eine missbräuchliche Nutzung des KIM Dienstes hinweisen. Zu Ihrem Schutz wurde der Inhalt dieser Nachricht durch diesen Text ausgetauscht. ~~Zusätzlich wurde der Absender der ursprünglichen Nachricht automatisch über diesen Vorfall informiert~~".

~~Darüber hinaus MUSS das KOM-LE-Clientmodul den Absender über die fehlgeschlagene Integritätsprüfung informieren. Aus dem Inhalt der Fehlernachricht MUSS hervorgehen, dass bei der Integritätsprüfung der gesendeten Nachricht beim Empfänger ein Fehler festgestellt wurde. Die Fehlernachricht ist weder zu signieren noch zu verschlüsseln und entspricht der Delivery Status Notification gemäß [RFC3461-3464].~~

~~In beiden Nachrichten~~ Zusätzlich MUSS das Clientmodul das Mail-Header-Attribut `X-KIM-IntegrityCheckResult` mit der dazugehörigen ID aus der Tabelle "Tab_Verm_Sig_Prüf" Fehlercode befüllen. Kommt es bei der Integritätsprüfung zu Fehlern, die nicht in der Tabelle "Tab_Verm_Sig_Prüf" definierte sind, MUSS das Clientmodul für diese Fehler das Mail-Header-Attribut `X-KIM-IntegrityCheckResult` mit einem herstellerspezifischen Fehlercode befüllen, welcher mit "X" beginnt.

<=

Hinweis: Sollten mehrere negative Ergebnisse aus der Integritätsprüfung hervorgehen KANN das Mail-Header-Attribut X-KIM-IntegrityCheckResult mehrmals verwendet werden.

Beispiel:

```
X-KIM-IntegrityCheckResult: 08
X-KIM-IntegrityCheckResult: X99
```

3.7.3 Deregistrierung KOM-LE-Teilnehmer

[...]

A_19464-03 - 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 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 der Zugriff auf das E-Mail-Konto zum Abholen von Nachrichten weiterhin möglich. Das Administrationsmodul MUSS die Rücknahme der Deregistrierung innerhalb der 30 Tage ermöglichen, um die E-Mail-Adresse wieder nutzen zu können. Hierfür MUSS das Administrationmodul die Operation `revokeDeregistration` am Account Manager aufrufen. ~~kein weiterer Zugriff auf das E-Mail-Konto möglich ist, das gelöschte Konto nicht wiederhergestellt werden und die damit verbundene E-Mail-Adresse nicht neu vergeben werden kann.~~

[<=]

2.2 Änderung in gemSpec_FD_KOMLE

2. Systemüberblick

[...]

Die Teilkomponente KOM-LE Attachment Service stellt dem Clientmodul eine Schnittstelle zum Ablegen bzw. Herunterladen von ~~Anhängen~~ verschlüsselten E-Mail-Daten zur Verfügung.

3.2 Funktionen des Account Managers

Über die Teilkomponente Accout Manager des Fachdienstes wird die Kontoverwaltung eines KOM-LE-Teilnehmers durchgeführt. Zu dem Funktionsumfang gehören:

- die Verwaltung des Nutzer-Accounts
  - Registrierung,
  - Deregistrierung,
  - Kennwortänderung,
  - Wechsel der Telematik-ID,
  - Löschfrist von ~~Anhängen~~ E-Mail-Daten,
  - Wechsel der eingesetzten KIM-Version
- die Verwaltung von Abwesenheitsnotizen
- die Bereitstellung der PKCS#12-Dateien

3.3 Funktionen des KOM-LE Attachment Services

Die Teilkomponente KAS des Fachdienstes dient als Speicherort für verschlüsselte ~~Anhänge von Mails~~ E-Mail-Daten, die durch Clientmodule aus Client-Mails extrahiert wurden. Damit wird die Übertragung von ~~großen~~ Mails größer 15 MiB ermöglicht. Das sendende KOM-LE Clientmodul legt die ~~großen Anhänge~~ E-Mail-Daten in verschlüsselter Form auf dem KAS ab. Das empfangende KOM-LE Clientmodul lädt die verschlüsselten E-Mail-Daten ~~Anhänge~~ nach dem ~~beim~~ Empfang der KOM-LE-Nachricht~~Mail~~ und stellt sie dem Clientsystem in entschlüsselter Form zusammen mit der ~~Mail~~ KOM-LE-Nachricht zur Verfügung. In der folgenden Abbildung wird die Funktionsweise des KAS gezeigt.

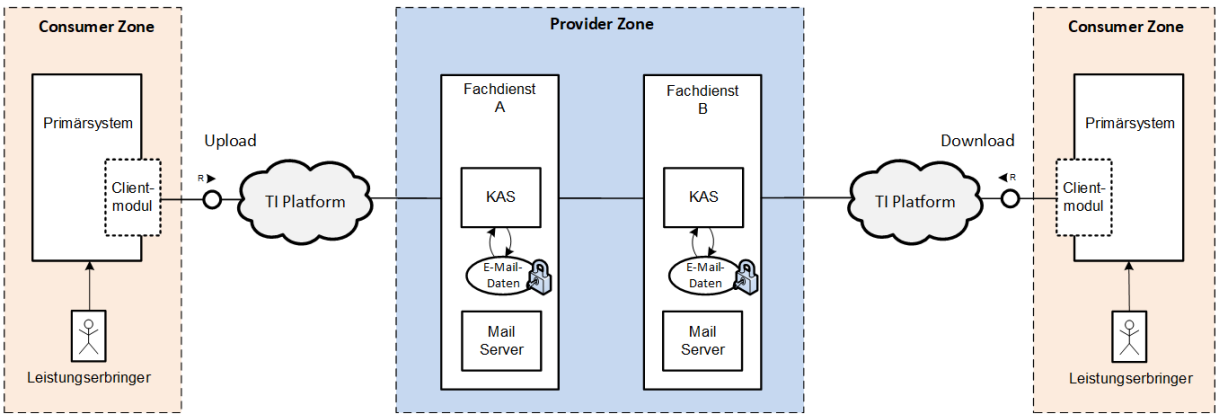

Abbildung 2: Abb_FD_KAS Funktionsweise des Attachment Service

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

Die maximale Gesamtgröße einer zu übermittelnden Client-Mail wird durch den Fachdienst definiert und dem Clientmodul zur Verfügung gestellt. Das Clientmodul prüft die Gesamtgröße der im Client erzeugten Mail ~~– inklusive aller Anhänge –~~ vor dem Versenden mit dem vom Fachdienst übermittelten Wert. Beim Hochladen der ~~Anhänge~~ verschlüsselten E-Mail-Daten auf den KAS prüft dieser den vorhandenen Speicherplatz gemäß dem mit dem Anbieter vereinbarten Speichervolumen für den Nutzeraccount (Quota). Die Gestaltung der jeweiligen Quota-Regelung bleibt dem Anbieter

überlassen (Marktmodell).

4.2 Schnittstelle I_Attachment_Services

Der KAS ermöglicht das Hoch- und Herunterladen von verschlüsselten ~~Anhängen~~ E-Mail-Daten, die durch Clientmodule aus Client-Mails extrahiert wurden ~~von Mails~~. Zum Bereitstellen der Funktionen wird die REST-Schnittstelle I_Attachment_Services definiert. Der Aufruf der Schnittstelle ist ausschließlich vom Clientmodul zulässig. Die Schnittstellenbeschreibung ist in [AttachmentServices.yaml] definiert.

[...]

Tabelle 5: Operationen vom KAS

Operation	URI	Methode	Request	Response	Beschreibung
`add_Attachment`	/attachment/	POST	recipients messageID expires binary <File>	string <Freigabelink>	Fügt ~~einen~~ verschlüsselten ~~Anhang~~ E-Mail-Daten im KAS hinzu
`read_Attachment`	/attachment/{attachmentId}	GET	recipient	binary <File>	Lädt ~~einen~~ die unter einem Freigabelink erreichbaren verschlüsselten ~~Anhang~~ E-Mail-Daten herunter

A_19375-04 - KAS – Implementierung der Schnittstelle

Der KAS MUSS die Schnittstelle I_Attachment_Services als REST-Webservices über HTTPS gemäß [AttachmentServices.yaml] in der Version 2.2.1 implementieren. Des Weiteren MUSS der KAS für alle in der [AttachmentServices.yaml] definierten Operationen den Zeichensatz UTF-8 unterstützen.

[<=]

[...]

A_19378-01 - KAS - prüfen der Größe der verschlüsselten E-Mail-Daten

Der KAS MUSS die Dateigröße ~~jedes übergebenen Dokumentes~~ der verschlüsselten E-Mail-Daten ermitteln, bevor ~~das Dokument~~ diese gespeichert ~~wird~~ werden. Der KAS MUSS die Verarbeitung ablehnen, wenn die Gesamtgröße ~~des Dokumentes~~ der verschlüsselten E-Mail-Daten den ~~diesen~~ Konfigurationswert des KAS übersteigt.

[<=]

A_19379-01 - KAS – Prüfung Zugriff auf E-Mail-Daten

Der KAS MUSS sicherstellen, dass nur über den dazugehörigen Freigabelink auf ~~das Dokument~~ die verschlüsselten E-Mail-Daten zugegriffen werden kann.

[<=]

Erzeugung des Freigabelinks

Der KAS generiert für jeden Upload ~~eines Anhanges~~ der E-Mail-Daten einen zufälligen und eindeutigen Freigabelink und sendet diesen als Antwort an den Client zurück. Durch Verwendung des Freigabelinks ~~kann~~ können die verschlüsselten E-Mail-Daten ~~der Anhang~~ vom KAS heruntergeladen werden.

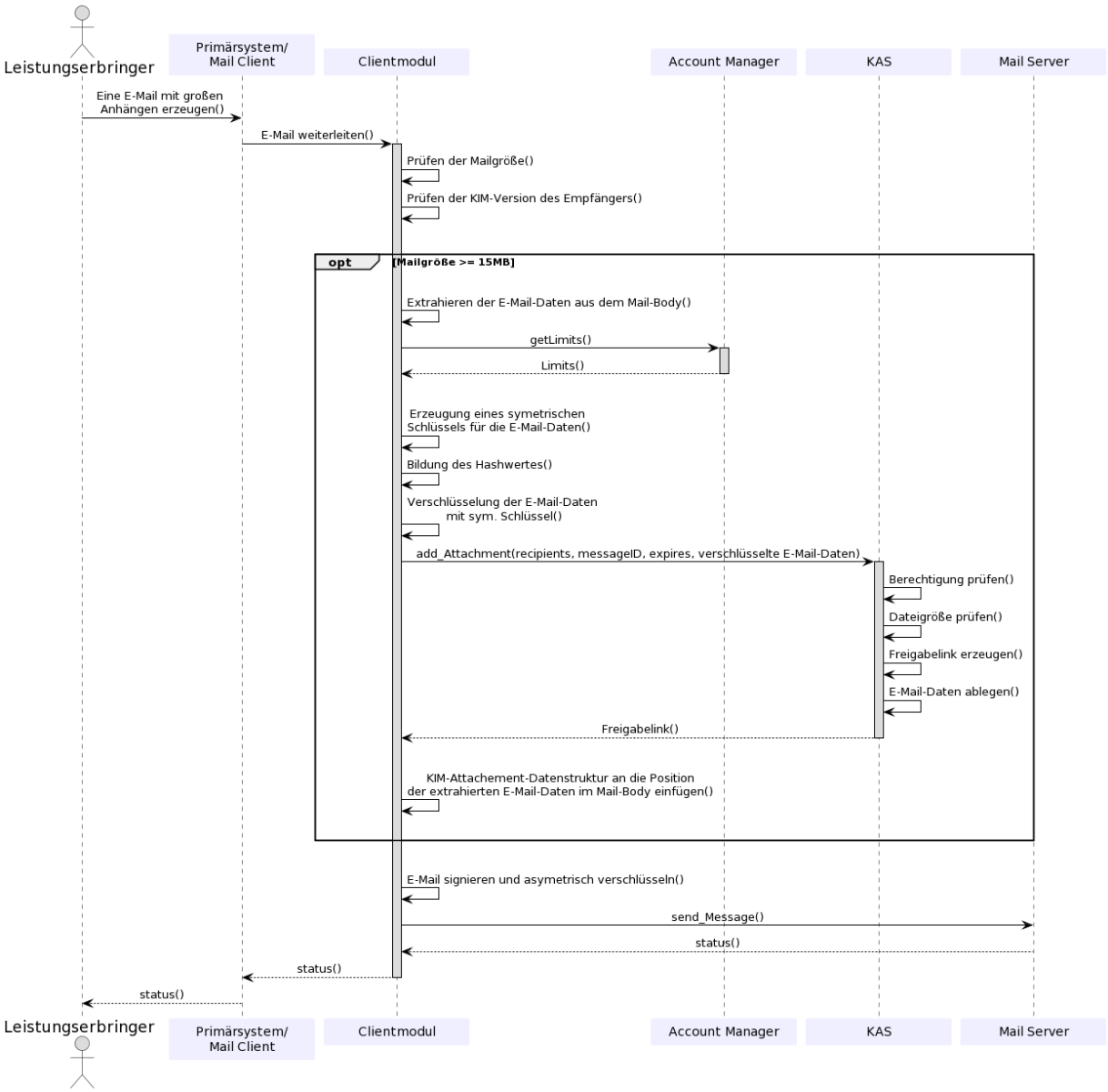

Abbildung 3 Abb_Anw_Dokument auf dem KAS hochladen

A_19380-01 - KAS – Erzeugung Freigabelink

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

[<=]

[...]

A_22410-01 - KAS – Prüfung: Aufruf des Empfängers

Der KAS MUSS das Herunterladen ~~eines Anhangesder~~ E-Mail-Daten mit dem HTTP-Fehlercode 40~~1~~3 ablehnen, wenn beim Abruf ~~des Anhangesder~~ E-Mail-Daten die Empfänger-Adresse (recipient) nicht mit einem für ~~den Anhang~~diese E-Mail-Daten beim KAS hinterlegten Empfänger (recipients) übereinstimmt.

[<=]

[...]

A_22411-01 - KAS - Zugriffs-Limitierung
Der KAS KANN den Zugriff mit dem HTTP-Fehlercode 429 verweigern, wenn eine Ressource zu oft von einem Client angefragt wird. Der KAS KANN für die Bestimmung der zulässigen Zugriffsrate folgende Faktoren berücksichtigen: Subject-DN des Clientmodul-Zertifikats, Freigabelink-URL, Anzahl der Empfänger der Ressource (~~Anhang~~E-Mail-Daten), Empfänger E-Mail-Adresse und Anzahl versuchter und erfolgreicher Downloads.
[<=]

[...]

A_22428-01 - KAS - Content-Length beim Download
Der KAS des KOM-LE-Fachdienstes MUSS bei der Übertragung ~~des Anhanges~~der E-Mail-Daten, das HTTP-Header-Element "`Content-Length`" immer mit der Gesamt-Länge des Bodys befüllen.
[<=]

[...]

A_19385-02 - KAS – Löschen von Ressource
Der Anbieter des KAS MUSS sicherstellen, dass alle gespeicherten ~~Anhänge~~E-Mail-Daten, mit abgelaufener Gültigkeit (`Expires`) gelöscht werden.
[<=]

Der Wert `Expires` (RFC822 date-time) entspricht dem Ablaufdatum ~~des Anhanges~~der E-Mail-Daten, der beim Aufruf der Operation add_Attachement() vom Clientmodule übergeben wird.

4.3 Schnittstelle I_AccountManager_Service

[...]

Tabelle 6: Operationen vom Account Manager

Operation	URI	Methode	Request	Response	Beschreibung
`registerAccount`	/account	POST	username password referenceID iniPassword kimVersion <JWT>	<Status>	Registrierung des Teilnehmers am KOM-LE-Fachdienst.
`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 <JWT>	<Status>	Aktualisierung des Accounts: - Passwort - kimVersion - dataTimeToLive
getAccount	/account/{username}	GET	username password <JWT>	<Status> username kimVersion regStat deregDate	Lesen der Account Attribute.
revokeDeregistration	/account/{username}/revokeDeregistration	GET	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_20063-03 - 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 implementieren. Des Weiteren MUSS der Account Manager für alle in der [AccountManager.yaml] definierten Operationen den Zeichensatz UTF-8 unterstützen.

[<=]

[...]

KOM-LE-A_2187-04 - 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 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 zwischen `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 Operationen:
  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.
[<=]

A_23175 - Account Manager - prüfen des Zeitraumes für die Rücknahme der Deregistrierung
Der KOM-LE Fachdienst MUSS bei Aufruf der Operation `revokeDeregistration` durch das Administrationsmodul prüfen, ob für den Benutzer-Account das `deregDate` überschritten wurde. Bei Überschreitung des `deregDate` ist eine Rücknahme der Deregistrierung zu unterbinden.
[<=]

4.4 Schnittstelle I_AccountLimit_Services

[...]

A_22413-01 - Account Manager – Implementierung der Schnittstelle
Die Teilkomponente Account Manager des Fachdienstes MUSS die Schnittstelle I_AccountLimit_Service als REST-Webservice über HTTPS gemäß [AccountLimit.yaml] in der Version 1.0.1 implementieren. Des Weiteren MUSS der Account Manager für alle in der [AccountLimit.yaml] definierten Operationen den Zeichensatz UTF-8 unterstützen.
[<=]

2.3 Anpassung - I_AccountManager_Service

Neue Operation `revokeDeregistration` für die Rücknahme einer Deregistrierung

```
/account/revokeDeregistration/{username}:
    get:
      tags:
      - Email-Account
      summary: Deregistrierung des Accounts zurücknehmen
      operationId: revokeDeregistration
      parameters:
      - name: username
        in: path
        description: Username/E-Mail des Accounts
        required: true
        schema:
          type: string
          format: email
      - in: header
        name: password
        description: Passwort für den Email-Account
        required: true
        schema:
          type: string
          format: password
      responses:
        204:
          description: Deregistrierung erolgreich zurückgenommen
        401:
          description: Authentifizierung fehlgeschlagen
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/Error'
        404:
          description: Mail Account nicht vorhanden
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/Error'
        500:
          description: Internal Server Error
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/Error'
        502:
          description: VZD nicht erreichbar bzw. liefert Fehler
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/Error'
```

2.4 Anpassung - Attachment_schema

```
{
    "title": "Structure of Attachment",
    "type": "object",
    "properties":
    {
      "name":           { "type": "string" },
      "link":           { "type": "string" },
      "k":              { "type": "string" },
      "hash":           { "type": "string" },
      "size":           { "type": "integer" },
      "type":           { "type": "string" }
    },
    "required": ["name", "link", "password", "hash", "size", "type"]
  }
```

2.5 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

Table 3 Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23169	Sicherstellung der Absenderintegrität	gemSpec_CM
A_23174	Sicherstellung der Empfängeradressen	gemSpec_CM
KOM-LE-A_2047-02	Fehlertexte bei fehlgeschlagener Entschlüsselung	gemSpec_CM
~~KOM-LE-A_2050-04~~	~~Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht~~	gemSpec_CM
KOM-LE-A_2050-05	Verhalten bei positiver Integritätsprüfung	gemSpec_CM
A_23165	Verhalten bei fehlgeschlagener Integritätsprüfung	gemSpec_CM
~~KOM-LE-A_2004~~	~~Größe einer E-Mail-Nachricht bis zu 25 MB~~	~~gemSpec_CM~~
KOM-LE-A_2004-01	Verarbeitung einer Client-Mail bis zu 15 MiB	gemSpec_CM
~~A_19366-02~~	~~Größe einer E-Mail-Nachricht größer 25 MB~~	~~gemSpec_CM~~
A_20650-05	Übermittlung von Fehlernachrichten	gemSpec_CM
A_22412-01	Behandlung von Zugriffs-Limitierung	gemSpec_CM
A_19356-05	Prüfen der Version des Empfängers	gemSpec_CM
~~A_19357-01~~	~~Extrahieren des Anhanges~~	~~gemSpec_CM~~
A_19357-02	Verarbeitung einer Client-Mail größer 15 MiB	gemSpec_CM
A_19358-01	Erzeugung symmetrischer Schlüssel	gemSpec_CM

A_19364-02	Freigabelink in die Mail aufnehmen	gemSpec_CM
A_19359-07	Einbetten von Informationen großer Nachrichten	gemSpec_CM
~~A_19360-01~~	~~Verschlüsselung der E-Mails~~	gemSpec_CM
A_19360-02	Verschlüsselung der E-Mail-Daten	gemSpec_CM
~~A_19363-02~~	~~Übertragung von Anhängen~~	~~gemSpec_CM~~
A_19363-03	Übertragung von E-Mail-Daten	gemSpec_CM
~~A_19365-01~~	~~Senden der Nachricht~~	~~gemSpec_CM~~
A_19365-02	Senden der KOM-LE-Nachricht	gemSpec_CM
A_22419-01	Behandlung von Quota-Überschreitung	gemSpec_CM
A_22427-01	I_Attachment_Services - Content-Length	gemSpec_CM
~~A_19369-01~~	~~Ermittlung der Informationen über die Anhänge~~	~~gemSpec_CM~~
A_19369-02	Ermittlung von Informationen der auf dem KAS abgelegten E-Mail-Daten	gemSpec_CM
~~A_19370-03~~	~~Download von Anhängen~~	~~gemSpec_CM~~
A_19370-04	Download von E-Mail-Daten	gemSpec_CM
~~A_19371-03~~	~~Entschlüsselung der Anhänge~~	~~gemSpec_CM~~
A_19371-04	Entschlüsselung vom KAS abgerufener E-Mail-Daten	gemSpec_CM
~~A_19372-02~~	~~Prüfen des Anhanges~~	~~gemSpec_CM~~
A_19372-03	Püfen der E-Mail-Daten	gemSpec_CM
A_19374-03	Zusammensetzen der Mail	gemSpec_CM
A_19464-03	Deregistrierungsdialog KOM-LE-Teilnehmer Administrationsmodul	gemSpec_CM

Änderungen in gemProdT_FD_KOMLE

Table 4 Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_19378~~	~~KAS – Dokumentengröße prüfen~~	~~gemSpec_FD~~
A_19375-04	Implementierung der Schnittstelle	gemSpec_FD
A_19378-01	KAS - prüfen der Größe der verschlüsselten E-Mail-Daten	gemSpec_FD
~~A_19379~~	~~KAS – Dokumentenzugriff~~	~~gemSpec_FD~~
A_19379-01	KAS – Prüfung Zugriff auf E-Mail-Daten	gemSpec_FD
A_19380-01	KAS – Erzeugung Freigabelink	gemSpec_FD
A_22410-01	KAS – Prüfung: Aufruf des Empfängers	gemSpec_FD
A_22411-01	KAS - Zugriffs-Limitierung	gemSpec_FD
A_22428-01	KAS - Content-Length beim Download	gemSpec_FD
A_19385-02	KAS – Löschen von Ressource	gemSpec_FD
A_20063-03	Account Manager - Implementierung der Schnittstelle	gemSpec_FD
KOM-LE-A_2187-04	Authentifizierung des KOM-LE-Teilnehmers über AUT-Zertifikat am AccountManager	gemSpec_FD
A_23175	Account Manager - prüfen des Zeitraumes für die Rücknahme der Deregistrierung	gemSpec_FD
A_22413-01	Account Manager – Implementierung der Schnittstelle	gemSpec_FD