Themengebiet: Änderungen in KIM 1.0 / KIM 1.5.2

C_10875

1 KIM R3.1.3-11 2

1.1 Änderung in gemSpec_CM_KOMLE 2

1.2 Änderungen in Steckbriefen 8

2 KIM 1.5.2 10

2.1 Änderung in gemSpec_CM_KOMLE 10

2.2 Änderung in gemSpec_FD_KOMLE 31

2.3 Änderung der api-kim/AttachmentService.yaml 33

2.4 Änderung der api-kim/AttachmentService.yaml 34

2.5 Änderung der api-kim/I_AccountManager_Service 35

2.6 Änderungen in Steckbriefen 36

© gematik – öffentlich_Entwurf

1 KIM R3.1.3-11

1.1 Änderung in gemSpec_CM_KOMLE

3.3.4.2.2 Integritätsprüfung

[...]

Tabelle 1: Tab_Verm_Sig_Prüf Vermerke mit Ergebnissen der Signaturprüfung

ID*	Prüfergebnis	Fehlercode	Ergebnis	Vermerk
01	VALID	-	Die Signatur der Nachricht wurde erfolgreich geprüft.	Die Signatur wurde erfolgreich geprüft.
02	INVALID	4115	Die Integrität der Nachricht wurde verletzt.	Die Prüfung der Signatur hat ergeben, dass die Nachricht manipuliert wurde.
03	INVALID	4253	Die digitale Signatur ist nicht vorhanden.	Die Nachricht ist nicht signiert. Die Nachricht ist deshalb eventuell manipuliert worden.
04	INVALID	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	4206	Der Zertifizierungspfad des Signaturzertifikats kann nicht validiert werden (abgelaufenes Zertifikat, der Zertifizierungspfad konnte nicht	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

© gematik – öffentlich_Entwurf

			aufgebaut werden usw.).	beteiligten Zertifikate validiert werden konnten.
06	INVALID	[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	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.
08	VALID	-	Die digitale Signatur ist mathematisch korrekt und der Zertifikatsstatus des Signaturzertifikats konnte erfolgreich geprüft werden, aber beim Vergleich der Header-Elemente ~~orig-date,~~ 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	-	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.

[...]

~~Zusätzlich wird eine PDF-Datei mit einem detaillierten Signaturprüfungsbericht als Anhang in die Nachricht eingefügt.~~

~~Der Dateiname des Signaturprüfungsberichtes ist Signaturpruefungsbericht.pdf und hat die folgende Struktur:~~

~~*Tab_Strukt_Sig_Prüf_Report Struktur Signaturprüfbericht*~~

Gesamtergebnis Abhängig vom Ergebnis der Signaturprüfung ist hier der Text entsprechend Vermerk aus Tabelle Tab_Verm_Sig_Prüf Vermerke mit Ergebnissen der Signaturprüfung einzufügen	
~~**A. Signaturdetails**~~	
~~Signaturzeitpunkt laut Unterzeichner:~~	~~Datum (tt.mm.jj) Uhrzeit (hh:mm:ss)~~
~~Datum der Signaturprüfung:~~	~~Datum (tt.mm.jj) Uhrzeit (hh:mm:ss)~~
~~Dokumentgröße in Bytes:~~	~~z.B.: 1987~~
~~Hashalgorithmus:~~	~~z.B.: SHA-256~~
~~Signaturalgorithmus:~~	~~z.B.: RSA Verschlüsselung mit SHA-256 Hash~~
~~Schlüssellänge in Bits:~~	~~z.B.: 2048~~

	~~Ergebnis der Prüfung der mathematischen Prüfung der Signatur (z.B.: Der vom Unterzeichner signierte Hashwert passt zu den signierten Daten)~~
~~B. Zertifikatsdetails~~	
~~Signaturzertifikatsdetails~~	
~~Inhaber des Zertifikats:~~	~~cn aus Zertifikat (z.B.: cn=Egon Mustermann)~~
~~Typ:~~	~~Nutzerzertifikat~~
~~Seriennummer (hex):~~	~~z.B.: 0x1597f~~
~~Zertifikat frühestens gültig seit:~~	~~Datum (tt.mm.jj) Uhrzeit (hh:mm:ss)~~
~~Zertifikat längstens gültig bis:~~	~~Datum (tt.mm.jj) Uhrzeit (hh:mm:ss)~~
~~Zeitpunkt der Gültigkeitsprüfung:~~	~~Datum (tt.mm.jj) Uhrzeit (hh:mm:ss)~~
~~Aussteller des Zertifikats:~~	~~dn des Ausstellers (z.B: cn=gematik SMC-B CA, o=gematik, c=de)~~
	~~Ergebnis der zeitlichen Gültigkeitsprüfung (z.B.: Zertifikat zeitlich gültig)~~
	~~Ergebnis der Prüfung der Signatur des Ausstellerzertifikats (z.B.: Das Zertifikat hat eine gültige Signatur vom Austellerzertifikat)~~
~~Herausgeberzertifikatsdetails (für alle Zertifikate in der Kette)~~	
~~Inhaber des Zertifikats:~~	~~cn aus Zertifikat (z.B.: cn=Egon Mustermann)~~
~~Typ:~~	~~Austellerzertifikat~~
~~Seriennummer (hex):~~	~~z.B.: 0x25d97f~~
~~Zertifikat frühestens gültig seit:~~	~~Datum (tt.mm.jj) Uhrzeit (hh:mm:ss)~~

~~Zertifikat längstens gültig bis:~~	~~Datum (tt.mm.jj) Uhrzeit (hh:mm:ss)~~
~~Zeitpunkt der Gültigkeitsprüfung:~~	~~Datum (tt.mm.jj) Uhrzeit (hh:mm:ss)~~
~~Aussteller des Zertifikats:~~	~~dn des Ausstellers~~
	~~Ergebnis der zeitlichen Gültigkeitsprüfung (z.B.: Zertifikat zeitlich gültig)~~
	~~Ergebnis der Prüfung der Signatur des Ausstellerzertifikats (z.B.: Das Zertifikat hat eine gültige Signatur vom Austellerzertifikat)~~
~~C. Online-Sperrabfrage für Signaturzertifikat~~	
~~Zugriff erfolgte am:~~	~~Datum (tt.mm.jj) Uhrzeit (hh:mm:ss)~~
~~OCSP-Status des Zertifikats:~~	~~good|revoked|unknown~~
~~Dienst:~~	~~URL OCSP-Responder (z.B.: http://www.gematik-smcb-ocsp.de)~~

[...]

Es folgt ein Beispiel einer entschlüsselten `multipart/mixed` Nachricht deren Signatur erfolgreich geprüft wurde. Die Nachricht enthält eine `text/plain` Einheit im Nachrichtentext und einen Arztbrief als PDF-Anhang~~sowie den Signaturprüfungsbericht ebenfalls als PDF-Anhang~~.

```
Date: Fri, 9 Feb 2012 12:07:17 +0100
MIME-Version: 1.0
From: mustermann@komle.de
To: musterfrau@komle.de
Subject: Arztbrief H. Muster
Content-Type: multipart/mixed;
X-KIM-Dienstkennung: KIM-Mail;Default;V1.0
boundary="unique-boundary-1"

This is a multi-part message in MIME format.
--unique-boundary-1
Content-Type: text/plain;    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
```

```
Sehr Geehrte Frau Dr. Musterfrau,
hiermit sende ich Ihnen den Arztbrief f=FCr Herrn H. Muster.
Mit Freundlichen Gr=FC=DFen
Dr. med. Mustermann
Arzt f=FCr Allgemeinmedizin
---------------------------------------------
Die Nachricht wurde entschl=FCsselt
Die Signatur wurde erfolgreich gepr=FCft.
--unique-boundary-1
Content-Type: application/pdf;
name="Arztbrief_Muster.pdf"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="Arztbrief_Muster.pdf"
JVBERi0xLjQNCiXDpMO8w7bDnw0KMiAwIG9iag0KPDwgL0xlbmd0aCAzIDAgUg0KICAgL0Zp
bHRlciAvRmxhdGVEZWNvZGUNCj4+DQpzdHJlYW0NCnicrVhda1sxDH0P5D/4uQ+3lvxxfaEM
...
OEJCQUExQzY0NDU+IF0NCj4+DQpzdGFydHhyZWYNCjIyNDU3Mg0KJSVFT0YNCg==
--unique-boundary-1
Content-Type: application/pdf;
name="Signaturpruefungsbericht.pdf"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="Signaturpruefungsbericht.pdf"
CjwhLS0gc2F2ZWQgZnJvbSB1cmw9KDAwMzgpaHR0cDovL2l3aS53aXdpLmh1LWJlcmxpbi5kZS9+
ZXZkb2tpbS8gLS0+CjxodG1sPjxoZWFkPjxtZXRhIGh0dHAtZXF1aXY9IkNvbnRlbnQtVHlwZSIg
...
PC9saT4KPC91bD4KCgo8L2JvZHk+PC9odG1sPg==
--unique-boundary-1--
```

[...]

KOM-LE-A_2048-01 - Prüfung der Signatur und Integrität einer KOM-LE-Nachricht

Das Clientmodul MUSS die Integrität der KOM-LE-Nachricht prüfen. Dabei müssen die digitale Signatur selbst, der Zertifizierungspfad für das verwendete Signaturzertifikat, die Integrität des Headers der äußeren Nachricht und die Integrität des `recipient-emails` Attributs geprüft werden.
Bei der Prüfung der Integrität des Headers der äußeren Nachricht sind die Header-Elemente ~~orig-date,~~ `from`, `sender`, `reply-to`, `to` und `cc` mit denen der signierten inneren Nachricht zu vergleichen.
Bei der Prüfung der Integrität des `recipient-emails` Attributs sind die Werte dieses

Attributs aus `signerInfos` und aus dem `enveloped-data` CMS-Objekt miteinander zu vergleichen.

<=

[...]

KOM-LE-A_2049-03 - Ergebnis der Signaturprüfung einer KOM-LE-Nachricht
Das Clientmodul MUSS das Ergebnis der Signaturprüfung der KOM-LE-Nachricht als Vermerk an den Text der Nachricht anhängen.~~Zusätzlich MUSS das Clientmodul eine PDF-Datei mit einem detaillierten Signaturprüfungsbericht als Anhang in die Nachricht einfügen. Der Name der PDF-Datei MUSS sich aus dem Wort "*Signaturpruefungsbericht*" und dem aktuellen minutengenauen Zeitstempel zusammensetzen. Es ist folgendes Format gemäß ISO 8601 anzuwenden:*Signaturpruefungsbericht_JJJJMMTT_hhmm.pdf*~~

<=

~~Durch die beschriebene Benamung des "Signaturpruefungsbericht" soll lediglich die Eindeutigkeit des Namens der erzeugten Datei sichergestellt werden.~~

KOM-LE-A_2180 - Struktur des Signaturprüfberichts
~~Der vom Clientmodul in einer PDF-Datei zu erzeugende Signaturprüfungsbericht MUSS der in Tabelle Tab_Strukt_Sig_Prüf_Report Struktur Signaturprüfbericht beschriebenen Struktur entsprechen.~~

<=

KOM-LE-A_2050-04 - Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht

Das Clientmodul MUSS abhängig vom Ergebnis der Signaturprüfung einer KOM-LE-Nachricht die in Tabelle Tab_Verm_Sig_Prüf definierten Vermerke 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.

<=

1.2 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

Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
KOM-LE-A_2048-01	Prüfung der Signatur und Integrität einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM-LE-A_2049-03	Ergebnis der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
~~KOM-LE-A_2180~~	~~Struktur des Signaturprüfberichts~~	gemSpec_CM_KOMLE
KOM-LE-A_2050-04	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE

Tabelle 3 Anforderungen zur sich.Techn. Eignung: "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
KOM-LE-A_2048-01	Prüfung der Signatur und Integrität einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM-LE-A_2050-04	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE

2 KIM 1.5.2

2.1 Änderung in gemSpec_CM_KOMLE

3.1 Allgemeine Anforderungen

[...]

A_20650-03 - Übermittlung von Fehlernachrichten
Das KOM-LE-Clientmodul MUSS bei der Übertragung von Fehlernachrichten ~~zum Fachdienst~~ ein Mail-Header-Attribut `X-KIM-Fehlermeldung` mit dem Wert aus der Tabelle Tab_Fehlercodes_KOMLE-Clientmodule befüllen.
[<=]

Tabelle 4 Tab_Fehlercodes_KOMLE-Clientmodule

Fehler	Wert
Empfänger entfernt, wegen falscher ~~KOM-LE~~ KIM-Version	~~cmgerr_1~~ 4001
Anhang konnte nicht zum KOM-LE-Attachment-Service übertragen werden	~~cmgerr_2~~ 4002
Anhang konnte nicht vom KOM-LE-Attachment-Service geladen werden	~~cmgerr_3~~ 4003
keine eindeutige Telematik-ID mit Verschlüsselungszertifikat gefunden	~~cmgerr_4~~ 4004
Nachricht nicht für alle Empfänger verschlüsselbar	~~cmgerr_5~~ 4005
Für einen Empfänger existieren mehrere Verschlüsselungszertifikate mit unterschiedlichen Telematik-IDs	4008
beim Entschlüsseln eines Anhangs ist ein Fehler aufgetreten	4009
Das verwendete Client-Modul unterstützt die in der Mail verwendete Version nicht	4010

© gematik – öffentlich_Entwurf

Die KIM-Nachricht konnte auf Grund eines nicht verfügbaren Schlüssels nicht entschlüsselt werden	4011
Die KIM-Nachricht konnte aufgrund des falschen Formats nicht entschlüsselt werden	4012
Der Konnektor steht für die Entschlüsselung nicht zur Verfügung	4013
Bei der Aktualisierung der PKCS#12-Datei ist ein Fehler aufgetreten	4014
Die KIM-Version des Client-Moduls ist kleiner als die im Verzeichnisdienst zu seinem Eintrag hinterlegte Version	4015
Die Prüfsumme des Anhangs stimmt nicht mit der dem Anhang beigefügten Prüfsumme überein. Der empfangene Anhang entspricht eventuell nicht dem originalen Anhang	4016
Anhang konnte nicht heruntergeladen werden, da durch zu häufigen Zugriff der KOM-LE-Attachment-Service den Abruf verweigert.	4017
Übernahme der Fehlercodes und Vermerke aus der Tabelle Tab_Verm_Sig_Prüf	[Fehlercode]

Die Fehlermeldungen beim Senden einer KIM-Mail ~~des Clientmodules~~ werden über den Fachdienst zurück an den Sender übermittelt, da eine direkte Rückgabe der Fehlernachricht zum Client nicht vorgesehen ist. Das Clientmodul befüllt im Fehlerfall das `X-KIM-Fehlermeldung`-Attribut und sendet dies anschließend über den Fachdienst an den Sender zurück. Die Fehlermeldungen beim Empfang einer KIM-Mail werden auf direkten Weg dem Empfänger zugestellt. Der Client (z. B. PVS) kann ~~diesen~~ die Fehlercodes aus der Tabelle Tab_Fehlercodes_KOMLE-Clientmodule ~~anschließend~~ auswerten.

[...]

Unter der Anforderung "A_20189-02 - Übermittlung der benötigten KOM-LE Version des Clientmoduls" wird der folgende Text ergänzt:

Die Übermittlung der KOM-LE-Version vom Anbieter kann hierbei postalisch erfolgen. Die jeweilige Client-Version kann aus dem LDAP-Directory Attribut: KOM-LE-Version vom VZD entnommen werden. Geltende KOM-LE-Versionen sind `1.0`, `1.5` und `2.0` und werden in der Form in das Header-Element KOM-LE-Version eingetragen.

[...]

A_21388-01 - Übermittlung der Clientmodul- und Produkttypversion
Das Clientmodul MUSS im Header Element `X-KIM-CMVersion` der äußeren Nachricht die VendorID, sowie die Produktversion des verwendeten Clientmoduls gemäß ~~den Vorgaben aus [gemSpec_OM] eintragen.~~ des Formates:
"[a-zA-Z0-9_]{1,5}_[0-9]{1,2}\.[0-9]{1,2}\.[0-9]{1,2}(-25[0-5]|-2[0-4][0-9]|-[0-1]?[0-9]?[0-9]){0,1}" eintragen.

Zusätzlich MUSS das Clientmodul im Header Element `X-KIM-PTVersion` der äußeren Nachricht die Produkttypversion des Clientmoduls gemäß ~~den Vorgaben aus [gemSpec_OM]~~ des Formates
"[0-9]{1,2}\.[0-9]{1,2}\.[0-9]{1,2}(-25[0-5]|-2[0-4][0-9]|-[0-1]?[0-9]?[0-9]){0,1}"eintragen.

Zusätzlich MUSS das Clientmodul im Header-Element `X-KIM-KONVersion` der äußeren Nachricht die Version des verwendeten Konnektors gemäß seiner Produktversion im Format "<Productname><ProductType><ProductTypeVersion><HWVersion><FWVersion> eintragen.
[<=]

Beispiel:
```
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>

3.2.1 Senden von Nachrichten mit großen Anhängen

[...]

A_19356-04 - 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: `KOM-LE-Version` aus dem Verzeichnisdienst [gemSpec_VZD#5] abfragen. Ist das LDAP-Directory Attribut: `KOM-LE-Version` undefiniert, dann muss ein KOM-LE-Clientmodul mit einer Version 1.0 angenommen werden.

Wenn eine Mail größer als 25 MB an einen Empfänger mit KOM-LE-Version < 1.5 versendet werden soll, MUSS das KOM-LE-Clientmodul diesen Empfänger aus der Mail entfernen~~und den Fehler X.3.3 gemäß [RFC3463] an den sendenden KOM-LE-Client zurückgeben~~. 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, dem Enhanced-StatusCodes „X.3.3" und der entsprechenden Fehlermeldung über den Fehlerfall informiert.**[<=]**

A_22340 - 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 unterstützen.**[<=]**

[...]

A_22341 - Prüfen der Nachrichtenanhänge
Das KOM-LE-Clientmodul MUSS die vom KOM-LE-Client erhaltene Nachricht auf Vorhandensein von MIME konformen Content-Headern mit Content-Type: `text/plain; charset=utf-8` sowie ein `Content-Disposition: x-kas` prüfen. Ist mindestens ein derartiger Content-Header in der Nachricht enthalten, wird dem KOM-LE-Client der SMTP-Antwortcode 451 mit dem Enhanced-StatusCodes "X.6.1" und die entsprechende Fehlermeldung "Media not supported" zurückgegeben.**[<=]**

A_19359-06 - Einbetten von Informationen großer Anhänge
Das KOM-LE-Clientmodul MUSS für jeden auf dem KAS abgelegten Anhang die folgende KIM-Attachment-Datenstruktur gemäß [Attachment_Schema] - an der Position des extrahierten Anhanges im Mail-Body - einfügen:

Tabelle 5 KIM-Attachment-Datenstruktur

Attribut in KIM-Attachment-Datenstruktur	Wert
`name`	Dateiname des Anhangs
`link`	Freigabelink des Anhangs
`k`	AES-GCM Key des Anhangs (symmetrischer Schlüssel) im Base64 Format
`hash`	Hashwert des Anhangs (entsprechend A_19644 [gemSpec_Krypt] zu bilden) im Base64 Format
`type`	MIME-Type des Anhanges
`size`	Größe des Anhangs 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.**[<=]**

[...]


```
  {
    "name":     "MR-2020-04-01-xyz.doc",
    "link":     "HTTPS://KIM-
FD1.telematik.de/CXFDTE82346dfzwr7634dfs76sd76sdtzq376e3tzsd",
    "k":        "RzVEY3M0MzkmNGZkc2RneCVoX2tkdFQlNXczZnZDdDM2ZGZ2eGZzJDYxIT
JndmR1VWpzKGk=",
    "hash":     "fcf7c1b8749cf99d88c5f34271d636178fb5d130
Z6A65Z2dasI2I00mM7uxtQjLsEwwl+WLMnDw8eLntaA=",
    "size":     143271,
    "type":     "application/msword"
   }
```


[...]


```
  {
    "name":     "Roentgenbild-375632378.jpg",
    "link":     "HTTPS://KIM-
FD1.telematik.de/Cduiz763478dfjkdfjhgow4784JHKZsdtq376e3t478d",
    "k":        "Ry80ZmRpdWhjczQzOSY0ZmRzZGd4JWhfa2R0VCU1dzNmdkzZkYXNlcmZnO
DkzNDV1aXNyZg==",
    "hash":     "fawer3q04985ofisdjüu3945ucg09j09309u3gj0o
tHp30Rx6T9aX8PUmyuASDDIAJ2lPAwbPdc5OSAMK49I=",
    "size":     32573,
    "type":     "image/jpeg"
   }
```


3.2.2 Empfangen von Nachrichten mit großen Anhängen

[...]

A_19371-03 - Entschlüsselung der Anhänge
Das KOM-LE-Clientmodul MUSS die heruntergeladenen Anhänge mit dem symmetrischen Schlüssel entschlüsseln.

Wenn beim Entschlüsseln eines Anhangs 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` 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. ~~Als~~ Im Betreff ~~ist Folgendes zu verwenden~~ der

entschlüsselten Nachricht ist Folgendes anzugeben:~~Subject:~~[Fehler beim Entschlüsseln eines Anhangs *_Fehlermeldung.txt] <Original-Subject>.
[<=]

A_19372-02 - Prüfen des Anhanges
Das KOM-LE-Clientmodul MUSS den Hash-Wert des entschlüsselten Anhanges entsprechend A_19644 bilden und mit dem aus dem Content-Header des Anhangs im Mail-Body entnommenen Hash-Wert vergleichen. Bei einer Nichtübereinstimmung MUSS das KOM-LE-Clientmodul die Nachricht dem Clientsystem mit dem Anhang und einem entsprechenden Vermerk zum Anhang übergeben.

Das KOM-LE-Clientmodul MUSS den Vermerk mit der folgenden Bildungsregel an den Text der Nachricht anhängen ~~aufnehmen~~:
"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.

[<=]

[...]

3.3.2.2 Verbindungsaufbau mit dem MTA

Der Aufbau des SMTP-Benutzernamens entspricht somit dem folgenden Muster und hat der den Parametern vorangestellten Nummer in der Reihenfolge zu entsprechen:

[0] Benutzername
[1] <Domain Adresse des SMTP-Servers>:<Port>
[2] MandantId
[3] ClientsystemId
[4] WorkplaceId
— <optional> —
[5] UserId
[6] KonnektorId
[...]

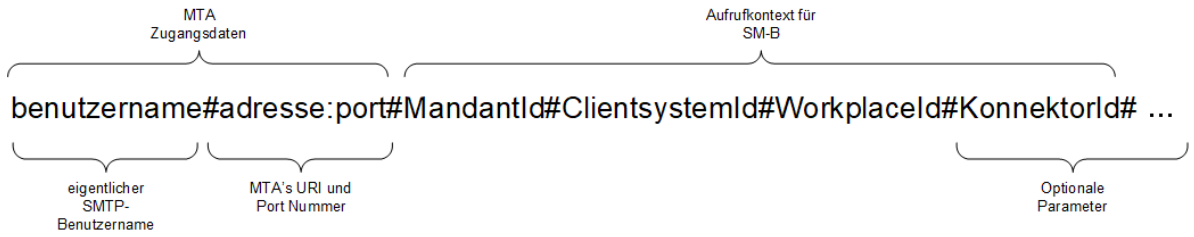

Abbildung 1: Abb_MTA_Nutzername Format des SMTP- Benutzernamens

[...]

A_21519-02 - Überprüfung des SMTP-Benutzernames

Das Clientmodul MUSS die übergebene SMTP-Benutzername-Zeichenkette auf Vollständigkeit überprüfen. ~~Das heißt, auch wenn der optionale Parameter im Aufrufkontext für SM-B nicht benötigt wird muss dieser durch den Plattzhalter ("*") gesetzt sein.~~ Werden optionale Bestandteile des SMTP-Benutzernamens nicht genutzt, MUSS sichergestellt werden, dass später folgende optionale Bestandteile in ihrer vorgegebenen Position platziert werden. Als Platzhalter ist in so einem Fall "*" zu verwenden. Wenn die SMTP-Benutzername-Zeichenkette nicht vollständig ist, MUSS das Clientmodul den SMTP Fehlercode gemäß Tabelle "Tab_SMTP_Verbindung SMTP-Antwortcodes für MTA-Verbindungsaufbau" an das Clientsystem senden und den Vorgang abbrechen.
[<=]

Beispiel einer vollständigen SMTP-Benutzername-Zeichenkette:

ohne optionale Bestandteile:

`erik.mustermann@hrst_domain.kim.telematik#hrst_domain.kim.telematik:995#1#KOM_LE#7`

`erik.mustermann@hrst_domain.kim.telematik#hrst_domain.kim.telematik:995#1#KOM_LE#7#*`

`KonnektorId` als optionaler Bestandteil:

`erik.mustermann@hrst_domain.kim.telematik#hrst_domain.kim.telematik:995#1#KOM_LE#7#Konn_1`

[...]

3.3.4.1.1 Bearbeitung einer ungeschützten Nachricht

[...]

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~~, die weder zu signieren noch zu verschlüsseln ist,~~ informieren. Die Fehlernachricht ist weder zu signieren noch zu verschlüsseln und entspricht der Delivery Status Notification gemäß [RFC3461-3464]. **[<=]**

[...]

KOM-LE-A_2024-01 - Information des Absenders über Empfänger, für die nicht verschlüsselt werden kann
Kann eine Nachricht auf Grund von fehlenden oder ungültigen Zertifikaten nicht für alle Empfänger verschlüsselt werden, MUSS das Clientmodul den Absender mit einer E-Mail über den Fehlerfall informieren. Aus dem Inhalt der Fehlernachricht müssen alle Empfänger, für die nicht verschlüsselt werden konnte, hervorgehen. Die Fehlernachricht

ist weder zu signieren noch zu verschlüsseln und entspricht der Delivery Status Notification gemäß [RFC3461-3464]. Die Originalnachricht darf an die Empfänger, für die nicht verschlüsselt werden konnte, nicht versendet werden.
[<=]

3.4.2.2 Verbindungsaufbau mit dem POP3-Server

Die Reihenfolge der Parameter entspricht dem folgenden Muster und hat der den Parametern vorangestellten Nummer in der Reihenfolge zu entsprechen:

[0] Benutzername
[1] <Domain Adresse des POP3-Servers>:<Port>
[2] MandantId
[3] ClientsystemId
[4] WorkplaceId
— <optional> —
[5] UserId
[6] KonnektorId
[...]

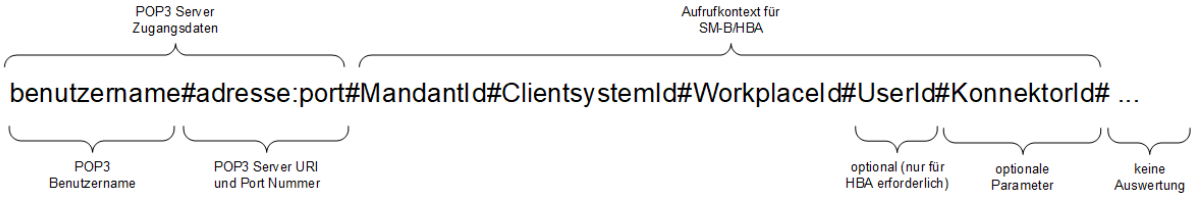

Abbildung 2: Abb_POP3_Nutzer_Name Format des POP3- Benutzernamens

[...]

A_21518-02 - Überprüfung des POP3-Benutzernames
Das Clientmodul MUSS die übergebene POP3-Benutzername-Zeichenkette auf Vollständigkeit überprüfen. ~~Das heißt, auch wenn die optionalen Parameter im Aufrufkontext für SM-B/HBA nicht benötigt werden müssen diese durch den Plattzhalter ("*") gesetzt sein.~~ Werden optionale Bestandteile des POP3-Benutzernamens nicht genutzt, MUSS sichergestellt werden das später folgende optionale Bestandteile in ihrer vorgegebenen Position platziert werden. Als Platzhalter ist in so einem Fall "*" zu verwenden. Wenn die POP3-Benutzername-Zeichenkette nicht vollständig ist, MUSS das Clientmodul den POP3 Fehlercode gemäß Tabelle "Tab_POP3_Verbindung Antwortcodes für POP3-Server-Verbindungsaufbau" an das Clientsystem senden und den Vorgang abbrechen.
[<=]

Beispiel einer vollständigen POP3-Benutzername-Zeichenkette:

ohne optionale Bestandteile:

```
erik.mustermann@hrst_domain.kim.telematik#hrst_domain.kim.telematik:995#1#KOM_LE#7
```

`erik.mustermann@hrst_domain.kim.telematik#hrst_domain.kim.telematik:995#1#KOM_LE#7#*`

`erik.mustermann@hrst_domain.kim.telematik#hrst_domain.kim.telematik:995#1#KOM_LE#7##`

nur`UserId` als optionaler Bestandteil:

`erik.mustermann@hrst_domain.kim.telematik#hrst_domain.kim.telematik:995#1#KOM_LE#7#13`

`erik.mustermann@hrst_domain.kim.telematik#hrst_domain.kim.telematik:995#1#KOM_LE#7#13#*`

keine `UserId` jedoch die`KonnektorId`:

`erik.mustermann@hrst_domain.kim.telematik#hrst_domain.kim.telematik:995#1#KOM_LE#7#*#Konn_1`

`UserId` und `KonnektorId` als optionale Bestandteile:

`erik.mustermann@hrst_domain.kim.telematik#hrst_domain.kim.telematik:995#1#KOM_LE#7#13#Konn_1`

[...]

3.4.4.1 Empfang und Weiterleitung einer Nachricht

[...]

A_21391-02 - Auswertung des X-KOM-LE-Version Header Elements
Das Clientmodul MUSS prüfen, ob das Header-Element X-KOM-LE-Version in der äußeren Nachricht eine vom Clientmodul unterstützte Version enthält. Wenn das nicht der Fall ist, 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, "~~Das verwendete Client-Module unterstützt die in der Mail verwendete Version nicht~~ Das verwendete Clientmodul unterstützt die in der empfangenen Nachricht angegebene KIM-Version `<KIMVersion>` nicht." 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~~KIM Version wird nicht unterstützt~~ KIM-Version der empfangenen Nachricht wird nicht unterstützt".
[<=]

Bei einer Nachricht mit dem Subject „Die ~~KIM Version wird nicht unterstützt~~ KIM-Version der empfangenen Nachricht wird nicht unterstützt" 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 dieser Nachricht die Aufbereitung wiederholt.

Für die Entschlüsselung und die Signaturprüfung verwendet das Clientmodul die Dienste der TI-Plattform, die dem Clientmodul über Schnittstellen des Konnektors zur Verfügung gestellt werden.

Für die vereinfachte Darstellung wird im Folgenden ein Beispiel einer Fehlernachricht ohne die Originalnachricht dargestellt:

```
From: "Sender" <sender@maildomain.de>
To: <empfaenger@maildomain.de>
Message-Id: <II8HEDLEUEU4.EG0B98QUZNPM2@STST-TEST>
Subject: Die KIM-Version der empfangenen Nachricht wird nicht unterstützt
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="=-hDUtypluINBWKuVpu2reTw=="

--=-hDUtypluINBWKuVpu2reTw==
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: quoted-printable

Das verwendete Clientmodul  unterstützt die in der empfangenen
Nachricht angegebene KIM-Version [2.0] nicht.
Das verwendete Clientmodul unterstützt Nachrichten einer KIM-
Version [1.5] und kleiner.

Es wird empfohlen, das verwendete Clientmodul zu aktualisieren!
Leiten Sie diese Mail an Ihre eigene KIM-E-Mail-Adresse weiter, um die
Nachrichtenverarbeitung beim nächsten Abruf der Nachricht zu
wiederholen.
```

3.4.4.2.1 Entschlüsselung

[...]

Bei einer Nachricht mit dem Subject „Die Nachricht konnte nicht entschlüsselt werden" 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 dieser Nachricht die Aufbereitung wiederholt.

Tab_Fehlertext_Entschl Fehlertexte für Entschlüsselungsfehler

Bedingung	Fehlertexte

Die KOM-LE-Nachricht konnte auf Grund eines nicht verfügbaren Schlüssels nicht entschlüsselt werden.	Der für die Entschlüsselung der Nachricht benötigte Schlüssel wurde nicht gefunden. Überprüfen Sie ob die entsprechende Karte gesteckt ist und leiten Sie diese Nachricht an Ihre eigene E-Mail-Adresse (<Email Adresse>) weiter. Beim nächsten Abholen wird der Entschlüsselungsvorgang wiederholt.
Die KOM-LE-Nachricht konnte aufgrund des falschen Formats nicht entschlüsselt werden (z.B. enthält die Nachricht das X-KOM-LE-Version Header-Element, entspricht aber nicht dem KOM-LE-S/MIME-Profil).	Die Nachricht wurde als eine verschlüsselte ~~KOM-LE~~ KIM-Nachricht gekennzeichnet, konnte aber auf Grund des falschen Formats nicht entschlüsselt werden. Die Verschlüsselte Nachricht befindet sich im Anhang.
Der Konnektor steht für die Entschlüsselung nicht zur Verfügung.	Die Entschlüsselung konnte nicht erfolgen, weil der Konnektor nicht antwortet. Stellen Sie sicher, dass der Konnektor wieder zur Verfügung steht und leiten Sie diese Nachricht an Ihre eigene E-Mail-Adresse (<Email Adresse>) weiter. Beim nächsten Abholen wird der Entschlüsselungsvorgang wiederholt.

KOM-LE-A_2047-01 - Fehlertexte bei fehlgeschlagener Entschlüsselung
Das Clientmodul MUSS bei fehlgeschlagener Entschlüsselung entsprechend der jeweiligen Bedingung die in Tabelle Tab_Fehlertext_Entschl definierten Fehlertexte in die `text/plain` MIME-Einheit der multipart/mixed MIME-Fehlernachricht aufnehmen.
[<=]

[...]

3.4.4.2.2 Integritätsprüfung

Tabelle 6: Tab_Verm_Sig_Prüf Vermerke mit Ergebnissen der Signaturprüfung

ID*	Prüfergebnis	Fehlercode	Ergebnis	Vermerk
01	VALID	-	Die Signatur der Nachricht wurde erfolgreich geprüft.	Die Signatur wurde erfolgreich geprüft.
02	INVALID	4115	Die Integrität der Nachricht wurde verletzt.	Die Prüfung der Signatur hat ergeben, dass die Nachricht manipuliert wurde.
03	INVALID	4253	Die digitale Signatur ist nicht vorhanden.	Die Nachricht ist nicht signiert. Die Nachricht ist deshalb eventuell manipuliert worden.
04	INVALID	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	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	[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	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.
08	VALID	cmgerr_6	Die digitale Signatur ist mathematisch korrekt und der Zertifikatsstatus des Signaturzertifikats konnte erfolgreich geprüft werden, aber beim Vergleich der Header-Elemente ~~orig-date,~~ 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	cmgerr_7	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.

~~Zusätzlich wird eine PDF-Datei mit einem detaillierten Signaturprüfungsbericht als Anhang in die Nachricht eingefügt.~~

~~Der Dateiname des Signaturprüfungsberichtes ist Signaturpruefungsbericht.pdf und hat die folgende Struktur:~~

~~**Tabelle 7: Tab_Strukt_Sig_Prüf_Report Struktur Signaturprüfbericht**~~

~~Gesamtergebnis~~ ~~Abhängig vom Ergebnis der Signaturprüfung ist hier der Text entsprechend Vermerk aus Tabelle Tab_Verm_Sig_Prüf Vermerke mit Ergebnissen der Signaturprüfung einzufügen~~	
~~**A. Signaturdetails**~~	
~~Signaturzeitpunkt laut Unterzeichner:~~	~~Datum (tt.mm.jj) Uhrzeit (hh:mm:ss)~~
~~Datum der Signaturprüfung:~~	~~Datum (tt.mm.jj) Uhrzeit (hh:mm:ss)~~
~~Dokumentgröße in Bytes:~~	~~z.B.: 1987~~
~~Hashalgorithmus:~~	~~z.B.: SHA-256~~
~~Signaturalgorithmus:~~	~~z.B.: RSA Verschlüsselung mit SHA-256 Hash~~
~~Schlüssellänge in Bits:~~	~~z.B.: 2048~~
	~~Ergebnis der Prüfung der mathematischen Prüfung der Signatur (z.B.: Der vom Unterzeichner signierte Hashwert passt zu den signierten Daten)~~
~~**B. Zertifikatsdetails**~~	
~~Signaturzertifikatsdetails~~	
~~Inhaber des Zertifikats:~~	~~cn aus Zertifikat (z.B.: cn=Egon Mustermann)~~
~~Typ:~~	~~Nutzerzertifikat~~
~~Seriennummer (hex):~~	~~z.B.: 0x1597f~~
~~Zertifikat frühestens gültig seit:~~	~~Datum (tt.mm.jj) Uhrzeit (hh:mm:ss)~~
~~Zertifikat längstens gültig bis:~~	~~Datum (tt.mm.jj) Uhrzeit (hh:mm:ss)~~

~~Zeitpunkt der Gültigkeitsprüfung:~~	~~Datum (tt.mm.jj) Uhrzeit (hh:mm:ss)~~
~~Aussteller des Zertifikats:~~	~~dn des Ausstellers (z.B: cn=gematik SMC-B CA, o=gematik, c=de)~~
	~~Ergebnis der zeitlichen Gültigkeitsprüfung (z.B.: Zertifikat zeitlich gültig)~~
	~~Ergebnis der Prüfung der Signatur des Ausstellerzertifikats (z.B.: Das Zertifikat hat eine gültige Signatur vom Austellerzertifikat)~~
~~Herausgeberzertifikatsdetails (für alle Zertifikate in der Kette)~~	
~~Inhaber des Zertifikats:~~	~~cn aus Zertifikat (z.B.: cn=Egon Mustermann)~~
~~Typ:~~	~~Austellerzertifikat~~
~~Seriennummer (hex):~~	~~z.B.: 0x25d97f~~
~~Zertifikat frühestens gültig seit:~~	~~Datum (tt.mm.jj) Uhrzeit (hh:mm:ss)~~
~~Zertifikat längstens gültig bis:~~	~~Datum (tt.mm.jj) Uhrzeit (hh:mm:ss)~~
~~Zeitpunkt der Gültigkeitsprüfung:~~	~~Datum (tt.mm.jj) Uhrzeit (hh:mm:ss)~~
~~Aussteller des Zertifikats:~~	~~dn des Ausstellers~~
	~~Ergebnis der zeitlichen Gültigkeitsprüfung (z.B.: Zertifikat zeitlich gültig)~~
	~~Ergebnis der Prüfung der Signatur des Ausstellerzertifikats (z.B.: Das Zertifikat hat eine gültige Signatur vom Austellerzertifikat)~~
~~C. Online-Sperrabfrage für Signaturzertifikat~~	
~~Zugriff erfolgte am:~~	~~Datum (tt.mm.jj) Uhrzeit (hh:mm:ss)~~
~~OCSP-Status des Zertifikats:~~	~~good|revoked|unknown~~

~~Dienst:~~	~~URL OCSP-Responder (z.B.: http://www.gematik-smcb-ocsp.de)~~

[...]

Es folgt ein Beispiel einer entschlüsselten `multipart/mixed` Nachricht deren Signatur erfolgreich geprüft wurde. Die Nachricht enthält eine `text/plain` Einheit im Nachrichtentext und einen Arztbrief als PDF-Anhang~~sowie den Signaturprüfungsbericht ebenfalls als PDF-Anhang~~.

```
Date: Fri, 9 Feb 2012 12:07:17 +0100
MIME-Version: 1.0
From: mustermann@komle.de
To: musterfrau@komle.de
Subject: Arztbrief H. Muster

Content-Type: multipart/mixed;
X-KIM-Dienstkennung: KIM-Mail;Default;V1.0
boundary="unique-boundary-1"

This is a multi-part message in MIME format.
--unique-boundary-1
Content-Type: text/plain;    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

Sehr Geehrte Frau Dr. Musterfrau,

hiermit sende ich Ihnen den Arztbrief f=FCr Herrn H. Muster.

Mit Freundlichen Gr=FC=DFen
Dr. med. Mustermann

Arzt f=FCr Allgemeinmedizin

----------------------------------------------
Die Nachricht wurde entschl=FCsselt
Die Signatur wurde erfolgreich gepr=FCft.
--unique-boundary-1
Content-Type: application/pdf;
name="Arztbrief_Muster.pdf"
Content-Transfer-Encoding: base64
```

```
Content-Disposition: attachment;
filename="Arztbrief_Muster.pdf"

JVBERi0xLjQNCiXDpMO8w7bDnw0KMiAwIG9iag0KPDwgL0xlbmd0aCAzIDAgUg0KICAgL0Zp
bHRlciAvRmxhdGVEZWNvZGUNCj4+DQpzdHJlYW0NCnicrVhda1sxDH0P5D/4uQ+3lvxxfaEM
...
OEJCQUExQzY0NDU+IF0NCj4+DQpzdGFydHhyZWYNCjIyNDU3Mg0KJSVFT0YNCg==
--unique-boundary-1
Content-Type: application/pdf;
name="Signaturpruefungsbericht.pdf"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="Signaturpruefungsbericht.pdf"

CjwhLS0gc2F2ZWQgZnJvbSB1emw9KDAwMzgpaHR0cDovL2l3aS53aXdpLmh1LWJlemxpbi5kZS9+
ZXZkb2tpbS8gLS0+CjxodG1sPjxoZWFkPjxtZXRhIGh0dHAtZXF1aXY9IkNvbnRlbnQtVHlwZSIg
...
PC9saT4KPC91bD4KCgo8L2JvZHk+PC9odG1sPg==
--unique-boundary-1--
```


[...]

KOM-LE-A_2048-01 - Prüfung der Signatur und Integrität einer KOM-LE-Nachricht
Das Clientmodul MUSS die Integrität der KOM-LE-Nachricht prüfen. Dabei müssen die digitale Signatur selbst, der Zertifizierungspfad für das verwendete Signaturzertifikat, die Integrität des Headers der äußeren Nachricht und die Integrität des `recipient-emails` Attributs geprüft werden.
Bei der Prüfung der Integrität des Headers der äußeren Nachricht sind die Header-Elemente ~~orig-date,~~ `from`, `sender`, `reply-to`, `to` und `cc` mit denen der signierten inneren Nachricht zu vergleichen.
Bei der Prüfung der Integrität des `recipient-emails` Attributs sind die Werte dieses Attributs aus `signerInfos` und aus dem `enveloped-data` CMS-Objekt miteinander zu vergleichen.
[<=]

KOM-LE-A_2049-03 - Ergebnis der Signaturprüfung einer KOM-LE-Nachricht
Das Clientmodul MUSS das Ergebnis der Signaturprüfung der KOM-LE-Nachricht als Vermerk an den Text der Nachricht anhängen.~~Zusätzlich MUSS das Clientmodul eine PDF-Datei mit einem detaillierten Signaturprüfungsbericht als Anhang in die Nachricht einfügen. Der Name der PDF-Datei MUSS sich aus dem Wort "*Signaturpruefungsbericht*" und dem aktuellen minutengenauen Zeitstempel zusammensetzen. Es ist folgendes Format gemäß ISO 8601 anzuwenden:*Signaturpruefungsbericht_JJJJMMTT_hhmm.pdf*~~
[<=]

~~Durch die beschriebene Benamung des "*Signaturpruefungsbericht*" soll lediglich die Eindeutigkeit des Namens der erzeugten Datei sichergestellt werden.~~

~~**KOM-LE-A_2180 - Struktur des Signaturprüfberichts**~~

~~Der vom Clientmodul in einer PDF-Datei zu erzeugende Signaturprüfungsbericht MUSS der in Tabelle Tab_Strukt_Sig_Prüf_Report Struktur Signaturprüfbericht beschriebenen Struktur entsprechen.~~

~~<=~~

[...]

KOM-LE-A_2050-04 - Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht
Das Clientmodul MUSS abhängig vom Ergebnis der Signaturprüfung einer KOM-LE-Nachricht die in Tabelle Tab_Verm_Sig_Prüf definierten Vermerke 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.
[<=]

3.7.1 Allgemeine Anforderungen

[...]

A_19456-02 - Domain Fachdienst Administrationsmodul
Das Administrationsmodul MUSS die ~~Konfiguration der Domain~~ Auswahl der genutzten Fachdienste ermöglichen.
[<=]

3.8.1 Erstellung der digitalen Signatur einer Nachricht mit einer SM-B

[...]

Die Signatur der KOM-LE-Nachricht erfolgt unter Verwendung der `SignDocument` Operation des Konnektors. Dabei werden die Parameter `Context` (dem Sender entsprechender Aufrufkontext), `CardHandle` (Handle der ausgewählten SM-B), `KeyReference` (C.OSIG_RSA ~~oder C.OSIG_ECC~~) verwendet. Die Verwendung weiterer Parameter muss unter Berücksichtigung der Anforderungen aus [gemSMIME_KOMLE] erfolgen.

4.1.1 Allgemeine Festlegungen

KOM-LE-A_2064-02 - Verwendung von X.509-Identitäten bei der TLS-Authentifizierung
Das Clientmodul KOM-LE MUSS bei der Verwendung von X.509-Identitäten für die TLS-Authentifizierung sowie dem Aufbau von TLS-Verbindungen die Vorgaben aus [gemSpec_Krypt] beachten. Hierbei sind ~~für die Schnittstelle Clientsystem-Clientmodul~~ zusätzlich auch Cipher-Suites und Kurven aus [BSI-TR-02102-2] Kapitel 3.3 akzeptabel um Kompatibilität mit gängigen Clientsystemen und PVSen bzw. Mailclients, sowie gängigen Plattformen für Fachdienste sicherzustellen.
[<=]

4.1.4 Transportsicherung zwischen Clientmodul und Fachdienst

Die Verbindungen zwischen KOM-LE-Clientmodul und KOM-LE-Fachdiensten (inklusive KAS) ~~sowie zwischen KOM-LE-Clientmodul und Verzeichnisdienst~~ erfolgen immer über TLS. Der TLS Handshake zwischen dem Clientmodul und dem MTA~~,~~ sowie POP3-Server ~~bzw. Verzeichnisdienst~~ findet unmittelbar nach dem Aufbau der entsprechenden TCP-Verbindung statt. Damit wird sichergestellt, dass die Anmeldungsdaten des Nutzers immer über die mit TLS geschützte Verbindung transportiert werden.

[...]

KOM-LE-A_2075-01 - Prüfung von TLS-Server-Zertifikaten
Das Clientmodul MUSS für die Prüfung von TLS-Server-Zertifikaten der KOM-LE-Fachdienste die Operation VerifyCertificate des Konnektors benutzen.Wird durch die Operation ein Prüfergebnis "INVALID" zurückgegeben, MUSS der beabsichtigte Verbindungsaufbau abgebrochen werden.
[<=]

A_22348 - 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.**[<=]**

KOM-LE-A_2182-01 - Verwendung des vom KOM-LE-Anbieter zur Verfügung gestellten Zertifikats für die clientseitige TLS-Authentifizierung
Das Clientmodul MUSS sich mit dem vom KOM-LE-Anbieter zur Verfügung gestellten TLS-Client-Zertifikat C.CM.TLS-CS gegenüber ~~dem Server~~ den KOM-LE-Fachdienst-Komponenten authentifizieren.
[<=]

4.4 Konfiguration

Tabelle 8: Tab_Konf_Param Standardkonfiguration allgemeine Parameter

Parameter	Beschreibung des Parameters	Defaultwert
PORT_SMTP	SMTP-Port für Clientsysteme	25
PORT_POP3	POP3-Port für Clientsysteme	995
TLS_AUTH_KONNEKTOR	Authentifizierung des Clientmoduls gegenüber dem Konnektor bei aktivierter TLS-Verbindung (zertifikatsbasiert, Basic-Athentifizierung, 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	Time to Live für gecachte Verschlüsselungszertifikateund Prüfergebnisse	24 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_2091-01 - Konfigurationsparameter

Das KOM-LE-Clientmodul MUSS die in Tabelle Tab_Konf_Param aufgelisteten Parameter ausschließlich dem berechtigten Akteur über eine Managementoberfläche oder eine Konfigurationsdatei zur Konfiguration anbieten.
[<=]

2.2 Änderung in gemSpec_FD_KOMLE

3.1 Funktionen des Mail Servers

[...]

A_21456-01 - Festlegung des Domainparts einer KIM-Adresse
Der KIM-Anbieter MUSS für die Beantragung seiner KIM spezifische Subdomain (`hrst_domain`) einer KIM-Adresse folgenden Zeichensatz verwenden:

- (`a-z`, `0-9`) sowie (Punkt~~,~~ und Bindestrich~~und Unterstrich~~),
- es wird nicht zwischen der Groß- und Kleinschreibung unterschieden,
- die Gesamtlänge des Domainparts darf maximal 189 Zeichen betragen,
- der Domainpart endet mit der Zeichenkette "`.kim.telematik`" (Produktivumgebung).

[<=]

3.4 Service Lokalisierung

A_19524-01 - Verwaltung Resource Records Typs für Service Discovery, KIM
Der KOM-LE-Fachdienst MUSS die aufgeführten Resource Records Types im Namensraum der TI gemäß folgender Tabelle verwalten.

Tabelle 9: Tab_KOMLE_Service Discovery

Resource Record Bezeichner	Resource Record Type	Beschreibung
_fdkimsmtp._tcp.kim.telematik	PTR	Ermittlung aller KOM-LE-Anbieter (SMTP)
<fdkim>.<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)
<fdkim>.<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

[<=]

4.1 Schnittstelle I_Message_Service

[...]

KOM-LE-A_2142 - Ports der Schnittstelle I_Message_Service
~~Die Schnittstelle I_Message_Service MUSS folgende Ports benutzen:~~

- ~~SMTPS: 465 und~~
- ~~POP3S: 995.~~

~~<=~~

4.3 Schnittstelle I_AccountManager_Service

[...]

KOM-LE-A_2302-01 - Erzeugung Schlüssel und Bezug TLS-Zertifikate für Clientmodule
Der KOM-LE-Anbieter MUSS die Schlüsselpaare für die Zertifikate für KOM-LE-Clientmodule erzeugen und für diese aus der Komponenten-PKI der TI die C.CM.TLS-CS-Zertifikate beziehen, sodass die Zertifikate ~~vor~~nach der Registrierung eines Nutzers zur Verfügung stehen.
[<=]

KOM-LE-A_2167-04 - Sperrung des Accounts
Der Fachdienst KOM-LE MUSS den Account eines Teilnehmers nach drei aufeinanderfolgenden Fehleingaben des Passwortes temporär gegen Brute-Force Angriffe schützen. Hierzu wird 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. ~~Für jeden weiteren Log-In Versuch erhöht sich diese Wartezeit exponenziell bis zu einem festen Maximalwert. Steigungsfaktor und Maximalwert MÜSSEN geeignet gewählt werden.~~ Im Fehlerfall wird dem KOM-LE-Client der Fehlercode 535 (*Authentication credentials invalid*) gemäß [RFC3463] zurückgegeben.

[<=]

2.3 Änderung der api-kim/AttachmentService.yaml

Angleichung der Notation von Parametern:

1) "`Shared-Link`" -> "`sharedLink`"
2) "`MaxMailSize`" -> "`maxMailSize`"

Type zum schema hinzufügen

```
/MaxMailSize:
    get:
      tags:
      - MaxMailSize
      summary: Die maximale Größe einer KIM-Mail ermitteln
      description: Gibt die maximale Größe einer gesamten KIM-Mail
inklusive aller Anhänge (Mail base64 kodiert) zurück.
      Dieser Wert wird auf dem Fachdienst definiert und bleibt über längere
Zeit konstant.
      Eine Abfrage ist deshalb nicht für jede Mail erforderlich (Empfohlen
wird die tägliche Abfrage)
      operationId: read_MaxMailSize

      responses:
       200:
         description: OK
                # Gibt die maximale Größe einer KIM-Mail in Bytes
zurück
       content:
         application/json:
          schema:
          type: object
          properties:
             MaxMailSize:
               type: "integer"
               format: int64
               example: 734003200
```

2.4 Änderung der api-kim/AttachmentService.yaml

```
 /account/{username}/cert:
    post:
      tags:
      - Certificate
      summary: Create TLS AUT certificate
      operationId: createCert
      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
      requestBody:
        content:
          application/json:
```

```
            schema:
             $ref: '#/components/schemas/CertificateParameters'

      responses:
        200:
          description: Zertifikat wird zurückgegeben.
          content:
           application/json:
            schema:
              type: object
              properties:
                file:
                  type: string
                  format: binary
                  description: Base64-encoded PKCS#12 Container. Der
Container ist mit dem Passwort aus dem Request geschützt.
        400:
           description: Fehler in den Eingangsdaten, Beschreibung des
Fehlers erfolgt in dem Fehlertext
                       # z.B. kein CommonName oder kein CertPassword
angegeben
           content:
             application/json:
               schema:
                 $ref: '#/components/schemas/Error'
        401:
          description: Authentifizierung fehlgeschlagen.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/Error'
        404:
           description: Email Account nicht vorhanden.
                        # z.B. user not registered
           content:
             application/json:
               schema:
                 $ref: '#/components/schemas/Error'
        500:
          description: Internal Server Error
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/Error'
```

2.5 Änderung der api-kim/I_AccountManager_Service

```
components:
  schemas:

[...]
```

```
    Account:
      type: object
      properties:
[...]
        kimVersion:
          type: string
          enum:
            - "1.0"
            - "1.5"
          example: 1.5
```

2.6 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

Tabelle 10: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_20650-03	Übermittlung von Fehlernachrichten	gemSpec_CM_KOMLE
A_21388-01	Übermittlung der Clientmodul- und Produkttypversion	gemSpec_CM_KOMLE
A_19356-04	Prüfen der Version des Empfängers	gemSpec_CM_KOMLE
A_19359-06	Einbetten von Informationen großer Anhänge	gemSpec_CM_KOMLE
A_19371-03	Entschlüsselung der Anhänge	gemSpec_CM_KOMLE
A_19372-02	Prüfen des Anhanges	gemSpec_CM_KOMLE
A_21519-02	Überprüfung des SMTP-Benutzernames	gemSpec_CM_KOMLE
A_21391-02	Auswertung des X-KOM-LE-Version Header Elements	gemSpec_CM_KOMLE
KOM-LE-A_2192-01	Fehlernachricht bei Empfänger mit unterschiedlichen Telematik-IDs in den Verschlüsselungszertifikaten	gemSpec_CM_KOMLE

KOM-LE-A_2024-01	Information des Absenders über Empfänger, für die nicht verschlüsselt werden kann	gemSpec_CM_KOMLE
A_21518-02	Überprüfung des POP3-Benutzernames	gemSpec_CM_KOMLE
A_22340	Cachen von KOM-LE-Versionen	gemSpec_CM_KOMLE
A_22341	Prüfen der Nachrichtenanhänge	gemSpec_CM_KOMLE
KOM-LE-A_2047-01	Fehlertexte bei fehlgeschlagener Entschlüsselung	gemSpec_CM_KOMLE
KOM-LE-A_2048-01	Prüfung der Signatur und Integrität einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM-LE-A_2049-03	Ergebnis der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM-LE-A_2050-04	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
A_19456-02	Überprüfung des SMTP-Benutzernames	gemSpec_CM_KOMLE
KOM-LE-A_2091-01	Konfigurationsparameter	gemSpec_CM_KOMLE
~~KOM-LE-A_2180~~	~~Struktur des Signaturprüfberichts~~	gemSpec_CM_KOMLE

Tabelle 11 Anforderungen zur funktionalen Eignung: "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_22348	Caching der Prüfergebnisse der TLS-Server-Zertifikate	gemSpec_CM_KOMLE

Tabelle 12 Anforderungen zur sich.Techn. Eignung: "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
KOM-LE-A_2048-01	Prüfung der Signatur und Integrität einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM-LE-A_2050-04	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM-LE-A_2064-02	Verwendung von X.509-Identitäten bei der TLS-Authentifizierung	gemSpec_CM_KOMLE

KOM-LE-A_2075-01	Prüfung von TLS-Server-Zertifikaten	gemSpec_CM_KOMLE
KOM-LE-A_2182-01	Verwendung des vom KOM-LE-Anbieter zur Verfügung gestellten Zertifikats für die clientseitige TLS-Authentifizierung	gemSpec_CM_KOMLE

Änderungen in gemProdT_FD_KOMLE

Tabelle 13 Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_19524-01	Verwaltung Resource Records Typs für Service Discovery, KIM	gemSpec_FD_KOMLE
KOM-LE-A_2167-04	Sperrung des Accounts	gemSpec_FD_KOMLE
~~KOM-LE-A_2142~~	~~Ports der Schnittstelle I_Message_Service~~	gemSpec_FD_KOMLE

Tabelle 14 Anforderungen zur funktionalen Eignung: "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_21456-01	Festlegung des Domainparts einer KIM-Adresse	gemSpec_FD_KOMLE

Tabelle 15 Anforderungen zur sich.Techn. Eignung: "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
KOM-LE-A_2302-01	Erzeugung Schlüssel und Bezug TLS-Zertifikate für Clientmodule	gemSpec_FD_KOMLE