Themengebiet: Änderungen in KIM 1.0 und KIM 1.5.1

C_10733

1 KIM 1.0 (R3.1.3-10)

1.1 Änderung in gemSpec_FD_KOMLE

3.1 Funktionen des Mail Server

[...]

A_21777 - Setzen des Parameters des RET-Kommandos (DSN)
Der Mail Server des KOM-LE-Fachdienstes MUSS, wenn er eine Nachricht mit angeforderter Delivery Status Notification (DSN) erhält, sicherstellen, dass eine DSN keine Teile des Bodies der originalen Nachricht enthält.

<=

[...]

~~**KOM-LE-A_2132-01 - Identifikation der Originalnachricht**~~
~~Zur Identifikation der vom Clientsystem versendeten Mail MUSS eine entsprechend als Delivery Status Notification erzeugte Nachricht sowohl den *Empfänger* und das *Versanddatum*, als auch das *In-Reply-To* Header Feld mit der *Message-ID* der ursprünglich versendeten Mail enthalten.~~

~~<=~~

[...]

A_21816 - Mail Server als geschlossener SMTP-Relay-Server
Der Mail Server des KOM-LE-Fachdienstes MUSS als ein geschlossener SMTP-Relay-Server konfiguriert werden. Das bedeutet, der Mail Server darf nur E-Mails weiterleiten, für die er als Sender und/oder Empfänger zuständig ist.

<=

4.1.1 Operation send_Message

[...]

KOM-LE-A_2147-02 - Generierung von Zustellbestätigungen
Erhält der Ziel-Mail-Server eine Nachricht, die eine Zustellbestätigung fordert, MUSS er diese unter Verwendung folgender Informationen aus der empfangenen Nachricht generieren und unverschlüsselt an den Absender weiterleiten:

- Empfänger (alle Empfänger der Original-Nachricht die dem Ziel-Mail-Server zugeordnet sind), pro Empfänger wird ein `per-recipient` Header Feld befüllt [RFC3464]
- Empfangszeitpunkt der originalen Nachricht beim Ziel-Mail-Server im Header Feld *Arrival-Date* (im Part Content-Type: message/delivery-status)
- Message-ID der äußeren Nachricht im Header Feld *In-Reply-To* (im Headerbereich der DSN selbst, mit dem Content-Type: multipart/report)

<=

1.2 Änderung in gemSpec_CM_KOMLE

3.3.4.1.1 Bearbeitung einer ungeschützten Nachricht

[...]

KOM-LE-A_2299-01 - Vorgehen bei Signatur und Verschlüsselung einer KOM-LE Nachricht
Zur Signatur und Verschlüsselung von KOM-LE Nachrichten MUSS das folgende Vorgehen umgesetzt werden:

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

<=

3.4.4.2.2 Integritätsprüfung

[...]

Tabelle 1: Tab_Verm_Sig_Prüf Vermerke mit Ergebnissen der Signaturprüfung

Prüfergebnis	Fehlercode	Ergebnis	Vermerk
VALID	-	Die Signatur der Nachricht wurde erfolgreich geprüft.	Die Signatur wurde erfolgreich geprüft.
INVALID	4115	Die Integrität der Nachricht wurde verletzt.	Die Prüfung der Signatur hat ergeben, dass die Nachricht manipuliert wurde.
INVALID	4253	Die digitale Signatur ist nicht vorhanden.	Die Nachricht ist nicht signiert. Die Nachricht ist deshalb eventuell manipuliert worden.
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.
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.
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.
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.
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.
VALID	-	Die digitale Signatur ist mathematisch korrekt und der Zertifikatsstatus des Signaturzertifikats konnte erfolgreich geprüft werden, aber das recipient-emails-Attribut	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

		aus signerInfos enthält nicht die gleichen Werte wie das recipient-emails-Attribut aus dem enveloped-data CMS-Objekt.	nicht in seinem Besitz ist, zu ermöglichen.

[...]

KOM-LE-A_2050-02 - 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.

<=

4.1.1 Allgemeine Festlegungen

[...]

KOM-LE-A_2064-01 - 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 zusätzlich auch Cipher-Suites und Kurven aus [BSI-TR-02102-2] Kapitel 3.3 akzeptabel um Kompatibilität mit gängigen Clientsystemen und PVSen sicherzustellen.

<=

1.3 Änderung in gemSMIME_KOMLE

2.2.5.1 Normative Beschreibung

[...]

KOM-LE-A_2114-01 - Attribut recipient-emails
Eine dem KOM-LE-S/MIME-Profil konforme Nachricht MUSS ein `recipient-emails` Attribut als ein ungeschütztes Attribut enthalten. Im Attribut werden die Zusammenhänge zwischen den für die Verschlüsselung verwendeten Zertifikaten und den E-Mail-Adressen der Empfänger gespeichert.

Der folgende Objekt-Identifikator identifiziert das recipient-emails Attribut:

id-recipientEmails OBJECT IDENTIFIER ::= {1.2.276.0.76.4.173}
Recipient-emails Attributwerte sind vom ASN.1 Typ RecipientEmails:
RecipientEmails ::= SET SIZE (1..MAX) OF RecipientEmail
RecipientEmail ::= SEQUENCE {
emailAddress IA5String, rid RecipientIdentifier }

<=

1.4 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_FD_KOMLE

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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_21777	Setzen des Parameters des RET-Kommandos (DSN)	gemSpec_FD_KOMLE
~~KOM-LE-A_2132-01~~	~~Identifikation der Originalnachricht~~	gemSpec_FD_KOMLE
A_21816	Mail Server als geschlossener SMTP-Relay-Server	
KOM-LE-A_2147-02	Generierung von Zustellbestätigungen	gemSpec_FD_KOMLE

Änderungen in gemProdT_CM_KOMLE

Tabelle 3: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
KOM-LE-A_2299-01	Vorgehen bei Signatur und Verschlüsselung einer KOM-LE Nachricht	gemSpec_CM_KOMLE
KOM-LE-A_2050-02	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM-LE-A_2064-01	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE

KOM-LE-A_2114-01	Attribut recipient-emails	gemSMIME_KOMLE

Änderungen in gemProdT_Basis-Consumer

Tabelle 4: Anforderungen zur funktionalen Eignung "funkt. Eignung: Test Produkt/FA"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
KOM-LE-A_2050-02	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE

Tabelle 5: Anforderungen zur funktionalen Eignung "funkt. Eignung: Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
KOM-LE-A_2114-01	Attribut recipient-emails	gemSMIME_KOMLE
KOM-LE-A_2064-01	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM-LE-A_2050-02	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE

Änderungen in gemProdT_KTR-Consumer

Tabelle 6: Anforderungen zur funktionalen Eignung "funkt. Eignung: Test Produkt/FA"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
KOM-LE-A_2050-02	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE

Tabelle 7: Anforderungen zur funktionalen Eignung "funkt. Eignung: Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
KOM-LE-A_2114-01	Attribut recipient-emails	gemSMIME_KOMLE
KOM-LE-A_2064-01	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM-LE-A_2050-02	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE

2 KIM 1.5.1-3

2.1 Änderung in gemSpec_FD_KOMLE

3.1 Funktionen des Mail Server

[...]

A_21777 - Setzen des Parameters des RET-Kommandos (DSN)
Der Mail Server des KOM-LE-Fachdienstes MUSS, wenn er eine Nachricht mit angeforderter Delivery Status Notification (DSN) erhält, sicherstellen, dass eine DSN keine Teile des Bodies der originalen Nachricht enthält.
[<=]

[...]

~~**KOM-LE-A_2132-01 - Identifikation der Originalnachricht**~~
~~Zur Identifikation der vom Clientsystem versendeten Mail MUSS eine entsprechend als Delivery Status Notification erzeugte Nachricht sowohl den *Empfänger* und das *Versanddatum*, als auch das *In-Reply-To* Header Feld mit der *Message-ID* der ursprünglich versendeten Mail enthalten.~~

~~<=~~

[...]

A_21816 - Mail Server als geschlossener SMTP-Relay-Server
Der Mail Server des KOM-LE-Fachdienstes MUSS als ein geschlossener SMTP-Relay-Server konfiguriert werden. Das bedeutet, der Mail Server darf nur E-Mails weiterleiten, für die er als Sender und/oder Empfänger zuständig ist.**[<=]**

4.1.1 Operation send_Message

[...]

KOM-LE-A_2147-02 - Generierung von Zustellbestätigungen
Erhält der Ziel-Mail-Server eine Nachricht, die eine Zustellbestätigung fordert, MUSS er diese unter Verwendung folgender Informationen aus der empfangenen Nachricht generieren und unverschlüsselt an den Absender weiterleiten:

- Empfänger (alle Empfänger der Original-Nachricht die dem Ziel-Mail-Server zugeordnet sind), pro Empfänger wird ein `per-recipient` Header Feld befüllt [RFC3464]
- Empfangszeitpunkt der originalen Nachricht beim Ziel-Mail-Server im Header Feld *Arrival-Date* (im Part Content-Type: message/delivery-status)
- Message-ID der äußeren Nachricht im Header Feld *In-Reply-To* (im Headerbereich der DSN selbst, mit dem Content-Type: multipart/report)

[<=]

4.3 Schnittstelle I_AccountManager_Service

[...]

KOM-LE-A_2187-03 - 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 ~~und~~
- ~~stimmt Username mit dem AUT-Zertifikatsinhaber (die Zuordnung von Zertifikat zu mail-Adresse ist durch den VZD-Eintrag gegeben) überein.~~

Für die Operationen gilt:

- bei Aufruf der Operation `registerAccount`:
  Die Fachdaten des KOM-LE-Teilnehmers müssen während der Registrierung 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.
[<=]

6.5.1 Dokumente der gematik

[...]

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemGlossar_TI]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemLH_KOM-LE]	gematik: Lastenheft Kommunikation Leistungserbringer (KOM-LE)
[gemSysL_KOM-LE]	gematik: Systemspezifisches Konzept Kommunikation Leistungserbringer (KOM-LE)
[gemSpec_CM_KOMLE]	gematik: Spezifikation Clientmodul KOM-LE
[gemSMIME_KOM-LE]	gematik: S/MIME-Profil Kommunikation Leistungserbringer (KOM-LE)
[AttachmentServices.yaml]	gematik: ~~https://github.com/gematik/api-kim/src/schema/Attachment_schema.json~~ https://github.com/gematik/api-kim/blob/master/src/openapi/AttachmentService.yaml
[AccountManager.yaml]	gematik: ~~https://github.com/gematik/api-kim~~ https://github.com/gematik/api-kim/blob/master/src/openapi/AccountManager.yaml
[Dienstkennung]	gematik: https://fachportal.gematik.de/toolkit/dienstkennung-kim-kom-le
[DirectoryApplicationMaintenance.yaml]	gematik: https://github.com/gematik/api-kim/blob/master/src/openapi/DirectoryApplicationMaintenance.yaml

2.2 Änderung in gemSpec_CM_KOMLE

Allgemein

Hinweis: Im Zuge der Überarbeitung der Spezifikation sind im Text enthaltene Verweise auf Abbildungen nicht korrekt. Die redaktionelle Anpassung der Bezeichner erfolgt direkt in der betroffenen Spezifikation [gemSpec_CM_KOMLE] und wird an dieser Stelle nicht weiter aufgeführt.

3.3.2.2 Verbindungsaufbau mit MTA

[...]

Das KOM-LE-Clientmodul bricht die Kommunikation mit dem entsprechende SMTP-Antwortcode ab (siehe Tabelle 2), wenn der erhaltene SMTP-Benutzername nicht alle erforderlichen Parameter enthält. Beinhaltet der SMTP-Benutzername zusätzliche optionale durch ‚#' abgegrenzte Parameter (z. B. #KonnektorId), ~~können~~ dann müssen diese Parameter vom Clientmodul ausgewertet werden und der Sendevorgang wird fortgesetzt.

[...]

Tabelle 4: Tab_SMTP_Verbindung SMTP-Antwortcodes für MTA-Verbindungsaufbau

Bedingung	**SMTP-Antwortcode (Clientmodul -> Clientsystem)**
Das Clientmodul hat sich erfolgreich gegenüber dem MTA mit den vom Clientsystem erhaltenen Anmeldungsdaten authentifiziert.	235 2.7.0 (Authentication successful)
Das Clientsystem verwendet für die SMTP-Authentifizierung einen anderen Mechanismus als PLAIN oder LOGIN.	504 5.7.4 (Security features not supported)
Die vom Clientsystem erhaltene SMTP-Authentifizierungsidentität ist nicht vollständig oder falsch formatiert (MTA-Adresse, MandantId, ClientSystemId, ~~oder~~ WorkplaceID oder Platzhalter fehlt – siehe Abbildung ~~6~~ "Abb_MTA_Nutzername Format des SMTP- Benutzernamens")	501 5.5.4 (Invalid command arguments)
Bei bei Übergabe der Parameter für den Aufrufkontext für SM-B (MandantID, ClientSystemID oder WorkplaceID) antwortet der Konnektor mit einem SOAP Fault (Code: 4004 - 4006)	501 (Syntax error in parameters or arguments)
Die Verbindung zwischen dem Clientmodul und dem MTA kann nicht aufgebaut werden.	454 4.7.0 (Temporary authentication failure)
Die Authentifizierung gegenüber dem MTA schlägt fehl.	535 5.7.8 (Authentication credentials invalid)

[...]

A_21519-01 - 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. Wenn die SMTP-Benutzername-Zeichenkette nicht vollständig ist, MUSS das Clientmodul den SMTP Fehlercode~~535~~ gemäß Tabelle "Tab_SMTP_Verbindung SMTP-Antwortcodes für MTA-Verbindungsaufbau" an das Clientsystem senden und den Vorgang abbrechen.
[<=]

3.3.4.1.1 Bearbeitung einer ungeschützten Nachricht

[...]

KOM-LE-A_2299-01 - Vorgehen bei Signatur und Verschlüsselung einer KOM-LE Nachricht
Zur Signatur und Verschlüsselung von KOM-LE Nachrichten MUSS das folgende Vorgehen umgesetzt werden:

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

[<=]

3.4.2.2 Verbindungsaufbau mit dem POP3-Server

[...]

Enthält der POP3-Benutzername nicht alle erforderlichen Parameter, bricht das KOM-LE-Clientmodul den Empfangsvorgang mit dem -ERR Antwortcode ab. Wenn der erhaltene POP3-Benutzername zusätzliche optionale durch das Zeichen ‚#' abgegrenzte Parameter enthält (z.B. #UserId#KonnektorId), ~~können~~ dann müssen diese Parameter vom Clientmodul ausgewertet werden und der Empfangsvorgang wird fortgesetzt.

[...]

Tabelle 6: Tab_POP3_Verbindung Antwortcodes für POP3-Server-Verbindungsaufbau

Bedingung	**POP3 Antwortcode (Clientmodul -> Clientsystem)**
Das Clientsystem hat sich erfolgreich gegenüber dem POP3-Server mit den vom Clientsystem erhaltenen Anmeldungsdaten authentifiziert.	+OK
Das Clientsystem verwendet für die POP3-Authentifizierung einen anderen Mechanismus als USER/PASS oder PLAIN.	-ERR
Die vom Clientsystem erhaltene POP3-Authentifizierungsidentität ist nicht vollständig oder falsch formatiert (POP3 Server Adresse, MandantId, ClientSystemId, ~~oder~~ WorkplaceID oder Platzhalter fehlt – siehe Abbildung ~~11~~ "Abb_POP3_Nutzer_Name Format des POP3- Benutzernamens").	-ERR
Bei bei Übergabe der Parameter für den Aufrufkontext für SM-B (MandantID, ClientSystemID oder WorkplaceID) antwortet der Konnektor mit einem SOAP Fault (Code: 4004 - 4006)	-ERR
Die Verbindung zwischen dem Clientmodul und dem POP3-Server kann nicht aufgebaut werden.	-ERR
Die Authentifizierung gegenüber dem MTA schlägt fehl.	-ERR

[...]

A_21518-01 - 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. Wenn die POP3-Benutzername-Zeichenkette nicht vollständig ist, MUSS das Clientmodul den~~SMTP~~ POP3 Fehlercode ~~535~~ gemäß Tabelle "Tab_POP3_Verbindung Antwortcodes für POP3-Server-Verbindungsaufbau" an das Clientsystem senden und den Vorgang abbrechen.
[<=]

3.4.4.2.2 Integritätsprüfung

[...]

Tabelle 8: Tab_Verm_Sig_Prüf Vermerke mit Ergebnissen der Signaturprüfung

Prüfergebnis	Fehlercode	Ergebnis	Vermerk
VALID	-	Die Signatur der Nachricht wurde erfolgreich geprüft.	Die Signatur wurde erfolgreich geprüft.
INVALID	4115	Die Integrität der Nachricht wurde verletzt.	Die Prüfung der Signatur hat ergeben, dass die Nachricht manipuliert wurde.
INVALID	4253	Die digitale Signatur ist nicht vorhanden.	Die Nachricht ist nicht signiert. Die Nachricht ist deshalb eventuell manipuliert worden.
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.
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.
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.
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.
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.
VALID	-	Die digitale Signatur ist mathematisch korrekt und der Zertifikatsstatus des Signaturzertifikats konnte erfolgreich geprüft werden, aber das recipient-emails-Attribut	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

		aus signerInfos enthält nicht die gleichen Werte wie das recipient-emails-Attribut aus dem enveloped-data CMS-Objekt.	nicht in seinem Besitz ist, zu ermöglichen.

[...]

KOM-LE-A_2050-02 - 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.
[<=]

4.1.1 Allgemeine Festlegungen

[...]

KOM-LE-A_2064-01 - 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 sicherzustellen.
[<=]

5.5.1 Dokumente der gematik

[...]

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemLH_KOM-LE]	gematik: Lastenheft Adressierte Kommunikation Leistungserbringer
[gemSpec_FD_KOMLE]	gematik: Spezifikation Fachdienst KOM-LE
[gemSpec_Kon]	gematik: Spezifikation Konnektor

[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_PKI]	gematik: Spezifikation PKI
[gemSMIME_KOMLE]	gematik: KOM-LE S/MIME Profil 1.0
[gemSysL_KOMLE]	gematik: Systemspezifisches Konzept KOM-LE
[AccountManager.yaml]	gematik: ~~https://github.com/gematik/api-kim~~ https://github.com/gematik/api-kim/blob/master/src/openapi/AccountManager.yaml
[Attachment_Schema]	gematik: ~~https://github.com/gematik/api-kim/src/schema/Attachment_schema.json~~ https://github.com/gematik/api-kim/blob/master/src/schema/Attachment_schema.json

2.3 Änderung in gemSMIME_KOMLE

2.2.5.1 Normative Beschreibung

[...]

KOM-LE-A_2114-01 - Attribut recipient-emails
Eine dem KOM-LE-S/MIME-Profil konforme Nachricht MUSS ein `recipient-emails` Attribut als ein ungeschütztes Attribut enthalten. Im Attribut werden die Zusammenhänge zwischen den für die Verschlüsselung verwendeten Zertifikaten und den E-Mail-Adressen der Empfänger gespeichert.

Der folgende Objekt-Identifikator identifiziert das recipient-emails Attribut:

id-recipientEmails OBJECT IDENTIFIER ::= {1.2.276.0.76.4.173}
Recipient-emails Attributwerte sind vom ASN.1 Typ RecipientEmails:
RecipientEmails ::= SET SIZE (1..MAX) OF RecipientEmail
RecipientEmail ::= SEQUENCE {
emailAddress IA5String, rid RecipientIdentifier }

[<=]

2.4 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_FD_KOMLE

Tabelle 9: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_21777	Setzen des Parameters des RET-Kommandos (DSN)	gemSpec_FD_KOMLE
~~KOM-LE-A_2132-01~~	~~Identifikation der Originalnachricht~~	gemSpec_FD_KOMLE
A_21816	Mail Server als geschlossener SMTP-Relay-Server	gemSpec_FD_KOMLE
KOM-LE-A_2147-02	Generierung von Zustellbestätigungen	gemSpec_FD_KOMLE
KOM-LE-A_2187-03	Authentifizierung des KOM-LE-Teilnehmers über AUT-Zertifikat am AccountManager	gemSpec_FD_KOMLE

Änderungen in gemProdT_CM_KOMLE

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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_21519-01	Überprüfung des SMTP-Benutzernames	gemSpec_CM_KOMLE
KOM-LE-A_2299-01	Vorgehen bei Signatur und Verschlüsselung einer KOM-LE Nachricht	gemSpec_CM_KOMLE
A_21518-01	Überprüfung des POP3-Benutzernames	gemSpec_CM_KOMLE
KOM-LE-A_2050-02	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM-LE-A_2064-01	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE

KOM-LE-A_2114-01	Attribut recipient-emails	gemSMIME_KOMLE

Änderungen in gemProdT_Basis-Consumer

Tabelle 11: Anforderungen zur funktionalen Eignung "funkt. Eignung: Test Produkt/FA"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
KOM-LE-A_2050-02	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE

Tabelle 12: Anforderungen zur funktionalen Eignung "funkt. Eignung: Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
KOM-LE-A_2114-01	Attribut recipient-emails	gemSMIME_KOMLE
KOM-LE-A_2064-01	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM-LE-A_2050-02	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE

Änderungen in gemProdT_KTR-Consumer

Tabelle 13: Anforderungen zur funktionalen Eignung "funkt. Eignung: Test Produkt/FA"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
KOM-LE-A_2050-02	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE

Tabelle 14: Anforderungen zur funktionalen Eignung "funkt. Eignung: Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
KOM-LE-A_2114-01	Attribut recipient-emails	gemSMIME_KOMLE
KOM-LE-A_2064-01	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE
KOM-LE-A_2050-02	Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht	gemSpec_CM_KOMLE