
C_12547 - KIM 1.5.5 - Adressierung Design-Schwächen (CCC) & Weitere

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	3
2 Adaption der Änderungen aus KIM Security Hotfix 1.5.2-10 - Schwachstellen.....	4
2.1 Änderungen bzgl. Prüfung von TLS-Zertifikaten.....	4
2.1.1 Änderung in gemSpec_CM_KOMLE.....	4
2.1.2 Änderung in gemSpec_FD_KOMLE.....	6
2.2 Änderungen bzgl. KAS-Freigabelink.....	7
2.2.1 Änderung in gemSpec_CM_KOMLE.....	7
2.2.2 Änderung in gemSpec_FD_KOMLE.....	9
2.3 Änderungen bzgl. Behandlung von Nachrichten die am Mail-Server des Fachdienstes eingeliefert werden.....	9
2.3.1 Änderung in gemSpec_FD_KOMLE.....	9
3 Änderungen bzgl. Transportsignatur und Integritätsprüfung von KIM-Nachrichten - Design-Schwächen.....	12
3.1 Änderung in gemSpec_CM_KOMLE.....	13
3.1.1 Nutzung HBA im KIM-Versand.....	13
3.1.2 Authentizität von KIM-Nachrichten.....	15
3.1.3 Erweiterung Integritätsprüfung von KIM-Nachrichten.....	19
3.2 Änderung in gemSpec_FD_KOMLE.....	20
3.2.1 Erweiterung der Prüfung der Absender-Integrität am KIM Fachdienst.....	20
3.3 Auswirkungen der Änderungen Transportsignatur und Integritätsprüfung von KIM-Nachrichten - Design-Schwächen.....	23
3.4 Betrachtung Missbrauch des Token aus "X-KIM-Auth".....	24
4 Änderungen bzgl. Ergebnis der Integritätsprüfung von KIM-Nachrichten - Design-Schwächen.....	27
4.1 Änderung in gemSpec_CM_KOMLE.....	27
5 Veränderung bzgl. E-Mail-Fehlernachrichten des KIM Clientmoduls - Design-Schwächen.....	31
5.1 Änderung in gemSpec_CM_KOMLE.....	32
5.1.1 Änderungen bestehender Anforderungen der E-Mail-Fehlernachrichten.....	33
6 Weiteres.....	38
6.1 Inkonsistenzen ESMTP & POP3 Capabilities.....	38
6.1.1 Änderung in gemSpec_CM_KOMLE.....	38
6.1.2 Änderung in gemSpec_FD_KOMLE.....	40

6.2 Änderung zur Absender-Integrität CM und Vermeidung von Folgefehler-Last.....	41
6.2.1 Änderung in gemSpec_CM_KOMLE.....	41
6.3 Angabe TI-User-Agent in HTTP-Requests.....	41
7 Änderungen gemSpec_DS_Anbieter.....	43
8 Änderungen gemSpec_Perf.....	44
9 Änderungen in der gemSpec_Krypt.....	46

1 Änderungsbeschreibung

Mit dem KIM 1.5.5 Spezifikations-Release sollen folgende Punkte adressiert werden:

- durch CCC gemeldete sicherheitsrelevante Schwachstellen und Designschwächen bzgl. der Nachrichten-Integrität bezüglich Signatur
- Adaption der Änderungen aus dem zugehörigen KIM Security Hotfix 1.5.2-10
- Problemszenarien im Umgang mit Fehlernachrichten und daraus unter anderem resultierenden Lastszenarien
- Behebung verschiedener technisch-fachlicher Konsistenz- und Textfehler, usw.

Basis dieser Änderungen ist der Release-Stand KIM 1.5.4

2 Adaption der Änderungen aus KIM Security Hotfix 1.5.2-10 - Schwachstellen

Die Änderungen mit dem KIM Security Hotfix 1.5.2-10 erfolgten auf dem Release-Stand KIM 1.5.2-9 und müssen äquivalent, aufbauend auf den aktuellen Release-Stand KIM 1.5.4 aufgenommen werden.

2.1 Änderungen bzgl. Prüfung von TLS-Zertifikaten

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

Aus CVDP-Meldung, folgendes Szenario

Ein "reguläres" KIM Clientmodul kommuniziert mit einem "böartigen" KIM Fachdienst, der missbräuchlich, als Serverzertifikat ein valides KIM Clientmodul Client-Server-Zertifikat verwendet (man in the middle). Voraussetzung ist Zugang zur TI und KIM.

Die Analyse der bestehenden Spezifikationslage zeigte, dass TLS-Zertifikate in KIM nicht ausreichend, gemäß der Möglichkeiten, geprüft werden und sowohl für das KIM Clientmodul als auch den KIM Fachdienst Optimierungen notwendig sind.

Die nachfolgenden Änderungen sollen eine entsprechende, mehrstufige Prüfung von TLS-Zertifikaten abbilden, welche Sicherheitsaspekte wie man in the middle, dns spoofing/cache poisoning ebenfalls adressieren.

2.1.1 Änderung in gemSpec_CM_KOMLE

geändert:

KOM-LE-A_2075-03 -Prüfung von TLS-Server-Zertifikaten

Das Clientmodul MUSS bei der Prüfung von TLS-Server-Zertifikaten der KOM-LE-Fachdienste prüfen, ob es sich um ein KOM-LE Fachdienst Zertifikat handelt ([gemSpec_OID] - Tab_PKI_406-* OID-Festlegung technische Rolle in X.509-Zertifikaten - C.FD.TLS-S; OID: 1.2.276.0.76.4.172). Zusätzlich MUSS das Clientmodul den FQDN für die Prüfung gemäß [GS-A_5077-*] anhand des Domainanteils, der zur Adressierung des Endpunkts relevanten KIM-Adresse, per DNS-Auflösung ermitteln. Resultiert eine dieser Prüfungen in einem negativen Ergebnis, MUSS der Verbindungsaufbau abgebrochen werden. Bei positivem Ergebnis der vorangegangenen Prüfschritte MUSS das Clientmodul die Operation "VerifyCertificate" nutzen, um die Gültigkeit des Zertifikats zu validieren. Wird durch diese Operation das Prüfergebnis "INVALID" zurückgegeben, MUSS der beabsichtigte Verbindungsaufbau abgebrochen werden.
[<=, Basis-Consumer, KIM-iCM, KOM-LE CM, Sich.techn. Eignung: Herstellererklärung]

Entfällt:

A_17503-01 - Prüfung von TLS-Server-Zertifikaten in der gemSpec_BasisKTR_Consumer, da redundant

geändert:

A_22348-02 -Caching der Prüfergebnisse der TLS-Server-Zertifikate

Das Clientmodul MUSS das Ergebnis der Zertifikatsprüfung für eine definierte Zeitdauer TTL_FD_CERT (Tabelle 15: Tab_Konf_Param Standardkonfiguration allgemeine

Parameter) temporär und manipulationssicher speichern. Für die Zuordnung sind eindeutige Identifikatoren, wie bspw. der Zertifikats-Fingerabdruck, zu verwenden. Bei erneuter Prüfung eines gleichen Zertifikats kann das vorangegangene Verifikations-Ergebnis dieses Zertifikats genutzt werden. Die Speicherdauer ist an die zeitliche Gültigkeit ("notAfter") des Zertifikats anzupassen, d.h. darf nicht über dessen Gültigkeit hinweg reichen. **Führt die Zertifikatsprüfung zu einem negativen Ergebnis erfolgt die Speicherung des Ergebnisses analog, jedoch für eine geringere Zeitdauer gemäß dem WertTTL_FD_CERT_ERR.**

[<=, Basis-Consumer, KIM-iCM, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

Tabelle 1: Tab_Konf_Param Standardkonfiguration allgemeine Parameter

Parameter	Beschreibung des Parameters	Defaultwert
TLS_AUTH_KONNEKTOR	Authentifizierung des Clientmoduls gegenüber dem Konnektor bei aktivierter TLS-Verbindung (zertifikatsbasiert, Basic-Authentifizierung, ohne)	zertifikatsbasiert
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_VZD_DATA	Time to Live für gecachte Daten vom VZD wie Verschlüsselungs-zertifikate und Prüfergebnisse und KOM-LE-Versionen (minimaler Wert 1 Stunde; maximaler Wert 24 Stunden)	12 Stunden
TTL_AM_DATA	Time to Live für gecachte Nutzer-Konfigurationsdaten (Operation getLimits) vom Account-Manager (minimaler Wert 1 Stunde; maximaler Wert 24 Stunden)	12 Stunden
TTL_EMAIL_ICCSN	Time to Live für gecachte Zuordnungen von E-Mail-Adressen der Sender bzw. Empfänger zu ICCSNs von deren HBAs/SM-Bs (minimaler Wert 10 Tage; maximaler Wert 30 Tage)	30 Tage
TTL_FD_CERT	Time to Live für gecachte TLS-Server-Zertifikate, nach erfolgreicher	24 Stunden

	OCSPZertifikats-Prüfung	
TTL_FD_CERT_ERR	Time to Live für gecachte TLS-Server-Zertifikate, nach negativer Zertifikats-Prüfung (minimaler Wert 1 Minute; maximaler Wert 60 Minuten)	5 Minuten
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
TTL_ERR_MSG	Time to Live für gecachte Informationen bzgl. bereits versendeter, gleicher KIM-Fehlerbenachrichtigungen (minimaler Wert 1 Stunde; maximaler Wert 24 Stunden)	12 Stunden
TTL_MSG_AUTH	Zeitliche Gültigkeit des Tokens aus X-KIM-AUTH [A_28582-*) (minimaler Wert 15 Minuten; maximaler Wert 120 Minuten)	60 Minuten

2.1.2 Änderung in gemSpec_FD_KOMLE

geändert (KOM-LE-A_2144-01):

KOM-LE-A_2144-03 -Schritte beim Aufbau der TLS-Verbindung

Beim Aufbau einer TLS-Verbindung MUSS der KOM-LE-Fachdienst folgende Schritte bei der Prüfung des vorgelegten TLS-Zertifikats (C.CM.TLS-CS-Zertifikat des Clientmoduls, C.FD.TLS-C Client-Zertifikat, C.FD.TLS-S Server-Zertifikate eines anderen KOM-LE-Fachdienstes oder C.ZD.TLS-S des Verzeichnisdienstes) durchführen:

- Prüfung, ob es sich um ein Zertifikat folgender technischer Rollen handelt ([gemSpec_OID] - Tab_PKI_406-* OID-Festlegung technische Rolle in X.509-Zertifikaten)
 - Für Kommunikation zwischen KOM-LE Fachdiensten: C.FD.TLS-C oder C.FD.TLS-S
OID: 1.2.276.0.76.4.172
 - Für Kommunikation zwischen KOM-LE Clientmodul und KOM-LE Fachdienste:
C.CM.TLS-CS; OID: 1.2.276.0.76.4.174
 - Für Kommunikation zwischen KOM-LE Fachdienst und VZD: C.ZD.TLS-S; OID:
1.2.276.0.76.4.171
- Prüfung des Vertrauensstatus der Aussteller-CA gegen die TSL,
- mathematische Prüfung der Zertifikatssignatur,
- Prüfung der zeitlichen Gültigkeit des Zertifikats und

- Prüfung des Zertifikatsstatus in der folgenden Reihenfolge
 - durch einen gültigen Eintrag im lokalen Cache
 - existiert kein Eintrag im lokalen Cache, durch Abfrage des relevanten OCSP-Responders.

Die Reihenfolge ist empfohlen z. B. hinsichtlich wirtschaftlicher Umsetzbarkeit (Offline-Schritte vor Online-Schritten), aber nicht zwingend vorgegeben. Vorbedingung für die Zertifikatsprüfung ist, dass eine validierte TSL in Form eines Trust Stores vorliegt.

Bei einer nicht positiven Prüfung im Verlauf eines dieser Schritte, MUSS der Verbindungsaufbau abgebrochen werden.

[<=, KOM-LE FD, funkt. Eignung: Herstellererklärung]

Entfällt:

~~KOM-LE-A_2228-01 – Ausschließliche Akzeptanz von TLS-Client-Zertifikaten von KOM-LE-Clientmodulen~~

2.2 Änderungen bzgl. KAS-Freigabelink

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

Aus CVDP-Meldung, folgendes Szenario

Im Anwendungsfall KAS – Versand KIM-Nachrichten > 15 MiB, werden E-Mail-Daten durch einen "Freigabelink" referenziert und dieser Link innerhalb einer KIM-Nachricht (KAS-Nachricht) übermittelt. Anhand des Links werden auf der Empfänger-Seite die Daten abgerufen. Eine solche KAS-Nachricht kann "missbräuchlich" gefälscht erstellt und mit einem beliebigen "Freigabelink" übermittelt werden. In der KIM-Nachrichtenverarbeitung wird dieser Link adressiert und kann so genutzt werden, um bspw. externe, öffentliche IP-Adressen von KIM-Teilnehmern zu ermitteln oder „böartige“ Daten/Inhalte bereitzustellen. Voraussetzung ist Zugang zur TI und KIM.

Die nachfolgenden Änderungen stellen sicher, dass die wesentlichen KAS-Endpunkt-Informationen stets ermittelt werden müssen und der empfangene KAS-Link nicht unbehandelt verwendet wird.

2.2.1 Änderung in gemSpec_CM_KOMLE

geändert:

A_19370-08 -Download von E-Mail-Daten

Das KOM-LE-Clientmodul MUSS die E-Mail-Daten anhand des entnommenen Freigabelinks via der Operation `readMailData` am KAS des Fachdienstes herunterladen zunächst anhand der Absender-Information aus der empfangenen E-Mail, mittels DNS Service Discovery den "host" und "port" des KAS ermitteln und diese Informationen als "authority"-Komponente [RFC3986] in der URL (Freigabelink) verwenden. Hierzu sind umliegende Festlegungen bzgl. der Absender-Information [A_23422-*) zu beachten. Daten werden in diesem Anwendungsfall stets vom KAS, der dem Absender zugehörig ist, bereitgestellt bzw. abgerufen. Anschließend MUSS das KOM-LE-Clientmodul die E-Mail-Daten anhand des resultierenden Freigabelinks, via der REST-API-Operation `readMailData` abrufen. Tritt beim Herunterladen der E-Mail-Daten ein Fehler auf, MUSS das Clientmodul eine Fehlnachricht gemäß [A_28602-*) und damit korrespondierendem Fehlertext

aus[Tab_Fehlertext_Download] erzeugen. Das subject Header-Element der neuen multipart/mixed Nachricht erhält den Wert „Die E-Mail-Daten konnten nicht abgerufen werden“. [≤, Basis-Consumer, KIM-iCM, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

KAS-LINK Beispiele anpassen, siehe über Abschnitt
https://gemspec.gematik.de/docs/gemSpec/gemSpec_CM_KOMLE/latest/#A_19360-02

[RFC3986] in 5.5.2 Weitere Dokumente aufnehmen

Änderungen bzgl. des Fehlerfalls, der Fehlernachricht werden hier im Abschnitt **Änderungen bestehender Anforderungen der E-Mail-Fehlernachrichten** beschrieben.

2.2.2 Änderung in gemSpec_FD_KOMLE

geändert:

A_19380-04 -KAS - Erzeugung Freigabelink

Der KAS MUSS bei Aufruf der REST-Operation addMailData einen Freigabelink als URL [RFC3986] erzeugen, der aus dem FQDN der Teilkomponente KAS und einer zufälligen und eindeutigen ID der Ressource z. B. einer UUID [RFC4122] besteht und diesen an den aufrufenden Client zurückgeben. Dieser MUSS das Schema „https“, als „host“ den FQDN der Teilkomponente KAS verwenden und die Ressource im „path“ mit einer zufälligen und eindeutigen ID (z. B. einer UUID [RFC4122]) referenzieren. Dieser Freigabelink wird gemäß [AttachmentService.yaml] an den aufrufenden Client zurückgeben.
[<=, KOM-LE FD, funkt. Eignung: Test Produkt/FA]

Hinweis:

Bildung Freigabelink KAS, inkl. Festlegungen aus [AttachmentService.yaml]:

`https://{KAS-FQDN}/attachments/{version}/attachment/{id}`

Beispiel Freigabelink KAS:

`https://kas.fqdn/attachments/v2.3/attachment/469bf002-701f-4362-a9bc-6585c1871250`

Entfällt:

A_19381 – KAS – Freigabelink Transportsicherheit

[RFC3986] in **6.5.2 Weitere Dokumente** aufnehmen

2.3 Änderungen bzgl. Behandlung von Nachrichten die am Mail-Server des Fachdienstes eingeliefert werden

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

Aus CVDP-Meldung, folgendes Szenario

Gemäß aktueller Spezifikation werden KIM-Fehlernachricht, in Annahme der Generierung durch zugelassene, technische Komponenten, weder signiert noch verschlüsselt übertragen. Eine solche Fehlernachricht kann, "missbräuchlich" erstellt, als reguläre KIM-Nachricht "getarnt" direkt übermittelt werden. Diese Nachrichten müssen sowohl der KIM Fachdienst als auch das empfangende KIM Clientmodul unbehandelt weiterleiten/zustellen. Folglich können "böartige" (phishing, falsche Daten, ...) Nachrichten, als scheinbar reguläre KIM-Nachrichten ungeprüft, ohne Signatur und Verschlüsselung übermittelt werden. Voraussetzung ist Zugang zur TI und KIM. Die nachfolgenden Änderungen stellen sicher, dass an zentraler Stelle, durch den KIM Fachdienst jede KIM-Fehlernachricht entsprechend behandelt wird.

2.3.1 Änderung in gemSpec_FD_KOMLE

geändert:

A_20771-03 -Generierung von Fehlermeldungen am Fachdienst

Der Fachdienst KOM-LE MUSS sicherstellen, dass eine E-Mail-Nachricht vom KOM-LE Clientmodul, auf welche mindestens eines der Prüfkriterien gemäß Tab_Fehlercodes_KOMLE-Fachdienst zutrifft, ausschließlich wie folgt behandelt wird.

Der Fachdienst KOM-LE MUSS eine Fehlernachricht entsprechend Delivery Status Notification gemäß [RFC3461-3464] erzeugen, das Header-Attribut X-KIM-Fehlernachricht mit den Werten aus der folgenden Tabelle befüllen und an den Absender übermitteln. Die originär eingelieferte E-Mail DARF NICHT übermittelt werden. Der Fachdienst KOM-LE MUSS sicherstellen, dass die DSN keine Teile des Bodies der originalen Nachricht enthält, sofern dies nachfolgend nicht näher definiert wurde.

Es gilt die Annahme der Unterscheidung zwischen einer Kommunikation

1. KOM-LE Clientmodul zu KOM-LE Fachdienst und
2. KOM-LE Fachdienst zu KOM-LE Fachdienst

Bekannte Unterscheidungsmöglichkeiten sind u.a. durch Clientzertifikats-Informationen (mTLS) und/oder Port-Differenzierung gegeben.

Im Fall 2) sind weitere, sog. "server-generierte" Nachrichtentypen relevant (DSN, NDR, Auto-Reply/Abwesenheitsnachricht, ...), die zwischen den Mail-Servern der KOM-LE Fachdienste ausgetauscht werden. Für diesen Fall kann diese Anforderung nicht gänzlich angewandt werden.

Tabelle 2: Tab_Fehlercodes_KOMLE-Fachdienst

Prüfkriterien	Fehler	Wert
Prüfung der Mailbody-Eigenschaften auf S/MIME-Konformität	Die Mail entspricht nicht dem KOM-LE S/MIME-Profil	fdgerr_1
Subject ungleich "KOM-LE-Nachricht"	Der Betreff der Mail ist ungültig	fdgerr_2
Header "X-KOM-LE-Version" ungültig	Die übergebene X-KOM-LE-Version ist ungültig	fdgerr_3
ContentType beginnt nicht mit "application/pkcs7-mime;" oder enthält nicht "smime-type=authenticated-enveloped-data"	Der ContentType der Mail ist ungültig	fdgerr_4
Prüfung der Mailgröße	Die maximale Größe der Mail wurde überschritten	fdgerr_5
Fehlernachricht, Benachrichtigung von KOM-LE Clientmodul Wenn Header "X-KIM-	Fehlernachricht/Benachrichtigung von KIM-Clientmodul. Prüfen Sie den Inhalt der Fehlernachricht/Benachrichtigung und kontaktieren sie ggf. Ihren/Ihre Systembetreuer*in. Nachfolgend der	fdgerr_6

Fehlermeldung" vorhanden, wird nur dieses Prüfkriterium betrachtet.	Text-Inhalt der eingegangenen Nachricht. <text/plain -Teil der empfangenen Fehlernachricht>	
---	--	--

【<=, KOM-LE FD, funkt. Eignung: Test Produkt/FA】

Entfällt:

~~A_20651-02 – Empfang von Fehlernachrichten des Clientmodules, muss entfallen~~
~~KOM-LE A_2146-03 – Verarbeitung von Nachrichten entsprechend S/MIME-Profil, kann entfallen da redundant~~

3 Änderungen bzgl. Transportsignatur und Integritätsprüfung von KIM-Nachrichten - Design-Schwächen

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

Aus CVDP-Meldung, folgendes Szenario

In KIM werden reguläre Nachrichten signiert und verschlüsselt übertragen. Dabei wird technisch nicht sichergestellt oder geprüft, ob die KIM-Absenderadresse zur Signatur bzw. technischen Identität gehört, welche die KIM-Nachricht signiert hat (vgl. S/MIME). Der Versand bietet keinen Nachweis zum Besitz des privaten Schlüsselmaterials → Kein Nachweis, dass Absender (in proximity) der berechtigten LEI angehört. Mit Kenntnis eines KIM-Accounts kann eine beliebige Umgebung mit KIM-Zugang "genutzt" werden, um KIM-Nachrichten zu versenden.

Ursachen

- In KIM wird lediglich mit einer "nutzbaren" SMC-B signiert, auch in Szenarien in denen mehrere SMC-B vorhanden sind
- Integritäts- und Signaturprüfung, nach Abruf einer Nachricht gibt lediglich Aussage über Validität der Signatur
- Es gilt/galt die Annahme "Versand erfolgte aus berechtigter LEI"
- Konfigurationen in Infrastruktur der LEI sowie des TI-Konnektors führen dazu, dass dieser Umstand ausgenutzt und eine nicht der Absender-Adresse zugeordnete SMC-B für die Signatur von KIM-Nachrichten genutzt werden kann

Ziele der Änderung

- Sicherstellung, dass eine KIM-Nachricht im Kontext der Identität = Telematik-ID (TID) signiert und versendet wird zu der die KIM-Absender-Adresse zugeordnet ist
- Abwärtskompatibilität
- Schnelle Umsetzbarkeit

Einordnung

- Mit Blick in die mögliche Zukunft TI & KIM 2.0 ff. wird diese Design-Schwäche generell als sicherheitsrelevant betrachtet und kann technisch bereits adressiert werden
- Eine eindeutige 1:1 Beziehung von KIM-Adresse zu Signaturzertifikat existiert aktuell nicht und würde grundlegende Änderungen oder S/MIME-Zertifikate notwendig machen
 - Mit der Annahme, dass eine Identität (TID) mehrere E-Mail-Adressen und mehrere Zertifikate besitzen kann, so wie in praktischer Anwendung eine Person mehrere E-Mail-Adressen & ... besitzen kann, ist die Zuordnung der KIM-Absender-Adresse und des Signaturzertifikat zu einer TID über den VZD möglich und geeignet!
- Primäre Schwierigkeit ist die notwendige Nutzung des HBA zur Signatur beim Versand von KIM-Nachrichten, sofern die KIM-Absender-Adresse einem HBA zugeordnet ist. Bisher wurde in diesem Fall der HBA inkonsistent, lediglich zum Abruf von KIM-Nachrichten benötigt.
- Verbreitung der HBA-Nutzung in KIM hängt von Zuordnung der KIM-Adresse zu einer HBA-Identität im VZD ab

- Stand 29.10.2025 befinden sich in der PU **854** KIM-Adressen, die einem HBA zugeordnet sind. Demgegenüber stehen >**200000** KIM-Adressen die einer SMC-B zugeordnet sind. Die gematik darf keine Kenntnis über die tatsächliche Nutzung dieser Adressen haben.
- Nachfolgende Maßnahmen ähnlich DomainKeys Identified Mail (DKIM)

3.1 Änderung in gemSpec_CM_KOMLE

3.1.1 Nutzung HBA im KIM-Versand

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

Bisher wird der HBA, sofern diesem eine KIM-Adresse zugeordnet ist, lediglich beim Abruf von KIM-Nachrichten, für die Entschlüsselung der Daten benötigt.

Damit ein HBA für entsprechende Operationen des TI-Konnektors genutzt werden kann, wird eine "UserId" als Bestandteil des Aufrufkontextes des TI-Konnektors benötigt.

Folglich muss die "UserId" im SMTP-Benutzernamen, analog dem POP3-Benutzernamen, als optionale Komponente aufgenommen werden. SMTP- und POP3-Benutzername müssen in KIM, aufgrund struktureller Abwärtskompatibilität, weiterhin getrennt betrachtet werden.

geändert:

3.3.2.2 Verbindungsaufbau mit MTA

[...]

Um mit SM-B/HBA über den Konnektor kommunizieren zu können, werden dem KOM-LE-Clientmodul ebenfalls als Teil des SMTP-Benutzernamens, die Parameter

- MandantId
- ClientSystemId
- Workplaceld
- KonnektorId (optional)
- UserId (optional – ist für einen Zugriff auf HBA erforderlich)

übergeben (siehe Kapitel 3.5 und [gemSpec_Kon] für Details zu MandantId, ClientSystemId, Workplaceld und UserId). Die Parameter entsprechen denen des aufrufenden Clients und werden voneinander durch das Zeichen '#' getrennt. Der optionale Parameter KonnektorId, als Bestandteil des Aufrufkontextes für SM-B, ermöglicht die Unterstützung von Multikonnektor-Umgebungen. Er kann entfallen, wenn das Clientmodul nicht mit mehreren Konnektoren kommunizieren muss. Der optionale Parameter UserId wird nur für den Zugriff auf einen HBA benötigt und kann entfallen, wenn kein HBA erforderlich ist.

Der Aufbau des SMTP-Benutzernamens entspricht dem folgenden Muster. Die Reihenfolge entspricht der den Parametern vorangestellten Nummer.

[0] Benutzername
[2] MandantId
[3] ClientSystemId

[4] Workplaceld
 — <optional> —
 [1] <Domain Adresse des SMTP-Servers>:<Port>
 [5] KonnektorId
 [6] UserId
 [...]

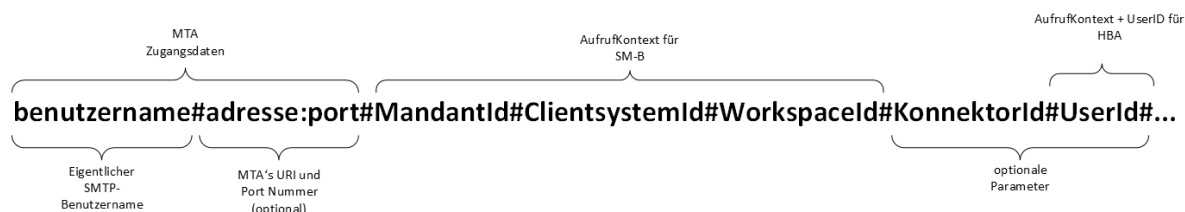


Abbildung 1: Abb_MTA_Nutzer_Name Format des SMTP-Benutzernamens

Beispiel:

Bei folgenden Informationen

- Benutzername des Clients = „erik.mustermann@hrst_domain.kim.telematik“,
- Domain Adresse des MTAs = „hrst_domain.kim.telematik“ und Portnummer = 465,
- MandantId = 1,
- ClientsystemId = KOM_LE,
- Workplaceld = 7
- KonnektorId = Konn_1
- **UserId = 13**

erwartet das Clientmodul, dass das Clientsystem ihm folgenden SMTP-Benutzernamen als String überträgt:

```
erik.mustermann@hrst_domain.kim.telematik#hrst_domain.kim.telematik:465#1#KOM_LE#7#Konn_1#13
```

Das Beispiel ohne den übergebenen Parameter "Domain Adresse des MTAs" sieht wie folgt aus:

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

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

[...]

geändert:

A_21387-04 -Prüfung der verwendeten Clientmodul-Version beim Senden

Das KOM-LE-Clientmodul MUSS mindestens einmal am Tag, vor dem Versenden einer Nachricht, die KOM-LE-Version des Absenders mittels des LDAP-Directory

AttributskimData aus dem Verzeichnisdienst [gemSpec_VZD#5] abfragen und in einem Cache gemäß TTL_VZD_DATA vorhalten.

Ist die KOM-LE-Version des Clientmoduls kleiner als die im Verzeichnisdienst eingetragene, so MUSS das Clientmodul den Absender mit einer KIM E-Mail darüber informieren. Aus dem Inhalt der E-Mail MUSS hervorgehen, dass die verwendete Clientmodul Version veraltet ist. Die E-Mail ist weder zu signieren noch zu verschlüsseln und entspricht der Delivery Status Notification gemäß [RFC3461-3464].

Ist die KOM-LE-Version des Clientmoduls größer als die im Verzeichnisdienst abgefragte Version MUSS das Clientmodul die Aktualisierung des LDAP-Directory AttributkimData für den Absender mit der neuen Version über den Account Manager durch den Aufruf der Operation setAccount veranlassen. ~~Handelt es sich bei der Mail-Adresse um einen HBA-Account, dann erfolgt die Aktualisierung der KOM-LE-Version nachdem ein POP3-Nachrichtenabruf erfolgt ist.~~ [\leq , KIM-iCM, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

Hinweis: Das Attribut kimData ist in [gemSpec_VZD] definiert. Für die Aktualisierung der KOM-LE-Version im Verzeichnisdienst ruft das Clientmodul die Operation SetAccount an der Schnittstelle I_AccountManager_Service am Fachdienst des Absenders auf.

Beispiel: empfaenger@hrst_domain.kim.telematik,1.5

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

3.1.2 Authentizität von KIM-Nachrichten

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

Bisher erfolgt in KIM die Transportsignatur ausschließlich als CMS-Signatur mit einer nutzbaren SM-B-Identität (SMC-B). Dies erfolgt unabhängig davon, ob dieser Identität auch die KIM-Adresse des Absender zugeordnet ist.

Die Sicherstellung, dass eine KIM-Nachricht im Kontext einer Identität (SM-B oder HBA) versendet wird, zu der auch die KIM-Absender-Adresse zugeordnet ist, wird nachfolgend beschrieben.

Die Signatur in KIM basiert bisher ausschließlich auf einer nonQES CMS-Signatur mittels SM-B. Eine CMS-Signatur mit HBA wäre nur als QES möglich. Dieser Umstand impliziert verschiedene Probleme und ist in realer Anwendung nicht praktikabel:

- Bei jedem Versand. im Kontext HBA, ist stets PIN-Eingabe oder Komfort-Signatur-Kontext notwendig
- Das zusätzlich zur ggf. vorangegangenen PIN-Eingabe zur regulären QES von u.a. eAU, eArztbrief, ...
- Komfortsignatur (nur 1-stufig für Primärsysteme gedacht) - Kontext müsste systemübergreifend verwaltet, synchronisiert werden

QES ist nicht für automatisiert, dunkel-verarbeitende (headless) Prozesse konzipiert, was in KIM häufig der Fall ist.

neu:

A_28582 -Authentisierung einer KIM-Nachricht

Das Clientmodul MUSS anhand der vollständig, vorverarbeiteten, originalen Mail vom Clientsystem, vor der CMS-Signatur gemäß [KOM-LE-A_2299-*], ein JSON-Web-Token

gemäß [RFC7519] mit den Elementen aus der folgenden Tabelle erzeugen und in der originalen Mail als Wert des Header-Element "X-KIM-Auth" einfügen.

Das Clientmodul MUSS sicherstellen, dass die Signatur des Tokens mit einem AUT-Zertifikat C.HP.AUT (HBA) oder C.HCI.AUT (SMC-B bzw. HSM-B) erfolgt, welches der gleichen Telematik-ID zugeordnet ist, wie auch die Absender-Adresse aus dem SMTP-Kommando MAIL FROM (RFC 5322 „addr-spec“). Das Clientmodul MUSS entsprechend [KOM-LE-A_2021-*) reagieren, wenn das Signieren des Tokens nicht gemäß der umliegenden Festlegungen möglich ist, oder bei der Erstellung der Signatur ein Fehler auftritt.

Das Clientmodul MUSS sicherstellen, dass dieses Header-Element nur ein mal vorkommt und stets das im Verarbeitungskontext neu-erzeugte Token als Wert dieses Header-Elements angegeben ist.

JSON Web Token	
Header	
alg	BP256R1 oder PS256
typ	JWT
x5c	[BASE-64 kodierte AUT-Cert]
Body	
nbf	[Gültigkeitsbeginn (Unixzeit)]
jti	UUID [RFC4122]
iss	Wert von X-KIM-CMVersion gemäß A_21388-*
sub	Absender-Adresse aus SMTP MAIL FROM (RFC 5322 „addr-spec“)
aud	Wert istI_Message_Service

Der Parameter alg wird in Abhängigkeit zum verwendeten Signature Type eingetragen und MUSS nach der Auswertung des XML-Attribut dss:SignatureObject/dss:Base64Signature/@Type in der vom ExternalAuthenticate zurückgegebenen ASN.1 Struktur ermittelt werden. Es sind die relevanten Implementierungshinweise im Kontext [A_19457-*) zu beachten.

[<=, Basis-Consumer, KIM-iCM, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

Schema der Angabe als Header der Mail:

X-KIM-Auth: Bearer <JWT>

Hinweise:

Die Notwendigkeit einer Identifikation eines AUT-Zertifikats zur Token-Signatur, welches der KIM-Adresse/dem KIM-Account zugeordnet ist, besteht bereits äquivalent im Kontext der Nutzung von Operationen des Interface I_AccountManager_Service [A_21387-, A_21381-*] beim Versand oder Abruf von KIM-Nachrichten.*

Die Ermittlung der TID kann anhand der beim Versand zu nutzenden VZD-Daten erfolgen. Darüber hinaus, kann anhand der Daten aus dem VZD ebenfalls eingeschränkt werden, ob eine SMC-B oder ein HBA genutzt werden muss.

Daten aus der dazu notwendigen Ermittlung lokaler Zertifikatsinformationen können synergetisch im Kontext anderer Anforderungen [KOM-LE-A_2061-] genutzt werden.*

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

Zwischen KOM-LE-A_2028 und KOM-LE-A_2193 einfügen?

Information zu A_28582 - Authentisierung einer KIM-Nachricht

Eine äquivalente Änderung bzgl. der bestehenden Anforderungslage zur CMS-Signatur mit SM-B (u.a. KOM-LE-A_2052 - Quellen zur Ermittlung der SM-B des Senders beim Signieren) ist nicht zielführend, da diese den HBA-Fall nicht berücksichtigen kann. Ohnehin würden diesbezügliche Änderungen in "alten" Clientmodulennicht, jedoch in zukünftigen Versionen der Clientmodule, noch vor der CMS-Signatur, für sowohl SM-B als auch HBA wirken. Folglich wird eine allgemeine Lösung für sowohl SM-B als auch die HBA-Variante favorisiert, welche in der realen Nutzung eine **geringe Auswirkung hat und abwärtskompatibel ist**. Die Signatur mittels AUT-Zertifikat ist sowohl mit HBA als auch mit SM-B nonQES möglich und verhält sich somit analog zu der bisherigen, bekannten KIM-Nutzung.

Mit dieser Lösung wird eine mehrschichtige Authentifizierung abgebildet, da das zusätzliche Token als Authentisierungsinformation innerhalb der CMS-Signatur und E2E-Verschlüsselung übertragen wird. Somit ist erreicht, dass:

- Abwärtskompatibilität gewährleistet ist, da zusätzliche Information gegeben und die bisherigen Festlegungen nicht verändert wurden
- Ein technisch einheitlicher Nachweis besteht, dass eine KIM-Nachricht im Kontext der Identität = telematik-id (TID) signiert und versendet wird, der die KIM-Absenderadresse zugeordnet ist
- Eine schnelle Umsetzbarkeit für Industrie im Marktmodell möglich ist, da bekannte Anforderungen & Feature nachgenutzt werden können

Für die Übermittlung des Tokens wurde ein KIM-spezifischer Header "X-KIM-Auth" definiert, da das sonst übliche Header-Element Authorization (RFC 7235) für HTTP-Requests gilt und semantische Inkonsistenz sowie potenzielle Wechselwirkungen mit bspw. Security-, Mail-Gateways vermieden werden soll.

Nachfolgend wird der "**aud**" claim ebenfalls für die bestehende Anforderung zur Erzeugung eines JWT aufgenommen.

geändert:

A_19457-05 -Client Authentisierung Administrationsmodul

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

Für die Authentisierung am Account Manager MUSS das Administrationsmodul ein JSON-Web-Token gemäß [RFC7519] mit den Elementen aus der folgenden Tabelle erzeugen und zusammen mit dem Passwort des Nutzers an den Account Manager übergeben.

JSON Web Token	
Header	
alg	BP256R1 oder PS256
typ	JWT
x5c	[BASE-64 kodierte AUT-Cert]
Body	
nbf	[Gültigkeitsbeginn (Unixzeit)]
aud	I_AccountManager_Service

Der Parameter alg wird in Abhängigkeit zum verwendeten Signature Type eingetragen und MUSS nach der Auswertung des XML-Attribut `dss:SignatureObject/dss:Base64Signature/@Type` in der vom ExternalAuthenticate zurückgegebenen ASN.1 Struktur ermittelt werden. [≤, KIM-iCM, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

3.1.3 Erweiterung Integritätsprüfung von KIM-Nachrichten

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

Die Integritätsprüfung von KIM-Nachrichten im KIM Clientmodul gibt bisher lediglich die Aussage, ob eine KIM-Nachricht nicht verändert und ob diese aus einer berechtigten Leistungserbringer-Institution (LEI) versendet wurde. Dies lässt bisher keine Aussage zu, ob der Absender der KIM-Nachricht der LEI angehört bzw. die Transportsignatur dem Absender zugeordnet ist.

geändert:

KOM-LE-A_2048-02 -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 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.

Prüfschritte bzgl. des Header-Element „X-KIM-Auth“ [A_28582-*) sind nur dann notwendig, wenn:

1. „X-KIM-Auth“ Header in der inneren und der äußeren Nachricht angegeben ist
2. Die Absender-Adresse aus Header-Element „from“ der entschlüsselten Mail, nicht der Telematik-ID im VZD zugeordnet ist, welche im signer-certificate der CMS-Signatur [RFC5652] angegeben ist [GS-A_4709-* - gemSpec_PKI]

Integritätsprüfungen im Bezug auf das Token aus dem Header-Element „X-KIM-Auth“:

1. Prüfung, dass das Header-Element „X-KIM-Auth“ in innerer und äußere Nachricht nur ein mal vorkommt
2. Prüfung, ob die Token aus innerer und äußerer Nachricht identisch sind
3. Claim "aud" hat Wert "I_Message_Service"
4. Zeitliche Gültigkeit des Tokens - Zeitwert aus Token claim "nbf" liegt nicht in der Zukunft
5. Prüfung, ob das Token korrekt ist (mit Validierung der erzeugten Signatur bzw. des Tokens)
6. Prüfung, ob die Absender-Adresse aus Token claim „sub“ mit dem Wert der Absender-Adresse aus Header-Element „from“ der entschlüsselten Mail übereinstimmt
7. Prüfung, ob die Absender-Adresse der Telematik-ID im VZD zugeordnet ist, welche im Token-Zertifikat („x5c“) angegeben ist [GS-A_4709-* - gemSpec_PKI]
8. Prüfung des Token-Zertifikats aus Token claim „x5c“ über die Operation VerifyCertificate

[<=, Basis-Consumer, KIM-ICM, KOM-LE CM, Sich.techn. Eignung: Herstellererklärung, funkt. Eignung: Test Produkt/FA]

Hinweis:

- Für den Prüfschritt VerifyCertificate besteht ein jeweils temporärer Edge-Case, da aufgrund der Lebensdauer von KIM-Nachrichten (dateTimeToLive in I_AccountLimit_Service) ein zu prüfendes Zertifikat zum Prüfzeitpunkt als "ungültig" gelten kann. Dieser Fall tritt bspw. dann ein, wenn SMC-B- oder HBA-Zertifikate offiziell ablaufen, die damit signierten Nachrichten beim Empfänger noch nicht abgerufen wurden. In Annahme, wird dies nur vereinzelte Nachrichten betreffen, die über langen Zeitraum nicht abgerufen oder kurz vor Ablauf des jeweiligen Zertifikats versendet wurden. Diese Szenario wird entsprechend [A_23165-*) behandelt, sodass kein Payload verloren geht.

- Die Auswertung von "nbf" bzgl. TTL_MSG_AUTH wird dezentral nicht vorgesehen, da die variable Lebensdauer von KIM-Nachrichten zentral, anhand einer Löschfrist abgebildet und im Kontext [A_23422-*] ausgewertet wird. Nachrichten, welche die Löschfrist/Lebensdauer überschreiten sind folglich nicht abrufbar und damit die Prüfung innerhalb dieser Anforderung nicht relevant.

Zur **Prüfung korrespondierender Eintrag in "Tabelle 9: Tab_Verm_Sig_Prüf Vermerke mit Ergebnissen der Signaturprüfung"** erfolgt in einem nachfolgenden Abschnitt.

3.2 Änderung in gemSpec_FD_KOMLE

3.2.1 Erweiterung der Prüfung der Absender-Integrität am KIM Fachdienst

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

Aufgrund der Anforderung "KOM-LE-A_2098-* - Header der äußeren Nachricht" (gemSMIME_KOMLE) wird das Header-Element "X-KIM-Auth" in die äußere Nachricht übernommen, welche zum Mailserver des KIM-Fachdienst übertragen wird. Folglich ist diese Information für u.a. die nachfolgende Zwecke zentral, am KIM Fachdienst auswertbar:

- Motivation zum Update von KIM-Clientmodulen
- Generelle Erweiterung der Absenderintegrität (erst sinnvoll wenn hinreichend große Verbreitung von "X-KIM-Auth")
- Anomalie-Erkennung
- ...

geändert:

A_23422-01 -Sicherstellung Absenderintegrität einer KOM-LE-Nachricht

Der Fachdienst KOM-LE MUSS vor der Verarbeitung einer KOM-LE-Nachricht folgende Prüfregelelemente umsetzen:

1. Der Fachdienst KOM-LE MUSS die Verarbeitung einer KOM-LE-Nachricht mit einem SMTP-Fehler ablehnen, wenn eines der folgenden Merkmale der „originator“ Header-Elemente (RFC 5322) zutrifft, zu beachten ist die unter (3) formulierte Ausnahme:
 - a. Es wurde keine Adresse im Header-Element „from“ angegeben
 - b. Es ist genau eine Adresse im Header-Element „from“ angegeben und diese stimmt nicht mit der Adresse aus dem SMTP-Protokollschritt „MAIL FROM“ überein (RFC 5322 „addr-spec“)
 - c. Es ist mehr als genau eine Adresse im Header-Element „from“ angegeben und die Adressen stimmen nicht mit der Adresse aus dem SMTP-Protokollschritt „MAIL FROM“ übereinstimmen (RFC 5322 „addr-spec“)
 - d. Ein „sender“-Header wurde angegeben und dessen Inhalt entspricht nicht der Adresse (RFC 5322 „addr-spec“) aus dem SMTP-Protokollschritt „MAIL FROM“

e. Es sind Adressdaten im Header-Element „reply-to“ angegeben und diese enden nicht mit den definierten KIM-Domainparts „.kim.telematik“ (PU) bzw. „.kim.telematik-test“ (RU/TU) (RFC 5322 „addr-spec“). Da heißt, es MUSS sichergestellt werden, dass die Angabe, an welche KIM-Adresse eine Antwort gerichtet werden soll, weiterhin möglich ist und dass dies nur für KIM-Adressen erlaubt ist.

2. Der Fachdienst KOM-LE MUSS, nach Prüfungen gemäß (1), die Verarbeitung einer KOM-LE-Nachricht mit einem SMTP-Fehler ablehnen, wenn bei Vorhandensein des Header-Elements „X-KIM-Auth“ [A_28582-*] einer der folgenden Prüfschritte zutrifft:

1. Header-Element „X-KIM-Auth“ ist nicht oder mehrfach vorhanden
2. Claim "aud" hat nicht den Wert "I_Message_Service"
3. Token ist nicht korrekt (mit Validierung der erzeugten Token-Signatur)
4. Absender-Adresse aus Token claim „sub“ stimmt nicht mit dem Wert der Adresse aus dem SMTP-Protokollschritt „MAIL FROM“ (RFC 5322 „addr-spec“) überein
5. Token ist zeitlich nicht gültig
 - a. Prüfzeitpunkt liegt zeitlich nicht zwischen dem Zeitwert aus claim "nbf" und "nbf" + TTL_MSG_AUTH (siehe Tabelle Tab_Konf_Param Standardkonfiguration allgemeine Parameter)
6. Es wurde ein ungültiges Zertifikat im Token claim „x5c“ angegeben. Prüfung gemäß:
 - a. Prüfung des Vertrauensstatus der Aussteller-CA gegen die TSL
 - b. Mathematische Prüfung der Zertifikatssignatur
 - c. Prüfung der zeitlichen Gültigkeit des Zertifikats
 - d. Prüfung, ob der Zertifikatstyp C.HP.AUT oder C.HCI.AUT entspricht [gemSpec_OID - Tab_PKI_405-* OID-Festlegung Zertifikatstyp in X.509-Zertifikaten; gemäß gemSpec_PKI erfolgt Angabe CertificatePolicies]

3. Der Fachdienst KOM-LE DARF die Verarbeitung einer empfangenen KOM-LE-Nachricht gemäß (1) & (2) NICHT ablehnen, wenn genau eine Adresse im SMTP-Protokoll „RCPT TO“ übermittelt wurde und diese Adresse der Absender Adresse aus dem SMTP-Protokollschritt „MAIL FROM“ (RFC 5322 „addr-spec“) entspricht.

4. Der Fachdienst KOM-LE MUSS die obigen Prüfregelein (1) & (2) oder granularer, jeweils konfigurativ (de-)aktivieren können. Im Fall der Deaktivierung müssen die Prüfergebnisse in der Protokollierung bzw. im Monitoring erfasst werden.

[<=, KOM-LE FD, funkt. Eignung: Test Produkt/FA]

Hinweise:

- Item (3) entspricht dem Anwendungsfall Versand/Weiterleitung „an sich selbst“.
- Die oben formulierten Prüfregelein gelten nur für SMTP vom Clientmodul kommend.
- Prüfungen im Kontext des Item (2), dürfen zur Einführung des „X-KIM-Auth“-Headers für eine Übergangszeit, gemäß (4) die Prüfergebnisse nur protokollieren, ins Monitoring überführen.
- Prüfung des Zertifikats aus Token claim "x5c" gegen OCSP oder weiterführend gemäß [GS-A_4652-*] wird aus dem Grund der Erzeugung von Last an den OCSP-Endpunkten und dem Mail-Server des KOM-LE Fachdienstes sowie der folgend notwendigen Prüfung beim Empfänger nicht gefordert [KOM-LE-A_2048-*].

- Eine Prüfung der Zuordnung Telematik-ID zu Absenderadresse ist i.d.R. technisch nicht ohne direkte Aufrufe an VZD oder KIM Account Manager abbildbar. Eine entsprechende Prüfung an dieser zentralen Stelle erzeugt Abhängigkeit, Last und Fehlerpotenzial. Diese Prüfung ist bereits auf Seite des Empfängers gefordert [KOM-LE-A_2048-*].
- Die Auswertung des Token claim "nbf" legt ebenfalls die zeitliche Gültigkeit des Tokens fest, was u.a. die Wiederverwendung des Tokens einschränken kann. Der Zeitwert der Gültigkeitsdauer basiert auf der Annahme, dass die Gesamt-Verarbeitungszeit beim Versand einer KIM-Nachricht (wesentlich sind Signatur, Verschlüsselung, ggf. KAS-Upload, SMTP DATA) diesen Zeitwert nicht überschreitet.

Nachfolgend wird die Auswertung des "aud" claims bzgl. [A_19457-*] auch in bestehender Anforderung, abwärtskompatibel aufgenommen.

geändert:

KOM-LE-A_2187-07 -Authentifizierung des KOM-LE-Teilnehmers über AUT-Zertifikat am Account Manager

Zur Pflege der Basisdaten des Verzeichnisdienstes und bei der Registrierung und Deregistrierung MUSS der Fachdienst die Authentizität des KOM-LE-Teilnehmers über das AUT-Zertifikat des HBA bzw. der SM-B über das vom Clientmodul übergebene Json-Web-Token prüfen. Hierzu MUSS der Fachdienst folgende Prüfschritte durchführen:

- ist das Token korrekt (mit Validierung der erzeugten Signatur),
- der claim "aud" muss den Wert "I_AccountManager_Service" haben oder darf aufgrund Abwärtskompatibilität nicht angegeben sein
- ist das Token zeitlich gültig (also die Verarbeitung erfolgt zwischen nbf + konfigurierter Ablaufzeitspanne (jwtExpiration)),
- 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 der Operation setAccount:
Wenn über setAccount Daten im VZD geändert werden sollen (z.B. kimVersion), dann muss der - in der Operation angegebene - Parameter username (E-Mail Adresse) in dem VZD-Datensatz mit der Telematik-ID des AUT-Zertifikats aus dem Token im mail Attribut der Fachdaten vorhanden sein.
- bei Aufruf der Operation deregisterAccount:
Der - in der Operation angegebene - Parameter username (E-Mail Adresse) muss in dem VZD-Datensatz mit der Telematik-ID des AUT-Zertifikats aus dem Token im mail Attribut der Fachdaten vorhanden sein.

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

[<=, KOM-LE FD, funkt. Eignung: Test Produkt/FA]

3.3 Auswirkungen der Änderungen Transportsignatur und Integritätsprüfung von KIM-Nachrichten - Design-Schwächen

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

1. Harmonisierung der HBA-Nutzung in KIM
 - a. Analog dem Abruf von KIM-Nachrichten, benötigen HBA-assozierte KIM-Accounts nun auch beim KIM-Versand die Angabe der "UserID" im Benutzernamen, sowie einen gesteckten HBA.
 - b. Es resultiert vertretbarer, analog bekannter Aufwand in Konfiguration und Nutzung
 - c. (Einzelfallbetrachtung) Sofern diese Änderung im Kontext der Nutzung von HBA-assozierten KIM-Accounts nicht tragbar ist, kann über das technische Feature "Wechsel der Telematik-ID" die KIM-Adresse auch einer SMC-B zugeordnet und entsprechend genutzt werden.
2. Edge-Case: KIM-Adresse wechselt die Telematik-ID
 - a. Wird die KIM-Adresse des Absenders vor dem Abruf einer KIM-Nachricht beim Empfänger einer anderen Telematik-ID zugewiesen, resultiert es in einem Fehler in der Integritätsprüfung.
 - b. Dieser Fehlerzustand ist bei der Integritätsprüfung erkennbar und wird in einer Fehlermeldung dem Empfänger angezeigt. Der originale Payload wird bei solchen Fehlerfällen aus der Integritätsprüfung trotzdem dem Empfänger bereitgestellt [A_23165-*].
3. Beim Versand von KIM-Nachrichten werden zusätzliche, verarbeitungstechnisch aufwandsarme, performante Aufrufe von Operationen des TI-Konnektors benötigt (*ReadCardCertificate*, *ExternalAuthenticate*)
 - a. Dieses Vorgehen ist jedoch bereits seit KIM 1.5, im Kontext der Anforderung [A_21387-*], gefordert und wird nachgenutzt.
4. Beim Abruf von KIM-Nachrichten wird im Fall der Integritätsprüfung bzgl. Token aus "X-KIM-Auth"-Header [KOM-LE-A_2048-02], welches im Kontext eines HBA erzeugt wurde, ein zusätzlicher Aufruf der Konnektor-Operation "VerifyCertificate" notwendig.
 - a. Vertretbar, da in diesem Fall die Prüfung der Authentizität einer KIM-Nachricht überhaupt möglich wird.
5. Die Prüfungen auf Basis des Tokens aus dem Header-Element "X-KIM-Auth", werden entsprechende Fehlerfälle verursachen, die auf Missbrauch oder unsachgemäße Konfigurationen des TI-Konnektors rückschließen lassen.
6. Diese Lösung ist Abwärtskompatibel und sollte bei regelgerechter, sachgemäßer Nutzung sowie Konfiguration der beteiligten Komponenten keine nachteiligen Auswirkungen bieten.
7. Insgesamt wird die Authentizität in der KIM-Kommunikation gestärkt.
8. Diese technische Lösung kann in der zukünftigen Fortentwicklung nachgenutzt werden.

3.4 Betrachtung Missbrauch des Token aus "X-KIM-Auth"

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

Aufgrund der Konstellation, dass mit Einführung des Header-Elements "X-KIM-Auth" auch weiterhin KIM-Systemkomponenten im Feld sind, welche diese Information noch nicht kennen sowie im Sicherheitskontext "never trust the client" bzw. dem Sicherheitsparadigma "ZeroTrust", gilt nachfolgende Betrachtung:

- Header-Element "X-KIM-Auth" wird für Primärsysteme sichtbar und könnte ("missbräuchlich") weitergenutzt werden
 - Die Wiederverwendung des Tokens kann stets gemäß [A_23422-01] behandelt werden.
 - Mit Blick in Zukunft, könnte Header-Element "X-KIM-Auth" durch Primärsysteme analog ausgewertet werden.
- Wird eine originale Nachricht bereits mit dem Header-Element "X-KIM-Auth" über KIM versendet, werden folgende Szenarien betrachtet (Primärsystem/Angreifer (PS); KIM Clientmodul (CM), KIM Fachdienst (FD)):
 - a. Sender PS -> Sender CM (alt) -> FD (alt, neu) -> Empfänger CM (alt) -> Empfänger PS
 - Sender CM (alt) leitet Header-Element "X-KIM-Auth" weiter
 - FD handelt gemäß [A_23422-01]
 - Empfänger CM (alt) wertet Information nicht aus, wie bisher = keine Auswirkung
 - b. Sender PS -> Sender CM (neu) -> FD -> Empfänger CM (alt) -> Empfänger PS
 - Sender CM (neu) überschreibt Header-Element "X-KIM-Auth", oder Abbruch gemäß [A_28582-*]
 - FD handelt gemäß [A_23422-01]
 - Empfänger CM (alt) wertet Information nicht aus, wie bisher = keine Auswirkung
 - c. Sender PS -> Sender CM (alt) -> FD -> Empfänger CM (neu) -> Empfänger PS
 - Sender CM (alt) leitet Header-Element "X-KIM-Auth" weiter
 - FD handelt gemäß [A_23422-01]
 - Empfänger CM (neu) für Integritätsprüfung gemäß [KOM-LE-A_2048-02] durch
 - d. Sender PS -> Sender CM (neu) -> FD -> Empfänger CM (neu) -> Empfänger PS
 - Sender CM (neu) überschreibt Header-Element "X-KIM-Auth", oder Abbruch gemäß [A_28582-*]
 - FD handelt gemäß [A_23422-01]
 - Empfänger CM (neu) für Integritätsprüfung gemäß [KOM-LE-A_2048-02] durch
 - e. Szenario (2) & (3) sind für den Fall, dass ein PS direkt an FD sendet analog zu betrachten.
- Verwendung des Token aus "X-KIM-Auth" anI_AccountManager_Service
 - Token könnte für Authentisierung am KIM Account Manager genutzt werden

- Verhinderung durch abwärtskompatible Einführung und Prüfung des Token claims "aud" gemäß [KOM-LE-A_2187-07]. Angabe des Token claim "aud" wird mit [A_28582]; [A_19457-05] und durch [KOM-LE-A_2187-07];[A_23422-01]; [KOM-LE-A_2048-02] prüft
- Token claim "nbf", als Angabe zum Gültigkeitsbeginn, wird im Kontext [KOM-LE-A_2187-07] & [A_23422-01] ausgewertet, um die Wiederverwendung von Token in KIM zentral einzuschränken.

Für KIM FD wurde angenommen, dass dieser die Feature bereits zentral bereitgestellt hat.

In Folge der Betrachtung, der sicherheitstechnischen Bewertung des Kontext JWT - "replay attack", ist die Wiederverwendung eines Token aus dem Header-Element "X-KIM-Auth" als unproblematisch anzusehen, da:

- das Token in Konstellationen "alter" KIM-Komponenten nicht ausgewertet wird,
- das Token keinen Zugriff o.ä. legitimiert, sondern Aussage über die Authentizität des Absenders beim Empfänger bietet,
- die Prüfung der Authentizität im Kontext der Integritätsprüfung gegeben ist, auf Empfängerseite stattfindet,
- das Token sogar durch Primärsysteme analog ausgewertet werden könnte,
- die Wiederverwendung durch [A_23422-01] am FD erkannt werden kann,
- die Kombination der zentralen Sicherstellung der Absender-Integrität [A_23422-01] und Integritätsprüfung auf Empfänger-Seite [KOM-LE-A_2048-02] auch bei Wiederverwendung eines solchen Tokens sicherstellt, dass die Nachricht vom zugehörigen Absender stammen muss.

4 Änderungen bzgl. Ergebnis der Integritätsprüfung von KIM-Nachrichten - Design-Schwächen

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

Im Kontext des Abrufs von KIM-Nachrichten erfolgt nach der Entschlüsselung eine Integritätsprüfung. Die aktuelle Umsetzung der Integritätsprüfung lässt es zu, dass im Fall technisch transienter Fehlerbilder KIM-Nachrichten nicht oder immer unbehandelt an den Empfänger ausgegeben werden. Folglich resultieren auch missbräuchlich induzierte, technisch transiente oder gänzlich persistente Fehlerbilder in einem positiven Ergebnis der Integritätsprüfung. Teil der Integritätsprüfung ist u.a. die Signaturprüfung, welche wiederum von einer Vielzahl technischer Komponenten (Konnektor, OCSP, ...) abhängig ist.

Aus Sicht der Sicherheit muss standardmäßig gelten, dass bei einem negativen Ergebnis der Integritätsprüfung, den empfangenen Daten nicht vertraut werden darf. Jedoch müssen auch in diesem Fall stets entsprechende Fehler-Informationen an den Empfänger ausgegeben werden, damit der Fehlerzustand erkannt und behandelt werden kann.

KIM wird zu einem Großteil als Transportschicht von Fachverfahren genutzt, bspw. eAU. Diese Verfahren sehen i.d.R. eine zusätzliche Authentizität des payloads vor, bspw. QES signierter eAU payload. Ein transientes Problem in der Integritätsprüfung, durch bspw. temporäre Störung OCSP, kann folglich zu massenhaften Fehlerfällen in der Verarbeitung der Fachverfahren des Empfangssystems führen. Folglich muss die Ausgabe des entschlüsselten payloads auch bei Fehlern in der Integritätsprüfung, als Teil der Fehlernachricht, konfiguratativ möglich sein. Die Authentizität des payloads kann durch das Empfangssystem (nach-)geprüft werden.

Abgeleitet gilt, dass eine KIM-Nachricht nur bei positiven Ergebnis der Integritätsprüfung, ohne nachfolgend beschriebene Fehlernachricht, an den Empfänger ausgegeben werden darf (Positiv-Fall). Die nachfolgenden Änderungen adressieren ebenfalls den Bedarf nach eindeutig identifizierbaren Fehler-Informationen, welche zusätzlich maschinell auswertbar sein sollen. In früheren Iterationen von KIM konnten Informationen zu Fehlern aus der Integrationsprüfung (Signaturprüfungsbericht, Vermerke) nicht eindeutig zugeordnet werden und waren fälschbar, ausblendbar.

Die nachfolgenden Änderungen zur Fehlernachricht aus der Integrationsprüfung sind als abwärtskompatibel anzusehen. Geeignete, maschinenauswertbare Informationen außerhalb des Fließtext werden weitergenutzt und Informationen ergänzt. Es resultieren wiederum mehr Möglichkeiten & Freiheitsgrade der maschinellen Auswertung durch Primärsysteme. Bestehende Sicherheitsmechanismen in Empfänger-Umgebungen werden durch diese Änderung nicht obsolet.

4.1 Änderung in gemSpec_CM_KOMLE

geändert:

A_23165-01 -Verhalten bei fehlgeschlagener Integritätsprüfung

Das Clientmodul MUSS nach einer fehlgeschlagenen Integritätsprüfung eine Fehlernachricht mit folgenden Inhalten generieren und an Stelle der entschlüsselten, originalen Mail an den aufrufenden Client zurückgeben. Entgegen [A_28602-*) gelten für

diese Fehlernachricht spezifische Festlegungen.

Das Clientmodul MUSS die Header-Elemente der entschlüsselten, originalen Mail als Header-Elemente der Fehlernachricht übernehmen und diese entsprechend umliegender sowie nachfolgender Anforderungen analog anpassen. Das Header-Elementsubject ist wie folgt anzugeben: "Fehler bei der Integritätsprüfung festgestellt"

Das Clientmodul MUSS eine UUID [RFC4122] als jene in diesem Fehler-Kontext aktuelle Referenz auf angehängte Daten generieren und diese als Wert des Header-Element X-KIM-IntegrityCheckRefID angeben. Das Clientmodul MUSS sicherstellen, dass dieses Header-Element nur ein mal vorkommt und stets die im Verarbeitungskontext neu-erzeugte UUID als Wert dieses Header-Elements angegeben ist.

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

~~Alternativ MUSS es möglich sein, über eine Konfiguration im Clientmodul, die-entschlüsselte (originale) Nachricht trotz fehlgeschlagener Integritätsprüfung und-Beachtung nachfolgender Anforderungen dem Empfänger weiterzuleiten.~~

Das Clientmodul MUSS gemäß einer Konfiguration im Clientmodul die entschlüsselte, originale Mail der Fehlernachricht als Anhang, mit folgenden Header-Elementen als MIME-Part anfügen können:

Content-Type: message/rfc822; name="<Wert von X-KIM-IntegrityCheckRefID>.eml"

Content-Disposition: attachment; filename="<Wert von X-KIM-IntegrityCheckRefID>.eml"

Diese Konfiguration MUSS standardmäßig deaktiviert sein.

Das Clientmodul MUSS bei negativem Ergebnis der Signaturprüfung den VerificationReport aus dem VerificationResult (oasis-dssx-1.0-profiles-vr-cd1.xsd) der VerifyDocumentResponse entnehmen (sofern vorhanden) und der Fehlernachricht als Anhang, mit folgenden Header-Elementen als MIME-Part anfügen:

Content-Type: application/xml; name="VerificationReport_<Wert von X-KIM-IntegrityCheckRefID>.xml"

Content-Disposition: attachment; filename="VerificationReport_<Wert von X-KIM-IntegrityCheckRefID>.xml"

(Hinweis: Sofern das Format des VerificationReports nicht xml entspricht, kann die Formatangabe in diesem MIME-Part entsprechend angepasst werden.)

Das Clientmodul MUSS im Mail-Body der Fehlernachricht genau einen text/plain MIME-Part mit folgendem Text angeben:

"Bei der Prüfung dieser abgerufenen KIM-Nachricht wurde eine Verletzung der technischen Integrität festgestellt. Somit darf den empfangenen Daten nicht vertraut werden."

Details:

<Angaben zum Prüfschritt und Ursache(n) aus der Integritätsprüfung. Zum Beispiel wenn negatives Ergebnis Zertifikatsprüfung, Details zum Zertifikat angeben, um zu Erkennen ob diese abgelaufen ist.>

Anhänge:

- (wenn vorhanden) Signaturprüfungsbericht „<Wert von X-KIM-

IntegrityCheckRefID>.xml“

- (abhängig von Konfiguration)Empfangene KIM-Nachricht „<Wert von X-KIM-IntegrityCheckRefID>.eml“, diese können Sie eigenverantwortlich, nach Prüfung (Virens Scanner oder Sonstige) mit E-Mail-Software, oder Andere öffnen und weiterverarbeiten.

Weitere Anhänge dieser Nachricht, welche nicht die Referenz<Wert von X-KIM-IntegrityCheckRefID>ausweisen, sind diesem Fehlerfall nicht zugeordnet.

Bitte kontaktieren Sie Ihren/Ihre Systembetreuer*in zum sicheren Umgang bzgl. der angehängten Daten sowie technischen Problembeseitigung!“

[<=, Basis-Consumer, KIM-iCM, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

Hinweis:

- Es muss sichergestellt werden, dass eine entschlüsselte KIM-Nachricht und damit nutzbarer Payload an den Empfänger ausgegeben wird. U.a. dürfen technisch transiente Ursachen nicht dazu führen, dass ggf. zeitkritischer Payload den Empfänger nicht erreicht. Es gilt in diesen Fällen die Sorgfalt und security policies der Empfängerumgebung einzubeziehen.
- Das Dateiformat ".eml", in dem die entschlüsselte, originale Mail der Fehlernachricht angehängt wird, kann geeignet nachverarbeitet, so auch in marktüblicher E-Mail-Client-Software geöffnet/importiert werden.
- 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

Anpassung Auflistung zu Fehlerfällen der Integritätsprüfung

Aufgrund der Erweiterung der Integrationsprüfung [A_23422-01] sowie Anpassung im Umgang mit Fehlern aus der Integrationsprüfung [A_23165-01], wird nachfolgend die Auflistung entsprechender Zustände angepasst.

geändert:

Tabelle 3: Tab_Verm_Sig_Prüf Vermerke mit Ergebnissen der Signaturprüfung

ID*	Fehlercode	Ergebnis
01	-	Die Signatur der Nachricht wurde erfolgreich geprüft.
02	4115	Die Integrität der Nachricht wurde verletzt.
03	4253	Die digitale Signatur ist nicht vorhanden.
04	4112	Die digitale Signatur konnte aufgrund des falschen Formats nicht geprüft werden.
05	4206	Der Zertifizierungspfad des Signaturzertifikats kann nicht validiert werden.
06	[Fehlercode]	Die digitale Signatur konnte aufgrund eines nicht zuordenbaren Fehlercodes des Konnektors nicht geprüft werden.
07	4264-	Die digitale Signatur ist mathematisch korrekt, der Zertifikatsstatus des Signaturzertifikats konnte aber nicht geprüft werden.
08	-	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.
09	-	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.
10	-	<p>Prüfung der Authentisierung der KIM-Nachricht (X-KIM-Auth) schlug fehl.</p> <p><i>Hinweis:</i> Fehlertext soll <ergänzende Information zum den Fehler auslösenden Prüfschritt> angeben.</p>

5 Veränderung bzgl. E-Mail-Fehlernachrichten des KIM Clientmoduls - Design-Schwächen

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

Das KIM-Clientmodul (CM) erzeugt im Verlauf technischer Funktionen zwei differenzierbare Typen von E-Mail-Fehlernachrichten:

1. E-Mail-Fehlernachricht, die als DSN - Delivery Status Notification gemäß [RFC3461-3464] an den KIM-FD versendet wird. Empfänger ist der Absender der ursprünglichen Nachricht, in deren Kontext der Fehlerfall aufgetreten ist.
2. E-Mail-Fehlernachricht, die beim Nachrichten-Abruf generiert und direkt, an Stelle der entschlüsselten, originalen E-Mail an den abrufenden Client ausgegeben werden.

Problem-Aspekte bzgl. E-Mail-Fehlernachrichten

- Eine als DSN generierte Fehlernachricht kann schützenswerte Daten der originalen Nachricht enthalten (Header-Element oder ganze Nachricht) und wird weder signiert noch verschlüsselt übertragen.
 - Es existieren keine Festlegungen zum Umgang des RET-Parameters (Werte: HDRS = nur Header, FULL = ganze Nachricht) gemäß RFC 3464.
 - Ist der RET-Parameter nicht in SMTP MAIL FROM angegeben, kann das System selbst entscheiden, welche Daten zusätzlich in der DSN angegeben werden.
- Festlegungen aus KIM Hotfix 1.5.2-10 zur Anforderung A_20771-02 behandeln bereits jede definierte E-Mail-Fehlernachricht zentral als DSN.
 - Gemäß RFC 3464 sollen DSN durch das tatsächlich zustellende System (MTA) generiert werden. Das KIM CM ist lediglich Proxy, sodass eine DSN-Erzeugung in CM architektonisch unsauber ist.
 - Festlegungen der A_20771-02 reduzieren das Datenschutzrisiko bereits, da nur ein Text-Teil der von CM eingelieferten DSN übernommen wird.
- Folglich entstehen unnötige Komplexität und Fehlerquellen im KIM CM bzgl. der Generierung von zu versendenden E-Mail-Fehlernachrichten als DSN.
- Redundante Festlegungen an verschiedenen Stellen der Spezifikation bzgl. o.g. Fehlernachrichten, begünstigen Komplexität und Risiko heterogener, fehlerhafter Umsetzungen.

Problem-Aspekt häufig wiederholter, redundanter E-Mail-Fehlerbenachrichtigung

- Primärsysteme rufen E-Mail- Fehlerbenachrichtigungen meist nicht ab oder werten diese nicht aus.
- Automatisiert arbeitende Primärsysteme verursachen wiederholt und in großer Menge gleiche Fehlerfälle, die wiederum zu massenhaft redundanten E-Mail-Fehlerbenachrichtigung führen, die das Gesamt-System KIM und die TI belasten.
 - Beispiel: Ein dunkel-verarbeitendes Labor-Primärsystem sendet pro Tag tausendfach automatisiert KIM-Nachrichten mit einem Empfänger aus KIM-fremder

E-Mail-Domain (@xyz.de). Daraus resultieren in mindestens gleicher Menge E-Mail-Fehlernachrichten, u.a. gemäß KOM-LE-A_2024-*, die den gleichen Inhalt haben

- Entsprechende Problem-Fälle sind auch an anderen Stellen der Spezifikation möglich, bekannt oder vorhanden.
- Redundante Festlegungen an verschiedenen Stellen der Spezifikation bzgl. o.g. Fehlernachrichten, somit Komplexität und Risiko heterogener, fehlerhafter Umsetzungen.

Diese Problem-Aspekte sollen durch die nachfolgenden neuen Anforderungen adressiert werden. Diese Anforderungen erzeugen eine notwendige Abstraktion und führen zu entsprechenden Änderungen, Vereinfachung sowie Reduktion der Komplexität in bestehenden Anforderungen, ohne jedoch diesbezügliche Bestandsfunktionalität wesentlich zu verändern. Die Menge der veränderten Anforderungen, welche in ihren Teilen die Generierung von E-Mail-Fehlernachrichten behandeln, ist damit begründet, dass redundante Festlegungen in diesen Anforderungen bestehen, welche in die nachfolgenden neuen Anforderungen herausgelöst, abstrahiert werden sollen.

5.1 Änderung in gemSpec_CM_KOMLE

neu:

A_28601 -Vorgaben für zu versendende E-Mail-Fehlernachrichten

Das Clientmodul MUSS eine E-Mail-Fehlernachricht so erzeugen, dass diese einen MIME-Part des Content-Type: text/plain; charset=utf-8 enthält, in dem ein Fehlertext angegeben ist. Das Clientmodul MUSS das Header-Element „X-KIM-Fehlermeldung“ mit einem dem Fehler entsprechenden Wert angeben.

Das Clientmodul MUSS sicherstellen, dass die generierte E-Mail-Fehlernachricht an die Empfängeradresse gesendet wird, welche als Absenderadresse im SMTP-Protokollschritt „MAIL FROM“ (RFC 5322 „addr-spec“) vom Clientsystem angegeben wurde und diese eine Adresse in den Header-Elementen „from“ und „to“ der E-Mail-Fehlernachricht angeben.

Veränderungen des Inhalts dieser E-Mail-Fehlernachricht, bspw. zusätzliche Header-Elemente, fehler-relevante Informationen durch spezifischere Festlegungen, MUSS möglich sein.

Die E-Mail-Fehlernachricht ist entgegen der Festlegung [KOM-LE-A_2019-*] weder zu signieren, noch zu verschlüsseln.

[<=, Basis-Consumer, KIM-iCM, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

neu:

A_28602 -Vorgaben für beim Nachrichten-Abruf generierten E-Mail-Fehlernachrichten

Das Clientmodul MUSS eine E-Mail-Fehlernachricht, die direkt dem aufrufenden Clientsystem zurückgegeben wird, mit dem Content-Type: multipart/mixed und den nachfolgenden Inhalten erzeugen:

- Übernahme der Header-Elemente orig-date, from, sender, reply-to, to, cc sowie alle mit X-KIM- beginnenden Header-Elemente der äußeren, abgerufenen KOM-LE-S/MIME-Nachricht als Header-Elemente der E-Mail-Fehlernachricht
- Ein MIME-Part des Content-Type: text/plain; charset=utf-8 in dem ein Fehlertext angegeben ist

- Ein MIME-Part Content-Type: message/rfc822, welcher die vom Fachdienst abgerufene verschlüsselte KOM-LE-S/MIME-Nachricht enthält

Eine Veränderungen des Inhalts dieser E-Mail-Fehlernachricht, bspw. zusätzliche Header-Elemente, fehler-relevante Informationen, durch spezifischere Festlegungen, MUSS möglich sein.

[<=, Basis-Consumer, KIM-iCM, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

Hinweis:

Entsprechend spezifischere Festlegungen existieren bspw. im Kontext von [A_23165-]*

neu:

A_28603 -Caching einer gesendeten E-Mail-Fehlerbenachrichtigung

Das Clientmodul MUSS sicherstellen, dass gleiche, für einen SMTP-Versand bestimmte E-Mail-Fehlerbenachrichtigungen, innerhalb des Zeitraums von TTL_ERR_MSG (siehe Tabelle Tab_Konf_Param Standardkonfiguration allgemeine Parameter), nur einmal an den gleichen Empfänger gesendet werden.

[<=, Basis-Consumer, KIM-iCM, KOM-LE CM, funkt. Eignung: Herstellererklärung, funkt. Eignung: Test Produkt/FA]

Hinweis:

Da Fehlernachrichten veränderlichen Inhalt haben können, wird ein caching anhand der normalisierten Empfängeradresse, des Fehlercodes sowie einem eindeutigen hash des Textinhalts des text/plain MIME-Parts empfohlen. So kann erkannt werden, dass ein Fehlerfall wiederholt, mit gleichem Informationskontext aufgetreten ist und verhindert werden, dass E-Mail-Fehlernachrichten mit gleicher Aussage mehrfach, in kurzem Abstand versendet wird.

5.1.1 Änderungen bestehender Anforderungen der E-Mail-Fehlernachrichten

A_24020-06 -Größe der auf dem KAS abgelegten Mail-Daten

Das Clientmodul MUSS beim Empfang einer KOM-LE-Nachricht mit einer KIM-Attachment-Datenstruktur die HTTP Head Methode an der OperationreadMailData der Schnittstelle I_Attachment_Service aufrufen, um die Größe der auf dem KAS abgelegten Mail-Daten über den Header Content-Length zu ermitteln. Der ausgelesene Wert wird für den Abgleich mit dem im Mail-Header Attribut X-KIM-KAS-EncSize hinterlegten Wert genutzt. Entspricht der Wert nicht dem dort hinterlegten Wert, dann wird der Download nicht durchgeführt und der Empfänger mit einer Fehlernachricht gemäß [A_28602-*] und korrespondierenden Fehlertext aus Tab_Fehlertext_Download informiert. [<=, Basis-Consumer, KIM-iCM, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

A_23512-03 -Auswertung der KOM-LE-Version bei Nachrichten mit KAS-Content

Das Clientmodul MUSS beim Empfang einer KOM-LE-Nachricht mit einer KIM-Attachment-Datenstruktur prüfen, ob für den Empfänger eine Freigabe zum Empfang großer Nachrichten vorliegt. Ist dies nicht der Fall, MUSS das Clientmodul die Weiterverarbeitung der Nachricht und damit dem Abruf der KAS-Daten unterbinden. ~~Das Clientmodul MUSS in diesem Fall eine Fehlernachricht an den Empfänger erzeugen. Als Fehlernachricht MUSS eine multipart/mixed MIME-Nachricht an das Clientsystem übermittelt werden, welche die verschlüsselte KOM-LE-S/MIME-Nachricht als eine message/rfc822 MIME-Einheit~~

beinhaltet. In diesem Fall muss eine Fehlernachricht gemäß [A_28602-*) an das Clientsystem ausgegeben werden. Das subject Header-Element der neuen multipart/mixed Nachricht Fehlernachricht erhält den Wert „Die KIM-Nachricht kann nicht empfangen werden, weil der Empfang großer Nachrichten nicht aktiviert wurde“. Im Fehlertext der Nachricht muss der Empfänger darauf hingewiesen werden, dass eine Nachricht empfangen wurde, die aufgrund deren Größe gemäß der Account-Einstellung (KOM-LE-Version) nicht verarbeitet werden darf. Das Header-Element X-KIM-Fehlermeldung MUSS den Fehlercode 4018 enthalten. Es MUSS im Fehlertext darauf hingewiesen werden, wie entsprechende Konfigurationen über den Account-Manager angepasst werden können und wie der Empfänger den Empfang durch Weiterleitung der Fehlernachricht wiederholen kann. So kann, nach Anpassung der KOM-LE-Version, die Nachricht an den Empfänger weitergeleitet und erneut abgerufen werden. Zusätzlich muss diese multipart/mixed MIME-Nachricht eine text/plain MIME-Einheit mit geeignetem Fehlertext enthalten. Die orig-date, from, sender, reply-to, to und cc Header-Elemente der neuen multipart/mixed Nachricht werden aus der empfangenen KOM-LE-S/MIME-Nachricht übernommen. [≤, Basis-Consumer, KIM-iCM, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

Weitere Änderungen von A_19370-08 - Download von E-Mail-Daten (in diesem Dokument in Abschnitt 2.1.2):

Die Unterscheidung zwischen persistentem und transientem Fehler wird entfernt, da:

- im Fall des persistenten Fehler die Abbildung als multipart/mixedMIME-Nachricht nicht korrekt war,
- Erhalt von Freiheits-Graden im Fall eines persistenten Fehlers
 - Persistenter Fehler an einem Interface kann nicht deterministisch aussagen, ob die Daten jemals, durch bspw. organisatorische Maßnahmen, Updates, Backups, doch wieder verfügbar, abrufbar, verarbeitbar werden,
- Harmonisierung & Komplexitätsreduktion der Fehlerbehandlung im Clientmodul,
- Erhalt von ggf. wichtigen Header-Information der abgerufenen KOM-LE-S/MIME-Nachricht, auch im Falle eines persistenten Fehlers,
- Die KOM-LE-S/MIME-Nachricht bedeutet an dieser Stelle nur eine geringe Datenmenge, da es sich um die verschlüsselte KAS-Nachricht handelt, so wie sie auch in allen verwandten, Fehlerfällen an dieser Stelle zurückgegeben wird.

Tabelle 4: Tab_Fehlertext_Download Fehlertext beim Download von E-Mail-Daten

Bedingung	Fehlertext
E-Mail-Daten konnten nicht heruntergeladen werden. (transienten Fehler)	Die 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. Bleibt der Fehler bestehen kontaktieren sie Ihren/Ihre Systembetreuer*in.
E-Mail-Daten konnten nicht entschlüsselt werden. (persistenter Fehler)	Die E-Mail-Daten dieser Nachricht konnten nicht entschlüsselt werden, bitte kontaktieren Sie den Absender der Nachricht.

E-Mail-Daten auf dem KAS passen nicht zu der, in der KIM-Attachment-Datenstruktur, angekündigten Größe.

Die E-Mail-Daten dieser Nachricht passen nicht zu der vom Sender angekündigten Größe. Eine erneute Abholung ist nicht sinnvoll.

A_22412-03 -Behandlung von Zugriffs-Limitierung

Das Clientmodul MUSS bei Aufruf der Operation readMailData und der Rückgabe des HTTP-Fehlercodes 429 vom KAS, eine Fehlernachricht gemäß [A_28602-*], mit dem Header-Element X-KIM-Fehlermeldung und Wert 4013 [Tab_Fehlercodes_KOMLE-Clientmodule] erzeugen und an das Clientsystem ausgeben. Als Fehlertext sind die korrespondierenden Texte aus den Tabellen [Tab_Fehlercodes_KOMLE-Clientmodule] und [Tab_Fehlertext_Download] anzugeben. Das subject Header-Element Fehlernachricht erhält den Wert „Die E-Mail-Daten konnten nicht abgerufen werden“.

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 gemäß der Tabelle "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“.

[<=, KIM-ICM, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

A_19356-09 -Prüfen der Version des Empfängers

Das Clientmodul MUSS, wenn es vom Clientsystem ein RCPT TO:<recipient-address> Kommando erhält, prüfen, welche KOM-LE-Version für den im Kommando aufgeführten Empfänger im LDAP-Directory Attribut: kimData im Verzeichnisdienst [gemSpec_VZD#5] eingetragen ist. Ist das LDAP-Directory Attribut: kimData für den Empfänger undefiniert, dann muss ein KOM-LE-Clientmodul mit einer Version 1.0 angenommen werden. Wenn eine Client-Mail größer als 15 MiB versendet werden soll, dann MUSS für jeden Empfänger durch Abfrage des Eintrags im Verzeichnisdienst geprüft werden, ob die KOM-LE-Version des Empfängers mit einem + (zum Beispiel Wert: 1.5+) erweitert wurde. Wenn eine Client-Mail größer als 15 MiB an einen Empfänger mit KOM-LE-Version < 1.5 versendet werden soll, oder die KOM-LE-Version nicht mit einem + (zum Beispiel Wert: 1.5+) erweitert wurde, MUSS das KOM-LE-Clientmodul diesen Empfänger aus der Mail entfernen. Beim Entfernen eines Empfängers MUSS das KOM-LE-Clientmodul den Absender mit einer E-Mail-Fehlernachricht gemäß [A_28601-*] 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]. Im Positivfall MUSS das Clientmodul das Kommando an den MTA weiterleiten. 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. [<=, Basis-Consumer, KIM-ICM, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

KOM-LE-A_2192-03 -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 E-Mail-Fehlernachricht gemäß [A_28601-*] informieren. Die Fehlernachricht ist weder zu signieren noch zu verschlüsseln und entspricht der Delivery Status Notification gemäß [RFC3461-3464].

[<=, Basis-Consumer, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

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

KOM-LE-A_2024-03 -Information des Absenders über Empfänger, für die nicht verschlüsselt werden kann

Eine Nachricht darf nur an Empfänger versendet werden, für die verschlüsselt werden konnte. Über alle anderen Empfänger, für die aufgrund von fehlenden oder ungültigen Zertifikaten nicht verschlüsselt werden konnte, MUSS das Clientmodul den Absender mit einer E-Mail-Fehlernachricht, gemäß [A_28601-*] und dem Mail-Header-Attribut X-KIM-Fehlermeldung mit dem Wert 4004, über den Fehlerfall informieren. Die Fehlernachricht entspricht der Delivery Status Notification gemäß [RFC3461-3464]. und enthält das Mail-Header-Attribut X-KIM-Fehlermeldung mit dem Wert 4004. Die Fehlernachricht ist weder zu signieren noch zu verschlüsseln.

[<=, Basis-Consumer, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

A_21391-04 -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 eine Fehlernachricht gemäß [A_28602-*], mit dem Fehlertext, "Das verwendete Clientmodul unterstützt die in der empfangenen Nachricht angegebene KIM-Version<KIMVersion> nicht." enthalten, an das Clientsystem zurückgeben. Zusätzlich muss diese neue multipart/mixed MIME-Nachricht eine text/plain MIME-Einheit mit dem Fehlertext, "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 der empfangenen Nachricht wird nicht unterstützt“.

[<=, Basis-Consumer, KIM-iCM, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

KOM-LE-A_2046-02 -Aufbau der Fehlernachricht bei fehlgeschlagener Entschlüsselung

Das Clientmodul MUSS eine empfangene, dem KOM-LE-S/MIME-Profil entsprechende Nachricht, die z.B. auf Grund des fehlenden Schlüssels nicht entschlüsselt werden kann, als eine Fehlernachricht gemäß [A_28602-*] dem Clientsystem übermitteln. Zusätzlich muss diese neue multipart/mixed MIME-Nachricht eine text/plain MIME-Einheit mit dem Fehlertext enthalten. Die orig-date, from, sender, reply-to, to und cc-Header-Elemente der neuen multipart/mixed-Nachricht und alle X-KIM-Header-Elemente werden aus der empfangenen Nachricht übernommen. Das subject-Header-Element der neuen multipart/mixed-Nachricht erhält den Wert „Die Nachricht konnte nicht entschlüsselt werden“. [<=, Basis-Consumer, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

A_21381-02 -Automatischer Abruf der PKCS#12-Datei

Das Administrationsmodul MUSS einen Monat vor Ablauf des TLS-Zertifikates automatisch ein neues Zertifikat über die Operation createCert() beantragen und herunterladen. Die

zeitliche Gültigkeit des Zertifikats muss vom Clientmodul beim TLS-Verbindungsaufbau geprüft werden. Zusätzlich MUSS geprüft werden, ob für den TLS-Verbindungsaufbau bereits ein ECC (NIST) Zertifikat im Clientmodul hinterlegt ist. Existiert bereits ein ECC (Brainpool) Zertifikat, darf dieses, bis zum **Laufzeitende**, genutzt werden. Ist dies nicht der Fall, MUSS über die Operation `createCert()`, ein neues Zertifikat beantragt und heruntergeladen werden.

Wenn während der Aktualisierung ein Fehler auftritt, dann MUSS das KOM-LE-Clientmodul den Absender mit einer **E-Mail-Fehlernachricht gemäß [A_28601-*]** über den Fehlerfall informieren. Aus dem Inhalt der Fehlernachricht MUSS hervorgehen, dass bei der Aktualisierung der PKCS#12-Datei ein Fehler aufgetreten ist. **Die Fehlernachricht ist weder zu signieren noch zu verschlüsseln und entspricht der Delivery Status Notification gemäß [RFC3461-3464].** Zusätzlich muss der vom Account Manager gemeldeter Fehlertext wie folgt eingefügt werden: Fehlertext: <message>.

[<=, KIM-iCM, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

Weitere:

1. In Abschnitt "3.4.1 Übersicht":

- Wenn die Integritätsprüfung der entschlüsselten KOM-LE-Nachricht fehlschlägt ...
"eine Fehlernachricht an den Empfänger der KOM-LE-Nachricht **gesendet zurückgegeben**"

2. In Abschnitt "3.4.4.2.1 Entschlüsselung":

Absatz zum Umgang mit Entschlüsselungsfehler ändert sich wie folgt:

Wenn die Entschlüsselung fehlschlägt, wird dem Clientsystem die verschlüsselte Nachricht im Anhang einer Fehlernachricht gemäß [A_28602-*] übermittelt. **Hierzu wird die angekommene KOM-LE-S/MIME-Nachricht als eine message/rfc822 MIME-Einheit in eine multipart/mixed MIME-Nachricht verpackt, die zusätzlich eine text/plain MIME-Einheit mit der Fehlermeldung enthält. Die orig-date, from, sender, reply-to, to und cc Header Elemente der neuen Nachricht werden aus der ursprünglichen Nachricht übernommen.** Der Betreff der neuen Nachricht enthält die Zeichenkette „Die Nachricht konnte nicht entschlüsselt werden“.

6 Weiteres

6.1 Inkonsistenzen ESMTP & POP3 Capabilities

6.1.1 Änderung in gemSpec_CM_KOMLE

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

Durch KIM 1.5 wurde die Möglichkeit geschaffen E-Mail-Daten bis zu 500 MB zu übermitteln. Die Kommunikation zu diesem Feature bezieht sich auf die Nutzersicht, sodass heterogene Funktionsweisen von E-Mail-Clients einbezogen werden müssen, die in KIM genutzt werden. Da E-Mail-Clients die Daten vor dem Versand, oft für den Nutzer nicht sichtbar "anpassen", nimmt die Brutto-Datenmenge durch bspw. base64-Kodierung (500 MB -> ~700 MB) zu. Daraus würde das Problem-Szenario entstehen, in dem ein Nutzer eine E-Mail mit 500 MB Datei-Anhang erstellt, diese aber nicht versenden kann, da das KIM-Clientmodul nicht die entsprechend größere Datenmenge zulässt. In solchen Fällen wären generell, aus Nutzersicht "nur" ~357 MB, statt der zugesagten 500 MB möglich.

Diese Funktionsweise ist bereits seit KIM 1.5 gegeben. Die nachfolgende Änderung passt lediglich die falsche Angabe des "alten" Werts von 35 MiB auf 700 MiB an, was ebenfalls Konsistenz zur geltenden Spezifikation bzgl. "maxMailSize" in I_AccountLimit_Service schafft.

geändert:

im Kapitel 3.3.2.1 Initialisierung

[...]

Tabelle Tab_SMTP_Ant_Init beschreibt Antworten, die das Clientmodul dem Clientsystem im CONNECT-Zustand sendet.

Tabelle 5: Tab_SMTP_Ant_Init Antworten Clientmodul im CONNECT-Zustand

SMTP-Kommando (Clientsystem -> Clientmodul)	SMTP-Antwortcode (Clientmodul -> Clientsystem)
HELO	"250 OK" Antwortcode
EHLO	"250 OK" Antwortcode mit folgenden EHLO Kennworten: SIZE <size> AUTH LOGIN PLAIN 8BITMIME ENHANCEDSTATUSCODES DSN und <size> gleich oder größer als 35882577734003200
AUTH	Anmeldungsdaten erhalten und Verbindungsaufbau mit

	dem MTA beginnen (siehe Kapitel 3.2.2.2)
RSET, NOOP	„250 OK“ Antwortcode
MAIL, RCPT, DATA	„530 5.7.0“ Antwortcode (Authentication required)
QUIT	„221 OK“ Antwortcode senden und die Verbindung mit dem Clientsystem schließen
Andere Meldungen	„502 5.5.1“ Antwortcode (Invalid command)

[...]

im Kapitel 3.4.2.2 Verbindungsaufbau mit dem POP3-Server

Unter die Anforderung "KOM-LE-A_2033-01 Verbindungsaufbau mit POP3-Server über Adresse und Portnummer" wird der folgende Hinweis ergänzt:

Hinweis: Sind die POP3-Adresse und die zugehörige Portnummer nicht Bestandteil des übergebenen POP3-Benutzernamens, dann ermittelt das Clientmodul diese fehlenden Parameter mit Hilfe des übergebenen Benutzernamens (Domainanteil) und damit ausgelöster DNS Service Discovery [gemSpec_FD_KOMLE#Tab_KOMLE_Service Discovery].

[...]

im Kapitel 4.1.4 Transportsicherung zwischen Clientmodul und Fachdienst

[...]

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

Die Anforderung A_23225 - lokales Caching von Sperrinformationen und Toleranzzeiten (gemSpec_PKI) beschreibt Funktionalität, welche bereits Teil der zu nutzenden Operation "VerifyCertificate" ist. Folglich wäre dies redundant zu [A_22348-*], sowie nicht adäquat durch das KIM Clientmodul umsetzbar.

Die Zuordnung der Anforderung A_23225 zum KIM CM/iCM wird gelöscht.

Hinweis:

~~Für das lokale Caching von Sperrinformationen und für die Toleranzzeiten gilt A_23225 – lokales Caching von Sperrinformationen und Toleranzzeiten.~~

~~Die Anforderung ist wie folgt zu interpretieren:~~

- ~~Als Sperrinformation gilt die Response des Konnektors zum Request VerifyCertificate.~~
- ~~Die Zeit zu der die Sperrinformation erzeugt wurde ist der Zeitpunkt der Response des Konnektors.~~
- ~~TUC_PKI_006 wird nicht verwendet, daher entfällt Punkt 4 der Anforderung.~~

6.1.2 Änderung in gemSpec_FD_KOMLE

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

Für das KIM Clientmodul wird gemäß "A_23554 - Weiterleitung MAIL FROM - SIZE-Parameter" gefordert, dass der Parameter "SIZE" übermittelt werden soll. Die Unterstützung dieses Parameters muss entsprechend vom KIM Fachdienst als SMTP-Response auf SMTP EHLO angegeben werden.

Ähnliches gilt für POP3 UIDL, welches zwingend durch die Primärsysteme zu nutzen ist und durch die KIM Clientmodule weitergeleitet wird.

Folglich werden zur Konsistenzbildung entsprechende Anforderung für den KIM-Fachdienst aufgenommen, die jedoch notwendigerweise bereits technisch umgesetzt sein müssten.

neu:

in Kapitel 4.1.1 Operation send_Message

...

A_28584 -SMTP Begrüßung am Fachdienst KOM-LE

Der Fachdienst KOM-LE MUSS, nachdem die SMTP-Verbindung zwischen dem Fachdienst KOM-LE und dem Clientmodul aufgebaut wurde, den SMTP-Dialog mit dem Clientmodul entsprechend Tabelle "Tab_SMTTP_Dialog_Fachdienst_KOM-LE" unterstützen. Um zu signalisieren, dass Extended SMTP unterstützt wird, MUSS die SMTP-Begrüßung „ESMTTP“ enthalten.

[<=, KOM-LE FD, funkt. Eignung: Test Produkt/FA]

Beispiel Antwort SMTP-Begrüßung: 220 KOM-LE-Fachdienst ESMTTP

Table 1 Tab_SMTTP_Dialog_Fachdienst_KOM-LE

SMTP-Kommando (Clientmodul -> Fachdienst KOM-LE)	SMTP-Antwortcode (Fachdienst KOM-LE -> Clientmodul)
HELO	"250 OK" Antwortcode
EHLO	"250 OK" Antwortcode mit folgenden EHLO Kennworten: SIZE 22020096 AUTH LOGIN PLAIN 8BITMIME ENHANCEDSTATUSCODES DSN

neu:

in Kapitel Operation receive_Message

A_28585 -POP3-Dialog mit Clientmodul

Der Fachdienst KOM-LE MUSS, nachdem die POP3-Verbindung zwischen dem Fachdienst KOM-LE und dem Clientmodul aufgebaut wurde den POP3-Dialog mit dem Clientmodul entsprechend Tabelle "Tab_POP3_Dialog_Fachdienst_KOM-LE" unterstützen. [<=, KOM-LE FD, funkt. Eignung: Test Produkt/FA]

Table 2 Tab_POP3_Dialog_Fachdienst_KOM-LE

Clientmodul -> Fachdienst KOM-LE	Fachdienst KOM-LE -> Clientmodul
CAPA	"+OK" Antwortcode mit folgenden CAPA Kennworten: TOP USER SASL PLAIN UIDL

6.2 Änderung zur Absender-Integrität CM und Vermeidung von Folgefehler-Last

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

Es traten/treten vermehrt Fehlerfälle auf, welche durch Fehladressierung an bspw. ("@xyz.de") E-Mail-Adressen begründet sind. Da eine Verarbeitung dieser Adressen gesichert Fehlerfälle sowie ggf. unnötige Abfragen an zentralen Diensten der TI (VZD) verursachen können, sollten diese Adressen direkt ignoriert und aus der Verarbeitung ausgeschlossen werden.

6.2.1 Änderung in gemSpec_CM_KOMLE

A_23174-03 -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 [A_19356-0x*, KOM-LE-A_2176-0x*] geprüft wurden, im Mail Header to, cc und, wenn vorhanden, bcc in der KOM-LE-Nachricht verbleiben. Das Clientmodul MUSS den Versandvorgang vor der Weiterverarbeitung mit SMTP-Fehlercode "553 Nicht zugelassene Empfängeradresse" abbrechen, wenn ein oder mehrere Empfänger-Adressen angegeben wurden, die keinen Domain-Part gemäß [A_21456-*] ausweisen.

[<=, Basis-Consumer, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

6.3 Angabe TI-User-Agent in HTTP-Requests

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

Dienste und Anwendungen wie KIM (inhaltsagnostisches Transportmedium), werden zunehmend auch als Teil automatisierter Prozesse (Dunkelverarbeitung) genutzt. Dies kann zu einer unbekannten Zusatzlast, Fehlfunktionen und Stabilitätsrisiken der involvierten Systemkomponenten führen. Um zukünftig eine bessere Aussage zur Nutzung dieser Dienste und Anwendungen treffen zu können, sollen Produkttypen (in diesem Fall der KOM-LE Fachdienst & Clientmodul), bei der HTTP-Kommunikation ein zusätzliches Header-Feld namens "TI-User-Agent" mit-übermitteln. Für den KIM Fachdienst sind das u.a. die Kommunikationsbeziehungen zum VZD, BDE, TSL und für das KIM Clientmodul zu den KIM Fachdienstteilen Account Manager und KAS. Dieses Header-

Feld ist auch in der bzw. für die Zukunft der TI und KIM relevant und notwendig. Folglich leitet sich identischer Nutzen auch für die KIM Fachdienstteile ab.

Generell soll zukünftig die gesamte Infrastruktur entsprechende Informationen liefern, um eine bessere Datengrundlage für Betrachtungen der Stabilität, Sicherheit und Skalierung abzubilden.

Für die Produkttypen

- **Fachdienst KOM-LE**
- **KOM-LE-Clientmodul**
- **Integriertes Clientmodul KIM (KIM-iCM)**
- **Basis-Consumer**

wird nachfolgende Anforderung aus gemSpec_Perf aufgenommen:

A_27784 -User-Agent - Senden eines User-Agents (Clientsysteme)

Das Clientsystem (z.B. FdV) MUSS in allen HTTP-Requests an Dienste der TI ein zusätzliches Header-Feld namens "TI-User-Agent" im Format <Client-ID>/<Version> erstellen und wie folgt befüllen:

- <Client-ID>: Alphanumerische Zeichen a-z,A-Z,0-9, sowie dem Trennzeichen "-" mit Länge von 3 bis 20 Zeichen → vergeben durch die gematik
- <Version>: Alphanumerische Zeichen a-z,A-Z,0-9, sowie dem Trennzeichen "." und "-" mit Länge von 3 bis 20 Zeichen → vergeben durch Clientsystem

Die Versionsnummer MUSS eindeutig sein und geändert werden, wenn es eine Änderung am Clientsystem gibt. Es ist empfohlen, dass das Format der Versionsnummer dabei dem grundlegenden Aufbau der TI-Versionsnummern gemäß [gemSpec_OM#GS-A_3695] entspricht.

Beispiel: "CLIENTID1234567890AB/2.1.12-45"

[<=, KOM-LE FD, Basis-Consumer, KIM-iCM, KOM-LE CM, funkt. Eignung: Test Produkt/FA]

Die Client-ID wird über einen gemeinsamen, organisatorischen Prozess den KIM Providern bereitgestellt.

7 Änderungen gemSpec_DS_Anbieter

Änderung der Zuordnung der Anforderung **A_27098-01 - Verpflichtung zur Umsetzung des TI Security Standards** zum KIM Fachdienst wurde korrigiert und ist nur noch dem Anbieter Fachdienste KOM-LE zugewiesen.

"Der Anbieter MUSS die im TI Security Standard (in seiner jeweils aktuell durch die gematik freigegebenen und veröffentlichten Fassung) festgelegten betrieblichen Pflichten in Abhängigkeit der ihm zugewiesenen Security Governance Stufe umsetzen."

8 Änderungen gemSpec_Perf

Die folgenden Informationen dienen lediglich dem besseren Verständnis und sind nicht Bestandteil der Spezifikation!

Die Performance-Anforderungen an KIM werden aktuell in zwei (A_26323, A_20129), teilweise redundanten, inkonsistenten Anforderungen abgebildet. Die marktanteiligen Spitzenlastvorgaben aus A_20129 können analog auf A_26323 angewendet werden, sodass A_20129 entfallen kann.

entfällt:

A_20129 – Performance – Fachdienst KIM – Spitzenlastvorgaben

Der Anbieter Fachdienst KIM MUSS das System so dimensionieren, dass für seine Nutzer der erwartete Spitzenlast gemäß "Tab_gemSpec_Perf_Fachdienst_KIM: Lastvorgaben" erfüllt werden. Die Lastvorgabe aus dieser Tabelle bezieht sich auf die Anzahl aller KIM-Teilnehmer. ---<=

Zur Erläuterung zu [A_20129]:

Der Anbieter muss die Anzahl seiner KIM-Teilnehmer kennen und sein System mindestens so dimensionieren, damit die Lastvorgaben eingehalten werden.

Beispielrechnung: Für 210.000 KIM-Teilnehmer (siehe Tabelle "Tab_Mengengerüst: Annahmen für Modellierung") ergibt sich auf Basis von 10.000 Teilnehmern eines Anbieters eine Lastvorgabe von mindestens 8 Anfragen pro Sekunde für das senden von Mails mit einer Nachrichtengröße von 100KB. (5% von 160 Anfragen pro Sekunde).

Tabelle : Tab_gemSpec_Perf_Fachdienst_KIM: Lastvorgaben

Anwendungsfall	Datenmenge in KB	Lastanforderungen
		Anfragen [1/sec]
Nachricht über KIM-Clientmodul empfangen	100	302
	25.600	15
Nachricht über KIM-Clientmodul Download	100	302
	25.600	15
Nachricht an KIM- FD senden	100	160
	25.600	8
Nachricht von	100	160

KIM-FD-empfangen	25.600	8
Aufbau TLS-Kanal zwischen KIM-Clientmodul und KIM-Fachdienst		820

[...]

Unterhalb der Anforderung **A_26323-01** wird eine Erläuterung hinzugefügt.

Erläuterung zu [A_26323-]:*

Der Anbieter muss die Anzahl seiner KIM-Teilnehmer kennen und sein System mindestens so dimensionieren, damit die Lastvorgaben eingehalten werden.

Beispielrechnung: Für 210.000 KIM-Teilnehmer (siehe Tabelle "Tab_Mengengerüst: Annahmen für Modellierung") ergibt sich auf Basis von 10.000 Teilnehmern eines Anbieters eine Lastvorgabe von mindestens 8 Anfragen pro Sekunde für das senden von Mails mit einer Nachrichtengröße von 100KB. (5% von 160 Anfragen pro Sekunde).

9 Änderungen in der gemSpec_Krypt

geändert:

A_19644-01 -Hashfunktion für Hashwert-Referenzen beim Fachdienst Download-Server (KAS)

Ein KOM-LE-Client ~~und der Fachdienst Download-Server (KAS)~~ **MÜSSEN MUSS** bei der Erzeugung und Verwendung von Hashwert-Referenzen für Anhänge - die auf dem Fachdienst Download-Server (KAS) abgelegt werden - die Hashfunktion SHA-256 [FIPS-180-4] verwenden. [\leq , Basis-Consumer, KIM-iCM, KOM-LE CM, Sich.techn. Eignung: Herstellererklärung]