Themengebiet: Optimierung KAS – KIM 1.5.2 C_10910

1 KIM 1.5.2 2
1.1 Änderung in gemSpec_CM_KOMLE 2
1.2 Änderung in gemSpec_FD_KOMLE 4
1.3 Änderung der api-kim/AccountManager.yaml 8
1.4 NEU: Schnittstellbeschreibung der api-kim/AccountLimit.yaml 9
1.5 Änderung der api-kim/AttachmentService.yaml 11
1.6 Änderungen in Steckbriefen 13

1 KIM 1.5.2

1.1 Änderung in gemSpec_CM_KOMLE

3.1 Allgemeine Anforderungen

[...]

A_22416 - Anfragen von technischen Konfigurationsdaten
Das KOM-LE Clientmodul MUSS beim Versenden einer E-Mail die Operation `getLimit` am Account Manager aufrufen, um alle technischen Konfigurationsdaten eines Nutzers zu erhalten. Das Clientmodul KANN für jeden Nutzer-Account die abgerufenen Daten 24 Stunden zwischenspeichern (cachen).
[<=]

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

[...]

Anpassung der Anforderung A_20650-03 um den Fehlercode 4017 bezüglich der Übermittlung von Fehlernachrichten. Siehe hierzu bitte den Änderungseintrag: C_10875

[...]

A_22412 - Behandlung von Zugriffs-Limitierung
Das Clientmodul MUSS bei Aufruf der Operation read_Attachment() bei der Rückgabe des HTTP-Fehlercodes 429, das Mail-Header-Attribut `X-KIM-Fehlermeldung` mit dem Wert gemäß Tabelle „Tab_Fehlercodes_KOMLE-Clientmodule“ `4017` befüllen und an der Position des Anhangs ein MIME-Element mit `Content-Type: text/plain; charset=utf-8` und `Content-Disposition: attachment; filename=<Original-Filename>_Fehlermeldung.txt` sowie folgende Informationen als Inhalt des Anhangs einfügen: Der Anhang { "`name`": "Dateiname des Anhangs", "`size`": Größe des Anhangs in Byte, "`type`": "MIME-Type des Anhangs" } konnte nicht abgerufen werden. Als Betreff ist Folgendes zu verwenden:`Subject:[Fehler beim Abruf eines Anhangs *_Fehlermeldung.txt] <Original-Subject>`.**[<=]**

3.2.1 Senden von Nachrichten mit großen Anhängen

[...]

A_22419 - Behandlung von Quota-Überschreitung
Wenn das Clientmodul beim Versand eines E-Mail-Anhanges vom KAS einen Fehlercode 507 erhält, MUSS es den Mailversand abbrechen und dem KOM-LE-Client den SMTP-Fehlercode 521 gemäß [RFC3463] zurückgegeben und die existierende SMTP-Verbindung zum Mail Server abbauen.
[<=]

A_22427 - I_Attachment_Services - Content-Length
Das KOM-LE-Clientmodul MUSS bei der Übertragung des Anhanges das http-Header-Element "Content-Length" immer mit der Gesamt-Länge des Bodys befüllen.**[<=]**

3.2.2 Empfangen von Nachrichten mit großen Anhängen

[...]

A_19370-03 - Download von Anhängen
Das KOM-LE-Clientmodul MUSS die Anhänge zu den entnommenen Freigabelinks via der Operation read_Attachment am KAS des Fachdienstes herunterladen.

Wenn beim Herunterladen eines Anhangs ein Fehler auftritt, dann MUSS das KOM-LE-Clientmodul ~~an der Position des Anhangs ein MIME-Element mit `Content-Type: text/plain; charset=utf-8` und `Content-Disposition: attachment; filename=<Original-Filename>_Fehlermeldung.txt` sowie folgende Informationen als Inhalt des Anhangs einfügen: Der Anhang { "`name`": "Dateiname des Anhangs", "`size`": Größe des Anhangs in Byte, "`type`": "MIME-Type des Anhangs" } konnte nicht heruntergeladen werden. Als Betreff ist folgendes zu verwenden:`Subject:[Fehler beim Herunterladen der Anhaenge *_Fehlermeldung.txt]` <Original-Subject>~~ die empfangene, dem KOM-LE-S/MIME-Profil entsprechende Nachricht, als eine message/rfc822 MIME-Einheit in einer neuen multipart/mixed MIME-Nachricht dem Clientsystem übermitteln. Zusätzlich muss diese neue multipart/mixed MIME-Nachricht eine text/plain MIME-Einheit mit dem Fehlertext [Tab_Fehlertext_Download] enthalten. Die orig-date, from, sender, reply-to, to und cc Header-Elemente der neuen multipart/mixed Nachricht werden aus der empfangenen Nachricht übernommen. Das subject Header-Element der neuen multipart/mixed Nachricht erhält den Wert „Mindestens ein Anhang der Nachricht konnte nicht heruntergeladen werden".
[<=]

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

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

- Wenn die empfangene Nachricht nicht vom Server gelöscht wurde, wird beim nächsten Abholen die Aufbereitung wiederholt.

Tabelle x enthält den Fehlertext, der in die Nachricht eingeführt wird, wenn der Download von Anhängen nicht durchgeführt werden konnte.

Tabelle x: Tab_Fehlertext_Download Fehlertext beim Download von Anlagen

Bedingung	Fehlertext
Mindestens ein Anhang der Nachricht konnte nicht heruntergeladen werden.	Nicht alle Anhänge dieser Nachricht konnten 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.

1.2 Änderung in gemSpec_FD_KOMLE

3.1 Funktionen des Mail Servers

[...]

A_22415 - Mail Server – Löschen von Ressourcen
Der Anbieter des Mail Servers MUSS sicherstellen, dass alle gespeicherten E-Mails eines Accounts mit abgelaufener Gültigkeit (Expires-Header) gelöscht werden.
[<=]

[...]

3.2 Funktionen des Account Managers

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

- die Verwaltung des Nutzer-Accounts
  - Registrierung,
  - Deregistrierung,
  - Kennwortänderung,
  - Wechsel der Telematik-ID
  - Löschfrist von Anhängen
  - Wechsel der eingesetzten KIM-Version

- die Verwaltung von Abwesenheitsnotizen
- die Bereitstellung der PKCS#12-Dateien

[...]

3.8 Konfiguration

KOM-LE-A_2139-01 - Konfiguration Fachdienst
Der Fachdienst KOM-LE MUSS dem Anbieter mindestens die in der Tabelle Tab_Konfig_Parameter dargestellten Parameter zur Konfiguration zur Verfügung stellen.**[<=]**

Parameter	Standardwert	Beschreibung
Löschfrist für automatisch generierte Mails	90 Tage	Diese Löschfrist gilt für Mails, die vom Server automatisch generiert werden, insbesondere Zustellbestätigungen (DSN) und Abwesenheitsnotizen (vacation)

4.2 Schnittstelle I_Attachment_Services

[...]

Tabelle 8: Operationen vom KAS

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

					n verschlüsselten Anhang herunter
~~read_MaxMailSize~~	~~/MaxMailSize~~	~~GET~~	~~-~~	~~int64~~	~~Gibt die maximal unterstützte Größe einer Mail (inklusive Anhänge und base64-Kodierung) zurück.~~

[...]

A_22410 - KAS – Prüfung: Aufruf des Empfängers
Der KAS MUSS das Herunterladen eines Anhanges mit dem HTTP-Fehlercode 401 ablehnen, wenn beim Abruf des Anhanges die Empfänger-Adresse (recipient) nicht mit einem für den Anhang beim KAS hinterlegten Empfänger (recipients) übereinstimmt.
[<=]

Hinweis: Bei der im Aufruf geforderten Empfänger-Adresse handelt es sich um die KIM-Mail-Adresse des Empfängers.

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

A_22418 - Umgang bei Überschreitung der Quota
Der KAS des KOM-LE-Fachdienstes KANN bei Überschreitung der Quota für einen Nutzer-Account den HTTP-Fehlercode 507 an das Clientmodul zurückgeben.
[<=]

A_19385-01 - KAS – Löschen von Ressource
~~Der Anbieter des KAS MUSS sicherstellen, dass alle gespeicherten Anhänge gemäß der in [KOM-LE-A_2139] definierten Löschfrist von Nachrichten zu löschen sind.~~
Der Anbieter des KAS MUSS sicherstellen, dass alle gespeicherten Anhänge, mit abgelaufener Gültigkeit (`Expires`) gelöscht werden.

[<=]

A_22428 - I_Attachment_Services - Content-Length beim Download
Der KOM-LE Fachdienst MUSS bei der Übertragung des Anhanges, das http Header Element "Content-Length" immer mit der Gesamt-Länge des Bodys befüllen.**[**<=**]**

4.3 Schnittstelle I_AccountManager_Service

[...]

Operation	URI	Methode	Request	Response	Beschreibung
setAccount	/account/{username}	PUT	username password(alt) password(neu) kimVersion maxMailSize dataTimeToLive <JWT>	<Status>	Aktualisierung des Accounts: - Passwort - kimVersion - maxMailSize - dataTimeToLive

4.4 ~~Genutzte Schnittstellen der TI-Plattform~~ Schnittstelle I_AccountLimit_Services

Der Account Manager stellt einen Webservice zur Abfrage von technisch konfigurierten Daten eines KOM-LE-Teilnehmers bereit. Die Schnittstellenbeschreibung I_AccountLimit_Service ist in [AccountLimit.yaml] definiert. Der Aufruf der REST-Schnittstelle ist ausschließlich vom Clientmodul zulässig.

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

Operation	URI	Methode	Request	Response	Beschreibung
getLimit	/limit/	GET	-	<Status> - maxMailSize - dataTimeToLive - quota -remainQuota	Abfragen der technisch konfigurierten Daten eines Nutzer-Accounts

A_22413 - Account Manager – Implementierung der Schnittstelle
Die Teilkomponente Account Manager des Fachdienstes MUSS die Schnittstelle I_AccountLimit_Service als REST-Webservice über HTTPS gemäß [AccountLimit.yaml] in

der Version 1.0.0 implementieren. Des Weiteren MUSS der Account Manager für alle in der [AccountLimit.yaml] definierten Operationen den Zeichensatz UTF-8 unterstützen.**[<=]**

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

A_22414 - Account Manager - HTTP-Basic-Authentifizierung
Der Account Manager MUSS bei Aufruf der Operation getLimit eine HTTPBasic-Authentifizierung durchführen.
[<=]

4.5 Genutzte Schnittstellen der TI-Plattform

1.3 Änderung der api-kim/AccountManager.yaml

```
- url: https://account-
manager.hrst1.kim.telematik/AccountMgmt/v2.2/

[…]

/account/{username}:
    put:

[…]

$ref: '#/components/schemas/Account'

[…]

Account:
[…]
      maxMailSize:
        type: integer
        format: int64
        example: 734003200
        description: Setzt die maximale Größe einer KIM-
Mail in Bytes
      dataTimeToLive
        type: integer
        maxLength: 3
        example: 90
```

```
        description: Angabe in Tagen
```

1.4 NEU: Schnittstellbeschreibung der api-kim/AccountLimit.yaml

```
openapi: 3.0.3
info:
  title: I_AccountLimit_Service
  description:  Über diese Schnittstelle werden die Limits
eines Accounts
                abgefragt
  version: 1.0.0

  ### 1.0.0
  # initial Version

externalDocs:
  description: GitHub - Dokumentation
  url: https://github.com/gematik/api-kim
servers:
- url: https://account-
manager.hrst1.kim.telematik/AccountLimit/v1.0/
tags:
- name: AccountLimit

paths:
##--
##------
  /limit:
    get:
      tags:
      - AccountLimit
      summary: Limits eines Accounts abgefragen
      description: Gibt die Limits eines Accounts zurück
      operationId: getLimits

      security:
        - basicAuth: []

      responses:
        200:
          description: OK
             # Rückgabe der technischen Konfigurationsdaten
eines Nutzer-
               Accounts
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/AccountLimit'
        401:
          description: Authentifizierung fehlgeschlagen
          content:
```

```
            application/json:
              schema:
                $ref: '#/components/schemas/Error'
        404:
          description: Mail Account nicht vorhanden
          content:
              application/json:
                schema:
                  $ref: '#/components/schemas/Error'
        500:
          description: Internal Server Error
          content:
            application/json:
              schema:
                $ref:
'#/components/schemas/Error'

##--
##------
components:

  schemas:

    AccountLimit:
      type: object
      properties:
        dataTimeToLive:
          type: integer
          maxLength: 3
          minimum: 10
          maximum: 365
          default: 90
          example: 90
          description: Speicherdauer von Mails und Anhängen
auf dem KAS
                       Fachdienst/KAS. Angabe in Tagen
        maxMailSize:
          type: integer
          format: int64
          example: 734003200
          description: Setzt die maximale Größe einer KIM-
Mail in Bytes
        quota:
          type: "integer"
          format: int64
          example: 160000000000
          description: Gibt das maximale Speichervolumen
für einen Nutzer-
                       Account an
        remainQuota:
          type: "integer"
          format: int64
          example: 112000000000
          description: Gibt das verbleibende
Speichervolumen für einen
                       Nutzer-Account an
```

```
    Error:
      type: object
      properties:
        message:
          type: string

  securitySchemes:
    basicAuth:
      type: http
      scheme: basic
```

1.5 Änderung der api-kim/AttachmentService.yaml

```
- url: https://kas.hrst1.kim.telematik/attachments/v2.2/

[…]

/attachment/{attachmentId}:
    get:

[…]

      - name: recipient
        in: header
        description: Die übergebene E-Mail-(KIM-)Adresse
des Empfängers
        required: true
        schema:
          type: string
          format: email


[…]

429:
  description: Anhang zu oft heruntergeladen.
  content:
    application/json:
      schema:
       $ref: '#/components/schemas/Error'

[…]

/attachment/:
    post:

[…]
      security:
        - basicAuth: []
        # Die Authentifizierung erfolgt mit
```

```
username/password von dem Mail Account

      requestBody:
        content:
          multipart/form-data:
            schema:
              type: object
              properties:
                messageID:
                    type: string
                    description: zugehörige MessageID zum
Anhang
                recipients:
                    type: array
                    description: Liste aller E-Mail-(KIM-
)Adressen der Empfänger
                    items:
                      type: string
                      format: email
                expires:
                    type: string
                    description: Zeitpunkt zu dem der
Anhang geloescht werden muss
                                    # (RFC822 date-time)
                attachment:
                   type: string
                   format: binary
                   description: Der Anhang

 […]

507:
  description: Nicht genügend Speicherplatz vorhanden
  content:
    application/json:
      schema:
       $ref: '#/components/schemas/Error'

 […]

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

```
    responses:
      200:
        description: OK
          # Gibt die maximale Größe einer KIM-Mail in
Bytes zurück
        content:
          application/json:
            schema:
              properties:
                MaxMailSize:
                  type: "integer"
                  format: int64
                  example: 734003200
      500:
        description: Internal Server Error
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/Error'
```

1.6 Änderungen in Steckbriefen

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

Änderungen in gemProdT_CM_KOMLE

Tabelle 1 Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_22416	Anfragen von technischen Konfigurationsdaten	gemSpec_CM_KOMLE
A_22417	Einfügen des Ablaufdatums in den äußeren Mail-Header	gemSpec_CM_KOMLE
A_22412	Behandlung von Zugriffs-Limitierung	gemSpec_CM_KOMLE
A_22419	Behandlung von Quota-Überschreitung	gemSpec_CM_KOMLE
A_22427	I_Attachment_Services - Content-Length	gemSpec_CM_KOMLE

Änderungen in gemProdT_FD_KOMLE

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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_22415	Mail Server – Löschen von Ressourcen	gemSpec_FD_KOMLE
KOM-LE-A_2139-01	Konfiguration Fachdienst	gemSpec_FD_KOMLE
A_22410	KAS – Prüfung: Aufruf des Empfängers	gemSpec_FD_KOMLE
A_22411	KAS - Zugriffs-Limitierung	gemSpec_FD_KOMLE
A_22418	Umgang bei Überschreitung der Quota	gemSpec_FD_KOMLE
A_22413	Account Manager – Implementierung der Schnittstelle	gemSpec_FD_KOMLE
A_22414	Account Manager - HTTP-Basic-Authentifizierung	gemSpec_FD_KOMLE
A_22420	I_AccountLimit_Services – TLS-gesicherte Verbindung	gemSpec_FD_KOMLE
A_22428	I_Attachment_Services - Content-Length beim Download	gemSpec_FD_KOMLE

Tabelle 3 Anforderungen zur funktionalen Eignung: "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_19385-01	KAS – Löschen von Ressource	gemSpec_FD_KOMLE