Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Fachdienst KOM-LE

Version:	1.~~10~~11.0 CC
Revision:	~~241921~~269890
Stand:	~~30.06~~17.08.2020
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_FD_KOMLE

ENTWURF

Dokumentinformationen

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.1.0	02.12		Ersterstellung	Projekt KOM-LE
	04. 13		Einfügen Anforderungen mit Afo-Makro	Projekt KOM-LE
1.0.0	27.01.14		Einarbeitung Kommentare	Projekt KOM-LE
1.1.0	28.02.14	3.1	Hinweis ergänzt	Projekt KOM-LE
1.2.0	25.07.14	4.3	Afo zu Schnittstellen der TI-Plattform ergänzt	Projekt KOM-LE
1.3.0	22.09.14		Begriff Betreiber durch Anbieter ersetzt	
1.4.0	06.05.15		Anpassung Anforderung KOM-LE-A_2146	Projekt KOM-LE
1.5.0	24.07.15	3.1	Präzisierung der Erstellung von Abwesenheitsnotizen (2 neue Afos)	P74
1.6.0	28.10.16	4.3	Anpassungen gemäß Änderungsliste	gematik
1.7.0	14.05.18		Anpassungen gemäß Änderungsliste	gematik
1.8.0	15.05.19		Anpassungen gemäß Änderungsliste P18.1	gematik
1.9.0	02.03.20		Anpassungen gemäß Änderungsliste P21.1	gematik

ENTWURF

1.10.0	30.06.20		Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0	gematik
1.11.0 CC	17.08.20		Anpassungen gemäß Änderungsliste P22.2 und Scope-Themen aus Systemdesign R4.0.1	gematik

31

ENTWURF

Inhaltsverzeichnis

ENTWURF

ENTWURF

ENTWURF

1 Einordnung des Dokuments

1.1 Zielsetzung und Einordnung des Dokuments

Dieses Dokument enthält die Anforderungen an den Produkttyp Fachdienst KOM-LE. Der Fachdienst ist verantwortlich für die Speicherung und Bereitstellung von KOM-LE-Nachrichten sowie für die Registrierung und Deregistrierung von KOM-LE-Teilnehmern.

Aus den Kommunikationsbeziehungen mit Clientmodul, Konnektor und Verzeichnisdienst resultieren vom Fachdienst anzubietende Schnittstellen, die in diesem Dokument normativ beschrieben werden. Vom Fachdienst genutzte Schnittstellen liegen zumeist in anderen Verantwortungsbereichen (z.B. Verzeichnisdienst). Diese werden in der entsprechenden Produkttypspezifikationen definiert.

1.2 Zielgruppe

Dieses Dokument richtet sich neben Personengruppen, die grundsätzlich am Fachdienst Kommunikation Leistungserbringer interessiert sind, an

- Hersteller und Entwickler des Fachdienstes
- Anbieter
- Verantwortliche für Zulassung und Test

1.3 Geltungsbereich

Das vorliegende Dokument enthält normative Anforderungen und Festlegungen, die von Herstellern und Anbietern von Komponenten und Diensten im Rahmen der Projekte der Neuausrichtung zur Einführung der elektronischen Gesundheitskarte und der Telematikinfrastruktur zu beachten sind. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

1.4 Arbeitsgrundlagen

Grundlagen für die Ausführungen dieses Dokumentes sind

- das systemspezifische Konzept KOM-LE [gemSysL_KOMLE]
- KOM-LE S/MIME Profil [gemSMIME_KOMLE]
- Gesamtarchitektur der TI [gemÜK_Arch_TI]
- Konzept Architektur der TI-Plattform [gemKPT_Arch_TIP]
- Konzept PKI der TI-Plattform [gemKPT_PKI_TIP]

ENTWURF

1.5 Abgrenzung des Dokuments

Spezifiziert werden in dem Dokument die vom Produkttyp bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert.

Die Systemlösung der Fachanwendung KOM-LE ist im systemspezifischen Konzept [gemSysL_KOMLE] beschrieben. Dieses Konzept setzt die fachlichen Anforderungen des Lastenheftes auf Systemebene um, zerlegt die Fachanwendung KOM-LE in die zugehörigen Produkttypen, darunter das KOM-LE-Clientmodul und der KOM-LE-Fachdienst. Ferner definiert es die Schnittstellen zwischen den einzelnen Produkttypen. Für das Verständnis dieser Spezifikation wird die Kenntnis von [gemSysL_KOM-LE] vorausgesetzt.

Die Anforderungen an das Clientmodul werden separat in der Spezifikation KOM-LE-Clientmodul [gemSpec_CM_KOMLE] beschrieben.

Die Anforderungen an das Format der KOM-LE-Nachrichten, die zwischen dem Clientmodul und dem Fachdienst übermittelt werden, werden separat im KOM-LE-S/MIME-Profil [gemSMIME_KOMLE] beschrieben.

Abbildung 1 zeigt schematisch die Einbettung des vorliegenden Dokuments in die Dokumentenlandschaft der Lastenheft- und Pflichtenheftphase in Form einer Dokumentenhierarchie.

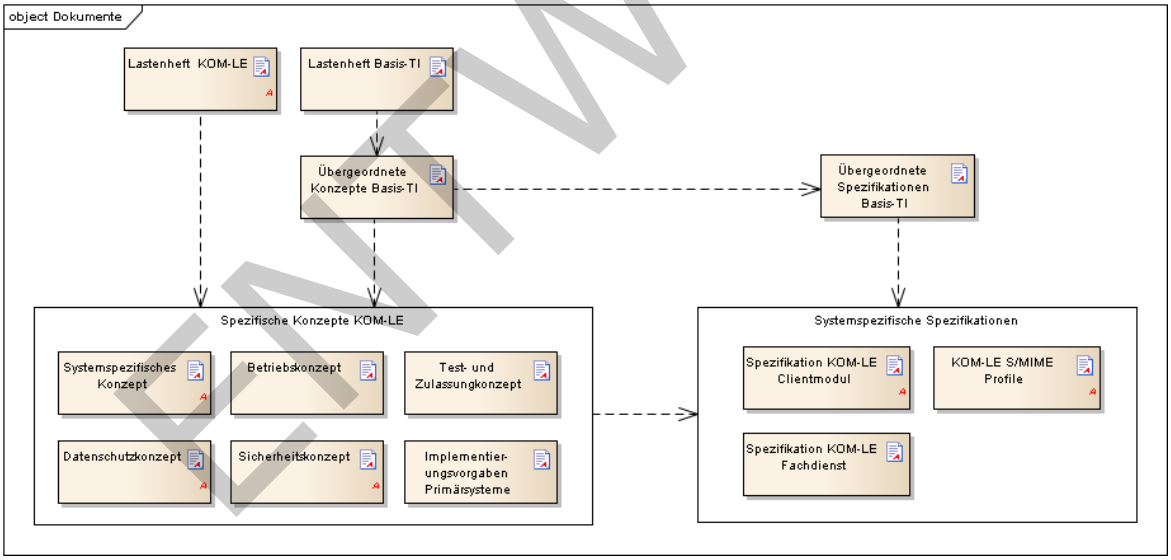

Abbildung 1: Abb_Dok_Hierachie_KOMLE Dokumentenhierarchie KOM-LE

1.6 Methodik

Das Vorgehen zur Erstellung dieser Spezifikation verwendet einen anforderungszentrierten und modellbasierten Entwicklungsprozess. Dabei werden Auftragsanforderungen über Umsetzungsanforderungen bis hin zu Blattanforderungen verfeinert. Auf Basis der vollständigen und nachvollziehbaren Anforderungen werden

ENTWURF

verbindliche Artefakte zur Fachanwendung modelliert. Der gesamte Prozess wird durch eine Qualitätssicherung begleitet.

1.6.1 Anforderungsmanagement

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

Dabei umfasst die Anforderung sämtliche innerhalb der Afo-ID und der Textmarke angeführten Inhalte.

1.6.2 Diagramme

Die Darstellung der Spezifikationen von Komponenten erfolgt auf der Grundlage einer durchgängigen Use-Case-Modellierung als

- technische Use Cases (eingebundene Graphik sowie tabellarische Darstellung mit Vor- und Nachbedingungen gemäß Modellierungsleitfaden),
- Sequenz- und Aktivitätendiagramme sowie
- Klassendiagramme
- XML-Strukturen und Schnittstellenbeschreibungen.

1.6.3 Nomenklatur

Sofern im Text dieser Spezifikation auf die Ausgangsanforderungen verwiesen wird, erfolgt dies in eckigen Klammern, z.B. [KOMLE-A_2015]. Wird auf Eingangsanforderungen verwiesen, erfolgt dies in runden Klammern, z.B. (KOMLE-A_202).

1.6.4 Hinweis auf offene Punkte <optional>

~~*Das Kapitel wird in einer späteren Version des Dokumentes ergänzt.*~~

Das Kapitel wird in einer späteren Version des Dokumentes ergänzt.

ENTWURF

2 Systemüberblick

Der Fachdienst KOM-LE ist in der Provider Zone an das zentrale Netz der TI-Plattform angeschlossen und besteht aus den Teilkomponenten Account Manager, Mail Server (SMTP und POP3-Server) und dem KOM-LE Attachment Service (KAS).

Die Teilkomponente Account Manager prüft die Authentizität des Leistungserbringers/KOM-LE-Teilnehmers sowie dessen Registrierungs- bzw. Deregistrierungsdaten. Nach erfolgreicher Prüfung der Daten erfolgt die Registrierung bzw. Deregistrierung des KOM-LE-Teilnehmers inklusive der Aktualisierung seines Verzeichniseintrages bezüglich der E-Mail-Adresse.

Die Teilkomponente Mail Server stellt dem KOM-LE-Clientmodul eine Schnittstelle zum Versenden und Abholen von E-Mails zur Verfügung. Die technische Umsetzung erfolgt über die Bereitstellung von entsprechenden TCP-Ports für SMTP- bzw. POP3.

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

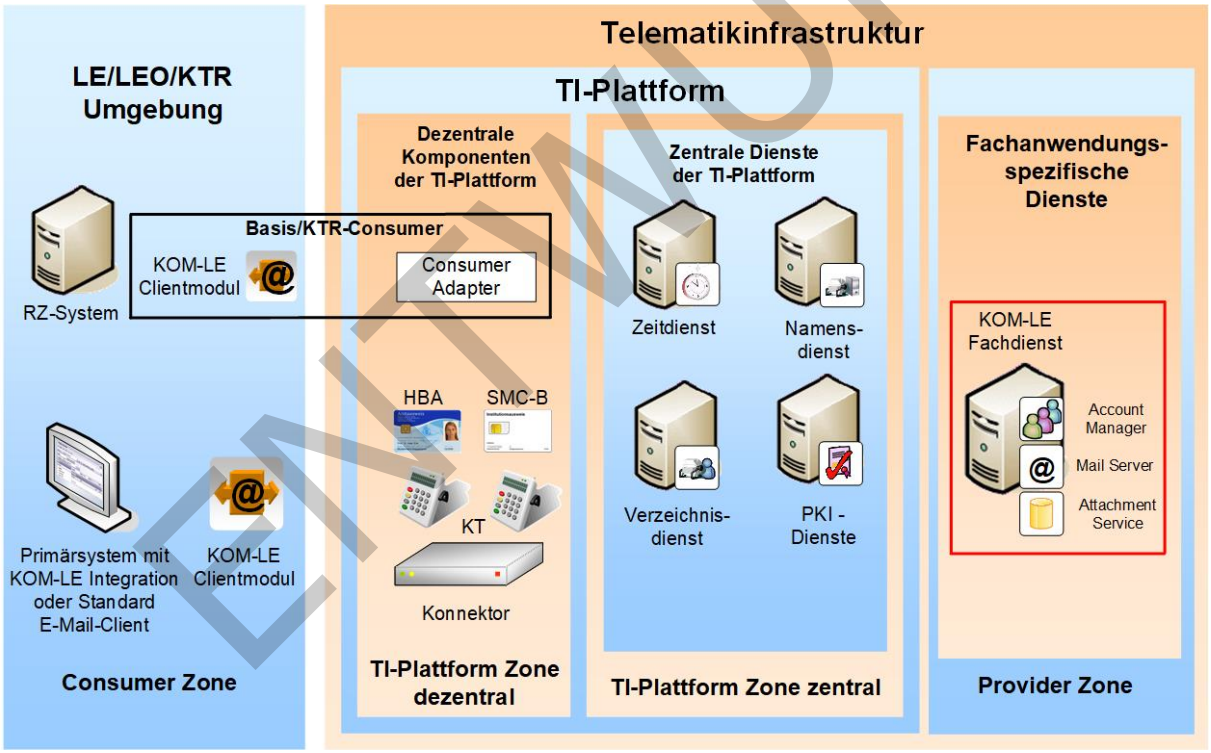

Abbildung 2: Abb_FD_Systemkontext Fachdienst KOM-LE im Systemkontext

ENTWURF

3 Funktionen

3.1 Funktionen des Mail Servers

Der Mail Server nimmt SMTP-Nachrichten von Clientmodulen oder anderen KOM-LE-Fachdiensten entgegen und leitet diese an die Ziel-Mail-Server weiter. Empfangene Nachrichten werden vom Mail Server zur Abholung bereitgestellt und auf Anforderung über POP3 an Clientmodule ausgeliefert. Die zugehörigen Anwendungsfälle sind im systemspezifischen Konzept [gemSysL_KOM-LE#3.1.1, 3.1.5] beschrieben.

KOM-LE-A_2185 - Mail Server darf nur Nachrichten aus der TI verarbeiten
Der Mail Server des KOM-LE-Fachdienstes MUSS ausschließlich Nachrichten, die innerhalb der TI versendet werden, verarbeiten. Der Zugriff auf einen Mail Server von außerhalb der TI ist nicht zulässig.
[<=]

~~**KOM-LE-A_2130 - Generieren einer Zustellbestätigung**~~**KOM-LE-A_2131 - Fehlernachricht bei fehlerhafter E-Mail-Adresse**
~~Der Ziel-Mail-Server MUSS, wenn die eingehende Nachricht eine Zustellbestätigung anfordert, diese entsprechend Delivery Status Notification vom Typ Success (RFC3461-3464) generieren und an den Absender übermitteln.~~
~~**[<=]**~~
~~**KOM-LE-A_2131 - Fehlernachricht bei fehlerhafter E-Mail-Adresse**~~
~~Können Nachrichten aufgrund einer fehlerhaften E-Mail-Adresse nicht weitergeleitet werden, MUSS der Mail Server eine Fehlernachricht entsprechend Delivery Status Notification erzeugen und diese an den Absender übermitteln.~~
~~**[<=]**~~

~~**KOM-LE-A_2132 - Identifikation der Originalnachricht**~~Können Nachrichten aufgrund einer fehlerhaften E-Mail-Adresse nicht weitergeleitet werden, MUSS der Mail Server eine Fehlernachricht entsprechend Delivery Status Notification erzeugen und diese an den Absender übermitteln.
[~~<=Zur Identifikation der Originalnachricht MUSS eine entsprechend Delivery Status Notification erzeugte Nachricht den Empfänger und das Versanddatum der Ursprungsnachricht enthalten.~~
~~**[<=**~~**]**

KOM-LE-A_2223 - Unterstützung Autoreply für Abwesenheitsnotiz
Der Mail Server SOLL eine Autoreply-Funktionalität für das Versenden von Abwesenheitsnotizen nach RFC5230 unterstützen.
[<=]

KOM-LE-A_2278 - Aufbau Autoreply für Abwesenheitsnotiz
Der Mail Server MUSS beim Versenden von automatischen Abwesenheitsnotizen folgende Bedingungen erfüllen:
SMTP MAIL FROM = <> (leer)
Subject = „Auto: " + Betreff der Nachricht beim Mailserver
Auto-Submitted field = „auto-replied" (siehe RFC5230, section 5).
[<=]

KOM-LE-A_2224 - Einstellen von Abwesenheitsnotizen
Der Mail Server SOLL es dem Nutzer ermöglichen, Abwesenheitsnotizen einstellen zu können.
[<=]

ENTWURF

KOM-LE-A_2277 - Versenden von Abwesenheitsnotizen ohne Signatur und Verschlüsselung
Der Mail Server MUSS den Nutzer beim Einrichten von automatischen Abwesenheitsnotizen informieren, dass diese nicht als verschlüsselte und signierte Nachrichten versendet werden.
[<=]

Die Pflege der Abwesenheitsfunktionen (z.B. Aktivieren, Deaktivieren und Notiztext) kann nicht mit dezentralen Komponenten der TI vorgenommen 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 Registrierung (mit inkludiertem Herunterladen der PKCS#12-Datei), die Deregistrierung, die Registerstatusabfrage sowie die Kennwortänderung. Eine weitere Aufgabe des Account Managers ist die Übertragung der vom Administrationsmodul gelieferte Clientversion in den Verzeichnisdienst. Die Operationen werden durch ein Webservice des Account Managers bereitgestellt. Ein weiterer wesentlicher Bestandteil dieser Operationen ist die zwingende Authentifizierung des KOM-LE Teilnehmers über sein AUT-Zertifikat. Die zugehörigen Anwendungsfälle sind im systemspezifischen Konzept [gemSysL_KOM-LE#3.1.7, 3.1.8] beschrieben.

KOM-LE-A_2133 - Durchführung eines Accountings zur Abrechnung
Führt der Anbieter ein Accounting für die Abrechnung unter Einhaltung der geltenden Anforderungen an Datenschutz und Informationssicherheit durch, KANN der Fachdienst die dafür notwendigen Funktionen implementieren.
[<=]

KOM-LE-A_2304 - Information an Nutzer zur bcc-Funktionalität
Der KOM-LE-Anbieter MUSS die KOM-LE-Teilnehmer im Rahmen der Registrierung zu KOM-LE und im KOM-LE-Nutzerhandbuch darüber informieren, dass auf eine Nutzung der bcc-Funktionalität eines E-Mail-Clients verzichtet werden sollte, da es technisch nicht ausgeschlossen ist, dass Nachrichtenempfänger ggf. auch alle bcc (blind carbon copy) Empfänger der Nachricht ermitteln werden können.**[<=]**

Es kann zusätzlich darauf hingewiesen werden, dass dies nicht die Klartext-Nachricht betrifft, die ein Empfänger letztlich in seinem Mail-Client empfängt, sondern nur die Daten, die das KOM-LE-Clientmodul verarbeitet. Es ist also durch den Empfänger ein Eingriff zur Analyse des Clientmoduls (z.B. mit Hilfe eines Debuggers) durchzuführen, um an die Daten zu gelangen.

A_19591 - Eintrag Clientmodul-Version in VZD, Account Manager
Der Account Manager MUSS die vom Clientmodul übermittelte KIM-Version im Verzeichnisdienst in den KOM-LE-Fachdaten für die betroffene "mail"-Adresse eintragen.**[<=]**

Es gelten die Festlegungen aus Kap.4.4., da der Verzeichnisdienst zur TI-Plattform gehört.

3.3 Funktionen des KOM-LE Attachment Services

Die Teilkomponente KAS des Fachdienstes dient als Speicherort für verschlüsselte Anhänge von Mails. Damit wird die Übertragung von großen Mails ermöglicht. Das

ENTWURF

sendende KOM-LE Clientmodul legt die großen Anhänge in verschlüsselter Form auf den KAS ab. Das empfangende KOM-LE Clientmodul lädt die Anhänge beim Empfang der Mail und stellt sie dem Client in entschlüsselter Form zusammen mit der Mail zur Verfügung.

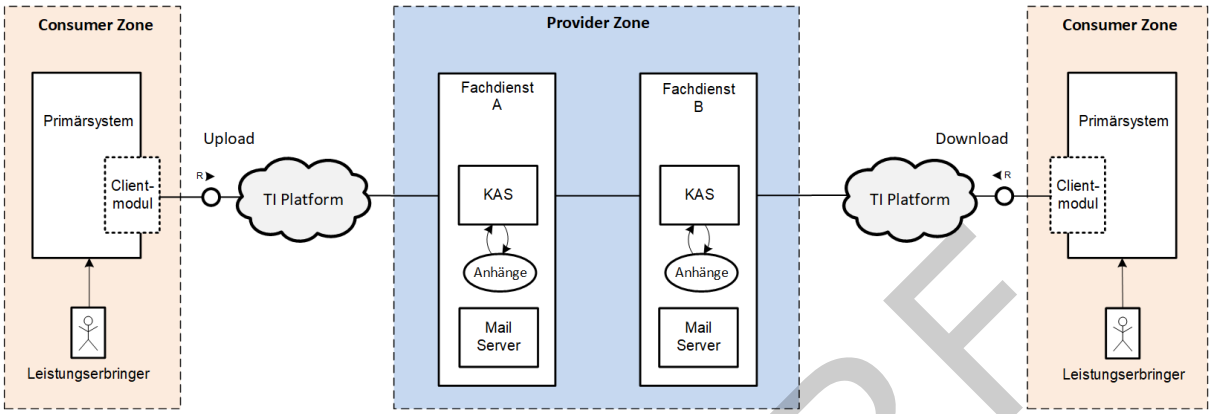

Abbildung 3: Abb_FD_KAS Funktionsweise des Attachment Service

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

Die maximale Gesamtgröße einer Mail wird durch den Fachdienst definiert und über die Operation I_Attachment_Services::read_MaxMailSize den Client Modulen zur Verfügung gestellt. Die Client Module prüfen die Gesamtgröße der Mail - inklusive aller Anhänge - vor dem Versenden. Mittels der Operation I_Attachment_Services::add_Attachment prüft der KAS die Größe der einzelnen Anlagen beim laden auf den Fachdienst.

3.4 Service Lokalisierung

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

Tabelle 1: Tab_KOMLE_Service Discovery

Resource Record Bezeichner	Resource Record Type	Beschreibung
_accmgr._tcp.kim.telematik	PTR	Ermittlung aller Account Manager Dienste

ENTWURF

		aller KOM-LE-Anbieter.
<accmgr_service_name>.<hrst_domain>.kim.telematik	SRV und TXT	SRV Resource Record zur Ermittlung der Ports und des FQDN des Accout Managers
_kas._tcp.kim.telematik	PTR	Ermittlung aller KAS-Dienste aller KOM-LE-Anbieter.
<kas_service_name>.<hrst_domain>.kim.telematik	SRV und TXT	SRV Resource Record zur Ermittlung der Ports und des FQDN des KAS

[<=]

Der Einträge in < > sind als Variable zu verstehen und durch konkrete Bezeichner zu ersetzen, z.B. für den Account Manager

```
_accmgr._tcp.kim.telematik 86400 IN PTR _accmgr._tcp.hrst1.kim.telematik
_accmgr._tcp.hrst1.kim.telematik 86400 IN SRV 5 10 8443 account-manager.hrst1.kim.telematik
_accmgr._tcp.hrst1.kim.telematik 86400 IN TXT „txtvers=1“ „path=/“
```

oder z.B. für den KAS

```
_kas._tcp.kim.telematik 86400 IN PTR _hrst1_kas._tcp.hrst1.kim.telematik
_kas._tcp.hrst1.kim.telematik 86400 IN SRV 5 10 8443 kas.hrst1.kim.telematik
_kas._tcp.hrst1.kim.telematik 86400 IN TXT „txtvers=1“ „path=/“
```

A_19533 - Verwaltung Resource Records FQDN, KIM
Der KOM-LE-Fachdienst MUSS im Namensraum der TI die Resource Records gemäß nachstehender Tabelle verwalten.

Tabelle 2: Tab_KOMLE_FQDN

Resource Record Typ	Beschreibung
FQDN	A Resource Records zur Namensauflösung von FQDN des KOM-LE-Fachdienstes des jeweiligen Anbieters in IP-Adressen

ENTWURF

[<=]

Nachfolgend sind exemplarisch FQDNs für den Account Manager und KAS dargestellt:

```
account-manager.hrst1.kim.telematik IN A 10.30.20.10
kas.hrst1.kim.telematik IN A 10.30.20.20
```

3.5 Fehlerbehandlung

KOM-LE-A_2134 - Aktionen bei Fehlerzuständen
Der Fachdienst KOM-LE MUSS mindestens die in Tabelle Tab_Fehler_Behandlung beschriebenen Fehlerzustände erkennen und die zugehörigen Aktionen durchführen.
[<=]

Tabelle 3: Tab_Fehler_Behandlung Fehlerbehandlung Fachdienst KOM-LE

Teilkomponente	Fehlerbeschreibung	durchzuführende Aktionen
Mail Server	Aufbau der TLS-Verbindung schlägt fehl	Protokollierung des Fehlers, Übermittlung Fehlercode an den Aufrufer (z.B. Clientmodul)
Mail Server	Authentifizierung über Benutzername und Passwort schlägt fehl	Protokollierung des Fehlers, Übermittlung Fehlercode an den Aufrufer (z.B. Clientmodul)
Mail Server	Nachricht ist nicht verschlüsselt	Protokollierung des Fehlers, Generierung einer entsprechenden Fehlernachricht an den Absender, Verwerfen der Originalnachricht
Mail Server	Absenderadresse fehlerhaft	Protokollierung des Fehlers, Verwerfen der Originalnachricht
Mail Server	Empfängeradresse fehlerhaft	Protokollierung des Fehlers, Generierung einer entsprechenden Fehlernachricht an den Absender mit der Originalnachricht im Anhang, Verwerfen der Originalnachricht

ENTWURF

Mail Server	Nachricht kann nicht weitergeleitet werden (z. B.: empfangender Mail Server oder TI-Netz nicht verfügbar)	Protokollierung des Fehlers, Versuch der erneuten Weiterleitung der Nachricht nach einem konfigurierbarem Zeitraum
Account Manager	Verzeichnisdienst nicht erreichbar	Protokollierung des Fehlers

3.6 Protokollierung

KOM-LE-A_2135 - Protokollierung von Vorgängen
Für die Nachvollziehbarkeit der Vorgänge am Fachdienst KOM-LE MÜSSEN Maßnahmen und Verfahren gemäß DSGVO i.V.m. BDSG installiert werden. Die Protokollierung der folgenden Informationen ist dabei zulässig:

- Anmeldung von Nutzern (Nutzername und Uhrzeit),
- Informationen über empfangene, weitergeleitete und abgeholte Nachrichten Absender, Empfänger, Uhrzeit) und
- Fehlermeldungen (Fehler mit Beschreibung und Uhrzeit).

[<=]

KOM-LE-A_2136 - Protokollierung außerhalb gesetzlicher und vertraglicher Pflichten
Der KOM-LE-Fachdienst MUSS sicherstellen, dass eine Protokollierung von personenbezogenen Daten außerhalb der gesetzlichen und vertraglichen Pflichten nur dann erfolgt, wenn dies zum Zwecke der Fehler- bzw. Störungsbehebung erforderlich ist.
[<=]

KOM-LE-A_2137 - Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung
Falls im KOM-LE-Fachdienst eine Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung erfolgt, MUSS der KOM-LE-Fachdienst unter Berücksichtigung des Art. 25 Abs. 2 DSGVO sicherstellen, dass in den Protokolldaten entsprechend dem Datenschutzgrundsatz nach Art. 5 DSGVO nur personenbezogene Daten in der Art und dem Umfang enthalten sind, wie sie zur Behebung erforderlich sind und dass die erzeugten Protokolldaten im Fachdienst nach der Behebung unverzüglich gelöscht werden.
[<=]

3.7 Monitoring

KOM-LE-A_2138 - Auskunftsfähigkeit über den Systemzustand
Die Administratoren des KOM-LE-Fachdienstes sind verpflichtet, zu jedem Zeitpunkt auskunftsfähig über den Systemzustand des Fachdienstes zu sein. Zur Unterstützung dieser Auskunftsfähigkeit KANN der KOM-LE-Fachdienst Monitoringfunktionen implementieren.
[<=]

ENTWURF

3.8 Konfiguration

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

Tabelle 4: Tab_Konfig_Parameter Konfigurationsparameter Fachdienst KOM-LE

Parameter	Standardwert	Beschreibung
Maximale Nachrichtengröße	500 MB	Die maximale Größe von Nachrichten in KOM-LE muss mindestens 500 MB netto betragen. Die Nachrichten werden unter Verwendung von S/MIME transportiert und auf dem Fachdienst gespeichert. Die Verwendung von S/MIME schließt die base64-Kodierung der Nachricht ein. Deshalb erhöht sich die Nachrichtengröße ca. um den Faktor 1,4.
Zeitraum für erneuten Weiterleitungsversuch	1 Stunde	Nach Ablauf des Zeitraums soll der Mail Server erneut versuchen Nachrichten weiterzuleiten, die nicht zugestellt werden konnten, weil der empfangende Mail Server oder das TI-Netz nicht verfügbar waren.
Löschfrist von Nachrichten	90 Tage	Nachrichten, die vom Fachdienst nicht abgeholt werden oder nach dem Abholen auf dem Fachdienst verbleiben, müssen nach der angegebenen Frist gelöscht werden.
Löschfrist von Logfiles	90 Tage	Die im Rahmen der Nachrichtenverarbeitung erzeugten Logfiles müssen nach der angegebenen Frist gelöscht werden.
Download- und Prüfzyklus der TSL	1 Tag	Regelmäßiger Zyklus in dem die aktuelle TSL zu laden und zu prüfen ist.
Downloadpunkt der TSL	-	IP-Adresse des verwendeten Downloadpunktes der TSL
IP-Adresse DNS-Server	-	IP-Adresse des verwendeten DNS-Servers der TI
IP-Adresse NTP-Server	-	IP-Adresse des verwendeten NTP-Servers der TI

ENTWURF

IP-Adresse Verzeichnisdienst	-	IP-Adresse des Verzeichnisdienstes der TI

410

ENTWURF

4 Schnittstellen

A_17240 - ECC-Migration, Unterstützung verschiedener kryptografischer Verfahren bei der TLS-Verwendung
Der Fachdienst KOM-LE MUSS parallel RSA und ECC unterstützen. Als TLS-Client MUSS der Fachdienst KOM-LE bevorzugt ECC verwenden, falls er auf einen TLS-Server, der beide Verfahren unterstützt, trifft.**[<=]**

4.1 Schnittstelle I_Message_Service

KOM-LE-A_2140 - Schnittstelle I_Message_Service
Die Teilkomponente Mail Server des KOM-LE-Fachdiensts MUSS die Schnittstelle I_Message_Service anbieten. I_Message_Service ist eine logische Schnittstelle, die Funktionalitäten zum Versenden und Empfangen von E-Mail-Nachrichten bereitstellt. Die Schnittstelle bietet die folgenden Operationen:

- send_Message(Nachricht, Anmeldedaten) und
- receive_Message(Anmeldedaten): Nachricht[ ].

Die Schnittstelle kann sowohl seitens des KOM-LE-Clientmoduls als auch eines anderen KOM-LE-Fachdienstes (nur send_Message Operation) aufgerufen werden. Erfolgt der Aufruf der Operation send_Message durch einen anderen Fachdienst, entfällt der Parameter Anmeldedaten.
[<=]

KOM-LE-A_2141 - Technische Umsetzung der Schnittstelle I_Message_Service
Die technische Umsetzung der Schnittstelle I_Message_Service erfolgt über die Bereitstellung von entsprechenden TCP-Ports am KOM-LE-Fachdienst für SMTP-bzw. POP3-Verbindungen. Die Schnittstelle MUSS ausschließlich über eine sichere Verbindung unter Verwendung von TLS mit beidseitiger zertifikatsbasierter Authentifizierung zugänglich sein.
[<=]

KOM-LE-A_2226 - Zuordnung TLS-Client-Zertifikat für Clientmodul
Der KOM-LE-Anbieter MUSS das KOM-LE Clientmodul mit einem TLS-Client-Zertifikat aus der Komponenten-PKI der TI für die TLS-Kommunikation mit dem KOM-LE Fachdienst ausstatten.
[<=]

KOM-LE-A_2227 - Zuordnung TLS-Server-Zertifikat für Clientmodul
Der KOM-LE-Anbieter MUSS das KOM-LE Clientmodul mit einem TLS-Server-Zertifikat aus der Komponenten-PKI der TI für die TLS-Kommunikation mit Clientsystemen ausstatten.
[<=]

KOM-LE-A_2228 - Ausschließliche Akzeptanz von TLS-Client-Zertifikaten von KOM-LE Clientmoduln
Der Fachdienst MUSS beim Aufbau einer TLS-Verbindung mit dem KOM-LE Clientmodul ausschließlich Client-Zertifikate akzeptieren, die KOM-LE Clientmoduln zugeordnet sind.
[<=]

ENTWURF

KOM-LE-A_2186 - Verwendung des C.FD.TLS-S Server-Zertifikats bei der TLS-Authentifizierung mit dem Clientmodul
Beim Aufbau der TLS-Verbindung mit dem Clientmodul MUSS sich der Fachdienst KOM-LE mit seinem C.FD.TLS-S Server-Zertifikat authentifizieren.
[<=]

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

- SMTPS: 465 und
- POP3S: 995.

[<=]

KOM-LE-A_2143 - Aufbau der TLS-Verbindung
Der Aufbau der TLS-Verbindung für die Schnittstelle I_Message_Service DARF NICHT über STARTTLS erfolgen.
[<=]

KOM-LE-A_2144 - Schritte beim Aufbau der TLS-Verbindung
Beim Aufbau der TLS-Verbindung MUSS der KOM-LE-Fachdienst folgende Schritte bei der Prüfung des vorgelegten Clientzertifikats (C.CM.TLS-CS-Zertifikat des Clientmoduls oder C.FD.TLS-C Client-Zertifikat eines anderen KOM-LE-Fachdienstes) durchführen:

- Prüfung des Vertrauensstatus der Aussteller-CA gegen die TSL,
- mathematische Prüfung der Zertifikatssignatur,
- Prüfung der zeitlichen Gültigkeit des Zertifikats und
- Prüfung des Zertifikatsstatus 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.
[<=]

KOM-LE-A_2145 - Validierung der TSL
Unabhängig von der Zertifikatsprüfung MUSS der KOM-LE-Fachdienst in regelmäßigen Zyklen die TSL-Validierung durchführen. Dabei sind folgende Schritte auszuführen:

- Download der aktuellen Liste vom relevanten Downloadpunkt,
- Validierung gegen das XML-Schema der TSL,
- Prüfung des Vertrauensstatus des TSL-Signaturzertifikats gegen einen sicher verwahrten TSL-Root-Schlüssel und
- Prüfung der XML-Signatur.

[<=]

4.1.1 Operation send_Message

Die Operation send_Message ermöglicht das Versenden von KOM-LE-Nachrichten über den Mail Server des KOM-LE-Fachdiensts. Die logischen Parameter dieser Operation werden in Tabelle ~~3~~ Tab_Para_send_Msg Parameter send_Message Fachdienst KOM-LE beschrieben. Die technische Implementierung dieser Operation erfolgt über die Bereitstellung eines TCP-Ports über den eine SMTP-Verbindung für das Versenden von KOM-LE-Nachrichten aufgebaut wird [RFC 5321].

ENTWURF

Tabelle 5: Tab_Para_send_Msg Parameter send_Message Fachdienst KOM-LE

Parameter		Beschreibung
Eingangsparameter	Anmeldedaten (optional)	Benutzername und Passwort für Authentifizierung des Clients gegenüber dem SMTP-Server seines KOM-LE-Anbieters. Bei der Kommunikation zwischen Clientmodul und SMTP-Server des Senders ist dieser Parameter zwingend erforderlich. Bei Dienst-zu-Dienst-Kommunikation (SMTP-Server des Senders und SMTP-Server des Empfängers) entfällt der Parameter.
	Nachricht	KOM-LE-Nachricht

KOM-LE-A_2146-01~~KOM-LE-A_2146~~ - Verarbeitung von Nachrichten entsprechend S/MIME-Profil

Der Mail Server DARF Nachrichten, die nicht entsprechend S/MIME-Profile [gemSMIME_KOMLE] verschlüsselt sind, NICHT weiterleiten bzw. im Postfach des Empfängers hinterlegen. Für alle servergenerierten Nachrichten wie ~~Zustellbestätigungen,~~ Fehlermeldungen und Abwesenheitsnotizen sowie vom Clientmodul generierte Fehlernachrichten, gilt diese Anforderung nicht.

~~[<=]~~

Die folgende Tabelle listet die damit möglichen Fehlermeldungen. Das Header-Attribut `X-kim-kgerr` wird mit dem Wert in der Tabelle befüllt.

Prüfkriterien	Fehler	Wert
Mail zu groß?	`"mail size too big"`	fdgerr_1
Einziger Empfänger ist gleich dem Absender	Abbruch weiterer Prüfungen, da es eine CM-generierte Fehlermail (an sich selbst) ist/sein könnte	fdgerr_2
Header "`X-KOM-LE-Version`" ungültig	`"invalid X-KOM-LE-Version header"`	fdgerr_3
Subject ungleich "KOM-LE-Nachricht"	`"invalid subject"`	fdgerr_4
ContentType beginnt nicht mit `"application/pkcs7-mime;"` oder enthält nicht `"smime-type=authenticated-enveloped-data"`	`"invalid content type"`	fdgerr_5

ENTWURF

Prüfung diverser Mailbody-Eigenschaften auf Verschlüsselung schlägt fehl	"invalid mail encryption"	fdgerr_6

[<=]

Die Übermittlung der Fehlernachrichten ermöglicht somit eine automatische Auswertung und Klassifizierung der eingehenden Nachrichten auf der Empfängerseite durch Auswertung des Mail-Header Attributs.

~~**KOM-LE-A_2147 - Generierung von Zustellbestätigungen**~~

~~Erhält der Mail Server eine Nachricht, die eine Zustellbestätigung fordert, MUSS er diese unter Verwendung folgender Informationen aus der empfangenen Nachricht:~~

- ~~Empfänger und~~
- ~~Empfangszeitpunkt~~

~~generieren und unverschlüsselt an den Absender weiterleiten.~~

~~[<=]~~

KOM-LE-A_2148 - Authentifizierungsmechanismen beim Nachrichtenversand

Der Mail Server MUSS die Authentifizierungsmechanismen PLAIN [RFC 4616], CRAM-MD5 [RFC 2195] und SCRAM-SHA-1 [RFC 5802] von SMTP-Auth [RFC 4954] unterstützen.

[<=]

KOM-LE-A_2149 - Kein Empfang von Nachrichten bei deregistriertem Konto

Der KOM-LE-Fachdienst MUSS Nachrichten, die an ein deregistriertes Konto gerichtet sind, bei Eingang verwerfen und an den Absender eine Fehler-E-Mail senden.

[<=]

KOM-LE-A_2150 - Kein Versenden von Nachrichten bei deregistriertem Konto

Der KOM-LE-Fachdienst DARF Nachrichten NICHT von einem deregistrierten Konto aus verschicken.

[<=]

A_20651 - Empfang von Fehlernachrichten des Clientmodules

Der KOM-LE-Fachdienst MUSS Nachrichten vom Clientmodul, die nicht signiert und verschlüsselt sind, nur entgegennehmen wenn das Mail-Header-Attribut `X-kim-kgerr` vorhanden ist. Als zulässige Befüllung dieses Attributs gelten die in der [gemSpec_CM_KOMLE#A_20650] festgelegten Werte. Nicht signierte und verschlüsselte Nachrichten ohne befülltem Mail-Header-Attribut `X-kim-kgerr` werden nicht entgegengenommen.**[<=]**

4.1.2 Operation receive_Message

Die Operation receive_Message ermöglicht das Abholen von KOM-LE-Nachrichten vom Mail Server des KOM-LE-Fachdiensts. Die logischen Parameter dieser Operation werden in Tabelle ~~4~~ Tab_Para_recive_Msg Parameter receive_Message Fachdienst KOM-LE beschrieben. Die technische Implementierung dieser Operation erfolgt über Bereitstellung eines TCP-Ports über den eine POP3-Verbindung für das Abholen von KOM-LE-Nachrichten aufgebaut wird [RFC 1939].

ENTWURF

549 **Tabelle 6: Tab_Para_recive_Msg Parameter receive_Message Fachdienst KOM-LE**

Parameter		Beschreibung
Eingangsparameter	Anmeldedaten	Benutzername und Passwort für Authentifizierung gegenüber dem POP3-Server.
Ausgangsparameter	Nachricht[ ]	KOM-LE-Nachrichten

550
551

552 **KOM-LE-A_2151 - Unterstützung des POP3-Kommandos APOP**
553 Der Mail Server MUSS sowohl die Authentifizierung mit Benutzername und Passwort als
554 auch über das POP3-Kommando APOP ermöglichen.
555 **[<=]**

556 **KOM-LE-A_2152 - Unterstützung des POP3-Kommandos UIDL**
557 Um die Kompatibilität mit dem KOM-LE-Clientmodul sicherzustellen MUSS der Mail Server
558 das POP3-Kommando UIDL unterstützen.
559 **[<=]**

560 **KOM-LE-A_2154 - Versand von Löschbenachrichtigungen**
561 Der KOM-LE-Fachdienst DARF den Sender NICHT über das automatische Löschen einer
562 von ihm versendeten aber nicht abgeholten Nachricht informieren.
563 **[<=]**

564 **KOM-LE-A_2155 - Nicht abgeholte Nachrichten nach der Deregistrierung**
565 Der KOM-LE-Fachdienst MUSS bereits eingegangene Nachrichten, die noch nicht vom
566 Teilnehmer abgerufen wurden, auch nach der Deregistrierung des Teilnehmers bis Ablauf
567 der Löschfrist der jeweiligen Nachricht zum Abrufen bereit halten und dann löschen.
568 **[<=]**

569 4.2 Schnittstelle I_Attachment_Services

570 Der KAS ermöglicht das Hoch- und Herunterladen von verschlüsselten Anhängen von
571 Mails. Zum Bereitstellen der Funktionen wird die REST-Schnittstelle
572 I_Attachment_Services definiert. Der Aufruf der Schnittstelle ist ausschließlich vom
573 Clientmodul zulässig. Die Schnittstellenbeschreibung ist in [AttachmentServices.yaml]
574 definiert.

575 In der folgenden Tabelle sind alle Ressourcen mit den jeweiligen HTTP-Methoden
576 dargestellt. Die jeweilige Operation ist eine Abstraktion auf einen Webservice Endpunkt.

577

578 **Tabelle 7: Operationen vom KAS**

Operation	URI	Method e	Reques t	Response	Beschreibun g

ENTWURF

add_Attachment	/	POST	binary <File>	string <Freigabelink>	Fügt einen verschlüsselten Anhang im KAS hinzu
read_Attachment	/ID_der_Ressource (Teil des Freigabelinks)	GET	-	binary <File>	Lädt einen unter einem Freigabelink erreichbaren verschlüsselten Anhang herunter
read_MaxMailSize	/MaxMailSize	GET	-	integer	Gibt die maximal unterstützte Größe einer Mail (inklusive Anhänge und base64-Kodierung) zurück.

A_19375 - KAS – Implementierung der Schnittstelle
Der KAS MUSS die Schnittstelle I_Attachment_Services als REST-Webservices über HTTPS gemäß [AttachmentServices.yaml] implementieren.
[<=]

A_19377 - KAS – TLS-gesicherte Verbindung
Der KAS MUSS die Schnittstelle I_Attachment_Services durch Verwendung von TLS mit beidseitiger Authentisierung sichern. Der KAS MUSS für diese TLS-Verbindungen TI-Zertifikate (analog zu Schnittstelle I_Message_Service) nutzen. Der KAS MUSS sich mit der Server-Identität von Schnittstelle I_Attachment_Services authentisieren.
[<=]

A_19378 - KAS – Dokumentengröße prüfen
Der KAS MUSS die Dateigröße jedes übergebenen Dokumentes ermitteln, bevor das Dokument gespeichert wird. Der KAS MUSS die Verarbeitung ablehnen, wenn die Gesamtgröße des Dokumentes diesen Konfigurationswert des KAS übersteigt.**[<=]**

A_19519 - KAS – Maximale Mail Größe bereitstellen
Der KAS MUSS seinen Clients die maximale Gesamtgröße einer Mail mit Operation read_MaxMailSize bereitstellen. Dieser Wert MUSS konfigurierbar sein. Der Wert für die maximale Gesamtgröße einer Mail MUSS mindestens 500 MB betragen.
[<=]

A_19379 - KAS – Dokumentenzugriff
Der KAS MUSS sicherstellen, dass nur über den dazugehörigen Freigabelink auf das Dokument zugegriffen werden kann.**[<=]**

Erzeugung des Freigabelinks

ENTWURF

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

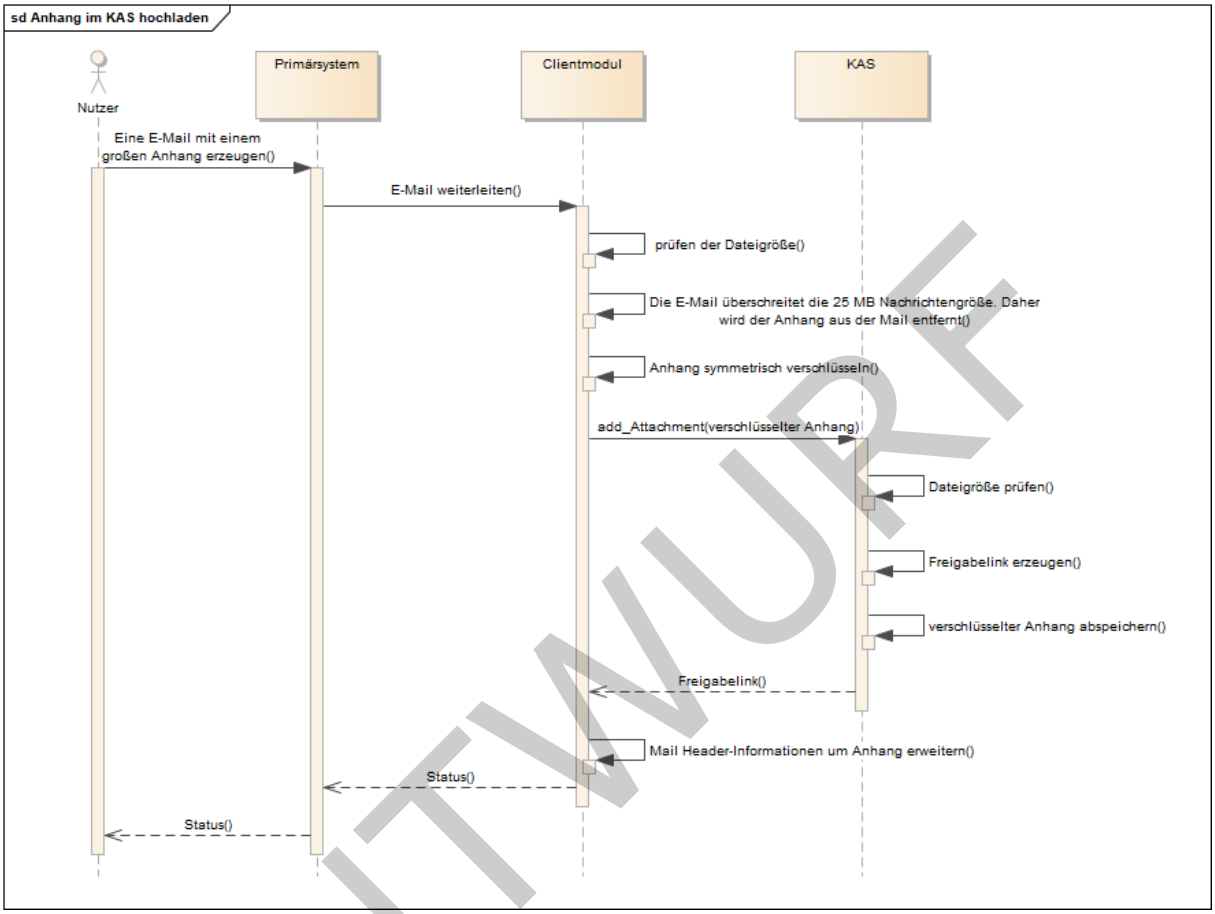

Abbildung 4 Abb_Anw_Dokument auf dem KAS hochladen

A_19380 - KAS – Erzeugung Freigabelink
Der KAS MUSS bei Aufruf der REST-Operation add_Attachment einen Freigabelink erzeugen, die aus dem FQDN der Teilkomponente KAS und einer zufälligen und eindeutigen ID der Ressource (Anhang) z.B. einer UUID [RFC4122] besteht und diesen an den aufrufenden Client zurückgeben.
[<=]

A_19381 - KAS – Freigabelink Transportsicherheit
Der KAS MUSS in den Freigabelink das https-Protokoll hinein generieren: "HTTPS://".
[<=]

A_19382 - KAS – Freigabelink löschen
Der KAS MUSS bei Löschung einer Ressource (Anhang) im KAS-Speicher gewährleisten, dass unter dem Freigabelink der gelöschten Ressource für ein Jahr keine Ressource abrufbar ist.
[<=]

ENTWURF

A_19383 - KAS – Keine Kopien von gelöschten Daten
Der KAS DARF von gelöschten Daten KEINE Kopien speichern.
[<=]

Anforderungen an den Anbieter

Im Folgenden werden weitere Anforderungen an den Anbieter der KAS-Komponente gestellt:

A_19384 - KAS – Sicher gegen Datenverlust
Der Anbieter des KAS MUSS den Dienst gegen Datenverlust absichern.
[<=]

A_19385 - 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.
[<=]

4.3 Schnittstelle I_AccountManager_Service

Der Account Manager stellt ein Webservices zur einfachen Verwaltung des Accounts eines KOM-LE-Teilnehmers bereit. Die Schnittstellenbeschreibung I_AccountManager_Service ist in [AccountManager.yaml] definiert. Der Aufruf der REST-Schnittstelle ist ausschließlich vom Clientmodul (Administrationsmodul) zulässig.

A_20209 - KOM-LE - Erfassung von Teilnehmerdaten und Bereitstellung von Zugangsdaten
Der KOM-LE Anbieter MUSS den KOM-LE Teilnehmern alle nötigen Zugangsdaten auf einem sicheren Weg bereitstellen.**[<=]**

In der folgenden Tabelle sind alle Ressourcen mit den jeweiligen HTTP-Methoden dargestellt. Die jeweilige Operation ist eine Abstraktion auf einen Webservice Endpunkt.

Tabelle 8: Operationen vom Account Manager

Operation	URI	Methode	Request	Response	Beschreibung
`register`	/accmgr/register/	POST	username password timestamp nonce signedHash	<Status> <PKCS#12-Datei>	Registrierung des Teilnehmers am KOM-LE-Fachdienst sowie das Herunterladen der PKCS#12-Datei.
`deregister`	/accmgr/deregister/	POST	username password timestamp nonce signedHash	<Status>	Deregistrierung des Teilnehmers am KOM-LE-Fachdienst.

ENTWURF

register_State	/accmgr/register-state/	GET	username password timestamp nonce signedHash	<Status>	Abfrage des Registrierungsstatus.
cm_Version	/accmgr/cm-version/	PUT	username password KOM-LE-Version timestamp nonce signedHash	<Status>	Übermittelung der KOM-LE-Version.
pw_Change	/accmgr/pw/	PUT	username password newPassword timestamp nonce signedHash	<Status>	Änderung des Passworts.

A_20063 - Account Manager - Implementierung der Schnittstelle
Die Teilkomponente Account Manager des Fachdienstes MUSS die Schnittstelle I_AccountManager_Service als REST-Webservice über HTTPS gemäß [AccountManager.yaml] implementieren.
[<=]

A_20064 - Account Manager - TLS-gesicherte Verbindung
Die Teilkomponente Account Manager des Fachdienstes MUSS die Schnittstelle I_AccountManager_Service bei der Registrierung durch Verwendung von TLS mit serverseitiger Authentisierung sichern.
[<=]

Mit den folgenden Anforderungen wird die Funktionsweise der Operationen des Webservices festgelegt.

KOM-LE-A_2187-01 - Authentifizierung des KOM-LE-Teilnehmers über AUT-Zertifikat am AccountManager
Zur Pflege der Basisdaten des Verzeichnisdienstes und bei der Registrierung und Deregistrierung MUSS der Fachdienst die Authentizität des KOM-LE-Teilnehmers über das AUT-Zertifikat des HBA bzw. der SM-B des Teilnehmers prüfen. Über die aus dem AUT-Zertifikat ermittelte Telematik-ID ist anschließend der Zugriff auf den Verzeichnisdienst möglich.
Der Fachdienst MUSS vor Ausführung der angefragten HTTP-Methoden den Client erfolgreich über sein AUT-Zertifikat authentisieren. Hierzu MUSS folgende Authentisierungsmethode verwendet werden:
Der Client MUSS eine zufällige 256bit Nonce und einen Unix-Timestamp in die Nachricht einfügen. Die Parameterinhalte der Nachricht müssen zu einem String zusammengefügt werden (in der Reihenfolge der Parameter Beschreibung der Operationen in der Datei [AccountManager.yaml]). Von diesem String MUSS der Hash entsprechend A_19644 [gemSpec_Krypt] gebildet werden. Dieser Hash MUSS mittels der externalAuthenticate

ENTWURF

Funktion des Konnektors mit dem AUT-Zertifikat des HBA bzw. der SMC-B signiert werden. Als Signature Type MUSS PKCS#1-Signatur gewählt werden (und nach Unterstützung durch alle Konnektoren ECDSA-Signatur). Diese Signatur MUSS ebenfalls in die Nachricht eingefügt werden.
Der Fachdienst MUSS eine Ablaufzeitspanne für I_AccountManager_Service Nachrichten konfigurieren, empfohlen sind 5min. Der Fachdienst MUSS eine Liste mit genutzten Nonces und Zeitstempel pro Nutzer führen. Ein Timestamp und auch die assoziierte Nonce sind zum Zeitpunkt Timestamp+Ablaufzeitspanne abgelaufen.
Bei Erhalt einer Nachricht MUSS der Fachdienst zunächst prüfen

- ob der Timestamp noch gültig ist, also vor weniger Zeit als der Ablaufzeitspanne erzeugt wurde,
- ob der signierte Hash korrekt ist
- ob Username und Passwort korrekt sind
- ob Username zu dem AUT-Zertifikatsinhaber (die Zuordnung von Zertifikat zu mail-Adresse ist durch den VZD Eintrag gegeben) passt und
- ob die Nonce noch nicht in der Liste für diesen Nutzer vorhanden ist.

Ist eine dieser Prüfungen nicht erfolgreich MUSS die Nachricht zurückgewiesen werden. Sind alle Prüfungen erfolgreich, ist die Nachricht valide und MUSS verarbeitet werden. Der Fachdienst MUSS die erhaltene Nonce einer validen Nachricht in die Nonceliste für den jeweiligen Nutzer aufnehmen. Der Fachdienst MUSS nur Nonces aus validen Nachrichten speichern. Nonces MÜSSEN so lange gespeichert werden, bis sie abgelaufen sind.
[<=]

KOM-LE-A_2305 - Mehrere KOM-LE Postfächer für einen KOM-LE-Teilnehmer
Der KOM-LE Fachdienst MUSS die Möglichkeit anbieten für einen KOM-LE-Teilnehmer, repräsentiert durch dasselbe AUTH Zertifikat, mehrere Postfächer mit jeweils eigener E-Mail-Adresse und eigenen Anmeldecredentials nutzen zu können.**[<=]**

KOM-LE-A_2158 - Protokollieren von Registrierung und Deregistrierung
Der KOM-LE-Fachdienst MUSS das Registrieren und Deregistrieren von KOM-LE-Teilnehmern protokollieren.
[<=]

KOM-LE-A_2159-01~~KOM-LE-A_2159~~ - Verwendung der Schnittstelle I_Directory_Application_Maintenance
Für die Änderung des Verzeichniseintrages (Eintragen ~~bzw.~~und Löschen der E-Mail-Adresse des KOM-LE-Teilnehmers sowie die vom Clientmodul verwendete KOM-LE-Version) MUSS der KOM-LE-Fachdienst die Schnittstelle I_Directory_Application_Maintenance der TI-Plattform verwenden.
[<=]

A_20212 - Verwendung der Schnittstelle I_Directory_Application_Maintenance, Lokalisierung Verzeichniseintrag
Für die Änderung des Verzeichniseintrages (Eintragen bzw. Löschen der E-Mail-Adresse des KOM-LE-Teilnehmers) MUSS der KOM-LE-Fachdienst zur Lokalisierung des VZD Eintrags die Telematik-ID aus dem AUT Zertifikat nutzen, mit dem sich der KOM-LE Teilnehmer an der Schnittstelle I_AccountManager_Service authentifiziert hat.
[<=]

KOM-LE-A_2160 - Kommunikation mit dem Verzeichnisdienst über TLS
Der Fachdienst KOM-LE MUSS bei der Änderung des Verzeichniseintrages über die Schnittstelle I_Directory_Application_Maintenance immer eine sichere Verbindung unter

ENTWURF

Verwendung von TLS mit beidseitiger zertifikatsbasierter Authentifizierung benutzen.
[<=]

KOM-LE-A_2189 - Verwendung des C.FD.TLS-C Client-Zertifikats bei der TLS-Authentifizierung mit dem Verzeichnisdienst
Beim Aufbau der TLS-Verbindung mit dem Verzeichnisdienst MUSS sich der Fachdienst KOM-LE mit seinem C.FD.TLS-C Client-Zertifikat authentifizieren.
[<=]

KOM-LE-A_2161 - Benutzername der KOM-LE-Teilnehmers
Der KOM-LE-Fachdienst MUSS bei der Registrierung die E-Mail-Adresse des KOM-LE-Teilnehmers als Benutzernamen verwenden.
[<=]

KOM-LE-A_2162 - Übermittlung der Passwörter zum Fachdienst
Die Fachanwendung KOM-LE MUSS gewährleisten, dass Passwörter der Teilnehmer nur vertraulichkeits-, integritäts- und authentizitätsgeschützt vom Client zum Fachdienst übermittelt werden.
[<=]

KOM-LE-A_2163 - Vorgaben zur Minimum-Qualität des Passwortes
Der KOM-LE-Anbieter MUSS Vorgaben zur Minimum-Qualität des Passwortes (entsprechend BSI GS M 2.11 „Regelung des Passwortgebrauchs“) machen und die Einhaltung dieser Vorgaben gewährleisten.
[<=]

KOM-LE-A_2164 - Passwörter nicht im Klartext speichern
Der Fachdienst KOM-LE DARF Passwörter der KOM-LE-Teilnehmer NICHT im Klartext speichern.
[<=]

KOM-LE-A_2165 - Möglichkeit der Änderung des Passwortes
Die Teilkomponente Account Manager des Fachdienstes KOM-LE MUSS dem KOM-LE-Teilnehmer die Möglichkeit anbieten das Passwort für die Anmeldung am KOM-LE-Fachdienst zu ändern.
[<=]

KOM-LE-A_2166 - Keine Änderung oder Löschung des Passwortes durch Dritte
Der KOM-LE-Fachdienst DARF das Ändern oder Löschen der bei ihm gespeicherten Passwörter der KOM-LE-Konten durch Dritte NICHT zulassen.
[<=]

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

KOM-LE-A_2303 - Übermittlung Schlüssel und TLS-Zertifikat für Clientmodule
Der KOM-LE-Anbieter MUSS über einen beidseitig authentisierten Kanal unter Wahrung der Vertraulichkeit und Integrität den privaten Schlüssel und das C.CM.TLS-CS-Zertifikat für das Clientmodul – sowohl initial für die Ersteinrichtung als auch periodisch vor Ablauf des jeweils aktuell verwendeten Zertifikats – an den KOM-LE-Nutzer übermitteln.**[<=]**

Dies kann bspw. mittels der Übertragung einer PKCS#12-Datei über einen beidseitig authentisierten TLS-Kanal unter Nutzung des Auth-Clients realisiert werden, wobei die Möglichkeit der Authentifizierung des Fachdienstes durch den Nutzer gegeben sein muss.

ENTWURF

KOM-LE-A_2167 - Sperrung des Accounts
Der Fachdienst KOM-LE MUSS den Account eines Teilnehmers nach drei aufeinanderfolgenden Fehleingaben des Passwortes temporär sperren. Nach dem Sperren des Accounts kann der Nutzer keine E-Mails mehr versenden bzw. abholen. Die Benutzerinformationen bleiben aber erhalten, so dass später ein Entsperren des Accounts möglich ist.
[<=]

KOM-LE-A_2168-01~~KOM-LE-A_2168~~ - Entsperren des Accounts
Der KOM-LE Anbieter MUSS einen Prozess implementieren, der es berechtigten Teilnehmern ermöglicht, mit Hilfe des KOM-LE Anbieters seinen gesperrten Account wieder freizuschalten. Der KOM-LE Anbieter MUSS den Teilnehmer mit Vetragsabschluss über diesen Prozess informieren. Der KOM-LE Anbieter ist der Owner des Prozesses.
[~~<=Der KOM-LE Anbieter MUSS praktikable Mechanismen zum Entsperren eines aufgrund fehlerhafter Passworteingaben gesperrten Accounts anbieten.~~
~~[<=~~]

KOM-LE-A_2169 - Authentifizierungsdaten beim Versenden und Empfangen von Nachrichten
Der KOM-LE-Fachdienst MUSS die im Registrierungsprozess vergebenen Daten für Benutzername und Passwort sowohl beim Versenden von Nachrichten über SMTP als auch beim Abholen von Nachrichten über POP3 für die Authentifizierung verwenden.
[<=]

A_18784 - Bereitstellung Schlüssel und Zertifikat für Clientmodul als passwortgeschützte PKCS#12 Datei
Der KOM-LE-Anbieter MUSS dem KOM-LE-Teilnehmer das Schlüsselmaterial und das Zertifikat für das KOM-LE-Clientmodul im Registrierungsprozess als passwortgeschützte PKCS#12-Datei zur Verfügung stellen. Die Übermittlung des zur p12-Datei gehörigen Passworts muss über eine verschlüsselte, authentifizierte und integritätsgeschützte Verbindung übertragen werden.
[<=]

A_19542 - Schnittstelle für den Download
DerAccount Manager MUSS eine Operation für das Herunterladen der PKCS#12-Datei bereitstellen.
[<=]

4.4 Genutzte Schnittstellen der TI-Plattform

Hier werden die durch den Fachdienst genutzten Schnittstellen der TI-Plattform aufgelistet. Die Spezifikation dieser Schnittstellen erfolgt durch das Projekt Basis-TI und wird in [gemKPT_Arch_TIP] beschrieben.

KOM-LE-A_2231 - Schnittstellen der TI-Plattform
Der Fachdienst KOM-LE MUSS die in der Tabelle Tab_Interface_TIP aufgeführten Schnittstellen der TI-Plattform benutzen.
[<=]

Tabelle 9: Tab_Interface_TIP Schnittstellen zur TI-Plattform des Fachdienstes KOM-LE

Schnittstelle	Operation	benutzt durch

ENTWURF

I_Directory_Application_Maintenance	add_Directory_FA-Attributes delete_Directory_FA-Attributes modify_Directory_FA-Attributes	Account Manager bei der Registrierung bzw. Deregistrierung
I_Directory_Query	search_Directory	Account Manager bei der Registrierung bzw. Deregistrierung
I_Directory_Maintenance	add_Directory_FA-Attributes delete_Directory_FA-Attributes modify_Directory_FA-Attributes	Account Manager zur Pflege der Basisdaten des Verzeichnisdienstes
I_NTP_Time_Information	sync_Time	Fachdienst für die Verwendung der korrekten Zeit z.B. beim Versenden und Weiterleiten von E-Mails/Empfangsbestätigungen oder bei der Erstellung von Logging-Einträgen
I_DNS_Name_Resolution	get_IP_Address	Mail Server beim Versenden und Weiterleiten von E-Mails
I_OCSP_Request	check_Revocation_Status	Mail Server beim Aufbau der TLS-Verbindung
I_TSL_Download	download_TSL	Mail Server als Vorbedingung beim Aufbau der TLS-Verbindung

ENTWURF

5 Nicht-Funktionale Anforderungen

5.1 Skalierbarkeit

KOM-LE-A_2171 - Skalierbarkeit KOM-LE-Fachdienst
Der KOM-LE-Fachdienst MUSS mit einer zunehmenden Anzahl von beteiligten Teilnehmern skalieren.
[<=]

5.2 Performance

Die durch den Fachdienst KOM-LE zu erfüllenden Performance-Anforderungen befinden sich in [gemSpec_Perf#4.4].

5.3 Mengengerüst

Das für den Fachdienst KOM-LE relevante Mengengerüst befindet sich in [gemSpec_Perf#3.1].

ENTWURF

6 Anhang A – Verzeichnisse

6.1 Abkürzungen

Abkürzung	Bedeutung
base64	Verfahren zur Kodierung von Binärdaten in eine Zeichenfolge, die nur aus lesbaren ASCII-Zeichen besteht
DNS	Domain Name System
HBA	Heilberufsausweis
ID	Identification
IP	Internet Protocol
MIME	Multipurpose Internet Mail Extensions
ISO	International Organization for Standardization
KB	Kilobyte
KAS	KOM-LE Attachment Service
MB	Megabyte
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
POP3	Post Office Protocol Version 3
RFC	Request for Comments
SMC (B/A/KTR)	Security Module Card
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
TI	Telematikinfrastruktur
TLS	Transport Layer Security, die Vorgängerbezeichnung ist SSL

ENTWURF

TSL	Trusted Service List
S/MIME	Secure Multipurpose Internet Mail Extensions
XML	Extensible Markup Language

6.2 Glossar

Das Glossar wird als eigenständiges Dokument, vgl [gemGlossar_TI] zur Verfügung gestellt.

6.3 Abbildungsverzeichnis

6.4 Tabellenverzeichnis

ENTWURF

6.5 Referenzierte Dokumente

6.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummer entnehmen Sie bitte der aktuellen, auf der Internetseite der gematik veröffentlichten Dokumentenlandkarte, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemGlossar_TI]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemLH_KOM-LE]	gematik: Lastenheft Kommunikation Leistungserbringer (KOM-LE)
[gemSysL_KOM-LE]	gematik: Systemspezifisches Konzept Kommunikation Leistungserbringer (KOM-LE)
[gemSpec_CM_KOMLE]	gematik: Spezifikation Clientmodul KOM-LE
[gemSMIME_KOM-LE]	gematik: S/MIME-Profil Kommunikation Leistungserbringer (KOM-LE)
[AttachmentServices.yaml]	gematik: https://github.com/gematik/api-kim
[AccountManager.yaml]	gematik: https://github.com/gematik/api-kim

ENTWURF

876 ### 6.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[DESTATIS_KRK]	Statistisches Bundesamt Deutschland, Eckdaten der Krankenhäuser 2010 http://www.destatis.de/
[RFC1939]	RFC 1939: Post Office Protocol – Version 3, J. Myers, M. Rose, Mai 1996
[RFC 2195]	J. Klensin, R. Catoe, P. Krumviede, RFC 2195: IMAP/POP AUTHorize Extension for Simple Challenge/Response, September 1997
[RFC4122]	A Universally Unique IDentifier (UUID) URN Namespace
[RFC 4616]	K. Zeilenga, RFC 4616: The PLAIN Simple Authentication and Security Layer (SASL) Mechanism, August 2006
[RFC 4954]	R. Siemborski, A. Melnikov, RFC 4954: SMTP Service Extension for Authentication, July 2007
[RFC 5321]	J. Klensin, RFC 5321: Simple Mail Transfer Protocol, October 2008
[RFC 5802]	C. Newman, A. Menon-Sen, A. Melnikov, N. Williams, RFC 5802: Salted Challenge Response Authentication Mechanism (SCRAM) SASL and GSS-API Mechanisms, July 2010

877
878

ENTWURF