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.

Änderungsbedarf in gemSpec_FD_KOMLE

In Kapitel 4.2 müssen die Anforderungen **KOM-LE-A_230x** und **KOM-LE-A_230x** ergänzt werden. Die Anforderung **KOM-LE-A_2187** muss wie folgt angepasst und die Anforderung **KOM-LE-A_2188** entfernt werden.

⌦ **A_13540 Pflege der Basisdaten des Verzeichnisdienstes**

Zusätzlich zur Schnittstelle für die Registrierung und Deregistrierung MUSS der Fachdienst dem KOM-LE-Teilnehmer eine Schnittstelle zur Pflege (erzeugen, lesen, ändern und löschen) der Basisdaten des Verzeichnisdienstes der TI anbieten. ⌫

⌦ **KOM-LE-A_2187 Authentifizierung des KOM-LE-Teilnehmers über AUT-Zertifikat**

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 ~~zum Eintragen (Registrierung) bzw. zum Löschen (Deregistrierung) der E-Mail-Adresse(n) des KOM-LE-Teilnehmers~~ möglich. ⌫

~~⌦ **KOM-LE-A_2188 Authentifizierung über AUT-Zertifikat unter Verwendung des Auth-Clients**~~

~~Der Fachdienst KOM-LE SOLL bei der Registrierung und Deregistrierung für die Prüfung der Authentizität des KOM-LE-Teilnehmers über dessen AUT-Zertifikat eine webbasierte Anwendung unter Verwendung des Auth-Clients [gemKPT_Auth-Client] anbieten.~~ ⌫

⌦ **A_13541 Verwendung der Schnittstelle I_Directory_Maintenance**

Für die Pflege der Basisdaten des Verzeichniseintrages MUSS der KOM-LE-Fachdienst die Schnittstelle I_Directory_Maintenance der TI-Plattform verwenden. ⌫

Änderungen in gemProdT_FD_KOMLE

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

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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_13540	Pflege der Basisdaten des Verzeichnisdienstes	gemSpec_FD_KOMLE
A_13541	Verwendung der Schnittstelle I_Directory_Maintenance	gemSpec_FD_KOMLE
KOM-LE-A_2187	Authentifizierung des KOM-LE-Teilnehmers über AUT-Zertifikat	gemSpec_FD_KOMLE
~~KOM-LE-A_2188~~	~~Authentifizierung über AUT-Zertifikat unter Verwendung des Auth-Clients~~	~~gemSpec_FD_KOMLE~~

Änderungsbedarf in gemKPT_Arc h_TIP

~~5.7.14 P_Directory_Administration_Registration (Provided)~~

~~**TIP1-A_5924 Organisatorische Schnittstelle P_Directory_Administration_Registration**~~

~~Die organisatorische Schnittstelle P_Directory_Administration_Registration MUSS alle zugehörigen Festlegungen erfüllen.~~

~~**Tabelle 2: Schnittstelle P_Directory_Administration_Registration**~~

~~P_Directory_Administration_Registration~~	~~Berechtigung: FAD, SÜV~~
~~Diese Prozessschnittstelle ermöglicht • FA-Anbieter können sich beim Verzeichnisdienst registrieren. Nach dieser Registrierung können Basisdaten im Verzeichniseintrag eines Teilnehmers über die Schnittstelle I_Directory_Maintenance erstellt, gepflegt und gelöscht werden. Bei der Registrierung gibt der FA-Anbieter an o TLS-Client-Identität seines Fachdienstes (ID.FD.TLS-C), o Telematik-ID des Verzeichniseintrags, für den er sich registriert o Nachweis der Berechtigung zur Datenadminstration durch den Betroffenen (Inhaber des HBA oder der SMC-B) o Name/Identität des Fachdienstes • FA-Anbieter können sich beim Verzeichnisdienst deregistrieren. Der Zugang über die Schnittstelle I_Directory_Maintenance ist danach für den betroffenen Verzeichniseintrag nicht mehr möglich.~~	
~~Verfügbarkeit: N, Nichtabstreitbarkeit: H~~	

Änderungsbedarf in gemSpec_VZD

Die Änderung C_6380 aus P15.2 wird storniert (Lösung mit Webanwendung). Die im Folgenden beschriebenen Änderungen beziehen sich auf gemSpec_VZD Version 1.5.0 (Release 2.1.1).

Änderungen in Kapitel 3.1

~~**TIP1-A_5610 VZD, Einwilligung muss vorliegen**~~

~~Der Anbieter des VZD MUSS sicherstellen, dass die informierte Einwilligung des betroffenen Leistungserbringers vorliegt, bevor er dessen Daten auf dem Verzeichnisdienst der TI speichert.~~⌫

Änderungen in Kapitel 3.2

⌦ **TIP1-A_5561 VZD, DNS-SD**

Der Anbieter des VZD MUSS alle erforderlichen Einträge zur Dienstlokalisierung der Außenschnittstellen gemäß [RFC6763] beginnend mit folgenden PTR Resource Record-Bezeichnern im Namensdienst der TI-Plattform anlegen:

- für den Zugriff auf die Schnittstelle I_Directory_Query:

  _ldap._tcp.vzd.telematik.

- für den Zugriff auf die Schnittstelle I_Directory_Maintenance:

  ~~_vzd-kon._tcp.vzd.telematik.~~

  _vzd-bd._tcp.vzd.telematik.

- für den Zugriff auf die Schnittstelle I_Directory_Application_Maintenance:

  _vzd-fd._tcp.vzd.telematik.⌫

Änderungen in Kapitel 4.2

⌦ **TIP1-A_5572 VZD, I_Directory_Maintenance, TLS-gesicherte Verbindung**

Der VZD MUSS die Schnittstelle I_Directory_Maintenance durch Verwendung von TLS mit beidseitiger Authentisierung sichern.

Der VZD muss sich mit der Identität ID.ZD.TLS-S authentisieren.

Der VZD muss das vom FAD übergebene AUT-Zertifikat C.FD.TLS-C hinsichtlich OCSP-Gültigkeit und Übereinstimmung mit einem Zertifikat eines zur Nutzung dieser Schnittstelle registrierten Fachdienstes prüfen. Bei negativem Ergebnis wird der Verbindungsaufbau abgebrochen.

~~Es dürfen nur Basisdaten-Einträge geändert werden, für die der FAD eine Autorisierung hat.~~⌫

Kapitel 4.6 entfällt

~~4.6 Prozessschnittstelle P_Directory_Administration_Registration (Provided)~~

~~⌦ TIP1-A_5612 VZD, Mandatsregistrierung für FAD zur Administration von Basisdaten~~

Der Anbieter des VZD MUSS einen Prozess implementieren, der es FAD ermöglicht eine Autorisierung für die Änderung eines Basisdateneintrags zu hinterlegen. Die Autorisierung muss für jeden Basisdateneintrag vorhanden sein.

Der FAD muss sich zuvor beim VZD registrieren. Der Anbieter des VZD muss bei der Registrierung des FAD dessen Client-Zertifikat überprüfen:

- Gültigkeit des TLS-Client-Zertifikats des FADs C.FD.TLS-C (Prüfschritte wie in TUC_PKI_018 und mit admission gemäß vom GBV vorgegebener OID-Liste).

Die Autorisierung für die Änderung eines Basisdateneintrags muss für jeden Basisdateneintrag vorhanden sein. Die Autorisierung beinhaltet folgende Schritte:

- Der VZD MUSS den Autorisierungsprozess durch beidseitige Authentisierung (FAD und VZD) sichern. Der VZD muss sich mit der Identität ID.ZD.TLS-S authentisieren. Der VZD muss das vom FAD übergebene Zertifikat C.FD.TLS-C hinsichtlich OCSP Gültigkeit und Übereinstimmung mit einem Zertifikat eines registrierten FAD prüfen.
- Der VZD fordert zur Autorisierung vom FAD an:
  - die Telematik-ID des Verzeichniseintrags, für den die Autorisierung erfolgen soll,
  - den Nachweis der Berechtigung zur Datenadminstration durch den Betroffenen (Inhaber des HBA oder der SMC-B)

Nach erfolgreicher Autorisierung können die Basisdaten im Verzeichniseintrag eines Teilnehmers über die Schnittstelle I_Directory_Maintenance erstellt, gepflegt und gelöscht werden.⌫

⌦ **TIP1-A_5613_VZD, Mandatsderegistrierung für FAD zur Administration von Basisdaten**

FAD KÖNNEN sich beim Verzeichnisdienst deregistrieren. Der Zugang über die Schnittstelle I_Directory_Maintenance ist danach für den betroffenen Verzeichniseintrag nicht mehr möglich.⌫

Änderungen in gemProdT_VZD

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

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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_5561	VZD, DNS-SD	gemSpec_VZD

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_5572	VZD, I_Directory_Maintenance, TLS-gesicherte Verbindung	gemSpec_VZD

Tabelle 4: Anforderungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~TIP1-A_5610~~	~~VZD, Einwilligung muss vorliegen~~	~~gemSpec_VZD~~
~~TIP1-A_5612~~	~~VZD, Mandatsregistrierung für FAD zur Administration von Basisdaten~~	~~gemSpec_VZD~~
~~TIP1-A_5613~~	~~VZD, Mandatsderegistrierung für FAD zur Administration von Basisdaten~~	~~gemSpec_VZD~~