Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Zugangsgateway des Versicherten ePA

Version:	1.6.4
Revision:	400833
Stand:	02.09.2021
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_Zugangsgateway_Vers

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
			initiale Erstellung	gematik
1.0.0	18.12.18		freigegeben	gematik
1.1.0	15.05.19		freigegeben	gematik
1.2.0	28.06.19		Einarbeitung P19.1, Begriffsanpassungen	gematik
1.3.0	02.10.19		Einarbeitung P20.1/2	gematik
1.4.0	02.03.20	6.2.2.2, 6.2.2.3	Aktualisierung (I_Proxy_Directory_Query Nutzung) entsprechend neuem VZD-Datenmodell	gematik
1.4.1 CC	26.05.20		Einarbeitung P21.3	gematik
1.5.0	30.06.20		Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0	gematik
1.6.0	12.11.20		Anpassungen gemäß Änderungsliste P22.2 und Scope-Themen aus Systemdesign R4.0.1	gematik
1.6.1	19.02.21		Anpassungen gemäß Änderungsliste P22.5	gematik
1.6.2	02.06.21	4.2	Einarbeitung Änderungsliste ePA_Maintenance_21.1	gematik
1.6.3	09.07.21	5	Einarbeitung Änderungsliste ePA_Maintenance_21.2	gematik
1.6.4	02.09.21	4.8	Einarbeitung Konn_Maintenance_21.5	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb des Zugangsgateways für Versicherte als Bestandteil des ePA-Aktensystems.

Dieses Dokument beschreibt die Komponente zur sicheren Anbindung von Client-Systemen in der Personal Zone mit den Versichertengeräten und deren beabsichtigtem Zugriff auf das ePA-Aktensystem. Das Zugangsgateway für Versicherte ist einerseits verantwortlich für die Authentifizierung des Versicherten und dessen Vertreter und andererseits für die Kommunikation mit dem Autorisierungsdienst und der Dokumentenverwaltung des ePA-Aktensystems sowie dem Schlüsselgenerierungsdienst ePA und dem Verzeichnisdienst. Aus den Kommunikationsbeziehungen der Client-Systeme mit dem ePA-Aktensystem resultieren vom Zugangsgateway für Versicherte anzubietende Schnittstellen. Dies wird in diesem Dokument sowie den fachanwendungsspezifischen Spezifikationen normativ geregelt.

1.2 Zielgruppe

Dieses Dokument richtet sich an Anbieter eines ePA-Aktensystems und Hersteller von Produkttypen, die hierzu eine Schnittstelle besitzen.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief) festgelegt und bekannt gegeben.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzungen

Spezifiziert werden in dem Dokument die von dem Produkttyp bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Kapitel 7.5).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten. Diese sind in dem Produkttypsteckbrief des Produkttyps ePA-Aktensystem verzeichnet.

1.5 Methodik

1.5.1 Anforderungen

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.

Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen.“ die Phrase „DARF NICHT“ semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird in diesem Dokument stattdessen „Eine leere Liste DARF KEIN Element besitzen.“ verwendet. Die Schlüsselworte werden außerdem um Pronomen in Großbuchstaben ergänzt, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

Anforderungen werden im Dokument wie folgt dargestellt:
<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und Textmarke [<=] angeführten Inhalte.

2 Systemüberblick

Das Zugangsgateway für Versicherte ermöglicht den Versicherten bzw. deren berechtigten Vertretern den Zugang zum zugehörigen Aktensystem über das Internet. Auf der einen Seite dient es der Abschottung des ePA-Aktensystems in Richtung Internet, auf der anderen Seite regelt es den kontrollierten Zugriff der Versicherten auf das Aktensystem mit seinen funktionalen Komponenten.

In der Abbildung 1 wird auf logischer Ebene die Einbindung des Zugangsgateways für Versicherte in das ePA-Aktensystem dargestellt. Zu sehen sind als integraler Bestandteil des Zugangsgateways für Versicherte eine für die Authentifizierung von Versicherten benötigte Komponente, ein LDAP-Proxy für Abfragen im zentralen Verzeichnisdienst der Telematikinfrastruktur (TI), ein Paketfilter zur Absicherung in Richtung Internet und mehrere Proxies, welche den Zugriff auf den Autorisierungsdienst, die Schlüsselgenerierungsdienste (SGD 1 und SGD 2) und die Dokumentenverwaltung ermöglichen.

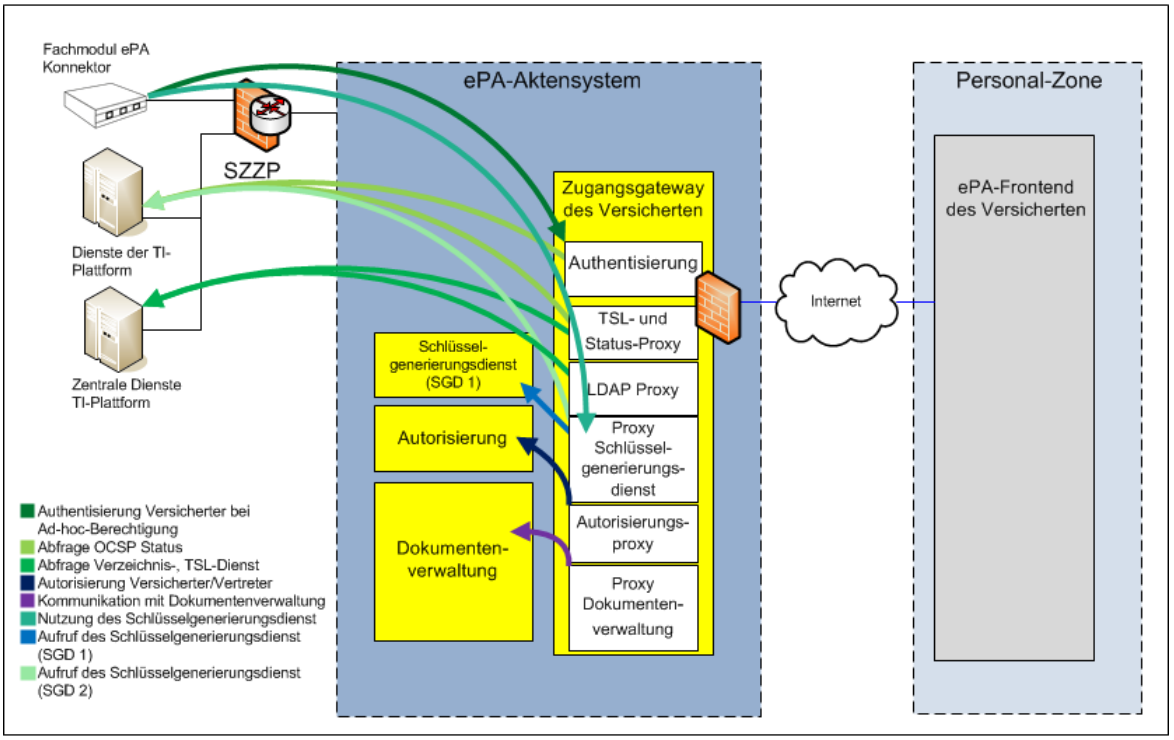

Abbildung 1: Zugangsgateway für Versicherte im ePA-Aktensystem

Diese Spezifikation beschreibt die Anforderungen und gibt Umsetzungshinweise zum Zugangsgateway des Versicherten ePA und den in der Komponente enthaltenen Proxies. Die Komponente Authentisierung des Versicherten ePA ist in [gemSpec_Authentisierung_Vers] beschrieben.

3 Systemkontext

Der folgende Abschnitt setzt die Komponente Zugangsgateway des Versicherten in den Systemkontext der Fachanwendung ePA.

3.1 Akteure und Rollen

Die Komponente Zugangsgateway des Versicherten wird als Provider von technischen Schnittstellen von weiteren technischen Komponenten und Produkttypen der Fachanwendung ePA aufgerufen.

Die Nutzer der Komponente sind gesetzlich Versicherte und deren Vertreter, welche mithilfe ihrer eGK über das ePA-Modul Frontend des Versicherten (ePA-Modul FdV) Zugang und Zugriff auf das ePA-Aktensystem erhalten.

Autorisierte Nutzer sind weiterhin berechtigt, zum Zweck der Berechtigungserteilung Abfragen an den Verzeichnisdienst über den im Zugangsgateway des Versicherten enthaltenen LDAP-Proxy durchzuführen.

Mit der Komponente Zugangsgateway des Versicherten, als Bestandteil des ePA-Aktensystems, interagiert der Anbieter des ePA-Aktensystems in seiner Rolle als Administrator zur Systempflege und Konfiguration.

3.2 Nachbarsysteme

Der folgende Abschnitt beschreibt die Positionierung der Komponente Zugangsgateway des Versicherten im Kontext der Fachanwendung ePA und stellt die Schnittstellen der Komponente schematisch dar.

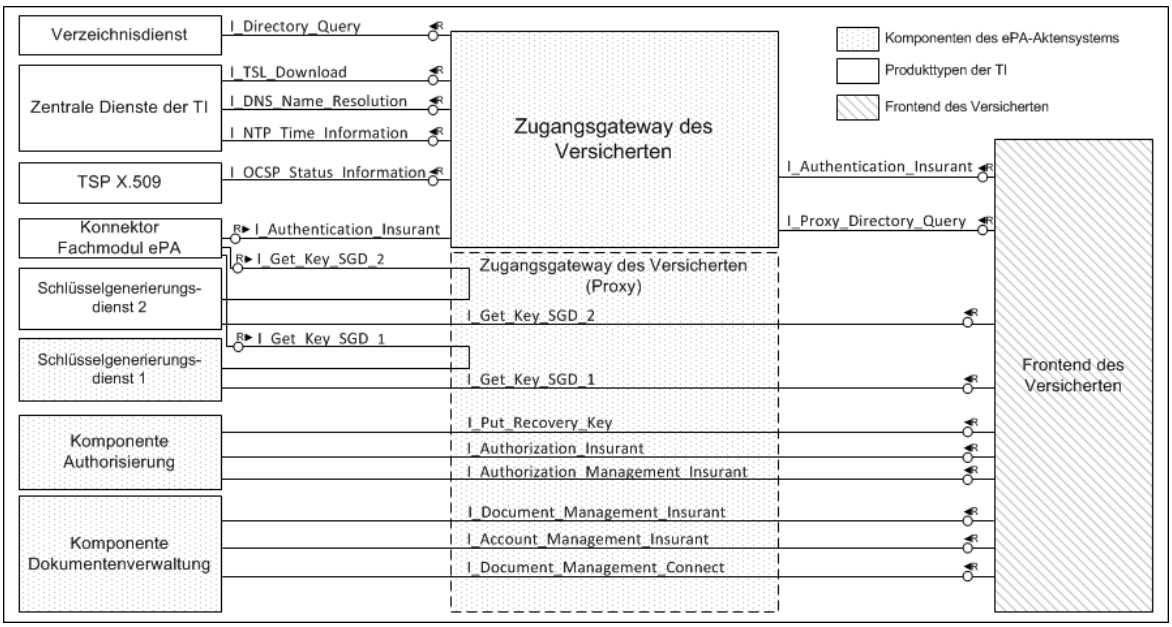

Abbildung 2: Nachbarsysteme des Zugangsgateways für Versicherte im ePA-Aktensystem

Die in Abbildung 2 dargestellten Nachbarsysteme des Zugangsgateway des Versicherten ePA sind:

- Fachmodul ePA im Konnektor [gemSpec_FM_ePA]
- ePA-Modul Frontend des Versicherten (ePA-Modul FdV) des Versicherten [gemSpec_ePA_FdV]
- Komponente Dokumentenverwaltung [gemSpec_Dokumentenverwaltung]
- Komponente Autorisierung ePA [gemSpec_Autorisierung]
- Schlüsselgenerierungsdienst SGD 1 [gemSpec_SGD_ePA] (Schlüsselgenerierungsdienst eines Fachanwendungsspezifischen Dienstes),
- Schlüsselgenerierungsdienst SGD 2 [gemSpec_SGD_ePA] (Schlüsselgenerierungsdienst der zentralen TI-Plattform),
- Verzeichnisdienst [gemSpec_VZD]
- Trust Service Provider X.509 [gemSpec_X_509_TSP]
- Netzwerknahe Dienste der TI: Namensdienst, Zeitdienst [gemSpec_Net], TSL-Dienst [gemSpec_TSL]

Wie in Abbildung 2 dargestellt, bietet die Komponente Schnittstellen für Aufrufe vom ePA-Modul Frontend des Versicherten (ePA-Modul FdV) und vom Fachmodul ePA an. Weiterhin werden Aufrufe des ePA-Modul Frontend des Versicherten (ePA-Modul FdV) durch Nutzung von Proxies an Komponenten des Aktensystems ePA als auch weitere Produkte der TI geleitet. Die Komponente selbst nutzt Schnittstellen verschiedener Produkte der TI.

Die Nutzung von Schnittstellen der beschriebenen Nachbarsysteme der Komponente als auch die Bereitstellung von Schnittstellen erfolgt in den Betriebsumgebungen der TI (RU/TU, PU).

A_14249 - Komponente Zugangsgateway des Versicherten - Separierung der Schnittstellen für verschiedene Umgebungen
Die Komponente Zugangsgateway des Versicherten MUSS die Bereitstellung von Schnittstellen für die Nutzung durch benachbarte Komponenten und Produkttypen aus verschiedenen Umgebungen der TI (RU/TU, PU) sicherstellen und voneinander separieren.**[**<=**]**

4 Zerlegung des Zugangsgateways des Versicherten ePA

Die folgende Abbildung stellt die einzelnen Komponenten des Zugangsgateways des Versicherten dar.

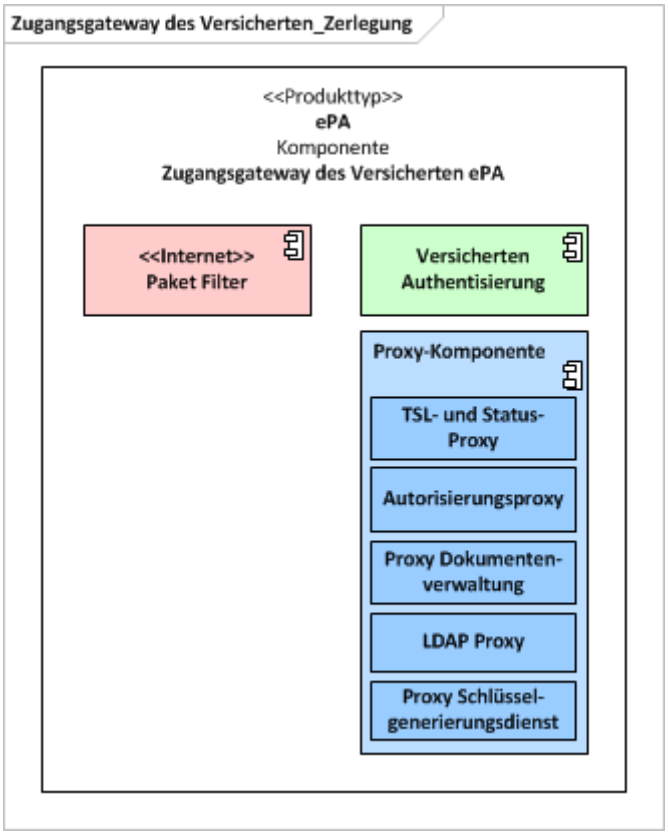

Abbildung 3: Komponenten des Zugangsgateway des Versicherten

Die grün dargestellte Komponente dient der Authentisierung von Versicherten. Die blau dargestellten Komponenten dienen der Kontrolle der Kommunikation mit dem Autorisierungsdienst, der Dokumentenverwaltung, den Schlüsselgenerierungsdiensten (jeweils SGD 1 und SGD 2), den TSP X.509 und dem Verzeichnisdienst. Die rosa dargestellte Komponente hat Schnittstellen in Richtung Internet.

4.1 Paketfilter

4.1.1 Funktion

Der Paketfilter stellt die Anbindung des ePA-Aktensystems an das Internet her und gewährleistet die Abschottung des ePA-Aktensystems in Richtung Internet.

A_14017 - Zugangsgateway des Versicherten, Sicherung zum Transportnetz Internet durch Paketfilter
Das ePA-Aktensystem MUSS zum Transportnetz Internet durch einen Paketfilter (ACL) gesichert werden, welcher ausschließlich die erforderlichen Protokolle weiterleitet. Der

Paketfilter der Komponente Zugangsgateway des Versicherten MUSS frei konfigurierbar sein auf der Grundlage von Informationen aus OSI-Layer 3 und 4, das heißt Quell- und Zieladresse, IP-Protokoll sowie Quell- und Zielport.**[<=]**

A_14018 - Zugangsgateway des Versicherten, Platzierung des Paketfilters Internet
Der Paketfilter der Komponente Zugangsgateway des Versicherten, zum Schutz in Richtung Transportnetz Internet, DARF NICHT auf den anderen, zum Zugangsdienst für Versicherte gehörenden, physischen Komponenten implementiert werden.**[<=]**

A_14019-01 - Zugangsgateway des Versicherten, Richtlinien für den Paketfilter zum Internet
Der Paketfilter der Komponente Zugangsgateway des Versicherten MUSS die Weiterleitung von IP-Paketen an der Schnittstelle zum Internet auf die nachfolgenden Protokolle beschränken:

1. HTTPS, und
2. OCSP-Zugriffe für das OCSP-Stapling nach A_15888 (vgl. Hinweis nach A_14019-01), ggf. notwendige DNS Anfragen (und Antworten)

Ein Verbindungsaufbau aus dem ePA-Aktensystem über das Zugangsgateway in Richtung Internet MUSS unterbunden werden, mit Ausnahme der Verbindungen aus Punkt 2 .**[<=]**

Hinweis zu A_14019-01:

Der Aktensystem-Anbieter muss für seine HTTPS-Schnittstelle ein TLS-Zertifikat von einem durch das CAB-Forum zulässigen TSP erwerben (dessen CA-Zertifikate also über einen aktuellen Webbrowser prüfbar ist, vgl. A_14776). Für dieses TLS-Zertifikat fragt das Zugangsgateway des Versicherten (die HTTPS-Schnittstelle ist Teil davon) regelmäßig für das OCSP-Stapling nach A_15888 den OCSP-Responder des TSP nach dem Sperrstatus des TLS-Zertifikats. Als Antwort erhält das Zugangsgateway des Versicherten eine OCSP-Response. Diese wird nach A_19126 geprüft und anschließend von der HTTPS-Schnittstelle verwendet (vgl. https://tools.ietf.org/html/rfc6066#section-8 und bspw. http://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_stapling).

Um dies zu ermöglichen, muss der Paketfilter entsprechende stateful-Firewall-Regeln gemäß A_14019-01 und A_19126 definieren.

A_19126 - Zugangsgateway des Versicherten, OCSP-Status für das OCSP-Stapling
Der Paketfilter der Komponente Zugangsgateway des Versicherten MUSS bezüglich des OCSP-Stapling gemäß A_15888 folgende Vorgaben umsetzen:

1. Für das vom Aktensystem-Anbieter erworbene TLS-Zertifikat (vgl. Hinweis zu A_14019-01) MUSS die Komponente initial die IP-Adresse (ggf. die IP-Adressen) des entsprechenden OCSP-Responsers ermitteln.
2. Diese IP-Adresse(n) MÜSSEN gemäß A_14019-01 per stateful-Firewalling Verbindungen von der HTTPS-Schnittstelle an den OCSP-Responder erlaubt werden (Whitelisting).
3. Gemäß OCSP-Stapling (https://tools.ietf.org/html/rfc6066#section-8) MUSS die Komponente regelmäßig eine OCSP-Response vom entsprechenden OCSP-Responder beziehen (Die Regelmäßigkeit wird vom zertifikatsausgebenden TSP und der Gültigkeitsdauer dessen OCSP-Responses bestimmt).
4. Die OCSP-Responses MÜSSEN von der Komponente geprüft werden (Signaturprüfung, CertID in der OCSP-Response passt zum angefragten

Zertifikat). Falls eine der Prüfung ein nicht-positives Ergebnis liefert so MUSS die erhaltene OCSP-Response verworfen werden.

5. Sollte die letzte in der Komponente vorhandene OCSP-Response zeitlich nicht mehr gültig sein (bspw. der OCSP-Responder im Internet war länger nicht erreichbar), so MUSS diese OCSP-Response verworfen werden und ein von einem Klienten (ePA FdV) initiierter TLS-Verbindungsaufbau der HTTPS-Schnittstelle ohne OCSP-Stapling durchgeführt werden.

[<=**]**

A_14776 - Zugangsgateway des Versicherten, Richtlinien zum TLS-Verbindungsaufbau
Die Komponente Zugangsgateway des Versicherten MUSS sich beim TLS-Verbindungsaufbau gegenüber dem Client mit einem Extended Validation TLS-Zertifikat eines Herausgebers gemäß [CAB Forum] authentisieren. Das Zertifikat MUSS an die Schnittstelle der Proxy-Komponente gebunden werden.**[**<=**]**

4.1.2 Redundanz

Die Anforderungen zur Verfügbarkeit ergeben sich aus [gemSpec_Perf#4.2]. Die Verfügbarkeit wird hergestellt durch Anzahl, Verteilung und Konfiguration der Zugangsgateways für Versicherte.

Die Auswahl der Zugangsgateways für Versicherte wird durch das ePA-Modul Frontend des Versicherten (ePA-Modul FdV) aus einer durch DNS übermittelten Liste vorgenommen. Auf die Auswahl des Zugangsdienstes für Versicherte kann der Anbieter des ePA-Aktensystems durch die Konfiguration und Anpassung der DNS-Einträge Einfluss nehmen. Die Verfügbarkeit ist hergestellt, wenn jeder Versicherte mit existierendem Konto beim Anbieter des ePA-Aktensystems oder dessen berechtigter Vertreter die Möglichkeit zum Verbindungsaufbau hat.

Eine hardwaretechnische Hochverfügbarkeit der einzelnen Zugangsgateways für Versicherte ist über grundlegende Maßnahmen, wie redundante Netzteile hinaus nicht erforderlich. Es steht dem Anbieter jedoch frei, zur Sicherstellung der Verfügbarkeitsanforderungen technische Lösungen, wie z.B. Load-Balancer und Stateful Failover innerhalb von Clustern einzusetzen, so dass jedes einzelne Zugangsgateway für Versicherte im Ergebnis eine höhere Verfügbarkeit oder Leistungsfähigkeit besitzt.

A_14026 - Zugangsgateway des Versicherten, Redundanz der Paketfilter im Zugangsdienst für Versicherte
Die Komponente Zugangsgateway des Versicherten MUSS sicherstellen, dass bei Ausfall eines von mehreren Paketfiltern die verbleibenden Paketfilter in dem-selben Standort den Datenverkehr aller Mandanten des ausgefallenen Paketfilters zusätzlich übernehmen können.**[**<=**]**

4.1.3 Konfiguration

A_14030 - Zugangsgateway des Versicherten, Verhalten des Zugangsdienstes für Versicherte bei Vollauslastung
Die Komponente Zugangsgateway des Versicherten MUSS den Paketfilter Internet so konfigurieren, dass bei Vollauslastung der Systemressourcen im ePA-Aktensystem keine weiteren Verbindungen angenommen werden.**[**<=**]**

Durch die Zurückweisung von Verbindungen wird sichergestellt, dass das ePA-Modul Frontend des Versicherten (ePA-Modul FdV) einen Verbindungsaufbau mit einem anderen Zugangsgateway für Versicherte des jeweiligen ePA-Aktensystems versucht, bei dem die erforderlichen Ressourcen zur Verfügung stehen.

4.1.4 Adressierung

4.1.4.1 Zugangsgateway für Versicherte zum Transportnetz Internet

A_14031 - Zugangsgateway des Versicherten, IPv4-Adressierung der Internetschnittstellen des Zugangsdienstes für Versicherte
Der Anbieter des ePA-Aktensystems MUSS jedem Zugangsgateway für Versicherte genau eine öffentliche IPv4-Adresse zuweisen. Diese Adresse MUSS auf der physischen Schnittstelle zum Internet konfiguriert werden. Die öffentlichen IP-Adressen des Zugangsgateways für Versicherte MÜSSEN vom Anbieter des ePA-Aktensystems zur Verfügung gestellt werden.**[<=]**

A_14032 - Zugangsgateway des Versicherten, IPv6-Adressierung der Internetschnittstellen des Zugangsdienstes für Versicherte
Der Anbieter des ePA-Aktensystems SOLL jedem Zugangsgateway für Versicherte eine IPv6-Adresse zuweisen. Diese Adresse MUSS auf der physischen Schnittstelle zum Internet konfiguriert werden. Die öffentliche IPv6-Adresse MUSS vom Anbieter des Zugangsgateways des Versicherten zur Verfügung gestellt werden.**[<=]**

4.1.4.2 ePA-Aktensystem zum Zentralen Netz

Die Adressen des ePA-Aktensystems am Übergang zur TI werden vom Anbieter des Zentralen Netzes aus dem Adressblock TI_Zentral zugewiesen.

4.2 Einbettung Authentisierung Versicherter

Die "Authentisierung des Versicherten ePA" dient der Bestätigung der Authentifizierung von Versicherten und deren berechtigten Vertretern. Die Teilkomponente ist in [gemSpec_Authentisierung_Vers] beschrieben.

Die Authentisierung Versicherter generiert bei erfolgreicher Authentifizierung eines Versicherten ein Token, wie in [gemSysL_Fachanwendung_ePA] und [gemSpec_Authentisierung_Vers] beschrieben.

Von dem Zugangsgateway des Versicherten wird bei Verbindungsaufbau durch ein ePA-Modul Frontend des Versicherten (ePA-Modul FdV) eine serverseitige Session erstellt. Die Session dient sowohl der Umsetzung von Anforderungen zum Beenden nach Inaktivität als auch der Kontrolle, dass ausschließlich authentifizierte ePA-Modul Frontend des Versicherten (ePA-Modul FdV) Zugriff auf die Komponente kryptographische Autorisierung und ausschließlich autorisierte ePA-Modul Frontend des Versicherten (ePA-Modul FdV) Zugriff auf die Dokumentenverwaltung, VAU und den LDAP-Proxy erhalten.

Bei erfolgreicher Authentisierung wird die für das ePA-Modul Frontend des Versicherten (ePA-Modul FdV) verwaltete Session vom Zugangsgateway des Versicherten mit dem Status "Authentisiert" markiert.

A_15197 - Zugangsgateway des Versicherten, Verwalten einer serverseitigen Session für Verbindungen vom ePA-Modul Frontend des Versicherten (ePA-Modul FdV)
Die Komponente Zugangsgateway des Versicherten MUSS bei einem Aufruf der Versicherten Authentisierung durch ein ePA-Modul Frontend des Versicherten (ePA-Modul FdV) eine serverseitige Session anlegen.**[**<=**]**

A_15198-02 - Zugangsgateway des Versicherten, Eine serverseitige Session für jede TLS Session vom ePA-Modul Frontend des Versicherten (ePA-Modul FdV)
Das ePA-Modul Frontend des Versicherten MUSS für jede Aktensession - außer für die Kommunikation mit dem Schlüsselgenerierungsdienst - genau eine TLS-Session nutzen.**[**<=**]**

Die für das ePA-Modul Frontend des Versicherten (ePA-Modul FdV) verwaltete Session dient im Weiteren der Aufgabe die Zugangskontrolle bei Zugriff auf die Komponenten Autorisierung, LDAP-Proxy und Dokumentenverwaltung zu ermöglichen.

Die serverseitig authentifizierte TLS gesicherte Verbindung vom ePA-Modul Frontend des Versicherten (ePA-Modul FdV) terminiert am Zugangsgateway des Versicherten. Hier kommen Anwendungsproxies zum Einsatz, welche der Zugangskontrolle auf weitere Komponenten der Fachanwendung ePA dienen.

Somit wird sichergestellt, dass ausschließlich authentisierte ePA-Modul Frontend der Versicherten (ePA-Modul FdV) auf die Komponenten Autorisierung und ausschließlich autorisierte ePA-Modul Frontend des Versicherten (ePA-Modul FdV) auf die Komponenten LDAP-Proxy, Dokumentenverwaltung und die VAU zugreifen können.

Bei negativen Ergebnissen, bei Fehlerfällen der Kommunikation mit Komponenten des ePA-Aktensystems oder nach Inaktivität des ePA-Modul Frontend des Versicherten (ePA-Modul FdV) wird die TLS-Session zum ePA-Modul Frontend des Versicherten (ePA-Modul FdV) abgebaut und die serverseitige Session entfernt.

A_14356 - Zugangsgateway des Versicherten, Prüfung Token Übergabe
Die Komponente Zugangsgateway des Versicherten MUSS die erfolgreiche Authentifizierung und Autorisierung anhand erfolgreicher Übergabe der Authentisierungs- und Autorisierungs-Token an das ePA-Modul Frontend des Versicherten (ePA-Modul FdV) prüfen. Es MUSS hierbei die erfolgreiche Ausgabe der Token ausgewertet werden. Das jeweilige Token selbst MUSS nicht geprüft werden.
[<=**]**

A_14359 - Zugangsgateway des Versicherten, Sessionverhalten
Die Komponente Zugangsgateway des Versicherten MUSS sicherstellen, dass der Autorisierungsdienst erst nach erfolgreicher Authentisierung und die Dokumentenverwaltung sowie der LDAP-Proxy erst nach erfolgreicher Autorisierung für die aufgebaute Session des Versicherten erreichbar sind.**[**<=**]**

4.3 Autorisierungsproxy

Der Autorisierungsproxy dient der Überprüfung, ob Aufrufe der Schnittstellen, welche in [gemSpec_Autorisierung] beschrieben sind, ausschließlich von authentisierten ePA-Modul Frontend des Versicherten (ePA-Modul FdV) getätigt werden.

Die von den Proxies auszuwertenden Aufrufparameter (FQDN und Pfadinformationen) sind in [gemSpec_Aktensystem] Kapitel 5.1 beschrieben. Beispielsweise wird die Komponente Autorisierung Versicherter durch einen Aufruf mit FQDN des Aktensystems im Internet (ePA_FQDN) und dem in [gemSpec_Aktensystem] Kapitel 5.1, Tabelle 2

angegebenen Pfad für "authz" aufgerufen. Verbindungsinformationen von Produkten der TI und weiterer Komponenten des ePA Aktensystems können per DNS Service Discovery abgerufen werden (siehe u.a. [gemSpec_Aktensystem] Kapitel 5.1, Tabelle 1).

Nach erfolgreicher Authentisierung ist die für das ePA-Modul Frontend des Versicherten (ePA-Modul FdV) verwaltete Session mit dem Status "Authentisiert" markiert. Nur unter dieser Voraussetzung darf der Autorisierungsproxy Aufrufe an den Autorisierungsdienst weiterleiten. Ist die Voraussetzung nicht erfüllt, muss die Verbindung zum ePA-Modul Frontend des Versicherten (ePA-Modul FdV) abgebaut werden.

Bei erfolgreicher Autorisierung wird die für das ePA-Modul Frontend des Versicherten (ePA-Modul FdV) verwaltete Session mit dem Status "Autorisiert" markiert. Dabei ist zu beachten, dass die Änderung des Status der Session nur bei erfolgreichem Aufruf der Operation "getAuthorizationKey" der Schnittstelle "I_Authorization_Insurant" am Autorisierungdienst erfolgen darf. Ein Aufruf anderer Operationen und Schnittstellen führt nicht zur Änderung des Status der Session.

Referenziert wird an dieser Stelle die bereits im Kapitel 4.2 "Authentisierung Versicherter" existierende Anforderung "A_14356 - Prüfung Token Übergabe".

A_14300 - Zugangsgateway des Versicherten, Zugriff auf Autorisierungsdienst
Der Autorisierungsproxy der Komponente Zugangsgateway des Versicherten MUSS sicherstellen, dass ausschließlich authentisierte ePA-Modul Frontend des Versicherten (ePA-Modul FdV) Zugriff auf den Autorisierungsdienst erhalten.
[<=]

4.4 Proxy Dokumentenverwaltung

Der Proxy Dokumentenverwaltung stellt sicher, dass die in [gemSpec_Dokumentenverwaltung] beschriebenen Schnittstellen ausschließlich von autorisierten ePA-Modul Frontend des Versicherten (ePA-Modul FdV) aufgerufen werden können.

Bei bestehender Session zum ePA-Modul Frontend des Versicherten (ePA-Modul FdV), wird von der Komponente bei jedem Aufruf von Operationen der in [gemSpec_Dokumentenverwaltung] beschriebenen Schnittstellen geprüft, ob die für das ePA-Modul Frontend des Versicherten (ePA-Modul FdV) verwaltete Session mit dem Status "Autorisiert" markiert ist. Ist dies nicht der Fall, muss der Aufruf unterbunden werden.

A_14301 - Zugangsgateway des Versicherten, Zugriff auf Dokumentenverwaltung
Der Proxy Dokumentenverwaltung der Komponente Zugangsgateway des Versicherten MUSS sicherstellen, dass ausschließlich autorisierte ePA-Modul Frontend des Versicherten (ePA-Modul FdV) Zugriff auf die Dokumentenverwaltung erhalten.
[<=]

Aufrufe des ePA-Modul Frontend des Versicherten (ePA-Modul FdV) werden an die Dokumentenverwaltung weitergeleitet. Diese Aufrufe richten sich an einen Kontext der Versicherten (VAU). Um der Dokumentenverwaltung zu ermöglichen, den korrekten Kontext des Versicherten (VAU) zu identifizieren, wird den Aufrufen vom Zugangsgateways der Versicherten eine über alle Zugangsgateways der Versicherten eines Anbieters eindeutige SessionID hinzugefügt.

A_14040 - Zugangsgateway des Versicherten, Weiterleitung eines Session-Tokens an die ePA-Dokumentenverwaltung
Die Komponente Zugangsgateway des Versicherten MUSS bei der Weiterleitung eines Requests vom ePA-Modul Frontend des Versicherten (ePA-Modul FdV) an die ePA-Dokumentenverwaltung das „request-header field:session" auf einen Wert setzen, der die vom Zugangsgateway geführte TLS-Session für die Dokumentenverwaltung eindeutig zuordenbar macht.
[<=]

4.5 LDAP-Proxy

Das Zugangsgateway für Versicherte ermöglicht ausschließlich einem autorisierten ePA-Modul Frontend des Versicherten (ePA-Modul FdV) durch Nutzung des LDAP-Proxies, Daten aus dem Verzeichnisdienst der TI-Plattform (VZD) abzufragen. Die Kommunikation vom LDAP-Proxy zum VZD erfolgt über das LDAPv3-Protokoll. Der LDAP-Proxy darf ausschließlich lesend auf den VZD zugreifen.

Die Abfragen vom ePA-Modul Frontend des Versicherten (ePA-Modul FdV) zum VZD, über den LDAP-Proxy, werden gemäß Directory Services Markup Language (DSML) [DSML2.0] Syntax verschickt. Der LDAP-Proxy stellt die dafür vorgesehene Schnittstelle in Richtung ePA-Modul Frontend des Versicherten (ePA-Modul FdV) zur Verfügung und führt die für den eigentlichen Zugriff auf den VZD notwendige Protokollwandlung in das LDAPv3-Protokoll durch.

Die Anzahl der pro Anfrage zurückgegebenen Einträge des Verzeichnisdienstes wird durch den Verzeichnisdienst [gemSpec_VZD#TIP1-A_5552] limitiert.

A_14470 - Zugangsgateway des Versicherten, Lokalisierung des Verzeichnisdienstes der TI-Plattform (VZD)
Der LDAP-Proxy der Komponente Zugangsgateway des Versicherten MUSS den FQDN und den Port des VZD durch eine DNS-SD-Namensauflösung gemäß [RFC6763] mit dem Bezeichner "_ldap._tcp.vzd.<DNS_TOP_LEVEL_DOMAIN_TI>." ermitteln.**[<=]**

A_14514-01 - Zugangsgateway des Versicherten, Verbindungsaufbau zum Verzeichnisdienstes der TI-Plattform (VZD)
Der LDAP-Proxy der Komponente Zugangsgateway des Versicherten MUSS eine LDAPS-Verbindung zum VZD aufbauen. Dabei wird das Serverzertifikat des Verzeichnisdienst C.ZD.TLS-S nach TUC_PKI_018 geprüft.
Parameter:

- PolicyList: oid_zd_tls_s (gemäß gemSpec_OID),
- intendedKeyUsage: digitalSignature,
- intendedExtendedKeyUsage: serverAuth,
- OCSP-Graceperiod: 60 Minuten
- Offlinemodus: nein,
- Prüfmodus: OCSP

Die vom TUC_PKI_018 zurückgegebene Rollen-OID MUSS auf den Wert „oid_vzd_ti" geprüft werden.
[<=]

4.6 TSL- und Status-Proxy

Das Zugangsgateway des Versicherten muss das ePA-Modul Frontend des Versicherten (ePA-Modul FdV) bei den Aufgaben unterstützen, regelmäßig die TSL-Aktualisierung vorzunehmen (A_15874) und Sperrinformationen für Zertifikate zu ermitteln (A_15873). Die OCSP-Responder und der TSL-Dienst haben deutlich höhere SLAs in Bezug auf die Verfügbarkeit innerhalb der TI. Manche OCSP-Responder besitzen keine direkte Anbindung an das Internet (Komponenten-PKI, Kontext: Prüfung Identität vertrauenswürdige Ausführungsumgebung). Es wird damit auch möglich, bessere Aussagen über die Verfügbarkeit von ePA-Anwendungsfällen zu treffen, weil weniger nicht-SLA-belegte Datenverbindungen für die Anwendungsfälle notwendig sind (Wenn eine funktionierende Datenverbindung zwischen ePA-Modul Frontend des Versicherten (ePA-Modul FdV) und Zugangsgateway des Versicherten besteht, dann kann eine in [gemSpec_Perf] definierte Verfügbarkeit garantiert werden). Aufgrund der Verwendung der Proxy-Funktionalität über die schon etablierte TLS-Verbindung sind OCSP-Requests des ePA-FdV nicht im Klartext im Internet sichtbar.

A_15868 - Zugangsgateway des Versicherten, Bereitstellung TSL
Ein Zugangsgateway des Versicherten MUSS folgende Vorgaben umsetzen:

1. Es MUSS mindestens einmal täglich aus der TI (TI-interne Verbindung) die "TSL(ECC-RSA)" und deren zugehörigen Hashwert aus der TI herunterladen.
2. Es MUSS unter dem Pfadnamen "/TSL.xml" über sein vom ePA-Modul Frontend des Versicherten (ePA-Modul FdV) schon genutztes HTTPS-Interface die "TSL(ECC-RSA)" der TI zur Verfügung stellen (HTTP-GET, HTTP Content-Type: text/xml).
3. Es MUSS unter dem Pfadnamen "/TSL.sha2" über sein vom ePA-Modul Frontend des Versicherten (ePA-Modul FdV) schon genutztes HTTPS-Interface den vom TSL-Dienst heruntergeladenen SHA-256 Hashwert der Datei TSL.xml aus Spiegelstrich 2 zur Verfügung stellen (HTTP Content-Type: text/plain, Hashwert als hexdump kodiert (64 Byte + Newline))

[<=]

Hinweise:

1. "TI-interne Verbindung" hat nur den Hintergrund, dass dort über SLAs eine ausreichende Verfügbarkeit gewährleistet ist.
2. Hashwert der TSL.xml bedeutet der Hashwert der Datei TSL.xml, so wie sie vom TSL-Dienst der TI bereitgestellt wird und als wenn man die Datei als Binärdatei interpretiert (vgl. [gemSpec_TSL]).

A_15869 - Zugangsgateway des Versicherten, Bereitstellung OCSP-Forwarder
Ein Zugangsgateway des Versicherten MUSS folgende Vorgaben umsetzen:

1. Es MUSS unter dem in [gemSpec_Aktensystem] Tabelle: Tab_ePA_FQDN angegeben Pfadnamen für den key "ocspf" einen Proxy zur Statusabfrage über sein vom ePA-Modul Frontend des Versicherten (ePA-Modul FdV) schon genutztes HTTPS-Interface zur Verfügung stellen (HTTP-POST, vgl. auch [RFC-6960, Appendix [gemSpec_PKI]).
2. Es MUSS über die Schnittstelle aus Spiegelstrich 1 OCSP-Requests [RFC-6960] entgegen nehmen.

3. Aus einem solchen OCSP-Request MUSS es aus dem issuerKeyHash [RFC-6960] die URL des entsprechenden OCSP-Responders in der TI ermitteln (Datengrundlage ist die TSL der TI) und den OCSP-Request an diese ermittelte URL weiterleiten.
4. Es MUSS die erhaltenen OCSP-Response an das die OCSP-Anfrage stellende ePA-Modul Frontend des Versicherten (ePA-Modul FdV) unverändert weiterreichen.

[<=]

Auf Anfrage stellt die gematik eine Beispielimplementierung für A_15869 Spiegelstrich 3 bereit.

A_15871 - Zugangsgateway des Versicherten, Caching OCSP-Antworten
Ein Zugangsgateway des Versicherten KANN OCSP-Antworten aus A_15869 bis zu 4 Stunden cachen und bei einer entsprechend passenden OCSP-Anfrage anstatt neu den OCSP-Responder anzufragen, die im Cache befindliche OCSP-Antwort ausliefern.**[<=]**

A_15888 - Zugangsgateway des Versicherten, OCSP-Stapling
Ein Zugangsgateway des Versicherten MUSS an der HTTPS-Schnittstelle zum Internet OCSP-Stapling [RFC-6066] unterstützen.**[<=]**

4.7 Proxy Schlüsselgenerierungsdienst

Zur Nutzung der in [gemSpec_SGD_ePA] beschrieben Schlüsselableitungsfunktionalität für den Schutz von Akten- und Kontextschlüssel einer ePA werden Aufrufe zu den Schlüsselgenerierungsdiensten SGD 1 und SGD 2 über den "Proxy Schlüsselgenerierungsdienst" ermöglicht.

Der Proxy SGD stellt sicher, dass ein ePA-FdV Aufrufe an den SGD 1 und SGD 2 durchführen kann.

Die Information, auf welche Anfragen (Pfade) des ePA-Modul Frontend des Versicherten (ePA-Modul FdV) der Proxy SGD aktiv wird ("/SGD1" für den SGD 1 und "/SGD2" für den SGD 2), sind in [gemSpec_SGD_ePA#2.2 Tabelle 2] angegeben.

Die FQDN und IP-Adresse des SGD wird vom Proxy SGD durch DNS Service Discovery in der TI bezogen. Hierzu wird der in [gemSpec_Aktensystem] Tabelle: Tab_ePA_Service Discovery angegebene PTR Record im Namensraum der TI abgerufen.

A_17495 - Zugangsgateway des Versicherten, Zugriff auf den Schlüsselgenerierungsdienst
Der Proxy Schlüsselgenerierungsdienst der Komponente Zugangsgateway des Versicherten MUSS sicherstellen, dass ePA-Modul Frontend des Versicherten (ePA-Modul FdV) auch ohne Authentisierung und Autorisierung Zugriff auf den SGD 1 und den SGD 2 erhalten.

[<=]

4.8 Tracing in Nichtproduktivumgebungen

Für die Fehlersuche - insbesondere bei IOP-Problemen zwischen Produkten verschiedener Hersteller in einer fortgeschrittenen Entwicklungsphase - hat es sich als notwendig erwiesen, dass ein Fehlersuchender den Klartext der Kommunikation zwischen ePA-Client

und VAU-Instanz mitlesen kann. Vgl. [gemSpec_Aktensystem#5.8. Tracing in Nichtproduktivumgebungen].

Das ZGdV stellt Informationen über die aktuell verfügbaren Sensorpunkte im AS bereit. Weiterhin exponiert das ZGdV die Daten der Sensorpunkte über TCP (i. s. v. nicht TLS-gesichert) bspw. über Port 8001,...,8009. Die dort von den Sensorpunkten ge-streamten Daten sind nur Testdaten, also keine Echtdaten, d. h. es sie haben keinen Schutzbedarf bez. Vertraulichkeit. Um die exponierten Sensordaten-Punkte vor DoS-Angriffen zu schützen, erlaubt das ZGdV im Fall der Fälle die TCP-Ports auf IP-Layer über Firewall-Regeln abzusichern.

A_21890 - Zugangsgateway des Versicherten, Sensorpunkt für Nichtproduktivumgebungen
Die Komponente Zugangsgateway des Versicherten (ZGdV) MUSS genau in Nichtproduktivumgebungen:

- die Daten der Sensorpunkte des Aktensystems auf TCP-Ports (bspw. ab Port 8000) öffentlich ohne TLS-Sicherung im Internet zur Verfügung stellen, indem die aktuell an den Sensorpunkten auflaufenden Daten auf dem TCP-Port am ZGdV öffentlich gestreamt werden.
- die Möglichkeit bieten, den Zugriff auf diese TCP-Ports durch Firewall-Einstellungen auf IP-Layer zu beschränken (Initial gibt es keine Beschränkungen).

Weiterhin MUSS das ZGdV über die URL /tracingpoints Informationen über die aktuell im AS verfügbaren und damit auch im ZGdV öffentlich exponierten Sensorpunkt-Daten als JSON-Array (=> Response-Type 'application/json) der folgenden Form bereitstellen:
[{ "name" : "direkt vor der VAU RZ1/B1", "port" : 8001 }, { "name" : "VAU RZ2/B1", "port" : 8002 }, ...]
Sollten keine Sensorpunkte aktuell im AS aktiviert sein (bspw. bei Lasttests) so ist das Array leer: [ ].
Die einzelnen Felder des Arrays sind associative array (oder auch maps oder dictionaries genannt). Diese KÖNNEN neben "name" und "port" beliebige vom AS definierbare, weitere key-value-Paare enthalten. Der Eintrag "port" gibt an, an welchem öffentlich erreichbaren TCP-Port des ZGdV die Sensordaten des entsprechenden Sensors abrufbar sind (gestreamt werden).**[<=]**

5 Übergreifende Festlegungen

A_14034 - Zugangsgateway des Versicherten, Übergang des ePA-Aktensystems zur TI
Die Komponente Zugangsgateway des Versicherten MUSS sicherstellen, dass der Zugriff auf Dienste der TI ausschließlich über einen Sicheren Zentralen Zugangspunkt (SZZP) erfolgt.**[**<=**]**

A_14036 - Zugangsgateway des Versicherten, Synchronisierung der Komponenten mit den Stratum-1-NTP-Servern der TI
Die Komponente Zugangsgateway des Versicherten MUSS alle Komponenten seines Zugangsdienstes für Versicherte mit denStratum-1-NTP-Servern der TI synchronisieren.**[**<=**]**

A_15518 - Zugangsgateway des Versicherten, Verhalten des Autorisierungsproxy, Proxy Dokumentenverwaltung, LDAP-Proxy
Die in der Komponente Zugangsgateway des Versicherten verwendeten Proxies MÜSSEN als transparente Proxies umgesetzt werden.**[**<=**]**

A_13879 - Zugangsgateway des Versicherten, Serverseitige Authentisierung
Die Komponente Zugangsgateway des Versicherten MUSS sich gegenüber dem ePA-Modul Frontend des Versicherten (ePA-Modul FdV) beim Aufbau der TLS-Session durch sein ExtendedValidation-Zertifikat authentisieren. Die Beschaffung des Zertifikats erfolgt durch den Anbieter über eine öffentliche CA.**[**<=**]**

A_14033 - Zugangsgateway des Versicherten, TLS Verschlüsselung
Die Komponente Zugangsgateway des Versicherten MUSS sicherstellen, dass jede Kommunikation mit dem ePA-Modul Frontend des Versicherten (ePA-Modul FdV) TLS verschlüsselt erfolgt.**[**<=**]**

Die Verwendung der SoapAction ermöglicht einer Reverse-Proxy-Komponente innerhalb des Zugangsgateways, die Nachrichten zu verarbeiten, ohne die http-Payload zu untersuchen.

A_14416 - Zugangsgateway des Versicherten, Verwendung der SoapAction
Bei einer fehlenden oder fehlerhaft gesetzten SoapAction MUSS die bestehende Session in Richtung des aufrufenden Systems durch das Zugangsgateway geschlossen werden.**[**<=**]**

A_14357 - Zugangsgateway des Versicherten, Abbau der Verbindung bei fehlgeschlagener Prüfung übergebener Token
Die Komponente Zugangsgateway des Versicherten MUSS bei negativem Ergebnis der Prüfung der Ausgabe eines Tokens durch eine der nachgelagerten Komponenten die für das ePA-Modul Frontend des Versicherten (ePA-Modul FdV) verwaltete Session und die Verbindung zum ePA-Modul Frontend des Versicherten (ePA-Modul FdV) nach Weiterleitung der eigentlichen Antwort des Token-Ausstellers an das ePA-Modul Frontend des Versicherten (ePA-Modul FdV) beenden.**[**<=**]**

A_14358 - Zugangsgateway des Versicherten, Verhalten bei Inaktivität
Die Komponente Zugangsgateway des Versicherten MUSS nach Inaktivität von 20 Minuten die Session zum ePA-Modul Frontend des Versicherten (ePA-Modul FdV) abbauen.**[**<=**]**

A_13876 - Zugangsgateway des Versicherten, Kein direkter Zugriff auf Dienste der zentralen TI-Plattform
Die Komponente Zugangsgateway des Versicherten MUSS einen direkten Zugriff aus dem Internet auf Dienste der zentralen TI-Plattform verhindern.**[<=]**

A_14016 - Zugangsgateway des Versicherten, Schutz vor Angriffen aus dem Internet
Die Komponente Zugangsgateway des Versicherten MUSS für alle vom Internet erreichbaren Schnittstellen Maßnahmen zum Schutz vor DoS-Angriffen auf Anwendungsebene treffen. Weitere Angriffe auf Anwendungsebene MÜSSEN mindestens durch Einsatz geeigneter IDS/IPS Lösungen verhindert werden.**[<=]**

A_15196 - Zugangsgateway des Versicherten, Schutz vor volumetrischen DoS-Angriffen
Die Komponente Zugangsgateway des Versicherten MUSS bei Beauftragung eines qualifizierten Dienstleisters zum Schutz vor volumetrischen DoS-Angriffen, Kriterien des BSI zur Auswahl qualifizierter Dienstleister umsetzen.**[<=]**

Als Maßnahme gegen volumetrische Denial-of-Service-Angriffe wird die Verwendung von DNS- oder BGP-Routing-Diensten empfohlen. Hinweise des BSI: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/Qualifizierte_Dienstleister/QDL_node.html

A_15599-02 - Zugangsgateway des Versicherten, Abbauen der Verbindung zum ePA-Modul Frontend des Versicherten (ePA-Modul FdV)
Die Komponente Zugangsgateway des Versicherten MUSS bei Fehlern in einer nachgelagerten Komponente die Verbindung zum ePA-Frontend des Versicherten (ePA-FdV) abbauen und die verwaltete Session löschen. Dies gilt für folgende Fehlerfälle:

Komponente	Fehler
Authentisierung	Alle spezifizierten wst:*-Fehler, ASSERTION_INVALID
Autorisierung	ASSERTION_INVALID, DEVICE_UNKNOWN, DEVICE_LOCKED
Dokumentenverwaltung	ASSERTION_INVALID, INVALID_AUT_KEY

[<=]

A_14028 - Zugangsgateway des Versicherten, Verbindungen bei Komponentenausfall beenden
Die Komponente Zugangsgateway des Versicherten MUSS sicherstellen, dass

- alle bestehenden Verbindungen zum Zugangsgateway für Versicherte beendet werden und
- keine neuen Verbindungen zugelassen werden,

wenn am jeweiligen Zugangsgateway-Standort eine an der Weiterleitung der Daten zum ePA-Aktensystem beteiligte Komponente ausfällt und dadurch die Nutzung des ePA-Aktensystems nicht mehr möglich ist.**[<=]**

6 Funktionsmerkmale

6.1 Versicherten Authentisierung

Die Schnittstellen der Versicherten Authentisierung sind in [gemSpec_Authentisierung_Vers] beschrieben.

6.2 Autorisierungsproxy, Proxy Dokumentenverwaltung, LDAP-Proxy

6.2.1 Schnittstelle I_Authorization_Insurant, I_Account_Management_Insurant, I_Authorization_Management_Insurant, I_Document_Management_Insurant, I_Document_Management_Connect

Aufrufe des ePA-Modul Frontend des Versicherten (ePA-Modul FdV) an die Komponenten Autorisierung, SGD 1 und Dokumentenverwaltung des Produkttyps ePA-Aktensystem sowie SGD 2 werden von der Komponente Zugangsgateway des Versicherten nicht verarbeitet, sondern nach Prüfung der Existenz und des Zustands (Authentisiert oder Autorisiert) der verwalteten Session an die Komponente Autorisierung bzw. die Dokumentenverwaltung weitergeleitet. Die fachliche Verarbeitung der Aufrufe wird in [gemSpec_Autorisierung_ePA] und in [gemSpec_Dokumentenverwaltung] beschrieben.

Rückgabeparameter von Funktionsaufrufen der Schnittstellen I_Authorization_Insurant, I_Account_Management_Insurant, I_Authorization_Management_Insurant an das ePA-Modul Frontend des Versicherten (ePA-Modul FdV), werden hinsichtlich der Existenz vom SOAP-Fehlercode ausgewertet.

6.2.2 Schnittstelle I_Proxy_Directory_Query

Die Schnittstelle I_Proxy_Directory_Query dient der Abfrage des Verzeichnisdienstes in der TI. Über diese Schnittstelle können Versicherte zum Zweck der Berechtigung von Leistungserbringern Einträge im Verzeichnisdienst suchen. Die Nutzung dieser Schnittstelle steht nur autorisierten Versicherten zur Verfügung. Die Autorisierung erfolgt über die korrespondierenden Funktionalitäten des Autorisierungsdienstes. Der DSML "authRequest" wird nicht genutzt.

6.2.2.1 Schnittstellendefinition

Die Schnittstelle wird auf Basis des OASIS Standards Directory Services Markup Language (DSML) v2.0 [DSML2.0] definiert.

A_14361 - Zugangsgateway des Versicherten, Schnittstelle I_Proxy_Directory_Query
Der LDAP-Proxy der Komponente Zugangsgateway des Versicherten MUSS den Webservice I_Proxy_Directory_Query mit der Operation "Search" gemäß

- Tabelle Tab_ePA_I_Proxy_Directory_Query und
- [DSML2.0]
  - mit SOAP Request/Response Binding
  - mit Nutzung der DSMLRequests und DSMLResponses Operationen entsprechend WSDL

für die Daten des Verzeichnisdienstes [gemSpec_VZD#5] anbieten.

Tabelle 1: Tab_ePA_I_Proxy_Directory_Query

Schnittstelle	**I_Proxy_Directory_Query**	
Version	2.0	
Namensraum	"urn:oasis:names:tc:DSML:2:0:core"	
Namensraum-Kürzel	DSML	
Operationen	**Name**	**Kurzbeschreibung**
	Search	Suche nach Leistungserbringern bzw. Leistungsbringerorganisationen im Verzeichnisdienst.
WSDL	[DSML.wsdl]	
XML-Schema	http://www.oasis-open.org/committees/dsml/docs/DSMLv2.xsd	

[<=]

A_14419 - Zugangsgateway des Versicherten, Schnittstelle I_Proxy_Directory_Query, Operationen
Der LDAP-Proxy der Komponente Zugangsgateway des Versicherten MUSS die Operation "Search" im Web Service I_Proxy_Directory_Query gemäß Tabelle Tab_ePA_I_Proxy_Directory_Query anbieten und als Antwort darauf entsprechend WSDL und XML-Schema das "SearchResponse" und "ErrorResponse" unterstützen.
[<=]

6.2.2.2 Umsetzung

A_14421 - Zugangsgateway des Versicherten, Schnittstelle I_Proxy_Directory_Query, Umsetzung über Verzeichnisdienst
Der LDAP-Proxy der Komponente Zugangsgateway des Versicherten MUSS für die Umsetzung des Webservices I_Proxy_Directory_Query die Schnittstelle I_Directory_Query des Verzeichnisdienstes [gemSpec_VZD] nutzen.**[<=]**

A_14467 - Zugangsgateway des Versicherten, Schnittstelle I_Proxy_Directory_Query, Aufrufe pro Zeiteinheit
Die Komponente Zugangsgateway des Versicherten MUSS die Anzahl der Operationen an der Schnittstelle I_Proxy_Directory_Query pro Versicherten Session und Minute auf einen - durch den Betreiber im Wertebereich 1 bis 15 - konfigurierbaren Wert beschränken. Der Defaultwert für diese Konfigurationsparameter MUSS 10 betragen. Wird diese Anzahl überschritten, MUSS ein HTTP-Response mit HTTP-Statuscode 429 entsprechend RFC6585 Kapitel 4 "429 Too Many Requests" an den Client zurückgegeben werden.
[<=]

A_14468 - Zugangsgateway des Versicherten, Schnittstelle I_Proxy_Directory_Query, Keine personenbezogenen Daten loggen
Der LDAP-Proxy der Komponente Zugangsgateway des Versicherten DARF personenbezogene Daten NICHT in das Logging aufnehmen.**[<=]**

A_17748-01 - Zugangsgateway des Versicherten, Schnittstelle I_Proxy_Directory_Query, Beschränkung auf ePA relevante Informationen
Der LDAP-Proxy der Komponente Zugangsgateway des Versicherten MUSS sicherstellen, dass ein anfragendes ePA-Modul Frontend des Versicherten (ePA-Modul FdV) ausschließlich die Informationen des Verzeichnisdienstes erhält, welche für die Erfüllung der Aufgaben benötigt werden. Folgende Vorgaben MÜSSEN eingehalten werden:

- Der LDAP-Proxy DARF NICHT Fachdaten an das anfragende ePA-Modul Frontend des Versicherten (ePA-Modul FdV) zurückgegeben.
- Es MUSS sichergestellt sein, dass ausschließlich Einträge des Verzeichnisdienstes mit Eintragstyp nach [gemSpec_VZD#Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID] == 3 oder 6 zurückgegeben werden.

[<=]

6.2.2.3 Nutzung

Für die Nutzung des Webservices I_Proxy_Directory_Query durch einen Client sind folgende Randbedingungen zu beachten:

- Die Datenstruktur des Verzeichnisdienstes [gemSpec_VZD#5]
- Die Einschränkungen des Verzeichnisdienstes.
  - Die Anzahl der pro "Search" Operation gelieferten Datensätze wird durch den Verzeichnisdienst [gemSpec_VZD#TIP1-A_5552]beschränkt.

Das ePA-Modul Frontend des Versicherten (ePA-Modul FdV) kann über den Webservices I_Proxy_Directory_Query alle in der Datenstruktur „Verzeichnisdienst_Eintrag_flache_Liste‟ (dn="dc=data,dc=vzd") des Verzeichnisdienstes [gemSpec_VZD#5] definierten Daten ermitteln.

Zur Suche im Verzeichnisdienst muss das ePA-Modul Frontend des Versicherten (ePA-Modul FdV) das "SearchRequest" entsprechend OASIS DSML v2.0 [DSML2.0] nutzen. Die DSML.wsdl schränkt die zugelassenen Operationen im Webservice I_Proxy_Directory_Query auf ein "SearchRequest" pro SOAP Request ein. Der LDAP-Proxy antwortet mit einem "SearchResponse" bzw. im Fehlerfall mit einem "ErrorResponse". Andere Operationen werden im Webservice I_Proxy_Directory_Query nicht unterstützt. Die Parameter der Nachrichten werden durch das OASIS DSML v2.0 Schema und Dokumentation [DSML2.0] definiert. Die Verarbeitung der "SearchRequest" erfolgt durch den Verzeichnisdienst entsprechend LDAPv3.

Beispiel für einen SearchRequest mit dem eine Orthopädiepraxismit Namen Schmidt gesucht wird:

ID: 7
Address: http://localhost:9098/services/DSML/1.0.0
Encoding: UTF-8
Http-Method: POST
Content-Type: application/soap+xml; action="http://ws.gematik.de/phr/dsml/v2#dsmlRequest"; charset=UTF-8
Headers: {Accept=[*/*], cache-control=[no-cache], clienttype=[fdv], Content-Length=[613], content-type=[application/soap+xml; action="http://ws.gematik.de/phr/dsml/v2#dsmlRequest"; charset=UTF-8], forwarded=[proto=https;host="localhost:9094";for="127.0.0.1:63936"], host=[localhost:9098], pragma=[no-cache], tlssession=[6660eee2226aebe2ab967e6fadb45825e34481b4852c1c303df36a185a77e731], user-agent=[Apache-CXF/3.3.5], x-forwarded-for=[127.0.0.1], x-forwarded-host=[localhost:9094], x-forwarded-port=[9094], x-forwarded-proto=[https]}
Payload:

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Body>
    <ns3:SearchRequest xmlns:ns2="urn:oasis:names:tc:DSML:2:0:core"
xmlns:ns3="http://ws.gematik.de/phr/dsml/v2" dn="dc=data,dc=vzd" scope="wholeSubtree"
derefAliases="neverDerefAliases">
      <ns2:filter>
        <ns2:and>
          <ns2:equalityMatch name="subject">
            <ns2:value>Orthopädie</ns2:value>
          </ns2:equalityMatch>
        </ns2:and>
      </ns2:filter>
      <ns2:attributes>
        <ns2:attribute name="displayName"/>
        <ns2:attribute name="street"/>
        <ns2:attribute name="postalCode"/>
        <ns2:attribute name="userCertificate"/>
      </ns2:attributes>
    </ns3:SearchRequest>
  </soap:Body>
</soap:Envelope>
```

Beispiel für ein Response auf den SearchRequest:

ID: 7
Response-Code: 200
Encoding: UTF-8
Content-Type: application/soap+xml
Headers: {}
Payload:

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Body>
    <ns3:DSMLsearchResponse xmlns:ns2="urn:oasis:names:tc:DSML:2:0:core"
```

xmlns:ns3="http://ws.gematik.de/phr/dsml/v2">
<searchResponse requestID="6">
<ns2:searchResultEntry dn="uid=7,dc=data,dc=vzd">
<ns2:attr name="street">
<ns2:value>Gaffelsteig 134</ns2:value>
</ns2:attr>
<ns2:attr name="postalCode">
<ns2:value>45879</ns2:value>
</ns2:attr>
<ns2:attr name="displayName">
<ns2:value>Praxis Prof. Gourmet</ns2:value>
</ns2:attr>
<ns2:attr name="userCertificate;binary">
<ns2:value>MIIEpTCCA42gAwIBAgIHAQ97rEzGnjANBgkqhkiG9w0BAQsFADCBmjELMAkGA
1UEBhMCREUxHzAdBgNVBAoMFmdlbWF0aWsgR21iSCBOT1QtVkFMSUQxSDBGBgNVBAsMP0lu
c3RpdHV0aW9uIGRlcyBHZXN1bmRoZWl0c3dlc2Vucy1DQSBkZXIgVGVsZW1hdGlraW5mcmFzdHJ1
a3R1cjEgMB4GA1UEAwwXR0VNLlNNQ0ItQ0EyNCBURVNULU9OTFkwHhcNMTkwMTAyMjMwMDA
wWhcNMjQwMTAyMjI1OTU5WjBUMQswCQYDVQQGEwJERTEcMBoGA1UECgwTMTAwMDIyMjA3I
E5PVC1WQUxJRDEnMCUGA1UEAwweUHJheGlzIFByb2YuIEdvdXJtZXQgVEVTVC1PTkxZMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyQOTyl8dB2G/rfc1lUU3so0Uwwe55mAlPCmOMM
7kdfYWVuTeXXFjSNFFreK43KPyT6cDN9x7Fl8auzErLg64kKLuS47vBD27/qmkaxitzLlRioGPfM79EC3
eflutpSSdEeNGWjHRWTnCB2MW8kBi4+dN93qTiYfG5X+QEWcQbOd7LMSbfXgp4/KgD3H/+cS2qR8
mL1q+RDwnkMgb3l05K0SzotlVHxZ18DpuXV63PTnYXGaz564CTF7nKSzA2ewCTLEBaMCtYXKY8x
2v2om0iUNaBToOc93eUegHq7EFpFrmX+b8PHnhollxZTduBUz0KtKjYQMFxYh/CrCkDt2OEQIDAQA
Bo4IBMzCCAS8wHQYDVR0OBBYEFCxL7gqLNViJxujRaQ8e84HFibC1MCwGA1UdHwQlMCMwIaAf
oB2GG2h0dHA6Ly9laGNhLmdlbWF0aWsuZGUvY3JsLzAMBgNVHRMBAf8EAjAAMEUGBSskCAMD
BDwwOjA4MDYwNDAyMBYMFEJldHJpZWJzc3TDpHR0ZSBBcnp0MAkGByqCFABMBDITDTEtMjB
WWkQwMDAwMDcwHwYDVR0jBBgwFoAUeunhb+oUWRYF7gPp0/0hq97p2Z4wIAYDVR0gBBkwFz
AKBggqghQATASBIzAJBgcqghQATARMMA4GA1UdDwEB/wQEAwIEMDA4BggrBgEFBQcBAQQsM
CowKAYIKwYBBQUHMAGGHGh0dHA6Ly9laGNhLmdlbWF0aWsuZGUvb2NzcC8wDQYJKoZIhvcNA
QELBQADggEBAD80QGann9YCqQ1adaKwv+CvSjY+svYlTIGKiRbBUI3zyVrlGlM3N8zZFF95NfabYL
XpKHppEX9FgekxHOgYC/vs40MSh19ioLpgfxI1fJh5t8H1Fs3XX2HAwd5dMwHgOZwibSBZhtkUmlbG
vpOQ+Q6OuZYVjAZRuWk4tAgnwRPilFVC+TQ9Xvy8o+PPHsjdorpuv2b9w1ttbKBbmP+oikl1YmTP6X
LKxuDlbMade4/8xdpP9ypRFvVlcdI2rZ73VjHJ01A47Q+11g8oGn+G4vnkC7EEwqtg8BD/MUKs6qfkTV
RZCSVj8vv6h0gMKrduytEUKKU72fNIqjfz/8sGHM4=</ns2:value>
</ns2:attr>
</ns2:searchResultEntry>
<ns2:searchResultEntry dn="uid=10,dc=data,dc=vzd">
<ns2:attr name="street">
<ns2:value>Caligariplatz 34</ns2:value>
</ns2:attr>
<ns2:attr name="postalCode">
<ns2:value>09111</ns2:value>
</ns2:attr>
<ns2:attr name="displayName">
<ns2:value>QXJ6dHplbnRydW0gT3J0aG9ww6RkaWU=</ns2:value>
</ns2:attr>
</ns2:searchResultEntry>
<ns2:searchResultDone requestID="6">
<ns2:resultCode code="0" descr="success"/>
</ns2:searchResultDone>
</searchResponse>
</ns3:DSMLsearchResponse>
</soap:Body>
</soap:Envelope>

7 Anhang A – Verzeichnisse

7.1 Abkürzungen

Kürzel	Erläuterung
ACL	Access Control List
BSI	Bundesamt für Sicherheit in der Informationstechnik
DNS	Domain Name System
DSML	Directory Services Markup Language
eGK	elektronische Gesundheitskarte
ePA	elektronische Patientenakte
IDS/IPS	Intrusion-Detection/Intrusion-Prevention System
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OSI	Open Systems Interconnection Model
SOAP	Simple Object Access Protocol
SZZP	Sicherer Zentraler Zugangspunkt
TI	Telematikinfrastruktur
TLS	Transport Layer Security
TSP	Trusted Services Provider
VAU	Vertrauenswürdige Ausführungsumgebung
VZD	Verzeichnisdienst der TI-Plattform

7.2 Glossar

Begriff	Erläuterung
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende, Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.

Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung gestellt.

7.3 Abbildungsverzeichnis

7.4 Tabellenverzeichnis

7.5 Referenzierte Dokumente

7.5.1 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 ist in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar
[gemSpec_Aktensystem]	gematik: Spezifikation ePA-Aktensystem

[gemSpec_Authentisierung_Vers]	gematik: Spezifikation Authentisierung des Versicherten ePA
[gemSpec_Autorisierung]	gematik: Spezifikation Autorisierung ePA
[gemSpec_Dokumentenverwaltung]	gematik: Spezifikation ePA-Dokumentenverwaltung
[gemSpec_ePA_FdV]	gematik: Spezifikation ePA-Frontend des Versicherten
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_Perf]	gematik: Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform
[gemSpec_TSL]	gematik: Spezifikation TSL-Dienst
[gemSpec_SGD_ePA]	gematik: Spezifikation Schlüsselgenerierungsdienst ePA
[gemSpec_VZD]	gematik: Spezifikation Verzeichnisdienst

7.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[DSML2.0]	OASIS: Directory Services Markup Language v2.0 December 18, 2001 https://www.oasis-open.org/standards http://www.oasis-open.org/committees/dsml/docs/DSMLv2.doc http://oasis-open.org/committees/dsml/errata https://www.oasis-open.org/committees/dsml/docs/DSMLv2.xsd
CAB-Forum	Liste vertrauenswürdiger Zertifikatsherausgeber (Root-CAs) für Anwendungen im Internet https://cabforum.org/members/