

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 Telematikinfrastuktur 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 Telematikinfrastuktur

Spezifikation ePA-Aktensystem

Version: [1.56.0 CC](#)
Revision: [245464269749](#)
Stand: [30.0617.08.2020](#)
Status: [zur Abstimmung](#) freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemSpec_Aktensystem

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
1.0.0	18.12.18		freigegeben	gematik
1.1.0	15.05.19		Einarbeitung Änderungsliste P18.1	gematik
1.2.0	28.06.19		Einarbeitung Änderungsliste P19.1	gematik
1.3.0	02.10.19		Einarbeitung Änderungsliste P20.1	gematik
1.4.0	02.03.20		Einarbeitung Änderungsliste P21.1	gematik
1.4.1	26.05.20		Einarbeitung Änderungsliste 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 CC	17.08.20		Einarbeitung Scope-Themen Zur Abstimmung freigegeben	gematik

Inhaltsverzeichnis

37	1 Einordnung des Dokumentes	7
38	1.1 Zielsetzung	7
39	1.2 Zielgruppe	7
40	1.3 Geltungsbereich	7
41	1.4 Abgrenzungen	7
42	1.5 Methodik	8
43	1.6 Erläuterungen zur Spezifikation des Außenverhaltens	8
44	2 Systemüberblick	9
45	3 Systemkontext	10
46	3.1 Nachbarsysteme	10
47	3.2 ePA-Aktensysteme unterschiedlicher Anbieter	10
48	4 Zerlegung des Produkttyps	11
49	5 Übergreifende Festlegungen	12
50	5.1 Akten- und Service-Lokalisierung	13
51	5.2 Protokollierung	18
52	5.2.1 Übergreifende Anforderungen zur Protokollierung	18
53	5.2.2 Internes Fehlerprotokoll	19
54	5.3 Fehlermeldungen	19
55	5.4 Redundanz	20
56	5.5 Sichere Produktentwicklung	21
57	5.6 Datenschutz und Sicherheit	21
58	5.7 Evidenzbasiertes Monitoring	26
59	5.8 Registrierung von KTR-AdV-Terminals	27
60	6 Funktionsmerkmale	29
61	6.1 Aktenkontomanagement	29
62	6.1.1 Kontoverwaltung und Zustandswechsel	29
63	6.1.2 Prozess der Aktenkontoeröffnung	33
64	6.1.3 Prozess der Änderung und Kündigung eines Aktenkontos	35
65	6.1.4 Prozess des Anbieterwechsels	36
66	6.2 Benutzerführung	38
67	7 Informationsmodell	40
68	8 Verteilungssicht	41

69	9 Anhang A – Verzeichnisse	42
70	9.1 Abkürzungen	42
71	9.2 Glossar	42
72	9.3 Abbildungsverzeichnis	43
73	9.4 Tabellenverzeichnis	43
74	9.5 Referenzierte Dokumente	43
75	9.5.1 Dokumente der gematik	43
76	9.5.2 Weitere Dokumente	44
77	1 Einordnung des Dokumentes	7
78	1.1 Zielsetzung	7
79	1.2 Zielgruppe	7
80	1.3 Geltungsbereich	7
81	1.4 Abgrenzungen	7
82	1.5 Methodik	8
83	1.6 Erläuterungen zur Spezifikation des Außenverhaltens	8
84	2 Systemüberblick	9
85	3 Systemkontext	10
86	3.1 Nachbarsysteme	10
87	3.2 ePA-Aktensysteme unterschiedlicher Anbieter	10
88	4 Zerlegung des Produkttyps	11
89	5 Übergreifende Festlegungen	12
90	5.1 Akten- und Service-Lokalisierung	13
91	5.2 Protokollierung	18
92	5.2.1 Übergreifende Anforderungen zur Protokollierung	18
93	5.2.2 Internes Fehlerprotokoll	19
94	5.3 Fehlermeldungen	19
95	5.4 Redundanz	20
96	5.5 Sichere Produktentwicklung	21
97	5.6 Datenschutz und Sicherheit	21
98	5.7 Evidenzbasiertes Monitoring	26
99	6 Funktionsmerkmale	29
100	6.1 Aktenkontomanagement	29
101	6.1.1 Kontoverwaltung und Zustandswechsel	29
102	6.1.2 Prozess der Aktenkontoeröffnung	33
103	6.1.3 Prozess der Änderung und Kündigung eines Aktenkontos	35
104	6.1.4 Prozess des Anbieterwechsels	36

105	6.2 Benutzerführung	38
106	7 Informationsmodell	40
107	8 Verteilungssicht	41
108	9 Anhang A – Verzeichnisse	42
109	9.1 Abkürzungen	42
110	9.2 Glossar	42
111	9.3 Abbildungsverzeichnis	43
112	9.4 Tabellenverzeichnis	43
113	9.5 Referenzierte Dokumente	43
114	9.5.1 Dokumente der gematik	43
115	9.5.2 Weitere Dokumente	44
116		
117		
118		

119

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die übergreifenden Anforderungen zu Herstellung, Test und Betrieb des Produkttyps ePA-Aktensystem. Hierbei handelt es sich insbesondere um übergreifende technische Anforderungen, die von allen Komponenten gleichermaßen umzusetzen sind, um organisatorische Anforderungen gegen den Anbieter des ePA-Aktensystems, die für die Realisierung der Anwendungsfälle zur Aktenkontoverwaltung benötigt werden, und um übergreifende Sicherheitsanforderungen. Die Systemzerlegung der Fachanwendung ePA in Komponenten und Produkttypen sowie die Verteilung der Komponenten auf Produkttypen der Telematikinfrastruktur (TI) sind in [gemSysL_ePA#2.1] und in [gemSysL_ePA#4.1] definiert.

Für die einzelnen Komponenten des Produkttyps ePA-Aktensystem existieren eigene Spezifikationsdokumente, in denen die spezifischen Anforderungen der jeweiligen Komponente beschrieben werden.

1.2 Zielgruppe

Das Dokument ist maßgeblich für Anbieter und Hersteller des Produkttyps ePA-Aktensystem sowie für Anbieter und Hersteller von Produkten, die die Schnittstellen des Produkttyps ePA-Aktensystem nutzen.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik mbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) 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 übergreifenden Anforderungen an den Produkttyp ePA-Aktensystem. Die bereitgestellten (angebotenen) Schnittstellen werden

155 in den Spezifikationen der einzelnen Komponenten des ePA-Aktensystems definiert.
156 Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen
157 beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird
158 referenziert (siehe auch Anhang A5).

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

162 1.5 Methodik

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

167

168 Sie werden im Dokument wie folgt dargestellt:

169 **<AFO-ID> - <Titel der Afo>**

170 Text / Beschreibung

171 [**<=**]

172 Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und Textmarke

173 [**<=**] angeführten Inhalte.

174 1.6 Erläuterungen zur Spezifikation des Außenverhaltens

175 Das „ePA-Aktensystem“ stellt einen komplexen Produkttyp dar. An dieser Stelle folgen
176 daher wesentliche Informationen, die das korrekte Verstehen der Spezifikation fördern:

- 177 • Die Spezifikation des ePA-Aktensystems ist eine Black-Box-Spezifikation, das
178 heißt, alle Festlegungen dienen ausschließlich der Beschreibung des von der
179 Komponente verlangten Verhaltens an der Außenschnittstelle des Produkttyps
180 ePA-Aktensystem.
- 181 • Normative Festlegungen, die eine Festlegung des inneren Verhaltens vermuten
182 lassen, sind nur in so weit normativ, wie ihre Festlegungen auf die
183 Außenschnittstelle wirken. Sie legen explizit nicht die intern zu verwendende
184 Implementierung fest. Die Notwendigkeit für diese Art der "scheinbaren internen
185 Beschreibung" ergibt sich aus der Komplexität der Gesamtkomponente, sowie
186 dem Bedarf, wiederholt ähnliche Verhaltensweisen in Außenschnittstellen
187 darstellen zu müssen. Die konkrete akteninterne Modularisierung bleibt dem
188 Hersteller freigestellt. Insbesondere bleibt es dem Hersteller freigestellt, intern
189 bereits Mechanismen für kommende Releases zu realisieren, sofern diese an der
190 Außenschnittstelle keine Auswirkung zeigen.
- 191 • Die einzige Abweichung von dieser Vorgehensweise ergibt sich für
192 Sicherheitsaspekte. Hier können interne Vorgänge normativ gefordert sein, die
193 sich an der Außenschnittstelle nicht manifestieren (Beispiel "Verpflichtung auf
194 sicheres Löschen eines temporären Schlüssels nach Gebrauch"). In diesem Fall
195 erfolgt die Überprüfung der Einhaltung dieser Anforderungen im Rahmen des
196 Nachweises der sicherheitstechnischen Eignung.

2 Systemüberblick

Das ePA-Aktensystem besteht aus den Komponenten

- Zugangsgateway TI,
- Authentisierung (Versicherter),
- Autorisierung,
- Dokumentenverwaltung

deren Funktionsweise in separaten Spezifikationen beschrieben sind. Zusätzlich zu diesen Komponenten muss der Anbieter des ePA-Aktensystems einen Schlüsselgenerierungsdienst Typ1 (SGD1) in der Provider Zone zur Verfügung stellen. Dieses Dokument bildet die Klammer über diese logischen Komponenten und spezifiziert insbesondere das Verhältnis des Anbieters und Betreibers zum ePA-Aktensystem sowie organisatorische Prozesse und Schnittstellen gegenüber dem Versicherten als "Kunden" des Anbieters des ePA-Aktensystems.

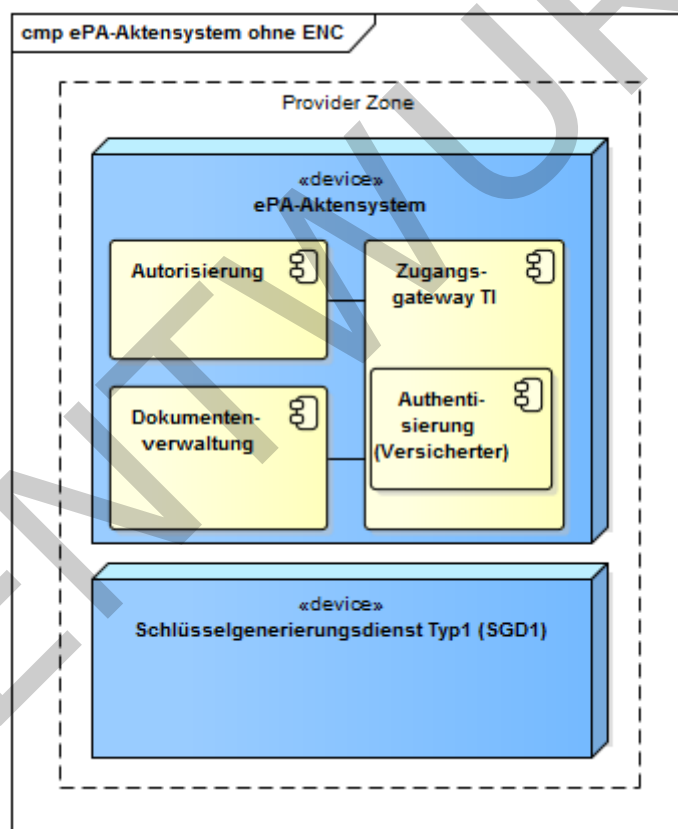


Abbildung 1: Komponenten des ePA-Aktensystems

3 Systemkontext

3.1 Nachbarsysteme

Das ePA-Aktensystem eines Anbieters kommuniziert in Richtung des Versicherten jeweils mit einem oder mehreren ePA-Modulen Frontend des Versicherten. Die ePA-Module FdV können dabei auch von unterschiedlichen Herstellern angeboten werden. In Richtung der Leistungserbringerinstitution kommuniziert das ePA-Aktensystem ausschließlich mit dem Fachmodul ePA im Konnektor. Das Fachmodul ePA im Konnektor übernimmt die Kommunikation mit den Primärsystemen. Das ePA-Aktensystem nutzt außerdem zentrale Dienste der TI-Plattform.

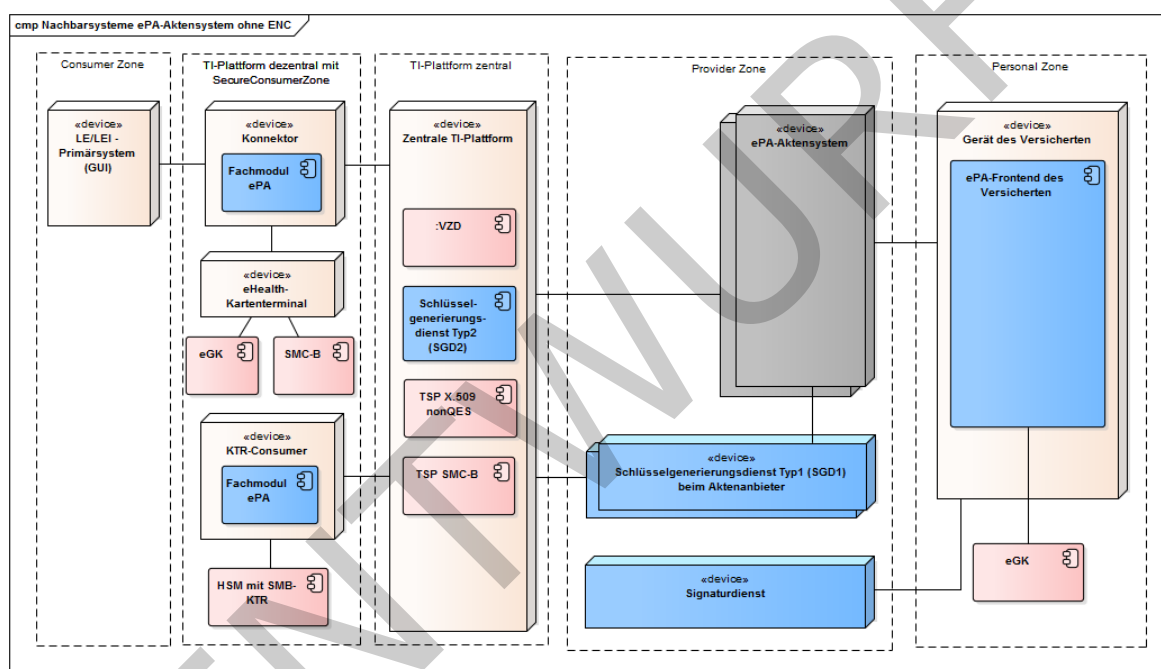


Abbildung 2: Nachbarsysteme des ePA-Aktensystems

3.2 ePA-Aktensysteme unterschiedlicher Anbieter

Sowohl bei der Registrierung eines Aktenkontos als auch bei einem Anbieterwechsel gibt es Kommunikationsbeziehungen zwischen den Systemen der Anbieter von ePA-Aktensystemen. Im Rahmen der Registrierung zur Eröffnung eines Aktenkontos erfolgt eine Abfrage zwischen den Anbietern, ob für den jeweiligen Versicherten ggf. bereits ein Aktenkonto existiert. Ist dies der Fall, kann eine Registrierung nur abgeschlossen werden, wenn für ein bereits bestehendes Aktenkonto der Status unknown, dismissed oder suspended zurückgemeldet wird.

Hat der Versicherte für den Anbieterwechsel die Migration seiner Daten vom Alt-Anbieter zu seinem neuen Anbieter vorgesehen, erfolgt die Übermittlung eines verschlüsselten Migrationspakets direkt zwischen den Systemen der Anbieter.

235

4 Zerlegung des Produkttyps

236

Der Produkttyp ePA-Aktensystem wird gemäß der funktionalen Zerlegung

237

in [gemSysL_ePA#4.1] in die dort definierten Komponenten aufgeteilt.

ENTWURF

238

5 Übergreifende Festlegungen

239 **A_17865 - Anbieter ePA-Aktensystem - Rollenausschluss für Anbieter eines** 240 **ePA-Aktensystems**

241 Der Anbieter des ePA-Aktensystems MUSS unabhängig von Anbietern von
242 Signaturdiensten und vom Anbieter des Schlüsselgenerierungsdienstes SGD2 der
243 zentralen TI-Plattform sein, d.h. es sind mindestens jeweils eigenständige
244 Rechtspersonlichkeiten mit eigenständigen operativen Geschäfts- und Betriebsführungen
245 und es ist eine strikte Vermeidung von Personenidentitäten bzw.
246 Doppelrollen in den Funktionen Geschäftsführung, leitende Mitarbeiter und
247 Zugangsberechtigte zum Betriebsort des Signaturdienstes,
248 Schlüsselgenerierungsdienstes SGD2 bzw. ePA-Aktensystems gewährleistet.
249

250 [\leq]

251 Hinweis: Die Anforderung schließt nicht aus, dass die Anbieter verbundene Unternehmen
252 im Sinne des § 15 AktG sind.

253 **A_18765 - Gemeinsame Kontaktstelle von Signaturdienst und ePA-Aktensystem**

254 Falls ein Anbieter eines ePA-Aktensystems und ein Anbieter eines Signaturdienstes den
255 Versicherten eine gemeinsame Kontaktstelle (z.B. User-Help-Desk) sowohl für Anfragen
256 zum ePA-Aktensystem als auch zum Signaturdienst anbieten, MÜSSEN sowohl der
257 Anbieter des ePA-Aktensystems als auch der Anbieter des Signaturdienstes sicherstellen,
258 dass

- 259 • die Kontaktstelle die Erstellung oder Änderungen von
260 Authentifizierungsmerkmalen beim Signaturdienst und die Erstellung oder
261 Änderungen der Mailadresse für die Geräteverwaltung im ePA-Aktensystem nur im
262 4-Augen-Prinzip beauftragt,
- 263 • die Kontaktstelle die Erstellung oder Änderungen von
264 Authentifizierungsmerkmalen beim Signaturdienst und die Erstellung oder
265 Änderungen der Mailadresse für die Geräteverwaltung im ePA-Aktensystem nur
266 auf Verlangen des Versicherten beauftragt und
- 267 • nachträglich von Dritten nachvollzogen werden kann, dass eine Erstellung oder
268 eine Änderung durch den Versicherten beauftragt wurde und welche Mitarbeiter
269 der Kontaktstelle die Erstellung oder Änderungen bzw. Aufträge zur Erstellung
270 oder Änderung ausgelöst haben.

271 [\leq]

272 **A_19124 - Mitarbeiter der Kontaktstelle haben keinen Zugriff auf das ePA-** 273 **Aktensystem und Signaturdienst**

274 Falls ein Anbieter eines ePA-Aktensystems und ein Anbieter eines Signaturdienstes den
275 Versicherten eine gemeinsame Kontaktstelle (z.B. User-Help-Desk) sowohl für Anfragen
276 zum ePA-Aktensystem als auch zum Signaturdienst anbieten, MÜSSEN sowohl der
277 Anbieter des ePA-Aktensystems als auch der Anbieter des Signaturdienstes sicherstellen,
278 dass die Mitarbeiter der Kontaktstelle die Anfragen der Versicherten lediglich an das ePA-
279 Aktensystem bzw. den Signaturdienst weiterleiten können und technisch verhindert wird,
280 dass die Mitarbeiter der Kontaktstelle Änderungen an den Systemen des ePA-
281 Aktensystems bzw. des Signaturdienstes selbstständig durchführen können.
282

[\leq]

A_19123 - Dokumentationspflicht zur gemeinsamen Kontaktstelle

Falls ein Anbieter eines ePA-Aktensystems und ein Anbieter eines Signaturdienstes den Versicherten eine gemeinsame Kontaktstelle (z.B. User-Help-Desk) sowohl für Anfragen zum ePA-Aktensystem als auch zum Signaturdienst anbieten, MÜSSEN sowohl der Anbieter des ePA-Aktensystems als auch der Anbieter des Signaturdienstes folgendes dokumentieren,

- Art und Umfang der Aufgaben der Kontaktstelle sowie der dafür erforderlichen Systemzugriff
- Die betrieblichen Prozesse der Kontaktstelle und deren Absicherung
- Wie die Systemschnittstellen zwischen der Kontaktstelle und Aktensystem sowie Signaturdienst absichert sind
- Eine umfassende Risikoanalyse mit Fokus auf Angriffe von Innentätern sowie Sozial-Engineering-Angriffe von Kunden

[<=]

5.1 Akten- und Service-Lokalisierung

A_15246 - Anbieter ePA-Aktensystem - OID als homeCommunityID für Aktenanbieter

Der Anbieter des ePA-Aktensystems MUSS als homeCommunityID [gemSpec_DM_ePA#2.1.4.6] eine OID verwenden, die er beim DIMDI beantragt.
[<=]

~~A_14127-02A_14127-01~~ - Anbieter ePA-Aktensystem - PTR für Anbieterliste (RFC Service-Discovery)

Der Anbieter des ePA-Aktensystems MUSS DNS [A](#), PTR und SRV Resource Records für sein Aktensystem im Namensraum der TI gemäß folgender Tabelle verwalten.

Tabelle 1: Tab_ePA_Service Discovery

Resource Record Bezeichner	Resource Record Type	Beschreibung
FQDN des authn Service	A	A Resource Records zur Namensauflösung von FQDN des authn Services ePA-Aktensystems des jeweiligen Anbieters in IP-Adressen
FQDN des authz Service	A	A Resource Records zur Namensauflösung von FQDN des authz Services ePA-Aktensystems des jeweiligen Anbieters in IP-Adressen
FQDN des docv Service	A	A Resource Records zur Namensauflösung von FQDN des docv Services ePA-Aktensystems des jeweiligen Anbieters in IP-Adressen

FQDN des sgd1 Service	A	A Resource Records zur Namensauflösung von FQDN des sgd1 Services ePA-Aktensystems des jeweiligen Anbieters in IP-Adressen
_authn._tcp.epa.telematik	PTR	Ermittlung aller ePA-Authentisierungs-Dienste ""<hcid> authn Service<hcid>""
_authz._tcp.epa.telematik	PTR	Ermittlung aller ePA-Autorisierungs-Dienste ""<hcid> authz Service<hcid>""
_docv._tcp.epa.telematik	PTR	Ermittlung aller ePA-Dokumentenverwaltungs-Dienste ""<hcid> docv Service<hcid>""
_sgd1._tcp.epa.telematik	PTR	Ermittlung des zum ePA-Aktensystem gehörigen Schlüsselgenerierungsdienstes (Typ 1) "sgd_typ1"<hcid> sgd1 Service<hcid>""
""<hcid> authn Service<hcid>""	SRV und TXT	SRV Resource Record zur Ermittlung des FQDN des authn-Dienstes; TXT Resource Record zur Ermittlung des Pfades der URL zum authn-Dienst " txtvers=1 " "hcid=<hcid>" "path=<Bezeichner der Komponente als Pfadbestandteil>"
""<hcid> authz Service<hcid>""	SRV und TXT	SRV Resource Record zur Ermittlung des FQDN des authz-Dienstes; TXT Resource Record zur Ermittlung des Pfades der URL zum authz-Dienst " txtvers=1 " "hcid=<hcid>" "path=<Bezeichner der Komponente als Pfadbestandteil>"
""<hcid> docv Service<hcid>""	SRV und TXT	SRV Resource Record zur Ermittlung des FQDN des docv-Dienstes; TXT Resource Record zur Ermittlung des Pfades der URL zur Schnittstelle I_Document_Management_Insurant, zum docv-Dienst " txtvers=1 " "hcid=<hcid>" "path=<Bezeichner der Komponente als Pfadbestandteil>"
"sgd_typ1"<hcid> sgd1 Service<hcid>""	SRV und TXT	SRV Resource Record zur Ermittlung des FQDN des sgd_typ1-Dienstes; TXT Resource Record zur Ermittlung des Pfades der URL zum sgd_typ1-Dienst " txtvers=1 " "hcid=<hcid>" "path=<Bezeichner der Komponente als Pfadbestandteil>"

311
312
313
314

[<=]

315 Wenn im Bezeichner die HCID verwendet wird, sollen . durch - ersetzt werden, da .
 316 Sonderzeichen im DNS darstellen.
 317 Beispiel: 1.2.276.0.76.3.1.91 wird zu 1-2-276-0-76-3-1-91

318 Beispiele zur Dienstlokalisierung

319 1. Für HCID: 1.2.276.0.76.3.1.91

320 _authn._tcp.epa.telematik. 86400 IN PTR _1-2-276-0-76-3-1-91._authn._tcp.epa.telematik.
 321 _1-2-276-0-76-3-1-91._authn._tcp.epa.telematik. 86400 IN SRV 5 10 443 authn.hrst1.epa.telematik.
 322 _1-2-276-0-76-3-1-91._authn._tcp.epa.telematik. 86400 IN TXT „txtvers=1“
 323 „[,hcid=1.2.276.0.76.3.1.91](#)“,path=/
 324 authn.hrst1.epa.telematik IN A 10.28.2.15

325 _authz._tcp.epa.telematik. 86400 IN PTR _1-2-276-0-76-3-1-91._authz._tcp.epa.telematik.
 326 _1-2-276-0-76-3-1-91._authz._tcp.epa.telematik. 86400 IN SRV 5 10 443 authz.hrst1.epa.telematik.
 327 _1-2-276-0-76-3-1-91._authz._tcp.epa.telematik. 86400 IN TXT „txtvers=1“
 328 „[,hcid=1.2.276.0.76.3.1.91](#)“,path=/
 329 authz.hrst1.epa.telematik IN A 10.28.2.16

330 _docv._tcp.epa.telematik. 86400 IN PTR _1-2-276-0-76-3-1-91._docv._tcp.epa.telematik.
 331 _1-2-276-0-76-3-1-91._docv._tcp.epa.telematik. 86400 IN SRV 5 10 443 docv.hrst1.epa.telematik.
 332 _1-2-276-0-76-3-1-91._docv._tcp.epa.telematik. 86400 IN TXT „txtvers=1“
 333 „[,hcid=1.2.276.0.76.3.1.91](#)“,path=/
 334 docv.hrst1.epa.telematik IN A 10.28.2.17

335 _sgd1._tcp.epa.telematik. 86400 IN PTR _1-2-276-0-76-3-1-91._sgd1._tcp.epa.telematik.
 336 _1-2-276-0-76-3-1-91._sgd1._tcp.epa.telematik. 86400 IN SRV 5 10 443 sgd1.hrst1.epa.telematik.
 337 _1-2-276-0-76-3-1-91._sgd1._tcp.epa.telematik. 86400 IN TXT „txtvers=1“
 338 „[,hcid=1.2.276.0.76.3.1.91](#)“,path=/
 339 sgd1.hrst1.epa.telematik IN A 10.28.2.14

340 2. Für HCID: 1.2.276.0.76.3.1.99

341 authn._tcp.epa.telematik. 86400 IN PTR _1-2-276-0-76-3-1-99._authn._tcp.epa.telematik.
 342 _1-2-276-0-76-3-1-99._authn._tcp.epa.telematik. 86400 IN SRV 5 10 443 authn.hrst2.epa.telematik.
 343 _1-2-276-0-76-3-1-99._authn._tcp.epa.telematik. 86400 IN TXT „txtvers=1“ „[,hcid=1.2.276.0.76.3.1.99](#)“
 344 „,path=/
 345 authn.hrst2.epa.telematik. IN A 10.28.2.25

346 _authz._tcp.epa.telematik. 86400 IN PTR _1-2-276-0-76-3-1-99._authz._tcp.epa.telematik.
 347 _1-2-276-0-76-3-1-99._authz._tcp.epa.telematik. 86400 IN SRV 5 10 443 authz.hrst2.epa.telematik.
 348 _1-2-276-0-76-3-1-99._authz._tcp.epa.telematik. 86400 IN TXT „txtvers=1“ „[,hcid=1.2.276.0.76.3.1.99](#)“
 349 „,path=/
 350 authz.hrst2.epa.telematik. IN A 10.28.2.26

351 _docv._tcp.epa.telematik. 86400 IN PTR _1-2-276-0-76-3-1-99._docv._tcp.epa.telematik.
 352 _1-2-276-0-76-3-1-99._docv._tcp.epa.telematik. 86400 IN SRV 5 10 443 docv.hrst2.epa.telematik.
 353 _1-2-276-0-76-3-1-99._docv._tcp.epa.telematik. 86400 IN TXT „txtvers=1“ „[,hcid=1.2.276.0.76.3.1.99](#)“
 354 „,path=/
 355 docv.hrst2.epa.telematik. IN A 10.28.2.27

356 _sgd1._tcp.epa.telematik. 86400 IN PTR _1-2-276-0-76-3-1-99._sgd1._tcp.epa.telematik.
 357 _1-2-276-0-76-3-1-99._sgd1._tcp.epa.telematik. 86400 IN SRV 5 10 443 sgd1.hrst2.epa.telematik.
 358 _1-2-276-0-76-3-1-99._sgd1._tcp.epa.telematik. 86400 IN TXT „txtvers=1“ „[,hcid=1.2.276.0.76.3.1.99](#)“
 359 „,path=/
 360 sgd1.hrst2.epa.telematik. IN A 10.28.2.24

A 14128-02A-14128-01 - Anbieter ePA-Aktensystem - Resource Records FQDN ePA

Der Anbieter des ePA-Aktensystems MUSS ~~im Namensraum der TI und~~ in den Nameservern Internet die Resource Records gemäß nachstehender Tabelle verwalten.

Tabelle 2: Tab_ePA_FQDN

Resource Record Type	Beschreibung
A	A Resource Records zur Namensauflösung von FQDN des ePA-Aktensystems des jeweiligen Anbieters in IP-Adressen
TXT	<p>TXT Resource Records zur Ermittlung der Aufruf-Schnittstellen der jeweiligen Module des ePA-Aktensystems. Alle für die Adressierung dieser Module benötigten Resource Records MÜSSEN bereitgestellt werden und deren Zugehörigkeit zum Aktensystem des Anbieters durch Clients (ePA-Modul Frontend des Versicherten, Fachmodul ePA) eindeutig zu erkennen sein. Die in den Klammern angegebenen Kürzel MÜSSEN für das jeweilige Modul verwendet werden.</p> <ul style="list-style-type: none">• HomeCommunityID (hcid)• Authentisierung (authn)• Abfrage Verzeichnisdienst (avzd) - nur im Namensraum Internet• Autorisierung (authz)• Dokumentenverwaltung (docv)• Status-Proxy (ocspf)• Schlüsselgenerierungsdienst SGD 1 (im Aktensystem)• Schlüsselgenerierungsdienst SGD 2 (unabhängig vom Aktensystem) nur im Namensraum Internet <p>Die key/value-Paare der TXT-Records haben folgende Struktur (die spitzen Klammern dienen der Abgrenzung eines Wertes):</p> <pre>"txtvers=1" "hcid=<HomeCommunityID>" "authn=/<pfad_authentisierung>/" "authz=/<pfad_autorisierung>/" "avzd=/<pfad_verzeichnisdienst_proxy>/" "docv=/<pfad_dokumentenverwaltung>/" "ocspf=/<pfad_status_proxy>/" "sgd1=/<pfad_Schlüsselgenerierungsdienst_typ1>/" "sgd2=/<pfad_Schlüsselgenerierungsdienst_typ2>/"</pre>

[<=]

A 17969-03A-17969-02 - Anbieter ePA-Aktensystem - Schnittstellenadressierung

Der Anbieter des ePA-Aktensystems MUSS alle nach außen angebotenen Dienste der Komponenten Autorisierung, Zugangsgateway (Authentisierung) sowie ePA-Dokumentenverwaltung unter den folgenden URLs zur Verfügung stellen und eingehende SOAP-Nachrichten entsprechend verarbeiten:

`https://<FQDN aus DNS Lookup>:443/<Komponente aus DNS Lookup>/<Fester Wert der Schnittstelle gemäß [gemSysL_ePA#4.2]>`

Daraus ergeben sich folgende Konstellationen für den Aufbau von komponentenspezifischen URLs (in spitzen Klammern dargestellte Werte sind dynamisch) für den Aufruf des Aktensystem vom

- ePA-Fachmodul:
 - `https://<FQDN des authn-Dienstes aus DNS Lookup>:443/<authn-Komponente aus DNS Lookup>/I_Authentication_Insurant`
 - `https://<FQDN des authz-Dienstes aus DNS Lookup>:443/<authz-Komponente aus DNS Lookup>/I_Authorization`
 - `https://<FQDN des authz-Dienstes aus DNS Lookup>:443/<authz-Komponente aus DNS Lookup>/I_Authorization_Management`
 - `https://<FQDN des docv-Dienstes aus DNS Lookup>:443/<docv-Komponente aus DNS Lookup>/I_Document_Management`
 - `https://<FQDN des docv-Dienstes aus DNS Lookup>:443/<docv-Komponente aus DNS Lookup>/I_Document_Management_Connect`
- ePA-Fachmodul KTR-Consumer:
 - `https://<FQDN des authz-Dienstes aus DNS Lookup>:443/<authz-Komponente aus DNS Lookup>/I_Authorization`
 - `https://<FQDN des docv-Dienstes aus DNS Lookup>:443/<docv-Komponente aus DNS Lookup>/I_Document_Management_Insurance`
 - `https://<FQDN des docv-Dienstes aus DNS Lookup>:443/<docv-Komponente aus DNS Lookup>/I_Document_Management_Connect`
- ePA-Modul Frontend des Versicherten:
 - `https://<FQDN des ePA-Aktensystems>:443/<authn-Komponente aus DNS Lookup>/I_Authentication_Insurant`
 - `https://<FQDN des ePA-Aktensystems>:443/<avzd-Komponente aus DNS Lookup>/I_Proxy_Directory_Query`
 - `https://<FQDN des ePA-Aktensystems>:443/<authz-Komponente aus DNS Lookup>/I_Authorization_Insurant`
 - `https://<FQDN des ePA-Aktensystems>:443/<authz-Komponente aus DNS Lookup>/I_Authorization_Management_Insurant`
 - `https://<FQDN des ePA-Aktensystems>:443/<docv-Komponente aus DNS Lookup>/I_Document_Management_Insurant`
 - `https://<FQDN des ePA-Aktensystems>:443/<docv-Komponente aus DNS Lookup>/I_Account_Management_Insurant`
 - `https://<FQDN des ePA-Aktensystems>:443/<docv-Komponente aus DNS Lookup>/I_Document_Management_Connect`

- ~~[<=]~~<https://<FQDN des ePA-Aktensystems>:443/<docv-Komponente aus DNS Lookup>/I Key Management Insurant>
- <https://<FQDN des ePA-Aktensystems>:443/<authz-Komponente aus DNS Lookup>/I Authorization Management Insurant>

[<=]

5.2 Protokollierung

Aufgrund der informationstechnischen Trennung der Komponenten des ePA-Aktensystems protokolliert jede Komponente für sich. Hierbei protokollieren das Zugangsgateway des Versicherten (Authentisierung_Vers) und die Komponente Autorisierung jeweils in ein eigenes Verwaltungsprotokoll und die Komponente Dokumentenverwaltung in das § 291a-konforme Protokoll und in ein Verwaltungsprotokoll für den Versicherten bzw. seine Vertreter. Die Komponenten des ePA-Aktensystems protokollieren gemäß der Festlegungen in [A_14471](#) [gemSpec_DM_ePA] und stellen dem ePA-Modul Frontend des Versicherten jeweils eine Schnittstelle für den Abruf der Protokolleinträge zur Verfügung.

5.2.1 Übergreifende Anforderungen zur Protokollierung

A_14513 - Anbieter ePA-Aktensystem - Schutz der Protokolldaten

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die Verwaltungsprotokolldaten und die Daten der Zugriffsprotokolle nach § 291a SGB V der Versicherten gegen Veränderung und unberechtigtes Löschen geschützt sind. [<=]

A_14512 - Anbieter ePA-Aktensystem - Anbieterkennung im Protokolleintrag für Verwaltungsprotokoll

Der Anbieter des ePA-Aktensystems MUSS Einträge des Verwaltungsprotokolls um seine HomeCommunityID sowie um seinen Namen, mit dem er gegenüber den Versicherten auftritt, gemäß den Festlegungen in [A_14471](#) ergänzen. [<=]

A_15141 - Anbieter ePA-Aktensystem - Verwaltungsprotokolle zur Problemlösung mit Zustimmung des Versicherten

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass ein Zugriff auf Verwaltungsprotokolle des Versicherten in den Komponenten des ePA-Aktensystems durch den Anbieter ausgeschlossen ist, außer für den Fall, dass die Zugriffe zur Lösung eines durch den Versicherten gemeldeten Problems erforderlich sind und der Versicherte dem Zugriff explizit zugestimmt hat. [<=]

A_19051 - Löschen von Protokolldaten

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass das ePA-Aktensystem die zum Zwecke der Datenschutzkontrolle für den Versicherten erstellten Verwaltungsprotokolldaten und Protokolldaten von Zugriffen und Zugriffsversuchen auf Daten der elektronischen Patientenakte des Versicherten in der Komponente Dokumentenverwaltung nicht früher als nach drei Jahren löscht. Nach dieser Frist MUSS unverzüglich eine automatisierte Löschung durch das ePA-Aktensystem erfolgen. [<=]

5.2.2 Internes Fehlerprotokoll

Um erwartete und unbeabsichtigte Abweichungen in der Bearbeitung von Operationsaufrufen nachvollziehen zu können, benötigt ein Administrator des ePA-Aktensystems geeignete Anhaltspunkte für die Fehlersuche. Hierfür ist ein Verlaufsprotokoll eine geeignete Lösung.

A_15064 - ePA-Aktensystem - Debugprotokoll

Die Komponenten des ePA-Aktensystems KÖNNEN im Testbetrieb ein Debug-Protokoll schreiben, welches eine erweiterte Protokollierung für Testzwecke ermöglicht.
[<=]

Hinweis: Die Anforderung A_15064 beschränkt den Debug-Modus auf Testzwecke. Im Produktivbetrieb ist der Debug-Modus nicht zulässig.

A_15065 - ePA-Aktensystem - Verlaufsprotokoll

Die Komponenten des ePA-Aktensystems, mit Ausnahme der VAU der Komponente ePA-Dokumentenverwaltung, MÜSSEN ein Verlaufsprotokoll schreiben, das geeignet ist, die aufgerufenen Operationen und internen Abläufe der Komponente nachzuvollziehen. Die Komponente MUSS im Verlaufsprotokoll Einträge mit folgendem Inhalt erfassen:
[Vorgangsbezeichner, Datum und Uhrzeit des Beginns des Vorgangs, Ergebnis des Vorgangs z.B. Erfolg/Misserfolg].
[<=]

A_15066 - ePA-Aktensystem - Zugriff auf Verlaufs- und Debugprotokoll

Die Komponenten des ePA-Aktensystems MÜSSEN den Zugriff auf Protokolldateien auf autorisierte Nutzer beschränken.
[<=]

A_15067 - ePA-Aktensystem - Personenbezug im Verlaufs- und Debugprotokoll

Die Komponenten des ePA-Aktensystems DÜRFEN personenbezogene Informationen, medizinische Informationen und kryptografisches Schlüsselmaterial NICHT protokollieren.[<=]

5.3 Fehlermeldungen

A_15185 - ePA-Aktensystem - Festlegungen für Fehlermeldungen auf Basis TelematikError.xsd

Die Komponenten des ePA-Aktensystems MÜSSEN für Fehlermeldungen, die auf dem XML-Schema [TelematikError.xsd] basieren, die unten aufgeführten Elemente wie folgt belegen:

- EventID = Spalte Name aus den Fehlertabellen der Operationen in den Spezifikationen der Komponenten des ePA-Aktensystems
- CompType = „AktensystemEPA“
- Code = Spalte Code aus den Fehlertabellen der Operationen in den Spezifikationen der Komponenten des ePA-Aktensystems
- ErrorText = Spalte Fehlertext aus den Fehlertabellen der Operationen in den Spezifikationen der Komponenten des ePA-Aktensystems
- ErrorType = „Business“
- Severity = „Error“

- Detail = Spalte Detail aus den Fehlertabellen der Operationen in den Spezifikationen der Komponenten des ePA-Aktensystems

Für alle übrigen Elemente gelten die Festlegungen aus [gemSpec_OM].[<=]

5.4 Redundanz

Die Anforderungen zur Verfügbarkeit ergeben sich aus [gemSpec_Perf]. Die Verfügbarkeit wird hergestellt durch Anzahl, Verteilung und Konfiguration der Komponenten des ePA-Aktensystems. In diesem Dokument werden zusätzliche Redundanzanforderungen spezifiziert, wenn die Anforderungen in [gemSpec_Perf] zur Verfügbarkeit nicht ausreichen.

Die Auswahl der Komponenten des ePA-Aktensystems wird durch die Konnektoren aus einer durch DNS übermittelten Liste vorgenommen. Auf die Auswahl der Komponenten des ePA-Aktensystems durch den Konnektor kann der Anbieter der Komponenten des ePA-Aktensystems durch die Konfiguration und Anpassung der DNS-Einträge Einfluss nehmen. Die Verfügbarkeit ist hergestellt, wenn jeder Konnektor die Möglichkeit hat, die Komponenten des ePA-Aktensystems zu erreichen. Von der Versichertenseite aus erfolgt der Zugriff auf die Komponenten des ePA-Aktensystems durch das ePA-Modul Frontend des Versicherten über das Zugangsgateway.

Eine hardwaretechnische Hochverfügbarkeit der einzelnen Komponenten des ePA-Aktensystems 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 jede einzelne Komponente des ePA-Aktensystems im Ergebnis eine höhere Verfügbarkeit oder Leistungsfähigkeit besitzt.

A_14921 - Anbieter ePA-Aktensystem - lokale Redundanz im Standort des ePA-Aktensystems

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass bei Ausfall einer oder mehrerer Komponenten des ePA-Aktensystems die verbleibenden Komponenten des ePA-Aktensystems in demselben Standort den Datenverkehr aller Clients der ausgefallenen Komponente zusätzlich übernehmen, die Konsistenz der persistenten Daten erhalten bleibt und die Verfügbarkeit der Komponenten gemäß den geforderten SLAs in [gemSpec_Perf] weiterhin gegeben ist.[<=]

A_14922 - Anbieter ePA-Aktensystem - standortübergreifende Redundanz der Komponenten des ePA-Aktensystems

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass bei Ausfall eines Rechenzentrums ein anderes Rechenzentrum an einem gemäß [BSI-Redundanz] entfernten Standort den Datenverkehr des ausgefallenen Standortes übernehmen kann.[<=]

A_15245 - Anbieter ePA-Aktensystem - standortübergreifende Redundanz und Verfügbarkeit

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass bei Ausfall eines Standorts (Rechenzentrum) die Konsistenz der persistenten Daten erhalten bleibt und die Verfügbarkeit der Komponenten gemäß der geforderten SLAs in [gemSpec_Perf] gegeben ist.[<=]

5.5 Sichere Produktentwicklung

Um ein sicheres Produkt zu entwickeln, muss der Anbieter die Sicherheits- und Datenschutzanforderungen während der Produktentwicklung berücksichtigen.

A_15151 - Anbieter ePA-Aktensystem - Implementierungsspezifische Sicherheitsanforderungen

Der Anbieter des ePA-Aktensystems MUSS während der Entwicklung des ePA-Aktensystems implementierungsspezifische Sicherheitsanforderungen dokumentieren und umsetzen. [<=]

A_15146 - Anbieter ePA-Aktensystem - Verwendung eines sicheren Entwicklungsprozesses

Der Anbieter des ePA-Aktensystems MUSS während der Entwicklung des ePA-Aktensystems einen sicheren Entwicklungsprozess verwenden. [<=]

Hinweis: es gibt mehrere Möglichkeiten, um einen sicheren Entwicklungsprozess (Englisch: Security Development Lifecycle) zu implementieren. Ein Beispiel von einem sicheren Entwicklungsprozess ist der Microsoft Security Development Lifecycle.

A_15147 - Anbieter ePA-Aktensystem - Sicherheitsrelevantes Softwarearchitektur-Review

Der Anbieter des ePA-Aktensystems MUSS ein sicherheitsrelevantes Software- und Sicherheitsarchitektur-Review durchführen und identifizierte Architekturschwachstellen beheben. [<=]

A_15148 - Anbieter ePA-Aktensystem - Durchführung einer Bedrohungsanalyse

Der Anbieter des ePA-Aktensystems MUSS eine Bedrohungsanalyse durchführen und Maßnahmen gegen die identifizierten Bedrohungen implementieren. [<=]

A_15149 - Anbieter ePA-Aktensystem - Durchführung regelmäßiger sicherheitsrelevanter Quellcode-Reviews

Der Anbieter des ePA-Aktensystems MUSS während der Entwicklung des ePA-Aktensystems regelmäßige sicherheitsrelevante Quellcode-Reviews oder automatisierte sicherheitsrelevante Quellcode-Scans durchführen und alle identifizierten kritischen Schwachstellen der Stufen "medium" oder "hoch" beheben. [<=]

A_15150 - Anbieter ePA-Aktensystem - Durchführung regelmäßiger Sicherheitstests

Der Anbieter des ePA-Aktensystems MUSS während der Entwicklung des ePA-Aktensystems regelmäßige automatisierte Sicherheitstests durchführen und alle identifizierten kritischen Schwachstellen der Stufen "medium" oder "hoch" beheben. [<=]

A_15152 - Anbieter ePA-Aktensystem - Sicherheitsschulung für Entwickler

Der Anbieter des ePA-Aktensystems MUSS alle Entwickler des ePA-Aktensystems in sicherer Entwicklung und Secure Coding-Techniken schulen. [<=]

5.6 Datenschutz und Sicherheit

A_15128 - Anbieter ePA-Aktensystem - Schutz der transportierten Daten im ePA-Aktensystem

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die Vertraulichkeit und Integrität der innerhalb des ePA-Aktensystems transportierten Daten gewährleistet ist. [<=]

587 Hinweis: Hierzu gehören insbesondere die Kommunikation zwischen der Komponente
588 Zugangsgateway und der Komponente Autorisierung, zwischen der Komponente
589 Zugangsgateway und der Komponente Dokumentenverwaltung sowie zwischen dem
590 Aktenkontenmanagement (inkl. Vertragsdatenmanagement) mit den Komponenten des
591 ePA-Aktensystems.

592 Die folgenden Anforderungen verhindern Profilbildungen über Versicherte und
593 Leistungserbringer(-institutionen) durch den Anbieter bzw. dessen Mitarbeiter.

594 **A_15103 - Anbieter ePA-Aktensystem - Konzept zur Verhinderung von** 595 **Profilbildung**

596 Der Anbieter des ePA-Aktensystems MUSS ein Konzept erstellen und umsetzen, dass
597 sicherstellt, dass Mitarbeiter des Anbieters die im ePA-Aktensystem verarbeiteten Daten
598 nicht für Profilbildungen über Versicherte oder Leistungserbringer(-institutionen) nutzen
599 können. [<=]

600 Hinweis: Das Konzept kann Teil des Sicherheits- oder Datenschutzkonzeptes des
601 Anbieters sein. Es ist nicht notwendigerweise ein eigenes Dokument erforderlich.

602 **A_15104 - Anbieter ePA-Aktensystem - Ordnungsgemäße IT-Administration**

603 Der Anbieter des ePA-Aktensystems MUSS die Maßnahmen für erhöhten Schutzbedarf
604 des BSI-Bausteins „OPS.1.1.2 Ordnungsgemäße IT-Administration“ [BSI-Grundsatz]
605 während des gesamten Betriebs des ePA-Aktensystems umsetzen. [<=]

606 Hinweis: Die Anforderungen des BSI-Bausteins sind entsprechend des dort genannten
607 Schlüsselwortes („MUSS, DARF NICHT/ DARF KEIN, SOLLTE; SOLLTE NICHT/SOLLTE
608 KEIN, KANN/DARF“) umzusetzen.

609 **A_15824 - Anbieter ePA-Aktensystem - Sichere Speicherung von Daten**

610 Unabhängig davon, ob die Daten schon verschlüsselt vorliegen, MUSS der Anbieter des
611 ePA-Aktensystems die Daten des ePA-Aktensystems bei der Speicherung
612 verschlüsseln. [<=]

613 Hinweis: Dies kann z.B. durch eine transparente Datenbankverschlüsselung oder eine
614 Festplattenverschlüsselung erfolgen.

615 **A_15105 - Anbieter ePA-Aktensystem - Zwei-Faktor-Authentisierung von** 616 **Administratoren**

617 Der Anbieter des ePA-Aktensystems SOLL sicherstellen, dass sich Administratoren
618 mindestens mit einer Zwei-Faktor-Authentisierung anmelden.
619 Eine Zwei-Faktor-Authentisierung ist nur zwingend notwendig, wenn die Administratoren
620 einen Zugriff auf Daten haben, die zur Profilbildung missbraucht werden könnten. Dies ist
621 z. B. bei der Komponente Autorisierung (Profile anhand der Berechtigungen) oder den
622 Komponenten zur Authentifizierung der Fall. [<=]

623

624 **A_15107 - Anbieter ePA-Aktensystem - Keine unzulässige Weitergabe von** 625 **Daten**

626 Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die in seinem Aktensystem
627 verarbeiteten Daten, außer an berechtigte Nutzer der Aktenkonten oder an den vom
628 Versicherten gewählten Anbieter beim Anbieterwechsel, nicht weitergegeben werden,
629 auch nicht in pseudonymisierter oder anonymisierter Form. [<=]

630 **A_15109 - Anbieter ePA-Aktensystem - Unterschiedliche Mitarbeiter für** 631 **Vertragsverwaltung und ePA-Aktensystem**

632 Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die Mitarbeiter, die die
633 Vertragsdaten verarbeiten, andere sind als jene mit Zugriff auf die Komponenten
634 Autorisierung, Authentisierung, Zugangsgateway und Dokumentenverwaltung. [<=]

A_15119 - Anbieter ePA-Aktensystem - Löschkonzept

Der Anbieter des ePA-Aktensystems MUSS in einem Löschkonzept für die im ePA-Aktensystem verarbeiteten personenbezogenen Daten mindestens folgende Aspekte beschreiben:

- die umgesetzten organisatorischen und technischen Löschmaßnahmen (dies beinhaltet insbesondere auch die Löschung von Backups, Protokollen etc.),
- die Löschregeln und Löschrufen zusammen mit einer nachvollziehbaren Begründung für die getroffenen Fristfestlegungen,
- wie sichergestellt wird, dass alle Auftragnehmer die Löschpflichten ihrerseits umsetzen.

[<=]

Hinweis: Das Löschkonzept kann Teil des Sicherheits- oder Datenschutzkonzeptes des Anbieters sein. Es ist nicht notwendigerweise ein eigenes Dokument erforderlich.

A_15125 - Anbieter ePA-Aktensystem - Information des Versicherten zur Wahrnehmung der Betroffenenrechte bei der Aktenkontoeröffnung

Der Anbieter des ePA-Aktensystems MUSS Versicherte bei der Aktenkontoeröffnung in einfacher und verständlicher Form darüber informieren, wie sie ihre Betroffenenrechte nach DSGVO in Verbindung mit BDSG gegenüber dem Anbieter wahrnehmen können, insbesondere auch, an welche datenschutzrechtliche Aufsichtsbehörde sie sich bei Datenschutzbeschwerden bzgl. des Anbieters wenden müssen. [<=]

A_15126 - Anbieter ePA-Aktensystem - Ausreichende Informationen für eine informierte Einwilligung bei der Aktenkontoeröffnung

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass den Versicherten bei der Aktenkontoeröffnung Informationen zum ePA-Aktensystem in allgemein verständlicher Form bereitgestellt werden, die für eine informierte Einwilligung notwendig sind; neben den Informationen gemäß Art. 13 DSGVO sind dies insbesondere die Funktionsweise der ePA und die wesentlichen Datenschutz- und Sicherheitsmaßnahmen. [<=]

A_17075 - Anbieter ePA-Aktensystem - Information über Verwendung zugelassener ePA-Module Frontend des Versicherten

Der Anbieter des ePA-Aktensystems MUSS den Versicherten mindestens im Rahmen der Einwilligung empfehlen, das Aktensystem nur mit einem zugelassenen ePA-Modulen FdV zu benutzen und den Versicherten informieren, wo er diese ePA-Module FdV beziehen kann. [<=]

A_15127 - Anbieter ePA-Aktensystem - Information der Versicherten und Leistungserbringer zur Wahrnehmung der Betroffenenrechte während der Aktennutzung

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass sich Versicherte und Leistungserbringer jederzeit in einfacher Weise beim Anbieter darüber informieren können, wie sie ihre Betroffenenrechte nach DSGVO in Verbindung mit BDSG gegenüber dem Anbieter wahrnehmen können. [<=]

A_15169 - ePA-Aktensystem - Verbot von Werbe- und Usability-Tracking

Die Komponenten des ePA-Aktensystems DÜRFEN im Produktivbetrieb ein Werbe- und Usability-Tracking NICHT verwenden.

Davon ausgenommen ist das Erfassen des standardmäßigen quantitativen Nutzerverhaltens zur Ermittlung der Standard-Aktennutzung entsprechend der Anforderung A_15154. [<=]

A_15154 - Anbieter ePA-Aktensystem - Ermittlung von Standard-Aktenutzung

Der Anbieter des ePA-Aktensystems MUSS mindestens einmal im Jahr Werte zu einer Standard-Aktenutzung von LE und Versicherten durch die Profilierung anonymer Zugriffsstatistiken auf das ePA-Aktensystem zum Zweck der Erkennung von Zugriffen gemäß A_15155 ermitteln. [<=]

A_15155 - Anbieter ePA-Aktensystem - Abweichung von Standard-Aktenutzung

Der Anbieter des ePA-Aktensystems MUSS Zugriffe und Zugriffsmuster, die nicht einer Standard-Aktenutzung entsprechen, erkennen und Maßnahmen zur Schadensreduzierung umsetzen. [<=]

A_15156 - Anbieter ePA-Aktensystem - Einsatz zertifizierter HSM

Der Anbieter des ePA-Aktensystems MUSS beim Einsatz eines HSM sicherstellen, dass dessen Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als Evaluierungsschemata kommen dabei Common Criteria, ITSEC oder Federal Information Processing Standard (FIPS) in Frage.

Die Prüftiefe MUSS mindestens

1. FIPS 140-2 Level 3,
2. Common Criteria EAL 4+ mit hohem Angriffspotenzial oder
3. ITSEC E3 der Stärke „hoch“ entsprechen.

[<=]

A_15157 - Anbieter ePA-Aktensystem - Sicherer Betrieb und Nutzung eines HSMs

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die auf dem HSM verarbeiteten privaten Schlüssel, Konfigurationen und eingesetzte Software nicht unautorisiert ausgelesen, unautorisiert verändert, unautorisiert ersetzt oder in anderer Weise unautorisiert benutzt werden können. [<=]

A_15158 - Anbieter ePA-Aktensystem - Informationstechnische Trennung

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass nicht miteinander kommunizierende Komponenten des ePA-Aktensystems informationstechnisch voneinander getrennt sind. [<=]

Hinweis: Komponenten des ePA-Aktensystems bezieht sich auf die Komponenten, die die gematik spezifiziert, sowie anbieterspezifische Komponenten, die die gematik nicht spezifiziert. Dieser Hinweis gilt für alle übergreifenden Sicherheits- und Datenschutzanforderungen.

A_15159 - Anbieter ePA-Aktensystem - Schutzmaßnahmen gegen die OWASP Top 10 Risiken

Der Anbieter des ePA-Aktensystems MUSS in allen Komponenten des ePA-Aktensystems technische Maßnahmen zum Schutz vor den in der aktuellen Version genannten OWASP-Top-10-Risiken umsetzen. [<=]

A_15160-01A_15160 - Anbieter ePA-Aktensystem - Zusätzliche Autorisierung von sensiblen Anwendungsfällen

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass für folgendeden Beginn der folgenden Anwendungsfälle eine nochmalige Authentifizierung erfolgt, wenn die letzte Authentifizierung mehr als 10 Minuten zurück liegt.

- Vertragsdaten ändern
- Aktenkonto schließen
- Geräte verwalten

- [Umschlüsselung \(Operation startKeyChange an der Autorisierung\).](#)

[<=]

A_15823 - Anbieter ePA-Aktensystem – Versicherte über sensible Änderungen informieren.

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass der Versicherte über Änderungen in den folgenden Anwendungsfällen informiert wird,

- Vertragsdaten ändern
- Aktenkonto schließen
- Geräte verwalten

und wenn der Anbieter des Aktensystems eine manuelle Änderung in einer Akte im Auftrag eines Versicherten durchführt.

[<=]

Hinweis: Dies kann z.B. durch eine Notifikations-E-Mail an dem Versicherter erfolgen. Solche E-Mails dürfen keine Details über die Änderungen beschreiben, sondern nur einen Hinweis geben, dass eine Änderung gemacht wurde und dass der Versicherte die Änderungen in seinem Aktenkonto prüfen sollte.

A_15163 - Anbieter ePA-Aktensystem - Angriffen entgegenwirken

Der Anbieter des ePA-Aktensystems MUSS Maßnahmen zur Erkennung von Angriffen und zur Reduzierung bzw. Verhinderung von Schäden aufgrund von Angriffen in allen Komponenten des ePA-Aktensystems umsetzen.

[<=]

A_15167 - Anbieter ePA-Aktensystem - Social Engineering Angriffen entgegenwirken

Der Anbieter des ePA-Aktensystems MUSS Maßnahmen zur Erkennung und Verhinderung von Social Engineering Angriffen umsetzen. [<=]

A_15168 - ePA-Aktensystem - Verbot vom dynamischen Inhalt

Die Komponenten des ePA-Aktensystems DÜRFEN dynamischen Inhalt von Drittanbietern NICHT herunterladen und verwenden.

[<=]

A_17080 - Verhindern von Session Hijacking

Die Komponenten des ePA-Aktensystems MÜSSEN geeignete Schutzmaßnahmen gegen Session-Hijacking implementieren.

[<=]

A_16322 - ePA-Aktensystem - Verbot von illegalem Inhalt

Der Anbieter des ePA-Aktensystems MUSS der Ablage von Dokumenten mit illegalen Inhalten mittels AGB auf Anbieterseite entgegenwirken. [<=]

A_16323 - ePA-Aktensystem - Verbot von medizinisch irrelevantem Inhalt

Der Anbieter des ePA-Aktensystems MUSS der Ablage von Dokumenten, die für die medizinische Versorgung oder für die Eigenorganisation medizinischer Belange des Versicherten irrelevant sind, mittels AGB auf Anbieterseite entgegenwirken.

[<=]

A_18954 - Sicherer Betrieb des Produkts nach Handbuch

Der Anbieter eines ePA-Aktensystems MUSS die im Handbuch des eingesetzten ePA-Aktensystems und des eingesetzten Schlüsselgenerierungsdiensts beschriebenen Voraussetzungen für den sicheren Betrieb des Produktes gewährleisten. [<=]

A_18953 - Darstellen der Voraussetzungen für sicheren Betrieb des Produkts im Handbuch

Der Hersteller des ePA-Aktensystems MUSS für sein Produkt im dazugehörigen Handbuch leicht ersichtlich darstellen, welche Voraussetzungen vom Betreiber und der Betriebsumgebung erfüllt werden müssen, damit ein sicherer Betrieb des Produktes gewährleistet werden kann. [≤]

A_19118 - Komponenten des Aktensystems, Schutz vor XSW-Angriffen

Die Komponenten des ePA-Aktensystems, die XML-Signaturen -- insbesondere Signaturen von SAML-Token -- prüfen, MÜSSEN geeignete Maßnahmen gegen XSW-Angriffe umsetzen. Mindestens MÜSSEN sie die FastXPath-Auswertung der XML-Daten und XML-Signaturen gemäß [GJLS-2009] (vgl. auch [BSI-XSpRES]) umsetzen (vgl. „Hinweise zu A_19118“). [≤]

Hinweise zu A_19118:

Aufgrund der hohen Flexibilität und damit der Komplexität der Auswertung und Verarbeitung von XML-signierten Daten, ist dort eine sichere Implementierung eine besondere Herausforderung. Die Authentisierungs- und Autorisierungstoken innerhalb des Aktensystems basieren auf SAML2.0, das ein spezielles XML-Format inkl. XML-Signaturen definiert. Bei Implementierungen dieses Standards gab es bereits erfolgreiche Angriffe [SHJSGI-2011].

In den Anwendungsfällen der Token innerhalb des ePA-Aktensystems treten nicht die Problemfälle aus [BSI-XSpRES#6.1] auf.

A_19122 - Anbieter ePA-Aktensystem – Trennung zu anderen Mandanten

Falls ein Anbieter eines ePA-Aktensystems einen Betreiber eines ePA-Aktensystem beauftragt, MUSS der Anbieter des ePA-Aktensystems sicherstellen, dass seine Daten von anderen Mandanten des Betreibers des ePA-Aktensystems organisatorisch und technisch getrennt sind. [≤]

5.7 Evidenzbasiertes Monitoring

Die Architektur des ePA-Aktensystems verhindert eine Einsichtnahme des Betreibers in Daten von Versicherten. Ebenso ist ein Monitoring der Verfügbarkeit der Schnittstellen und Operationen der Komponente Dokumentenverwaltung aufgrund der verschlüsselten Kommunikation mit Clientsystemen erschwert. Mit der Anlage eines Prüfkontos für eine Prüfidentität kann die korrekte Funktionsweise durch Simulation eines Clientsystems überwacht werden. Die folgenden Anforderungen richten sich an den Betreiber eines Aktensystems, um den korrekten Umgang mit Prüfidentitäten der Telematikinfrastruktur sicherzustellen.

A_18168 - Anbieter des ePA-Aktensystem - Aktenkonto für gematik

Der Anbieter des ePA-Aktensystems MUSS der gematik zur Messung der Verfügbarkeit die Eröffnung und Nutzung eines Aktenkontos für eine Prüfidentität gemäß [gemSpec_PK_eGK] ermöglichen und dabei die Besonderheiten der IK-Nummer und Versichertennummer der Prüfidentität beachten. Die gematik wird mit diesem Aktenkonto folgende Anwendungsfälle durchführen:

- Login durch einen Versicherten
- Logout durch einen Nutzer
- Dokumente durch einen Versicherten einstellen
- Dokumente durch einen Versicherten löschen
- Dokumente durch einen Versicherten anzeigen

[<=]

A_18169 - Anbieter des ePA-Aktensystem - Aktenkonto für eigene Zwecke der Betriebsüberwachung

Der Anbieter des ePA-Aktensystems KANN für eigene Zwecke seiner Betriebsüberwachung ein Aktenkonto für eine Prüfidentität gemäß [gemSpec_PK_eGK] einrichten.[<=]

A_18170 - Anbieter des ePA-Aktensystem – eingeschränkte Anwendungsfälle für Prüfidentitäten

Falls der Anbieter des ePA-Aktensystems ein Aktenkonto für eigene Zwecke eingerichtet hat, MUSS er sicherstellen, dass für das Aktenkonto seiner Prüfidentität gemäß [gemSpec_PK_eGK] ausschließlich folgende Anwendungsfälle gemäß [gemSysL_ePA] ausgeführt werden können:

- Login durch einen Versicherten
- Logout durch einen Nutzer
- Dokumente durch einen Versicherten einstellen
- Dokumente durch einen Versicherten löschen
- Dokumente durch einen Versicherten anzeigen

[<=]

Hinweis: Hiermit sollen insbesondere die Anwendungsfälle zur Berechtigungsvergabe durch Versicherte ausgeschlossen werden.

5.8 Registrierung von KTR-AdV Terminals

~~Der Zugriff auf das ePA-Aktenkonto eines Versicherten mittels KTR-AdV-Terminal erfolgt über das zum ePA-Aktensystem gehörende Zugangsgateway. Ein Zugriff über das Zugangsgateway des ePA-Aktensystems ist nur mit einem Gerät möglich, das durch den Versicherten registriert wurde. Für die Freischaltung des Gerätes wird hierzu eine E-Mail an den Versicherten gesendet, die dieser bestätigen muss. Da das KTR-AdV-Terminal jedoch insbesondere von Nutzern ohne eigene IT genutzt werden können soll, ist auf Wunsch des Versicherten eine Registrierung des KTR-AdV-Terminals erforderlich, die ohne eigene IT möglich ist.~~

~~**A_19964 – ePA-Aktensystem: Registrierungsprozess für KTR-AdV-Terminals**~~

~~Der Anbieter des ePA-Aktensystems MUSS einen Registrierungsprozess für KTR-AdV-Terminals bereitstellen, um die Geräteidentitäten von KTR-AdV-Terminals im Aktenkonto von Versicherten hinzuzufügen.[<=]~~

~~**A_19965 – ePA-Aktensystem: Registrierung von KTR-AdV-Terminals nur auf Verlangen des Versicherten**~~

~~Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass~~

- ~~1. der Versicherte, wenn er den Zugriff über ein KTR-AdV-Terminal beim Anbieter beantragt, angemessen identifiziert wird,–~~
- ~~2. KTR-AdV-Terminals nur auf Verlangen des Versicherten und~~
- ~~3. nur genau die vom Versicherten verlangten KTR-AdV-Terminals–~~

~~im Aktenkonto des Versicherten registriert werden.[<=]~~

~~A_19966—ePA-Aktensystem: Deregistrierungsprozess für KTR-AdV-Terminals~~

~~Der Anbieter des ePA-Aktensystems MUSS einen Deregistrierungsprozess für KTR-AdV-Terminals bereitstellen, um auf Verlangen des Versicherten die Geräteidentitäten von KTR-AdV-Terminals im Aktenkonto von Versicherten zu entfernen. [<=]~~

~~Hinweis: Versicherten könnte auch die Möglichkeit gegeben werden, ein KTR-AdV-Terminal direkt am KTR-AdV-Terminal eigenständig zu deregistrieren.~~

~~A_19972—ePA-Aktensystem: Sperren von KTR-AdV-Terminals~~

~~Der Anbieter des ePA-Aktensystems MUSS einen Prozess zum Sperren eines KTR-AdV-Terminals umsetzen, so dass gesperrte KTR-AdV-Terminals nicht mehr erfolgreich auf das ePA-Aktensystem zugreifen können. [<=]~~

~~A_19973—ePA-Aktensystem: Gründe zum Sperren von KTR-AdV-Terminals~~

~~Der Anbieter des ePA-Aktensystems MUSS KTR-AdV-Terminals unverzüglich sperren, falls a) die Zulassungsgrundlage entfallen ist (insbesondere bei ausnutzbaren Schwachstellen) oder b) bei Diebstahl. [<=]~~

~~A_19967—ePA-Aktensystem: Kenntnis der Geräteidentität nur durch Betreiber~~

~~Das ePA-Aktensystem MUSS technisch sicherstellen, dass die Geräteidentitäten von KTR-AdV-Terminals ausschließlich dem Betreiber des ePA-Aktensystems bekannt sein können. [<=]~~

~~Hinweis: Die Anforderung schließt insbesondere auch die Kenntnisnahme der Geräteidentität durch den Anbieter des ePA-Aktensystems aus.~~

6 Funktionsmerkmale

6.1 Aktenkontomanagement

6.1.1 Kontoverwaltung und Zustandswechsel

Das Aktenkonto eines Versicherten wird bei einem Anbieter in verschiedenen Zuständen geführt. Die folgende Abbildung zeigt die möglichen Zustände eines Kontos mit den entsprechenden Zustandsübergängen.

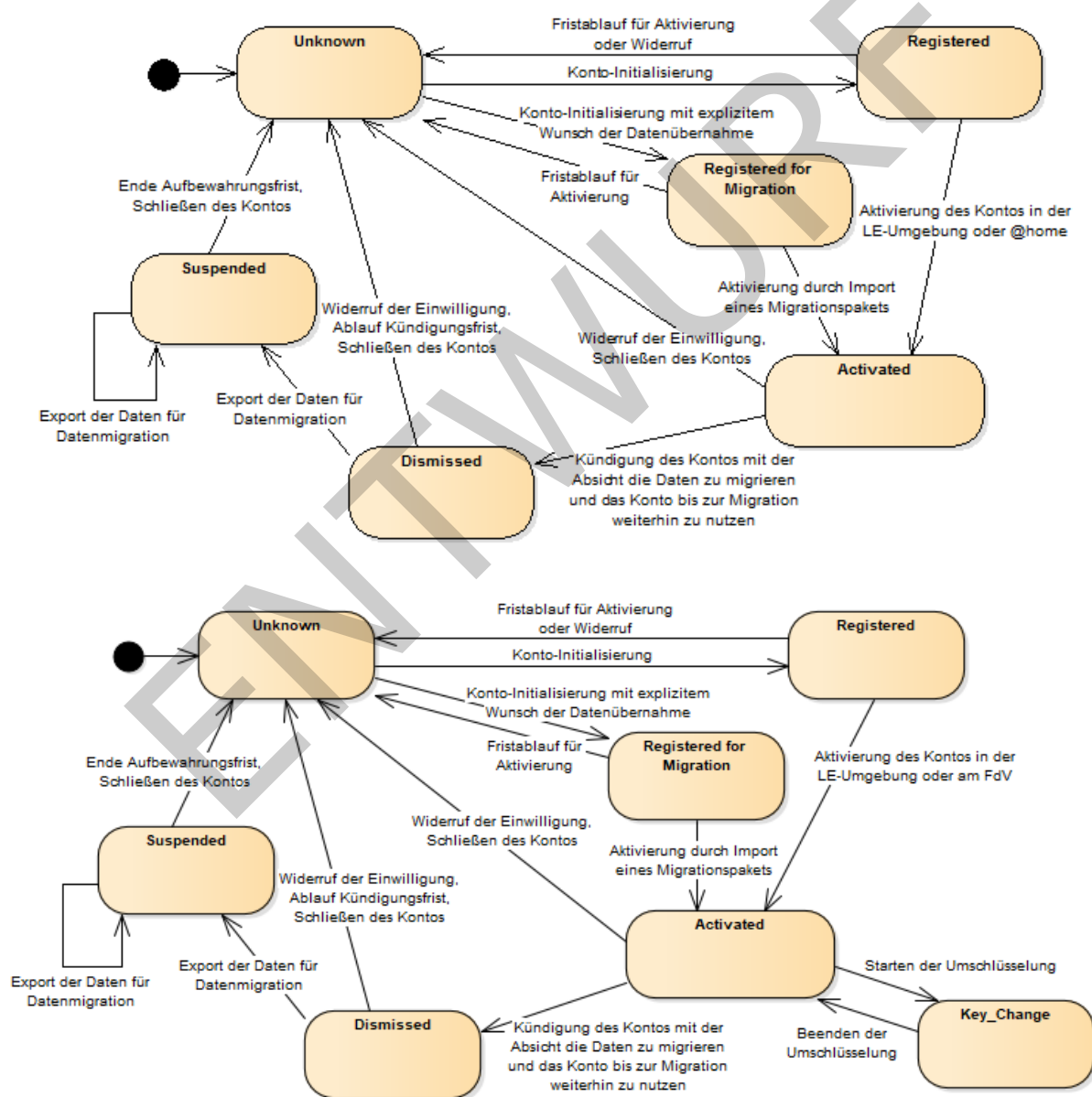


Abbildung 3: Zustandsdiagramm zum Lebenszyklus einer Akte bei einem Anbieter

891 Die Akte eines Versicherten durchläuft bei einem Anbieter maximal sechs verschiedene
 892 Zustände. Die folgende Tabelle listet die in jedem Zustand zulässigen Transitionen mit
 893 den entsprechenden Folgezuständen.

894

895 **Tabelle 3: Zustandswechsel im Lebenszyklus einer Akte**

Zustand	Erläuterung	zulässige Transitionen	Folgezustand
Unknown	Der Versicherte ist unbekannt, es existiert für diesen kein Konto (mehr).	Konto initialisieren	Registered
Registered	Das Konto wurde beantragt und initialisiert, es können aber noch keine medizinischen Dokumente gespeichert werden.	Fristablauf für Aktivierung oder Widerruf der Einwilligung in ePA oder in die Datenverarbeitung durch den Anbieter	Unknown
		Aktivierung des Kontos durch den Versicherten in seiner Umgebung oder in der LE-Umgebung	Activated
Registered for Migration	Das Konto wurde beantragt und initialisiert, es können aber noch keine medizinischen Dokumente gespeichert werden.	Fristablauf für Aktivierung oder Widerruf der Einwilligung in ePA oder in die Datenverarbeitung durch den Anbieter	Unknown
		Aktivierung des Kontos durch den Import eines Migrationspaketes von einem alten Anbieter	Activated
Activated	Das Konto ist aktiv und kann von Berechtigten genutzt werden.	Kündigung des Kontos durch den Versicherten mit der Absicht, die Daten zu einem neuen Anbieter zu migrieren	Dismissed
		Schließen des Kontos auf Wunsch des Versicherten oder Widerruf der Einwilligung in ePA oder in die Datenverarbeitung durch den Anbieter	Unknown
		Umschlüsselung auf Wunsch des Versicherten	Key Change
Dismissed	Das Konto wurde beim Anbieter gekündigt,	Erstellung eines Migrationspaketes (Export der	Suspended

	kann aber weiterhin genutzt werden bis zum Ende einer möglichen Kündigungsfrist oder Start der Migration der Daten des Versicherten.	Daten) für die Migration zu einem anderen Anbieter	
		Ablauf einer Kündigungsfrist oder Schließen des Kontos auf Wunsch des Versicherten oder Widerruf der Einwilligung in ePA oder in die Datenverarbeitung durch den Anbieter	Unknown
Suspended	Die Daten des Kontos des Versicherten wurden exportiert, um sie zu einem neuen Anbieter zu migrieren. Beim alten Anbieter kann auf das Konto nur noch lesend zugegriffen werden.	Schließen des Kontos auf Wunsch des Versicherten oder Widerruf der Einwilligung in ePA oder in die Datenverarbeitung durch den Anbieter	Unknown
		Erstellung eines Migrationspaketes (Export der Daten) für die Migration zu einem anderen Anbieter	Suspended
<u>Key_Change</u>	<u>Für das Konto wird eine Umschlüsselung vorgenommen. Während der Umschlüsselung sind alle Operationen verboten, die nicht explizit im Rahmen der Umschlüsselung erlaubt sind.</u>	<u>Wenn die Umschlüsselung abgebrochen oder beendet wird, geht die Akte wieder in den Zustand "Activated" über.</u>	<u>Activated</u>

896

897 Die folgenden Anforderungen legen die zulässigen Zustandswechsel eines Kontos fest.
 898 Soweit nur der "Wunsch des Versicherten" als auslösendes Ereignis genannt wird, ist die
 899 Willensbekundung des Versicherten auf elektronischem, postalischem oder einem
 900 anderem geeigneten Weg gemeint.

901 **A_15037 - Anbieter ePA-Aktensystem - Status Konto initialisieren**

902 Der Anbieter des ePA-Aktensystems MUSS beim Initialisieren (Beantragen) des Kontos
 903 durch den Versicherten einen Datensatz KeyChain in der Komponente Autorisierung
 904 anlegen mit dem Status entweder `RecordState = REGISTERED_FOR_MIGRATION` wenn der
 905 Versicherte eine Datenübernahme von einem bestehenden, gekündigten Konto wünscht
 906 oder `RecordState = REGISTERED` wenn er dies nicht wünscht oder bisher kein Konto
 907 besaß. [\leq]

908 **A_15038 - Anbieter ePA-Aktensystem - Initialisiertes Konto löschen**

909 Der Anbieter des ePA-Aktensystems MUSS ein initialisiertes Konto (`RecordState =`
 910 `REGISTERED` oder `RecordState = REGISTERED_FOR_MIGRATION`) schließen, wenn der
 911 Versicherte dieses nicht innerhalb einer geeigneten Frist aktiviert oder seine Einwilligung
 912 in die Nutzung der ePA oder in die Datenverarbeitung durch den Anbieter entzieht. [\leq]

913 Den Status des aktivierten Kontos (`RecordState = ACTIVATED`) setzt die Komponente
914 Autorisierung im Vorgang der Aktivierung des Kontos in der Umgebung der
915 Leistungserbringer oder in der Personal Zone des Versicherten bei Hinterlegung des
916 Schlüsselmaterials für den Versicherten.

917 **A_15039-01A_15039 - Anbieter ePA-Aktensystem - Aktives Konto löschen**

918 Der Anbieter des ePA-Aktensystems MUSS ein aktives Konto (`RecordState = ACTIVATED`
919 oder KEY CHANGE) schließen, wenn der Versicherte sein Konto schließen möchte oder
920 seine Einwilligung in die Nutzung der ePA oder in die Datenverarbeitung durch den
921 Anbieter entzieht. [`<=`]

922 **A_15040 - Anbieter ePA-Aktensystem - Aktives Konto kündigen**

923 Der Anbieter des ePA-Aktensystems MUSS bei Kündigung des Versicherten mit der
924 Absicht die Daten zu migrieren, den Status `RecordState` im Datensatz `KeyChain` des
925 Versicherten in der Komponente Autorisierung auf den Wert `RecordState = DISMISSED`
926 setzen. [`<=`]

927 **A_20176 - Anbieter ePA-Aktensystem - Kündigung Konto zurücknehmen**

928 Der Anbieter des ePA-Aktensystems KANN eine Kündigung des Versicherten
929 zurücknehmen, die dazu geführt hat, dass der Status `RecordState` im Datensatz
930 `KeyChain` des Versicherten in der Komponente Autorisierung auf dem Wert `RecordState`
931 `= DISMISSED` steht, indem dieser Wert wieder auf `RecordState = ACTIVATED` gesetzt
932 wird, wenn sicher gestellt ist, dass der Versicherte nicht bei einem anderen Aktenanbieter
933 ein Konto eröffnet hat. [`<=`]

934 **A_15041 - Anbieter ePA-Aktensystem - Gekündigtes Konto löschen**

935 Der Anbieter des ePA-Aktensystems MUSS ein gekündigtes Konto (`RecordState =`
936 `DISMISSED`) schließen, wenn der Versicherte sein Konto schließen möchte oder seine
937 Einwilligung in die Nutzung der ePA oder in die Datenverarbeitung durch den Anbieter
938 entzieht. [`<=`]

939 **A_15042 - Anbieter ePA-Aktensystem - Gekündigtes Konto einfrieren**

940 Der Anbieter des ePA-Aktensystems MUSS für ein gekündigtes Konto (`RecordState =`
941 `DISMISSED`) den Status `RecordState` im Datensatz `KeyChain` des Versicherten in der
942 Komponente Autorisierung auf den Wert `RecordState = SUSPENDED` setzen, sobald für
943 den Versicherten in der Komponente Dokumentenverwaltung ein Migrationspaket für den
944 Versicherten erstellt wurde. [`<=`]

945 **A_15043 - Anbieter ePA-Aktensystem - Eingefrorenes Konto löschen**

946 Der Anbieter des ePA-Aktensystems MUSS ein gekündigtes und eingefrorenes Konto
947 (`RecordState = SUSPENDED`) schließen, wenn der Versicherte sein Konto schließen
948 möchte, seine Einwilligung in die Datenverarbeitung durch den Anbieter entzieht oder
949 eine angemessene Aufbewahrungsfrist für die Daten des Versicherten abgelaufen
950 ist. [`<=`]

951 **A_15187 - Anbieter ePA-Aktensystem - Vertragsdaten ändern**

952 Der Anbieter des ePA-Aktensystems MUSS es dem Versicherten ermöglichen, seine
953 Vertragsdaten zu ändern. [`<=`]

954 **A_15188 - Anbieter ePA-Aktensystem - Ausschluss einer Änderung der KVNR im Aktenkonto**

955 Der Anbieter des ePA-Aktensystems MUSS verhindern, dass die KVNR des Versicherten
956 im ePA-Aktensystem geändert werden kann. [`<=`]

958 **A_18083 - Anbieter ePA-Aktensystem - Validierung Mailadresse vor Übernahme**

959 Der Anbieter des ePA-Aktensystems MUSS jede Änderung einer Mailadresse vor der
960 Übernahme der Änderung validieren, sodass ausgeschlossen wird, dass eine ungültige
961 Mailadresse eine gültige Mailadresse überschreibt. [`<=`]

Das Validieren einer Mailadresse kann über die Generierung eines Bestätigungslinks geschehen, der an genau diese Mailadresse verschickt wird und vom Empfänger geklickt werden muss, um die Mailadresse als gültig zu erachten.

A_18782 - Anbieter ePA-Aktensystem - E-Mail-Notifikation an alte Mailadresse

Der Anbieter des ePA-Aktensystems MUSS vor der Übernahme der Änderung einer Mailadresse eine Notifikation an die alte Mailadresse senden. [<=]

~~**A_18084 - ePA-Aktensystem - Schriftliche Benachrichtigung bei Identitätswechsel**~~

~~Der Anbieter des ePA-Aktensystems MUSS den Versicherten postalisch über einen Identitätswechsel (Einsatz einer neuen, bisher nicht verwendeten eGK des Versicherten) gemäß [gemSpec_Autorisierung#A_17840] informieren, wenn eine automatische Benachrichtigung mangels hinterlegter oder wegen ungültiger Mailadresse nicht möglich ist. Eine postalische Benachrichtigung bei Identitätswechsel eines berechtigten Vertreters ist nicht erforderlich. [<=]~~

A_18084-01 - ePA-Aktensystem - Benachrichtigung bei Identitätswechsel

Der Anbieter des ePA-Aktensystems MUSS den Versicherten über einen Identitätswechsel (Einsatz einer neuen, bisher nicht verwendeten eGK des Versicherten) gemäß [gemSpec_Autorisierung#A_17840] informieren. Wenn eine automatische Benachrichtigung mangels hinterlegter oder wegen ungültiger Mailadresse nicht möglich ist, muss eine alternative Methode gewählt werden. Eine Benachrichtigung bei Identitätswechsel eines berechtigten Vertreters ist nicht erforderlich. [<=]

6.1.2 Prozess der Aktenkontoeröffnung

Der Prozess der Kontoeröffnung durch einen Versicherten wird zweistufig realisiert. Im ersten Schritt der Initialisierung beantragt der Versicherte ein Aktenkonto bei einem Anbieter. Die vertragsrelevanten Daten werden vom Versicherten über einen vom Anbieter bereitgestellten Kommunikationskanal (postalisch, via Internetpräsenz, telefonisch, o.ä.) bereitgestellt.

Der zweite Schritt besteht in der Aktivierung des Aktenkontos des Versicherten, in dem er seine Identität im System bekannt macht und sicheres kryptografisches Schlüsselmaterial für den Versichertenzugang erzeugt wird.

Zwischen der Kontointialisierung und Kontoaktivierung obliegt es dem Anbieter einer Aktenlösung mittels administrativer Eingriffe in die verschiedenen Komponenten, die Systeme auf die Nutzung durch diesen Versicherten vorzubereiten bzw. zu konfigurieren.

A_14993 - Anbieter ePA-Aktensystem - Mailadresse validieren

Der Anbieter des ePA-Aktensystems MUSS im Rahmen der Beantragung eines Aktenkontos durch einen Versicherten eine mitgeteilte Mailadresse auf Gültigkeit hin validieren. [<=]

Das Validieren einer Mailadresse kann über die Generierung eines Bestätigungslinks geschehen, der an genau diese Mailadresse verschickt wird und vom Empfänger geklickt werden muss um die Mailadresse als gültig zu erachten.

A_15545 - Anbieter ePA-Aktensystem - Mailadresse für Gerätefreischaltung zur Kontoaktivierung

Der Anbieter des ePA-Aktensystems MUSS eine im Rahmen der Beantragung eines Aktenkontos durch einen Versicherten mitgeteilte und gültige Mailadresse in der Komponente Autorisierung als Benachrichtigungsadresse für die Gerätefreischaltung durch den Versicherten hinterlegen. [<=]

- 1009 **A_14994 - Anbieter ePA-Aktensystem - Schriftliche Kontoeröffnung**
 1010 Der Anbieter des ePA-Aktensystems MUSS einem Versicherten erlauben, ein Aktenkonto
 1011 schriftlich zu beantragen. [\leq]
- 1012 **A_15024 - Anbieter ePA-Aktensystem - Elektronische Kontoeröffnung**
 1013 Der Anbieter des ePA-Aktensystems MUSS einem Versicherten erlauben, ein Aktenkonto
 1014 auf elektronischem Weg zu beantragen. [\leq]
- 1015 **A_15896 - Anbieter ePA-Aktensystem - Ausschluss automatisierte**
 1016 **Computerprogramme bei der Kontointialisierung**
 1017 Der Anbieter des ePA-Aktensystems MUSS bei der elektronischen Kontoeröffnung durch
 1018 technische Maßnahmen sicherstellen, dass ein Konto nicht durch ein Computerprogramm
 1019 (z.B. Bot) automatisch ohne Mitwirkung des Versicherten eröffnet werden kann. [\leq]
- 1020 **A_14996 - Anbieter ePA-Aktensystem - Manuelle Ergänzung Mailadresse**
 1021 Der Anbieter des ePA-Aktensystems MUSS es dem Versicherten auf geeignetem Weg
 1022 ermöglichen, die Registrierung einer Mailadresse für die Geräteverwaltung der
 1023 Komponente Autorisierung auch nachträglich vorzunehmen. [\leq]
- 1024 **A_15025 - Anbieter ePA-Aktensystem - Übernahme Mailadresse für**
 1025 **Geräteverwaltung**
 1026 Der Anbieter des ePA-Aktensystems MUSS eine vom Versicherten genutzte valide
 1027 Mailadresse als Benachrichtigungsadresse der Geräteverwaltung in die Komponente
 1028 Autorisierung übernehmen. [\leq]
- 1029 **A_14997 - Anbieter ePA-Aktensystem - Einwilligung dokumentieren**
 1030 Der Anbieter des ePA-Aktensystems MUSS die Einwilligung des Versicherten
 1031
 - zur Datenverarbeitung gegenüber dem Anbieter
 1032
 - in die Nutzung von ePA gegenüber dem Anbieter
 1033 im Rahmen der Kontoeröffnung einholen und dokumentieren. [\leq]
- 1034 **A_15433 - Anbieter ePA-Aktensystem - Einsicht der Einwilligung durch**
 1035 **Versicherten**
 1036 Der Anbieter des ePA-Aktensystems MUSS es dem Versicherten ermöglichen, die
 1037 Dokumentation der Einwilligung jederzeit einsehen zu können, bei einer elektronischen
 1038 Einwilligung auf elektronischem Wege. [\leq]
- 1039 **A_15026 - Anbieter ePA-Aktensystem - Keine Kontoeröffnung bei Nicht-**
 1040 **Einwilligung**
 1041 Der Anbieter des ePA-Aktensystems MUSS die Kontoeröffnung durch einen Versicherten
 1042 abbrechen und alle bisher erfassten Daten löschen, wenn der Versicherte gegenüber dem
 1043 Anbieter
 1044
 - nicht in die Datenverarbeitung einwilligt oder
 1045
 - nicht in die Nutzung von ePA einwilligt.
 1046 [\leq]
- 1047 **A_15002-01A_15002 - Anbieter ePA-Aktensystem - Abbruch bei existierendem**
 1048 **Konto**
 1049 Der Anbieter des ePA-Aktensystems MUSS in der Initialisierungsphase die Operation
 1050 `I_Authorization_Management::checkRecordExists` bei allen anderen Anbietern von
 1051 ePA-Aktensystemen mit der KVNR des beantragenden Versicherten aufrufen und die
 1052 Kontobeantragung abbrechen, sobald ein Anbieter mit einem Status `REGISTERED`,
 1053 `REGISTERED_FOR_MIGRATION`, `KEY_CHANGE` oder `ACTIVATED` antwortet. [\leq]

A_15897 - Anbieter ePA-Aktensystem – Ausschluss automatisierter Computerprogramme bei der Prüfung auf existierenden Konten

Der Anbieter des ePA-Aktensystems DARF es NICHT ermöglichen, die Existenz einer Akte durch alleinige Eingabe der KVNR im Registrierungsprozess automatisch ohne Mitwirkung des Versicherten am ePA-Aktensystem zu erfragen (z.B. Ein Bot fragt im Aktensystem eine große Anzahl von KVNR an).

[<=]

A_15870 - Anbieter ePA-Aktensystem - Abbruch bei Nichtverfügbarkeit anderer Anbieter

Der Anbieter des ePA-Aktensystems MUSS die Kontobeantragung abbrechen, wenn die Operation `I_Authorization_Management::checkRecordExists` mindestens eines anderen Anbieters eines ePA-Aktensystems eine technische Fehlermeldung liefert oder nicht erreichbar ist. [<=]

A_15617 - Anbieter ePA-Aktensystem - Abfrage Datenübernahme aus Altsystem bei Kontoinitialisierung

Der Anbieter des ePA-Aktensystems MUSS in der Initialisierungsphase den Wunsch des Versicherten zur Datenübernahme abfragen, wenn die Operation

`I_Authorization_Management::checkRecordExists` bei einem anderen Anbieter eines ePA-Aktensystems den Status `DISMISSED` oder `SUSPENDED` zurückliefert. [<=]

6.1.3 Prozess der Änderung und Kündigung eines Aktenkontos

Das Schließen des Aktenkontos eines Versicherten ist gleichzusetzen mit dem Widerruf der Einwilligung in die Datenverarbeitung durch den Anbieter. Ein mögliches Vertragsverhältnis wird damit beendet. Die Daten des Versicherten sind in diesem Fall zu löschen. Ein Schließen des Aktenkontos nach Tod des Versicherten ist hier ausdrücklich nicht dargestellt und funktioniert analog einer schriftlichen Kündigung durch den Versicherten ebenso durch eine Kündigung durch einen Bevollmächtigten oder Erben.

A_15028 - Anbieter ePA-Aktensystem - Kündigung Schriftform

Der Anbieter des ePA-Aktensystems MUSS es dem Versicherten ermöglichen, sein Konto auf schriftlichem Weg zu kündigen, sodass es innerhalb einer Kündigungsfrist weiterhin nutzbar ist, ohne automatisch geschlossen zu werden. [<=]

A_15029 - Anbieter ePA-Aktensystem - Schließen des Aktenkontos elektronisch

Der Anbieter des ePA-Aktensystems MUSS es dem Versicherten ermöglichen, sein Konto auf elektronischem Weg zu kündigen, sodass es innerhalb einer Kündigungsfrist weiterhin nutzbar ist, ohne automatisch geschlossen zu werden. [<=]

A_15434 - Anbieter ePA-Aktensystem - Schließen des Kontos nach Ablauf der Kündigungsfrist

Der Anbieter des ePA-Aktensystems MUSS ein gekündigtes Aktenkonto nach Ablauf der Kündigungsfrist schließen. [<=]

A_14995 - Anbieter ePA-Aktensystem - Schließen des Aktenkontos Schriftform

Der Anbieter des ePA-Aktensystems MUSS es dem Versicherten ermöglichen, seine Einwilligung in die Datenverarbeitung schriftlich zu widerrufen und sein Konto damit zu schließen. [<=]

A_15822 - Anbieter ePA-Aktensystem - Schließung der Akte nur durch den Besitzer

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass eine Schließung der Akte nur durch den Besitzer der Akte erfolgen kann.

[<=]

Hinweis: Dies kann z.B. durch eine telefonische Rückfrage mit dem Versicherten erfolgen.

A_15027 - Anbieter ePA-Aktensystem - Schließen des Aktenkontos elektronisch

Der Anbieter des ePA-Aktensystems MUSS es dem Versicherten ermöglichen, seine Einwilligung in die Datenverarbeitung auf elektronischem Weg zu widerrufen und sein Konto damit zu schließen.

[<=]

A_15780 - Anbieter ePA-Aktensystem - Widerspruchsfrist bei Kontolöschung

Der Anbieter des ePA-Aktensystems MUSS den Versicherten über das beabsichtigte Löschen der Daten des Versicherten im Rahmen der Kontoschließung informieren und diesem eine angemessene Widerspruchsfrist einräumen.[<=]

A_15435 - Anbieter ePA-Aktensystem - Löschen aller Daten beim Schließen des Aktenkontos

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass beim Schließen eines Aktenkontos eines Versicherten alle zu diesem Aktenkonto gehörenden Daten in den Systemen des Anbieters unter Beachtung der eingeräumten Widerspruchsfrist und der gesetzlichen Aufbewahrungsfristen gelöscht werden.[<=]

Hinweis: Hierzu gehören neben den Daten in den Komponenten des ePA-Aktensystems insbesondere auch die Vertragsdaten.

A_15436 - Anbieter ePA-Aktensystem - Kündigung durch Anbieter ePA-Aktensystem

Falls der Anbieter des ePA-Aktensystems dem Versicherten kündigt, MUSS der Anbieter dem Versicherten die Möglichkeit geben, in angemessener Zeit seinen Anbieter zu wechseln bzw. seine Daten lokal zu sichern.[<=]

6.1.4 Prozess des Anbieterwechsels

Der Prozess des Anbieterwechsels wird durch das ePA-Modul Frontend des Versicherten gesteuert. Dem Anbieter des ePA-Aktensystems obliegt es, den Status des Kontos nach Abschluss des Exports in der Komponente Autorisierung zu setzen (s.o.) und das erstellte Migrationspaket an einen neuen Anbieter herauszugeben, der dieses über eine generierte URL abrufen kann.

A_16411 - Anbieter ePA-Aktensystem - Information des Versicherten über die Erstellung des Exportpakets

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass der Versicherte über die Bereitstellung des Exportpakets über den gemäß [gemSpec_Autorisierung#A_15752] definierten Benachrichtigungskanal informiert wird.

[<=]

A_16412 - Anbieter ePA-Aktensystem - Information des Versicherten nach Abschluss des Imports des Exportpakets

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass der Versicherte über den Abschluss des Imports des Exportpakets über den gemäß [gemSpec_Autorisierung#A_15752] definierten Benachrichtigungskanal informiert

1145 wird.
1146 [`<=`]

1147 **A_15659 - Anbieter ePA-Aktensystem – Exportpaket unter URL verfügbar**
1148 **machen**

1149 Der Anbieter des ePA-Aktensystems MUSS das erstellte Exportpaket unter der als
1150 Rückgabeparameter der Operation `I_Account_Management_Insurant::SuspendAccount`
1151 an das ePA-Modul Frontend des Versicherten übermittelten `PackageURL` für die anderen
1152 Anbieter ePA-Aktensystem mittels HTTPS abrufbar machen.[`<=`]

1153 Der Download des Migrationspakets über eine URL setzt die konzeptionelle Operation
1154 `I_Account_Management::GetExportPackage` um.

1155 **A_15051 - Anbieter ePA-Aktensystem - Authentisierung gegenüber einem**
1156 **neuen Aktenanbieter**

1157 Der Anbieter des ePA-Aktensystems, welches das Migrationspaket zur Verfügung stellt,
1158 MUSS sich beim Abruf des Migrationspakets durch ein anderes ePA-Aktensystem mit der
1159 TLS-Identität der Dokumentenverwaltung `oid_epa_mgmt` mittels des Zertifikats C.FD-
1160 TLS-S authentisieren.
1161 [`<=`]

1162 **A_15048 - Anbieter ePA-Aktensystem - Authentifizierung des neuen**
1163 **Aktenanbieters**

1164 Der Anbieter des ePA-Aktensystems MUSS den Abruf des Migrationspakets durch ein
1165 anderes ePA-Aktensystem ablehnen, wenn sich der abrufende Client nicht als ePA-
1166 Aktensystem in der Rolle `oid_epa_mgmt` in einem TLS-Zertifikat C.FD.TLS-C
1167 authentisiert.[`<=`]

1168 **A_17236 - ePA-Aktensystem - Prüfung der TLS-Zertifikate**

1169 Das ePA-Aktenystem MUSS bei der Authentifizierung eines anderen Aktensystems beim
1170 Abruf des Migrationspakets die Prüfung der verwendeten TLS-Zertifikate entsprechend
1171 TUC_PKI_018 durchführen. Zur Prüfung des TLS-Zertifikats C.FD-TLS-S sind dabei die
1172 Parameter `PolicyList=oid_fd_tls_s`, `IntendedKeyUsage=digitalSignature`,
1173 `intendedExtendedKeyUsage=id-kp-serverAuth`, `OCSP-Graceperiod=60 Minuten`, `Offline-`
1174 `Modus=nein` zu verwenden. Zur Prüfung des TLS-Zertifikats C.FD-TLS-C sind dabei die
1175 Parameter `PolicyList=oid_fd_tls_c`, `IntendedKeyUsage=digitalSignature`,
1176 `intendedExtendedKeyUsage=id-kp-clientAuth`, `OCSP-Graceperiod=60 Minuten`, `Offline-`
1177 `Modus=nein` zu verwenden.

1178
1179
1180 [`<=`]

1181 **A_15595 - Anbieter ePA-Aktensystem - Kontoschließung nach Abruf des Export-**
1182 **Pakets**

1183 Der Anbieter des ePA-Aktensystems MUSS nach erfolgreichem Abruf des Export-Pakets
1184 durch ein anderes ePA-Aktensystem den Status des Aktenkontos in der Komponente
1185 Autorisierung auf den Wert `Suspended` setzen.[`<=`]

1186 **A_15703 - Anbieter ePA-Aktensystem - Verfügbarkeit Export-Paket**

1187 Der Anbieter des ePA-Aktensystems MUSS ein erstelltes Export-Paket für mindestens
1188 sieben Tage zum Abruf durch einen anderen Anbieter eines ePA-Aktensystems
1189 bereithalten.[`<=`]

1190 **A_15660 - Anbieter ePA-Aktensystem – Verantwortlichkeit für das Exportpaket**

1191 Der Anbieter des ePA-Aktensystems MUSS die Verfügbarkeit und Integrität des
1192 Exportpakets bis zum vollständigen Abschluss des Abrufs des Exportpakets durch den
1193 neuen Anbieter ePA-Aktensystem des Versicherten sicherstellen.[`<=`]

6.2 Benutzerführung

Bietet der Anbieter des ePA-Aktensystems dem Versicherten die Aktenkontoeröffnung, die Änderung von Vertragsdaten und die Aktenkontoschließung auf einem elektronischen Weg an, dann muss die Bedienung für den Nutzer intuitiv gestaltet werden.

A_15842 - Anbieter ePA-Aktensystem - Ergonomie der Benutzerführung

Der Anbieter des ePA-Aktensystems MUSS eine ergonomisch gestaltete Benutzerführung nach den Vorgaben zur Ergonomie in [DIN EN ISO 9241-171] anbieten. [≤]

DIN-Normen und Verordnungen zur Beachtung:

Zusätzlich zu den in diesem Kapitel aufgeführten Anforderungen zur Benutzerführung sollen auch die in der ISO 9241 aufgeführten Qualitätsrichtlinien zur Sicherstellung der Ergonomie interaktiver Systeme und Anforderungen aus der Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung – BITV 2.0) beachtet werden.

Insbesondere soll der Fokus auf die nachfolgend aufgeführten Teile der ISO 9241 gerichtet sein:

DIN EN ISO 9241 – Teile mit Bezug zur Software-Ergonomie

- Teil 8: Anforderungen an Farbdarstellungen
- Teil 9: Anforderungen an Eingabegeräte – außer Tastaturen
- Teil 110: Grundsätze der Dialoggestaltung (ersetzt den bisherigen Teil 10)
- Teil 11: Anforderungen an die Gebrauchstauglichkeit – Leitsätze
- Teil 12: Informationsdarstellung
- Teil 13: Benutzerführung
- Teil 14: Dialogführung mittels Menüs
- Teil 15: Dialogführung mittels Kommandosprachen
- Teil 16: Dialogführung mittels direkter Manipulation
- Teil 17: Dialogführung mittels Bildschirmformularen
- Teil 171: Leitlinien für die Zugänglichkeit von Software BITV 2.0

BITV 2.0 - Barrierefreie Informationstechnik-Verordnung

Die Umsetzung der Verordnung dient zur behindertengerechten Umsetzung von Webseiten und anderen grafischen Oberflächen.

Insbesondere sollen deshalb neben der Übernahme der international anerkannten Standards für barrierefreie Webinhalte, die Web Content Accessibility Guidelines (WCAG) 2.1, auch die Belange gehörloser, hör-, lern- und geistig behinderter Menschen berücksichtigt werden.

Die BITV 2.0 regelt unter anderem den sachlichen Geltungsbereich, die einzubeziehenden Gruppen behinderter Menschen und die anzuwendenden Standards.

Weitere Richtlinien und Empfehlungen zur digitalen Barrierefreiheit sind die EU-Richtlinie 2016/2102 für öffentliche Stellen und die europäische Norm EN 301 549 V2.1.2 mit dem Titel "Accessibility requirements for ICT products and services".

- 1234 **A_15846 - Anbieter ePA-Aktensystem - Schnittstellen für die Unterstützung der**
1235 **barrierefreien Bedienungsmöglichkeit**
1236 Der Anbieter des ePA-Aktensystems SOLL die Schnittstellen für die Unterstützung der
1237 barrierefreien Bedienungsmöglichkeit, welche vom Betriebssystem zur Verfügung gestellt
1238 werden, unterstützen.[<=]

ENTWURF

1239

7 Informationsmodell

1240

Ein gesondertes Informationsmodell der durch den Produkttypen verarbeiteten Daten

1241

wird nicht benötigt.

ENTWURF

1242

8 Verteilungssicht

1243

Eine Darstellung der hardwareseitigen Verteilung des Produkttyps bzw. seiner

1244

Teilsysteme und der Einbettung in die physikalische Umgebung wird nicht benötigt.

ENTWURF

1245

9 Anhang A – Verzeichnisse

1246

9.1 Abkürzungen

Kürzel	Erläuterung
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
DSGVO	Datenschutz-Grundverordnung
DIN	Deutsches Institut für Normung
DNS	Domain Name System
eGK	elektronische Gesundheitskarte
ePA	elektronische Patientenakte
FIPS	Federal Information Processing Standard
ITSEC	Information Technology Security Evaluation Criteria
LE	Leistungserbringer
OID	Object Identifier
RFC	Request for Comment
SGB V	Sozialgesetzbuch Fünftes Buch
SGD	Schlüsselgenerierungsdienst
TI	Telematikinfrastruktur

1247

9.2 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.
KeyChain	Schlüsselring oder Schlüsselbund gemäß Informationsmodell [gemSpec_Autorisierung]

1248

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

1249

9.3 Abbildungsverzeichnis

Abbildung 1: Komponenten des ePA-Aktensystems	9
Abbildung 2: Nachbarsysteme des ePA-Aktensystems	10
Abbildung 3: Zustandsdiagramm zum Lebenszyklus einer Akte bei einem Anbieter	29
Abbildung 1: Komponenten des ePA-Aktensystems	9
Abbildung 2: Nachbarsysteme des ePA-Aktensystems	10
Abbildung 3: Zustandsdiagramm zum Lebenszyklus einer Akte bei einem Anbieter	29

9.4 Tabellenverzeichnis

Tabelle 1: Tab_ePA_Service Discovery	13
Tabelle 2: Tab_ePA_FQDN	16
Tabelle 3: Zustandswechsel im Lebenszyklus einer Akte	30
Tabelle 1: Tab_ePA_Service Discovery	13
Tabelle 2: Tab_ePA_FQDN	16
Tabelle 3: Zustandswechsel im Lebenszyklus einer Akte	30

9.5 Referenzierte Dokumente

9.5.1 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 Versionsnummern sind in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemSysL_ePA]	gematik. Systemspezifisches Konzept ePA
[gemSpec_Perf]	gematik: Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform

1277 **9.5.2 Weitere Dokumente**

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI-Redundanz]	BSI Hinweise zur räumlichen Entfernung zwischen redundanten Rechenzentren https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/RZ-Abstand.pdf?__blob=publicationFile
[BSI-Grundschutz]	BSI Grundschutz https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/FD_BS_Kompodium.pdf?__blob=publicationFile&v=3
[BSI-XSpRESS]	XML Spoofing Resistant Electronic Signature, Sichere Implementierung für XML Signature, 2012, BSI, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SOA/XSpRESS.pdf
[GJLS-2009]	Analysis of Signature Wrapping Attacks and Countermeasures, Sebastian Gajek, Meiko Jensen, Lijun Liao, Jörg Schwenk, 2009 https://lists.w3.org/Archives/Public/public-xmlsec/2009Nov/att-0019/Camera-Ready.pdf
[SHJSG I-2011]	All Your Clouds are Belong to us – Security Analysis of Cloud Management Interfaces, Juraj Somorovsky, Mario Heiderich, Meiko Jensen, Jörg Schwenk, Nils Gruschka, Luigi Lo Iacono, 2011, https://www.nds.ruhr-uni-bochum.de/media/nds/veroeffentlichungen/2011/10/22/AmazonSignatureWrapping.pdf

1278