

1  
2  
3  
4  
5  
6  
7  
8  
9  
10

11 **Elektronische Gesundheitskarte und Telematikinfrastruktur**

12  
13  
14  
15  
16  
17  
18  
19

20

## Feature:

# Sektorale Identity Provider

21  
22  
23  
24  
25  
26  
27

Version: 1.0.0 CC  
Revision: 413552  
Stand: 27.10.2021  
Status: zur Abstimmung freigegeben  
Klassifizierung: öffentlich\_Entwurf  
Referenzierung: gemF\_sektoraleIDP

28  
29

30

---

## Dokumentinformationen

---

### 31 Änderungen zur Vorversion

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

34

### 35 Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0 CC	27.10.21		initiale Erstellung des Dokuments	gematik

36

37

## Inhaltsverzeichnis

38	<b>1 Einordnung des Dokuments .....</b>	<b>4</b>
39	<b>1.1 Zielsetzung .....</b>	<b>4</b>
40	<b>1.2 Zielgruppe .....</b>	<b>4</b>
41	<b>1.3 Abgrenzungen .....</b>	<b>4</b>
42	<b>1.4 Methodik .....</b>	<b>4</b>
43	1.4.1 Anforderungen.....	4
44	<b>2 Einordnung in die Telematikinfrastruktur .....</b>	<b>6</b>
45	<b>3 Spezifikation .....</b>	<b>7</b>
46	<b>3.1 [gemSpec_Perf] .....</b>	<b>7</b>
47	<b>3.2 [gemSpec_IDP_Frontend] .....</b>	<b>17</b>
48	3.2.1 Registrierungsdaten des Authenticator-Moduls.....	19
49	<b>3.3 [gemSpec_IDP_Dienst] .....</b>	<b>21</b>
50	3.3.1 Aufbau des Discovery Document .....	21
51	3.3.2 Third-Party Authorization Endpoint.....	22
52	3.3.2.1 Authorization-Endpunkt Eingangsdaten .....	24
53	3.3.2.2 Authorization-Endpunkt Ausgangsdaten .....	25
54	3.3.3 Token-Endpunkt Ausgangsdaten .....	26
55	<b>3.4 [gemSpec_IDP_FD] .....</b>	<b>27</b>
56	<b>3.5 [gemSpec_FD_eRp] .....</b>	<b>29</b>
57		
58		

59

---

## 1 Einordnung des Dokuments

---

### 60 1.1 Zielsetzung

61 Im Rahmen der Zugänglichmachung des E-Rezepts für Versicherte ohne NFC-fähige eGK  
62 sollen ab dem 01.01.2022 Kassen-eigene Authentifizierungssysteme an das E-Rezept  
63 angebunden werden. Diese werden im Folgenden als sektorale Identity Provider  
64 bezeichnet, um sie vom zentralen IDP-Dienst abzugrenzen, welcher die Authentisierung  
65 der Nutzer direkt oder indirekt über die eGK realisiert und die bereitgestellten Attribute  
66 von dieser ableitet.

### 67 1.2 Zielgruppe

68 Das Dokument richtet sich an Hersteller und Anbieter von Produkten, welche bereits  
69 innerhalb der Telematikinfrastuktur im Rahmen des E-Rezeptes realisiert wurden. Es  
70 beschreibt die Änderungen, welche sich an ihren Komponenten ergeben, um die  
71 Anbindung von Kassen-eigenen Authentifizierungssystemen zu ermöglichen.

### 72 1.3 Abgrenzungen

73 Das Dokument umfasst im Kapitel 3 Änderungen an bestehenden Spezifikationen bzw.  
74 Steckbriefen der gematik und ist daher als Ergänzung zur entsprechenden Spezifikation  
75 der gematik zu verstehen und zu lesen. Der als Teil dieses Features neu eingeführte  
76 Produkttyp des "sektoralen Identity Provider" wird detailliert im neuen Dokument  
77 [gemSpec\_IDP\_Sek] spezifiziert und hier nur referenziert werden. Das neue Dokument  
78 für den Produkttyp sowie die entsprechenden Steckbriefe werden ergänzend zur Feature-  
79 Spezifikation veröffentlicht.

### 80 1.4 Methodik

#### 81 1.4.1 Anforderungen

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

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

91 Anforderungen werden im Dokument wie folgt dargestellt:

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

93 Text / Beschreibung  
94 [ <= ]  
95 Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und Textmarke [ <= ]  
96 angeführten Inhalte.  
97

ENTWURF

98

---

## 2 Einordnung in die Telematikinfrastuktur

---

99 Als sektoraler Identity Provider (IDP) wird ein Dienst bezeichnet, welcher nach vorheriger  
100 Authentifizierung Identitätsinformationen für eine bestimmte Gruppe von Nutzern  
101 innerhalb der Telematikinfrastuktur des Gesundheitswesens bereitstellt, welche  
102 anschließend verwendet werden, um auf verschiedene Fachdienste und deren Fachdaten  
103 und -prozesse zuzugreifen. Sektoren sind insbesondere die Krankenkassen mit den  
104 Versicherten als Nutzer, zukünftig allerdings auch andere Personengruppen wie z.B. Ärzte  
105 oder Pflegeinstitutionen.

106 Zur Einbindung eines sektoralen Identity Provider wird im ersten Schritt der zentrale IDP-  
107 Dienst als Mittler zwischen dem Anwendungsfondend, den sektoralen Identity Providern  
108 und den Fachdiensten (primär dem E-Rezept) eingesetzt.

109 Dies wird später mit der Etablierung einer Föderation von Identity Providern abgelöst.

110

ENTWURF

111

## 3 Spezifikation

112 Neben dem neuen Dokument [gemSpec\_IDP\_Sek] und den zugehörigen neuen  
113 Steckbriefen [gemProdT\_IDP\_Sek] und [gemAnbT\_IDP\_Sek] ergeben sich untenstehende  
114 Änderungen an bereits bestehenden Dokumenten und Produkten:

115

### 116 3.1 [gemSpec\_Perf]

117 Die folgende Anforderung wird unverändert neben dem IDP-Dienst auch den sektoralen  
118 Identity Providern zugewiesen:

119 A\_20244 Performance - IDP-Dienst – Skalierung

#### 120 **A\_22357 - Verfügbarkeit sektoraler IDP**

121 Der Produkttyp sektoraler Identity Provider MUSS zur Hauptzeit eine Verfügbarkeit von  
122 99,9 % und zur Nebenzeit eine Verfügbarkeit von 99,0 % haben.

123 Wartungsfenster dürfen nur in der Nebenzeit liegen. Genehmigte Wartungsfenster  
124 werden nicht als Ausfallzeit gewertet.

125 Hauptzeit ist Montag bis Sonntag von 6 bis 22 Uhr, ausgenommen bundeseinheitliche  
126 Feiertage. Alle übrigen Stunden der Woche sind Nebenzeit. [≤]

#### 127 **A\_22225 - Definition Marktanteil (MA) des Anbieters einer Anwendung oder 128 eines Dienstes**

129 Der Anbieter MUSS entsprechend seines Marktanteils (MA) Performancevorgaben und  
130 Service Level erfüllen. Der Marktanteil ist der numerische Wert zwischen 1,00 und 0,01  
131 [ohne Einheit, zwei Nachkommastellen, aufgerundet], der den Anteil der eigenen Kunden  
132 des Anbieters im Verhältnis zur Gesamtnutzerzahl repräsentiert. Die Gesamtnutzerzahl  
133 ist die Zahl aller Versicherten (privat + gesetzlich) oder die Anzahl aller  
134 Leistungserbringer, die diese Anwendung nutzen. [≤]

#### 135 **A\_22228 - Performance - Sektoraler Identity Provider - Anzahl paralleler 136 Sessions - Internet**

137 Der Anbieter eines sektoralen Identity Providers MUSS mindestens 2.400.000 x MA  
138 gleichzeitige Sessions für Versicherte unterstützen. MA ist der Marktanteil des Anbieters  
139 gemäß [A\_22225].

140 [≤]

#### 141 **A\_22227 - Performance – IDP-Dienst – Bearbeitungszeit unter Last**

142 Der Produkttyp IDP-Dienst MUSS die Bearbeitungszeitvorgaben unter Last aus  
143 Tab\_gemSpec\_Perf\_IDP-Dienst erfüllen.

144

145 Es wird davon ausgegangen, dass der IDP-Dienst eingeschwungen ist und z.B.  
146 Lokalisierungsanfragen lokal zwischengespeichert sind sowie Verbindungen nicht neu  
147 ausgehandelt werden.

148 Im Fall der Authorization Requests zählt die Zeit von Anfrage des Authenticator  
149 (Challenge) bis zum Eintreffen der Antwort (Response) nicht zur Bearbeitungszeit. Die  
150 Dauer für die OCSP-Anfrage ist jedoch berücksichtigt.

151

152 Für die Zulassung ist je Anwendungsfall der Nachweis bei einer Last von 100 Anfragen  
153 pro Sekunde zu erbringen.

154

155 **Tabelle 1: Tab\_gemSpec\_Perf\_IDP-Dienst: Bearbeitungszeitvorgaben**

ID	Anwendungsfälle	Lastvorgaben	Bearbeitungszeitvorgaben	
			Spitzenlast [1/sec]	Mittelwert [msec]
IDP.UC_1	Authorization Requests (TI)	450	1500	1964
IDP.UC_2	Token Requests (TI)	450	500	664
IDP.UC_3	Authorization Requests (Internet)	450	1500	1964
IDP.UC_4	Token Requests (Internet)	450	500	664

156 [ $\leq$ ]

157

158 **A\_22226 - Performance – Sektoraler Identity Provider – Bearbeitungszeit unter Last**

159 Der Anbieter eines sektoralen Identity Providers MUSS die Bearbeitungszeitvorgaben unter Last aus Tab\_gemSpec\_Perf\_Sek\_IDP erfüllen.

162 Es wird davon ausgegangen, dass der sektorale Identity Provider eingeschwungen ist und z.B. Lokalisierungsanfragen lokal zwischengespeichert sind, sowie Verbindungen nicht neu ausgehandelt werden.

165 MA ist der Marktanteil des Anbieters gemäß [A\_22225].

166 Im Fall der Authorization Requests zählt die Zeit von Anfrage des Authenticator (Challenge) bis zum Eintreffen der Antwort (Response) nicht zur Bearbeitungszeit. Die Dauer für die OCSP-Anfrage ist jedoch berücksichtigt.

169

170 **Tabelle 2: Tab\_gemSpec\_Perf\_sek\_IDP: Bearbeitungszeitvorgaben**

ID	Anwendungsfälle	Lastvorgaben	Bearbeitungszeitvorgaben	
			Spitzenlast [1/sec]	Mittelwert [msec]
IDP.UC_20	Processing of Client-Response (third-party-based authentication, Internet)	10 + (450 x MA)	1500	1964
IDP.UC_21	Token Request (third-party-based authentication, Internet)	10 + (450 x MA)	500	664

171 [ $\leq$ ]

172

173 **A\_22057 - Performance - Rohdaten - Verpflichtung des Anbieters**  
174 **(Rohdatenerfassung v.02)**

175 Der Anbieter von Produkten, deren zugeordnete Produkttypen ihre Performance-  
176 Messwerte in Rohdaten-Performance-Berichten übermitteln, MUSS die Erfassung,  
177 Aufbereitung und Übermittlung der Rohdaten bezüglich Umfang, Lieferintervalle und  
178 Format gemäß der allgemeinen und spezifischen Anforderungen (Rohdatenerfassung  
179 v.02) gewährleisten. [ <= ]

180

181 **A\_22002 - Performance - Rohdaten - Übermittlung (Rohdatenerfassung v.02)**

182 Produkttypen, die ihre Performance-Messwerte in Rohdaten-Performance-Berichten  
183 übermitteln, MÜSSEN zur Übertragung der Berichte die Schnittstelle  
184 I\_OpsData\_Update::fileUpload gemäß [gemSpec\_SST\_LD\_BD#A\_17733] verwenden.

185  
186 Die Übermittlung des Rohdaten-Performance-Berichts MUSS pro logischer Produktinstanz  
187 (CI ID - Configuration Item ID) erfolgen. [ <= ]

188

189 **A\_22000 - Performance - Rohdaten - zu liefernde Dateien (Rohdatenerfassung**  
190 **v.02)**

191 Produkttypen, die ihre Performance-Messwerte in Rohdaten-Performance-Berichten  
192 übermitteln, MÜSSEN folgende zwei Dateien in den jeweils individuell konfigurierbaren  
193 Berichtsintervallen senden:

194 - einen "Rohdaten-Performance-Bericht" mit den zu liefernden Rohdaten  
195 und

196 - eine Datei zur "Selbstauskunft" gemäß [gemSpec\_OM#GS-A\_4543] im XML-Format  
197 [ProductInformation.xsd].

198  
199 Dabei MÜSSEN beide Dateien separat an die Betriebsdatenerfassung gesendet  
200 werden. [ <= ]

201

202 **A\_22004 - Performance - Rohdaten - Korrektheit (Rohdatenerfassung v.02)**

203 Produkttypen, die ihre Performance-Messwerte in Rohdaten-Performance-Berichten  
204 übermitteln, MÜSSEN die Berichte vollständig, zeitlich lückenlos (auch über Ausfälle  
205 hinweg), überlappungsfrei, intervalltreu, syntaktisch und semantisch korrekt  
206 senden. [ <= ]

207 "Intervalltreu" bedeutet hierbei: Jeder Eintrag muss in dem Rohdaten-Performance-  
208 Bericht gesendet werden, in dessen Berichtsintervall sein Endezeitpunkt \$timestamp +  
209 \$duration\_in\_ms liegt.

210

211 **A\_22005 - Performance - Rohdaten - Frist für Nachlieferung**  
212 **(Rohdatenerfassung v.02)**

213 Produkttypen, die ihre Performance-Messwerte in Rohdaten-Performance-Berichten  
214 übermitteln, MÜSSEN, falls im Ausnahmefall eine Lieferung nicht wie gefordert erfolgt,  
215 die Datei(en) in der geforderten Qualität bis zum Ende des folgenden Werktages (Mo-Fr  
216 ausgenommen bundeseinheitliche Feiertage) nachliefern. [ <= ]

217

218 **A\_22003 - Performance - Rohdaten - Nachlieferung auf Anforderung**  
219 **(Rohdatenerfassung v.02)**

220 Produkttypen, die ihre Performance-Messwerte in Rohdaten-Performance-Berichten  
221 übermitteln, MÜSSEN auf Anforderung des Gesamtverantwortlichen TI eine erneute

222 Lieferung/Nachlieferung der Rohdaten-Berichte bis zum 5. Werktag (Mo-Fr,  
223 ausgenommen bundeseinheitliche Feiertage) des auf dem Berichtszeitraum folgenden  
224 Monats ermöglichen. [ <= ]

225 Die vorgeschriebenen Aufbewahrungspflichten bleiben hiervon unberührt.

226

#### 227 **A\_21976 - Performance - Rohdaten - Konfigurierbarkeit der Lieferintervalle** 228 **(Rohdatenerfassung v.02)**

229 Produkttypen, die ihre Performance-Messwerte in Rohdaten-Performance-Berichten  
230 übermitteln, MÜSSEN die Lieferintervalle der Berichtsdateien flexibel zwischen 1 Minute  
231 und 24 Stunden (1440 Minuten) mit einer Taktung von 1 Minute konfigurieren können,  
232 ohne ein Produktupdate durchführen zu müssen. [ <= ]

233

#### 234 **A\_21975 - Performance - Rohdaten - Default-Werte für Lieferintervalle** 235 **(Rohdatenerfassung v.02)**

236 Produkttypen, die ihre Performance-Messwerte in Rohdaten-Performance-Berichten  
237 übermitteln, MÜSSEN - sofern nicht explizit spezifiziert - folgende Lieferintervalle als  
238 Standardeinstellung voreinstellen:

- 239 • Rohdaten-Performance-Berichte: 5-minütig.
- 240 • Selbstauskunft: 60-minütig.

241 [ <= ]

#### 242 **A\_21978 - Performance - Rohdaten - Trennung der Lieferintervalle** 243 **(Rohdatenerfassung v.02)**

244 Produkttypen, die ihre Performance-Messwerte in Rohdaten-Performance-Berichten  
245 übermitteln, MÜSSEN eine voneinander getrennte Anpassung der Lieferintervalle für die  
246 Lieferungen von Rohdaten-Performance-Berichten, Selbstauskünften und ggf. weiteren  
247 Lieferungen (z.B. Bestandsdatenlieferung) ermöglichen. [ <= ]

248

#### 249 **A\_21979 - Performance - Rohdaten - Bezug der Lieferverpflichtung** 250 **(Rohdatenerfassung v.02)**

251 Produkttypen, die ihre Performance-Messwerte in Rohdaten-Performance-Berichten  
252 übermitteln, MÜSSEN sich bei der Lieferung der Berichtsdateien ausschließlich am  
253 Lieferintervall orientieren (NICHT z.B. an der Datenmenge). [ <= ]

254

#### 255 **A\_21980 - Performance - Rohdaten - Leerlieferung (Rohdatenerfassung v.02)**

256 Produkttypen, die ihre Performance-Messwerte in Rohdaten-Performance-Berichten  
257 übermitteln, MÜSSEN die Lieferung der Berichtsdateien gemäß des konfigurierten  
258 Lieferintervalls leisten, auch wenn im dazugehörigen Berichtsintervall keine  
259 Operationsausführung stattgefunden hat. In diesem Fall ist der Rohdaten-Performance-  
260 Bericht mit dem Inhalt 'leer' (4 Zeichen) zu übertragen. Für die Selbstauskunft ergeben  
261 sich daraus keine Besonderheiten, sodass diese wie definiert zu übertragen ist. [ <= ]

262

#### 263 **A\_22001 - Performance - Rohdaten - Name der Berichte (Rohdatenerfassung** 264 **v.02)**

265 Produkttypen, die ihre Performance-Messwerte in Rohdaten-Performance-Berichten  
266 übermitteln, MÜSSEN beim Dateinamen der Berichte folgende Namenskonvention  
267 umsetzen:

268

269 <CI-ID>\_<Start>\_<Ende>\_<Version der Datei>\_<Dateityp>.<Endung>  
270

- 271 • <CI-ID> = identifiziert die Produktinstanz, siehe Anforderung [A\_17764] in  
272 [gemRL\_Betr\_TI#6.1.1].
- 273 • <Start> = Startzeitpunkt des Berichtsintervalls als Unixzeit-Zeitstempel in  
274 Millisekunden  
275 (immer volle Minuten, erster Zeitraum des Tages beginnt um 00:00 Uhr UTC).
- 276 • <Ende> = Endezeitpunkt des Berichtsintervalls als Unixzeit-Zeitstempel in  
277 Millisekunden  
278 (offenes Intervallende, d.h. erster Zeitpunkt, der gerade nicht mehr zum Intervall  
279 gehört, immer volle Minuten).
- 280 • <Version der Datei> = im Normalfall "1". Wird jeweils um 1 hochgezählt bei  
281 Korrekturlieferung zu einer Datei.
- 282 • <Dateityp>.<Endung> = "perf.log" / "inf.xml"
- 283 • perf.log = Performance Protokoll
- 284 • inf.xml = XML-Datei zur Selbstauskunft.

285 [**<=**]

### 286 **A\_21981 - Performance - Rohdaten - Format des Rohdaten-Performance-** 287 **Berichtes (Rohdatenerfassung v.02)**

288 Produkttypen, die ihre Performance-Messwerte in Rohdaten-Performance-Berichten  
289 übermitteln, MÜSSEN bei der Erstellung folgende Konventionen erfüllen:

290 Diese Produkttypen:

- 291 • MÜSSEN ein **CSV-Format** mit den Feldern  
292 ***timestamp; duration\_in\_ms; operation; size\_in\_byte; status; message*** mit  
293 folgender Bedeutung verwenden:
  - 294 • timestamp = unix-Epoch Zeitstempel in Millisekunden (Integer),
  - 295 • duration\_in\_ms = Dauer der Ausführung gemäß produkttypspezifischer Definition  
296 in Millisekunden (Integer),
  - 297 • operation = Operationsbezeichnung gemäß produkttypspezifischer Definition  
298 (String),
  - 299 • size\_in\_byte = Datenvolumen (in Byte) gemäß produkttypspezifischer Definition  
300 (Integer),
  - 301 • status = max. 5-stelliger Statuscode gemäß Tab\_gemSpec\_Perf\_Standard-  
302 Statuscodes und produkttypspezifischer Definition (Integer),
  - 303 • message = String bzw. JSON-formatierter String gemäß produkttypspezifischer  
304 Definition (String).
- 305 • MÜSSEN das **Semikolon ";"** als Feldtrennzeichen verwenden.
- 306 • DÜRFEN das Feldtrennzeichen innerhalb der CSV-Felder **NICHT** inhaltlich  
307 verwenden.
- 308 • DÜRFEN Feldinhalte **NICHT** quotieren.
- 309 • DÜRFEN Feldinhalte weggelassen, sofern diese Produkttyp- oder  
310 operationsbedingt entfallen können, was ggf. zu direkt aufeinanderfolgenden  
311 Semikola führt.

- 312 • MÜSSEN **UTF-8** Zeichensatzkodierung **ohne ByteOrderMark** verwenden.
- 313 • MÜSSEN **CR-LF**-Zeilenumbrüche (ASCII-13-Zeichen (Carriage return), ASCII-10-
- 314 Zeichen (Line feed)) verwenden.
- 315 • DÜRFEN Kommentierungen **NICHT** verwenden.
- 316 • DÜRFEN leeren Zeilen **NICHT** verwenden.
- 317 • DÜRFEN Tausendertrennzeichen **NICHT** verwenden.
- 318 • DÜRFEN einen CSV-Header **NICHT** verwenden.
- 319 • MÜSSEN Leerzeichen am Rand der Feldinhalte entfernen, sofern diese nicht
- 320 intendiert sind, da sie nicht automatisch ignoriert werden.

321 **Tabelle 3: Tab\_gemSpec\_Perf\_Standard-Statuscodes**

Statuscode	Name	Beschreibung
20000	OPERATION_OK	Es ist kein Fehler aufgetreten.
40000	INTERNAL_ERROR	Es ist ein nicht näher benannter, interner Fehler aufgetreten.
60000	EXTERNAL_ERROR	Es ist ein nicht näher benannter, externer Fehler aufgetreten.

322 [**<=**]

323 **A\_21982 - Performance - Rohdaten - Message-Block (Rohdatenerfassung v.02)**

324 Produkttypen, die ihre Performance-Messwerte in Rohdaten-Performance-Berichten  
 325 übermitteln, MÜSSEN bei der Erstellung des Message-Blocks (message-Feld im CSV-  
 326 formatierten Rohdaten-Performance-Bericht) folgende Festlegung berücksichtigen:  
 327 Diese Produkttypen:

- 328 • DÜRFEN das JSON-Format NICHT verwenden, wenn im Message-Block nur eine
- 329 Information in Form einer ID übertragen werden soll. Dabei DARF die ID NICHT
- 330 mit einer geschweiften Klammer "{" beginnen.
- 331 • MÜSSEN das JSON-Format (gem. [RFC 8259] oder [ECMA-404]) für den gesamten
- 332 Message-Block verwenden, wenn mehr als eine ID bzw. andere Informationen
- 333 übermittelt werden.

334 [**<=**]

335 Die Übermittlung einer einzelnen ID kann auch in Form einer JSON-Formatierung  
 336 erfolgen. Wird der Messageblock jedoch nicht in JSON formatiert, wird die enthaltene  
 337 Information in jedem Fall als ID interpretiert. In der produkttypspezifischen Definition ist  
 338 dies ergänzend definiert.

339

340 **A\_21983 - Performance - Rohdaten - Message-Block im Fehlerfall**  
 341 **(Rohdatenerfassung v.02)**

342 Produkttypen, die ihre Performance-Messwerte in Rohdaten-Performance-Berichten  
 343 übermitteln, KÖNNEN bei der Erstellung des Message-Blocks (message-Feld im CSV-  
 344 formatierten Rohdaten-Performance-Bericht) im Fehlerfall auf die Angabe der ID/des  
 345 betroffenen Key-Value-Paares verzichten, sofern die Information aufgrund des Fehlers  
 346 nicht vorliegt.[**<=**]

347

**A\_21984 - Performance - Rohdaten - Size-Block (Rohdatenerfassung v.02)**

348 Produkttypen, die ihre Performance-Messwerte in Rohdaten-Performance-Berichten  
349 übermitteln, MÜSSEN bei der Erstellung des Size-Blocks (size\_in\_byte-Feld im CSV-  
350 formatierten Rohdaten-Performance-Bericht) folgende Festlegung berücksichtigen:  
351

- 352 • Der Size-Block gibt die gemessene, übertragene Datenmenge einer Operation in  
353 Byte an.
- 354 • Ob der Size-Block befüllt werden muss, ist in der Produkttyp-spezifischen  
355 Definition festgelegt.
- 356 • Welchen Umfang die Berechnung der Size-Größe hat (Request, Response, Header,  
357 ...), ist in der Produkttyp-spezifischen Definition festgelegt.

358 [**<=**]

359 Ein Beispiel für drei Einträge, generisch (I), ohne (II) und mit (III) JSON-formatiertem  
360 Message-Block, sowie mit (II) und ohne (III) Inhalt des Size-Blocks:

361 I: timestamp;duration;operation;size;status;{"key1":"quote-value","key2":non-quote-  
362 value}

363 II: 1000212390109;447;Beispielprodukt.Beispieloperation;1024;200;12

364 III: 1000212470109;12;Beispielprodukt.Beispieloperation;;40001;{"ID":12,"Antwort":  
365 gesperrt"}

366

**A\_22012 - Performance - Rohdaten - Spezifika IDP - Duration (Rohdatenerfassung v.02)**

369 Der Produkttyp IDP-Dienst MUSS bei Rohdaten-Performance-Berichten bzgl. der  
370 "duration\_in\_ms"-Felder die Angabe aus der Tabelle  
371 Tab\_gemSpec\_Perf\_Berichtsformat\_IDP-Dienst in der Spalte "Duration" berücksichtigen.  
372 Die Messung zur Ermittlung der Dauer beginnt mit der Annahme der Aufrufnachricht an  
373 der annehmenden Schnittstelle des Produkttyps und endet mit dem vollständigen  
374 Versenden der Antwortnachricht an die annehmende Schnittstelle des Empfängers.  
375 Registriert wird dabei der Zeitpunkt aus dem Header.[**<=**]

376

**A\_22013 - Performance - Rohdaten - Spezifika IDP - Operation (Rohdatenerfassung v.02)**

379 Der Produkttyp IDP-Dienst MUSS bei Rohdaten-Performance-Berichten bzgl. der  
380 "operation"-Felder die Angabe aus der Tabelle Tab\_gemSpec\_Perf\_Berichtsformat\_IDP-  
381 Dienst in der Spalte "Operation" berücksichtigen.[**<=**]

382

**A\_22014 - Performance - Rohdaten - Spezifika IDP - Size (Rohdatenerfassung v.02)**

385 Der Produkttyp IDP-Dienst MUSS bei Rohdaten-Performance-Berichten bzgl. der  
386 "size\_in\_byte"-Felder die Angabe aus der Tabelle  
387 Tab\_gemSpec\_Perf\_Berichtsformat\_IDP-Dienst in der Spalte "Size" berücksichtigen.[**<=**]

388

**A\_22230 - Performance - Rohdaten - Spezifika IDP - Status (Rohdatenerfassung v.02)**

391 Wenn bei der Durchführung der Operation/des Use Case ein Fehler aufgetreten ist, MUSS  
392 der Produkttyp "Sektoraler IDP" bei Rohdaten-Performance-Berichten bzgl. des "status"-

393 Feldes den Statuscode gem. Tabelle Tab\_gemSpec\_Perf\_Fehlercodes\_Sektoraler\_IDP  
 394 festlegen, sofern ein spezifischer Fehlercode bestimmt werden kann. Ist dies nicht  
 395 möglich, MUSS der definierte Standardcode für interne bzw. externe Fehler verwendet  
 396 werden.  
 397

398 **Tabelle 4: Tab\_gemSpec\_Perf\_Fehlercodes\_Sektoraler\_IDP**

Statuscode	Definition	Beschreibung
79000	IDP_ERROR	alle internen Fehler des IDP

399 [**<=**]

400 **A\_20242-01 - Performance - Rohdaten-Performance-Berichte - Format der**  
 401 **Einträge des Performance-Berichts IdP-Dienst**

402 Der Produkttyp IdP-Dienst MUSS beim Übermitteln der Performance-Messwerte in einem Rohdaten-  
 403 Performance-Bericht sämtliche Zeilen (Einträge) der Berichte in der folgenden Weise formatieren:  
 404 INFO: start[\$timestamp] time[\$duration\_in\_ms] tag[\$operation] size[\$size\_in\_kb] message["UA:" +  
 405 \$useragent],  
 406 mit

- 407 • \$timestamp ein Unixzeit-Zeitstempel in Millisekunden,
- 408 • \$duration\_in\_ms die gemessene Bearbeitungszeit einer Operation in Millisekunden,
- 409 • \$operation die ausgeführte Operation des Produkttyps gemäß
  - 410 • Tab\_gemSpec\_Perf\_Berichtsformat\_IdP-Dienst
- 411 • \$size\_in\_kb ist die gemessene, übertragene Datenmenge einer Operation in Kilobyte. Wenn  
 412 ein fachlicher Anwendungsfall die Größe der übertragenen Datenmenge nicht  
 413 ermitteln kann, entfällt der Wert für "\$size\_in\_kb". Die Struktur der Nachricht  
 414 bleibt bestehen mit leerem Wert: " size[] ".
- 415 • \$message dient gemäß [gemSpec\_Perf#A\_17668-01] der Gruppierung  
 416 verschiedener Einträge zu einem fachlichen Anwendungsfall durch einen den  
 417 einzelnen Anwendungsfall identifizierende Zeichenkette, welche selbst die Zeichen  
 418 "[" und "]" nicht enthält. Wenn ein fachlicher Anwendungsfall durch einen  
 419 einzelnen Eintrag abgebildet wird, entfällt "message[\$message]".

420 [**<=**]

421

422 **Tabelle 5: Tab\_gemSpec\_Perf\_Berichtsformat\_IDP-Dienst**

\$IDP-Dienst-Operation	Produkttyp	Operation	Schnittstelle zu
IDP.UC_1	IDP-Dienst	Processing of Authorization Requests	TI
IDP.UC_5	IDP-Dienst	Processing of Client-Response (pairing-based authentication)	TI
IDP.UC_6	IDP-Dienst	Processing of Client-Response (SSO_TOKEN)	TI

IDP.UC_7	IDP-Dienst	Processing of Client-Response (Card-based authentication)	TI
IDP.UC_2	IDP-Dienst	Token Requests	TI
IDP.UC_3	IDP-Dienst	Processing of Authorization Requests (smartcard based)	Internet
IDP.UC_8	IDP-Dienst	Processing of Client-Response (pairing-based authentication)	Internet
IDP.UC_9	IDP-Dienst	Processing of Client-Response (SSO_TOKEN)	Internet
IDP.UC_10	IDP-Dienst	Processing of Client-Response (Card-based authentication)	Internet
IDP.UC_4	IDP-Dienst	Token Request	Internet
IDP.UC_11	IDP-Dienst	Processing of Authorization Requests (external authentication)	Internet
IDP.UC_12	IDP-Dienst	Processing of Client-Response (external authentication)	Internet
IDP.UC_20	sektoraler IDP	Processing of Client-Response (third-party-based authentication)	Internet
IDP.UC_21	sektoraler IDP	Token Request (third-party-based authentication)	Internet

423

424

425 *Hinweise:*

426 Die Duration für IDP.UC\_1 und IDP.UC\_3 beginnt mit der Annahme des Authorization Request und endet mit der Produktion der signierten Challenge.

427 Die Duration für IDP.UC\_5 bis IDP.UC\_10 beginnt mit der Annahme der signierten Authentication\_Data-Struktur am Authorization-Endpunkt und endet mit der Rückgabe der produzierten Authorization\_Codes und SSO\_TOKEN an das Authenticator-Modul.

431 Die Duration für IDP.UC\_11 beginnt mit der Annahme des Authorization Request und endet mit der Redirect-Antwort zum Authenticator Modul.

433 Die Duration für IDP.UC\_20 und IDP.UC\_21 beginnt mit der Annahme der signierten Authentication\_Data-Struktur am Authorization-Endpunkt und endet mit der Herausgabe des Token.

436

437

438

439

440 Erweiterung der Tabelle: Tab\_gemSpec\_Perf\_Fehlercodes

\$Dienst-Operation	Produkttyp	\$errorcode	Definition	Beschreibung
OCSP-Abfrage	IDP-Dienst	79001	OCSP_ERROR_NO_RESPONSE	Keine Antwort des OCSP oder Timeout
OCSP-Abfrage	IDP-Dienst	79879	OCSP_ERROR_WRONG_SIGNATUR E	Falsche oder fehlende Signatur in der OCSP Antwort
OCSP-Abfrage.failed	IDP-Dienst	79875	OCSP_ERROR_WRONG_DATA	Format der OCSP Anfrage fehlerhaft
OCSP-Abfrage	IDP-Dienst	79881	OCSP_ERROR_INVALID_RESPONS E	Antwort des OCSP fehlerhaft
OCSP-Abfrage	IDP-Dienst	79873	OCSP_CERT_MISSING	OCSP-Zertifikat nicht in TSL-enthalten
Sek-IDP-Abfrage	IDP-Dienst	79101	SEK_IDP_ERROR_NO_RESPONSE	Keine Antwort des sektoralen IDP oder Timeout
Sek-IDP-Abfrage	IDP-Dienst	79102	SEK_IDP_ERROR_INVALID_RESPO NSE	Antwort des sektoralen IDP fehlerhaft
IDP.failed	IDP-Dienst	79000	IDP_ERROR	alle internen Fehler des IDP

441

442

443 **A\_22229 - Performance - Rohdaten - Spezifika Sektoraler Identity Provider-**  
 444 **Message (Rohdatenerfassung v.02)**

445 Der Produkttyp "Sektoraler Identity Provider" MUSS bei Rohdaten-Performance-Berichten  
 446 bzgl. der "message"-Felder den Useragent im JSON-Format übermitteln:

447 **{ "Produktname": "name", "Produktversion": "version", "Herstellername": "hn**  
 448 **ame", "ID": "clientID" }**

449

450 (die Werte der jeweiligen Key-Value-Paare sind gemäß A\_20015-x zu befüllen)  
 451

452 **Tabelle 6: Tab\_gemSpec\_Perf\_Berichtsformat\_Sek\_IDP**

<b>\$IDP-Dienst-Operation</b>	<b>Produkttyp</b>	<b>Operation</b>	<b>Schnittstelle zu</b>
IDP.UC_20	sektoraler Identity Provider	Processing of Client-Response (third-party-based authentication)	Internet
IDP.UC_21	sektoraler Identity Provider	Token Request (third-party-based authentication)	Internet

453  
 454 Die Duration für IDP.UC\_20 und IDP.UC\_21 beginnt mit der Annahme der signierten  
 455 Authentication\_Data-Struktur am Authorization-Endpunkt und endet mit der Herausgabe  
 456 des Token.  
 457 [**<=**]

458

459 **A\_22048 - Performance - Rohdaten - Übermittlung bei dislozierten CIs**  
 460 **(Rohdatenerfassung v.02)**

461 Der Produkttyp "IDP-Dienst" KANN die Übermittlung der Rohdaten-Performance-Berichte  
 462 in Absprache mit dem Gesamtverantwortlichen TI je Standort vollziehen, wobei diese  
 463 Standorte dann eindeutig identifizierbar sein müssen, sofern das Configuration Item (CI)  
 464 über mehrere Standorte verteilt ist. [**<=**]

465 **3.2 [gemSpec\_IDP\_Frontend]**

466 **A\_22296 - Einlesen und Prüfen der Liste der alternativen**  
 467 **Authentisierungsanwendungen**

468 Das Authenticator-Modul des IDP-Dienstes MUSS die Liste der bekannten alternativen  
 469 Authentisierungsanwendungen unter der im Discovery Document des IDP-Dienstes  
 470 unter "kk\_app\_list\_uri" gefundenen Adresse beziehen und ihre Integrität prüfen.  
 471 Die Signatur des unter "kk\_app\_list\_uri" heruntergeladenen JWS muss mathematisch  
 472 geprüft und auf ein zeitlich gültiges C.FD.SIG-Zertifikat mit der Rollen-OID "oid\_idpd"  
 473 zurückgeführt werden, welches von einer dem Authenticator-Modul bekannten CA der  
 474 Komponenten-PKI ausgestellt wurde. [**<=**]

475 **A\_22294 - Ermöglichen der Nutzung von sektoralen Identity Providern zur**  
 476 **Authentisierung**

477 Das Authenticator-Modul des IDP-Dienstes MUSS dem Nutzer die Option zur Verwendung  
 478 von sektoralen Identity Providern zur Authentisierung ermöglichen. Hierzu MÜSSEN ihm  
 479 die Namen "kk\_app\_name" der verfügbaren alternativen  
 480 Authentisierungsanwendungen, aus der zuvor heruntergeladenen Liste, in  
 481 nachvollziehbarer Form auf der Benutzeroberfläche dargestellt und ihm eine Auswahl  
 482 angeboten werden. [**<=**]

483 **A\_22295 - Anfrage zur Authentisierung bei einem sektoralen Identity Provider**  
484 **beim IDP-Dienst**

485 Bei Auswahl eines sektoralen Identity Provider durch den Nutzer MUSS das  
486 Authenticator-Modul des IDP-Dienstes einen Authorization-Request an den Third-Party  
487 Authorization Endpoint des IDP-Dienstes senden. Der Authorization Request entspricht  
488 der in [gemSpec\_IDP\_Dienst#7.1] genannten Form, aber MUSS um einen weiteren  
489 Parameter "kk\_app\_id" ergänzt werden, dessen Wert dem Identifikator (kk\_app\_id) des  
490 Authenticator-Moduls eines sektoralen IDP-Dienstes entspricht, welcher zum vom  
491 Benutzer ausgewählten Namen (kk\_app\_name) gehört. [ <= ]

492 **A\_22299 - Weiterleitung des Authorization Request an einen sektoralen**  
493 **Identity Provider**

494 Im Falle der Nutzung von alternativen Authentisierungsanwendungen MUSS das  
495 Authenticator-Modul des IDP-Dienstes die Antwort des IDP-Dienstes als Authorization  
496 Request an die in der target\_url des redirect enthaltene URI weiterleiten und sich dabei  
497 den verwendeten "state" Parameter merken, um später erhaltene Antworten des  
498 sektoralen Identity Provider zuzuordnen. [ <= ]

499 *Hinweis: Es wird hierbei angenommen, dass auf dem Endgerät des Nutzers ein zum*  
500 *sektoralen Identity Provider gehörendes Authenticator-Modul existiert, das für die*  
501 *angegebene URL als Handler registriert ist.*

502 **A\_22313 - Absicherung des Aufrufs zu Authenticator-Modulen von sektoralen**  
503 **Identity Providern**

504 Das Authenticator-Modul des IDP-Dienstes MUSS für Aufrufe zu Authenticator-Modulen  
505 sektoraler Identity Provider die Verifikationsmechanismen des Betriebssystems  
506 verwenden. Die folgenden Parameter müssen gesetzt sein:

507 Android: Keine weiteren.

508 iOS: .universalLinksOnly:false [ <= ]

509 *Hinweis: Durch den Verzicht auf die zwingende Nutzung von Universal Links hat der*  
510 *Anbieter des sektoraler Identity Providers die Möglichkeit über die Webseite eine*  
511 *Fehlerbehandlung bei nicht installiertem Authenticator-Modul zu machen.*

512

513 **A\_22300 - Registrierung zur App-zu-App-Kommunikation**

514 Das Authenticator-Modul des IDP-Dienstes MUSS sich um App-zu-App-Aufrufe zu  
515 verarbeiten im Betriebssystem unter der URI [https://das-e-rezept-fuer-](https://das-e-rezept-fuer-deutschland.de)  
516 [deutschland.de](https://das-e-rezept-fuer-deutschland.de) registrieren. [ <= ]

517 **A\_22301 - Annahme des Authorization Code über App2App-Kommunikation**

518 Das Authenticator-Modul des IDP-Dienstes MUSS den Authorization Code  
519 "AUTHORIZATION\_CODE\_IDP", den state-Parameter sowie den Parameter  
520 "kk\_app\_redirect\_uri", welche mittels App2App-Kommunikation vom Authenticator-Modul  
521 des sektoralen Identity Provider übergeben werden, akzeptieren, wenn der state mit dem  
522 Wert einer kürzlich vom IDP-Dienst erhaltenen Anfrage übereinstimmt. [ <= ]

523 **A\_22302 - Weiterleitung des Authorization Code an den IDP-Dienst**

524 Das Authenticator-Modul des IDP-Dienstes MUSS den empfangenen Authorization Code  
525 "AUTHORIZATION\_CODE\_IDP", den state-Parameter sowie den Parameter  
526 "kk\_app\_redirect\_uri" als HTTP-POST an den im Discovery Document referenzierten  
527 Third-Party Authorization Endpoint des IDP-Dienstes weiterleiten. [ <= ]

528

529 **3.2.1 Registrierungsdaten des Authenticator-Moduls**

530 **A\_22349 - Funktionsfähigkeit des Authenticator-Modul des IDP-Dienstes**

531 Der Anbieter des Authenticator-Modul des IDP-Dienstes MUSS sicherstellen, dass die  
 532 durch das Betriebssystem notwendigen Voraussetzungen für die Funktionsfähigkeit des  
 533 Authenticator-Moduls des IDP (z.B. Manifest, Entitlement, Dateien im .well-known  
 534 Verzeichnis der verwendeten Domain aus A\_22300) erfüllt sind. [**<=**]

535

536 **A\_22291 - Registrierungsdaten des Authenticator-Moduls auf dem Endgerät**  
 537 **(Android)**

538 Das Authenticator-Modul des IDP-Dienstes MUSS zur korrekten Funktion der App2App-  
 539 Kommunikation in seiner Android-Distribution in seinem Manifest mindestens den  
 540 folgenden Intent aufnehmen:

Objekt	Ausgestaltung	Ergänzung
AndroidManifest.xml/Intent	<pre>                     &lt;intent-filter android:autoVerify="true"&gt;                     &lt;action android:name="android.intent.action.VIEW"                     /&gt;                     &lt;category                     android:name="android.intent.category.DEFAULT"/&gt;                     &lt;category                     android:name="android.intent.category.BROWSABLE"/&gt;                     &lt;data android:scheme="https" android:host="https://das-                     e-rezept-fuer-deutschland.de"/&gt;                     &lt;/intent-filter&gt;                 </pre>	Das Flag "autoVerify" MUSS auf "true" gesetzt werden. Der Parameter <URL> MUSS dem beim zentralen IDP-Dienst registrierten Wert entsprechen.

541 [**<=**]

542 *Hinweis: Das gesetzte Flag ist notwendige Voraussetzung für die Etablierung der App als*  
 543 *Default Handler für die im Host-Parameter genannten URL.*

544 **A\_22292 - Registrierungsdaten des Authenticator-Moduls auf dem Endgerät**  
 545 **(iOS)**

546 Das Authenticator-Modul des IDP-Dienstes MUSS zur korrekten Funktion der App2App-  
 547 Kommunikation in seiner iOS-Distribution mindestens das folgende Entitlement

548 aufnehmen:  
549

Objekt	Inhalt
*.entitlement	<pre>&lt;?xml version="1.0" encoding="UTF-8"?&gt; &lt;!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd"&gt; &lt;plist version="1.0"&gt; &lt;dict&gt;   &lt;key&gt;com.apple.developer.associated-domains&lt;/key&gt;   &lt;array&gt;     &lt;string&gt;applinks:erezept.dev.gematik.solutions&lt;/string&gt;   &lt;/array&gt;   &lt;key&gt;com.apple.developer.default-data-protection&lt;/key&gt;   &lt;string&gt;NSFileProtectionCompleteUnlessOpen&lt;/string&gt;   &lt;key&gt;com.apple.developer.nfc.readersession.formats&lt;/key&gt;   &lt;array&gt;     &lt;string&gt;TAG&lt;/string&gt;   &lt;/array&gt; &lt;/dict&gt; &lt;/plist&gt;</pre>

550 [ <= ]

551 **A\_22293 - Serverseitige Daten des Authenticator-Moduls**

552 Das Authenticator-Modul des IDP-Dienstes MUSS sicherstellen, dass unter [https://das-](https://das-e-rezept-fuer-deutschland.de)  
553 [e-rezept-fuer-deutschland.de](https://das-e-rezept-fuer-deutschland.de) die Dateien folgenden Inhalts im Verzeichnis ./well-  
554 known hinterlegt sind:

Plattform	Dateiname	Inhalt
Google/Android	assetLink.json	<pre>{   "relation": ["delegate_permission/common.handle_all_urls"],   "target": {     "namespace": "android_app",     "package_name": "&lt;Beispiel:com.example.erpfasttrack&gt;",     "sha256_cert_fingerprints":     [...]   } }</pre>
Apple/iOS	apple-app-site-association	<pre>{   "applinks": {     "details": [       {         "appIDs": [ "A9FL89PFFL.de.gematik.erp4ios.eRezept" ],         "paths": ["*"]       }     ]   },   .... }</pre>

555 [ <= ]

556 **3.3 [gemSpec\_IDP\_Dienst]**

557

558 **A\_22280 - Registrierung des IDP-Dienstes als Client bei sektoralen Identity**  
 559 **Providern**

560 Der Anbieter des IDP-Dienstes MUSS diesen bei allen sektoralen Identity Providern als  
 561 Confidential Client (gemäß [RFC6749#section-2.1]) registrieren. Hierbei müssen die  
 562 folgenden Metadaten verwendet werden:

Datenobjekt	Wert	Anmerkungen
client_id	"zentraler-idp-dienst"	
redirect_uri	URIs, von denen der sektorale Identity Provider Authorization Requests entgegennimmt	Der sektorale Identity Provider muss hier den IDP-Dienst mit all jenen "kk_app_redirect_uri"-Adressen registrieren, die er unterstützt.
PuK_IDP_SIG_Sek	öffentlicher Authentifizierungsschlüssel des zentralen IDP-Dienstes gegenüber den sektoralen Identity Providern	Mindestens ein Schlüssel ist zu übergeben.

563 [**<=**]

564 **A\_22282 - Periodisches Einlesen der Discovery Documents und Schlüssel der**  
 565 **sektoralen Identity Provider**

566 Der IDP-Dienst MUSS die Discovery Documents und JWKS-Schlüsselsätze der sektoralen  
 567 Identity Provider, bei denen er registriert ist, mindestens einmal stündlich  
 568 aktualisieren. [**<=**]

569 *Hinweis: Erfolgreich eingelesene Discovery Documents und Schlüssel dürfen im Fall einer*  
 570 *Nicht-Erreichbarkeit des Downloadpunktes bis maximal 24 Stunden verwendet werden.*

571

572 **3.3.1 Aufbau des Discovery Document**

573 **A\_22283 - Bereitstellung einer Liste der registrierten Authenticator-Module von**  
 574 **sektoralen Identity Providern**

575 Der IDP-Dienst MUSS unter einer dedizierten URL eine Liste der registrierten  
 576 Authenticator-Module von sektoralen Identity Providern bereitstellen, die eine Vielzahl  
 577 von Einträgen des folgenden Typs enthält:

Datum	Erläuterung	Anmerkung
kk_app_name	Ein für den Benutzer der Anwendungsfrontends interpretierbarer Name der Anwendung. Maximal 128 Zeichen.	Wird durch sektoralen Identity Provider festgelegt.

kk_app_id	ID des sektoralen IDP, welcher die Authentisierung für Versicherte dieser Krankenkasse durchführt. Maximal 32 VSCHAR (analog client_id nach [RFC6749]).	Wird durch IDP-Dienst festgelegt.
-----------	---	-----------------------------------

578 [ $\leq$ ]

579 **A\_22288 - Weitere Informationen zu registrierten sektoralen Authenticator-**  
 580 **Modulen**

581 Neben den gemäß A\_22283 bereitgestellten Informationen MUSS der IDP-Dienst für  
 582 jedes registrierte Authenticator-Module eines sektoralen Identity Providers die folgenden  
 583 Werte erfassen:

Datum	Erläuterung	Anmerkung
kk_app_uri	Aufzurufende URI für die Authentisierung. Hiermit ist die entsprechende App auf dem Gerät registriert. (URL).	Wird durch sektoralen Identity Provider festgelegt.
idp_iss	iss-Wert des sektoralen Identity Provider (URL).	Wird durch sektoralen Identity Provider festgelegt

584 [ $\leq$ ]

585 **A\_22284 - Festlegungen zur Signatur der Liste der registrierten Authenticator-**  
 586 **Module von sektoralen Identity Providern**

587 Der IDP-Dienst MUSS die Signatur der Liste der registrierten Authenticator-Module von  
 588 sektoralen Identity Providern durch die Verwendung einer JSON Web Signature (JWS)  
 589 [RFC7515 # section-3 - Compact Serialization] und des Schüssels "PrK\_DISC\_SIG"  
 590 gewährleisten. Als Algorithmus ist dementsprechend "BP256R1" zu wählen. Der IDP-  
 591 Dienst MUSS bei der Signaturerstellung das Signaturzertifikat des "PUK\_DISC\_SIG" im  
 592 x5c-Claim einbetten. [ $\leq$ ]

593 **A\_22285 - Vergabe einer eindeutigen ID je Authenticator-Modul der sektoralen**  
 594 **Identity Provider**

595 Der Anbieter des IDP-Dienstes MUSS für alle registrierten Authenticator-Module der  
 596 sektoralen Identity Provider eine eindeutige "kk\_app\_id" vergeben. [ $\leq$ ]

597 **A\_22286 - Erweiterung des Discovery Document des IDP-Dienstes**

598 Der IDP-Dienst MUSS im Discovery Document unter dem Schlüssel "kk\_app\_list\_uri" die  
 599 URL der Liste der registrierten Authenticator-Module der sektoralen Identity Provider  
 600 publizieren. [ $\leq$ ]

601 **A\_22287 - Veröffentlichung des Third-Party Authorization Endpoint**

602 Der IDP-Dienst MUSS die URL des angebotenen Third-Party Authorization Endpoint im  
 603 Discovery Document unter dem Schlüssel "third\_party\_authorization\_endpoint"  
 604 publizieren.

605 [ $\leq$ ]

606 **3.3.2 Third-Party Authorization Endpoint**

607 Der IDP-Dienst muss einen Third-Party-Authorization Endpoint bereitstellen, an  
 608 welchem Authorization Requests eingereicht werden, bei denen die eigentliche  
 609 Authentisierung anschließend unter Nutzung eines sektoralen Identity Provider  
 610 durchgeführt werden soll. Nach erfolgreicher Authentisierung erzeugt der IDP-Dienst aus den

611 Daten des abgerufenen ID-Token die eigenen Token für das Anwendungsfrontend und  
 612 den Fachdienst.

613 **A\_22262 - Bereitstellung eines Third-Party Authorization Endpoint**

614 Der IDP-Dienst MUSS einen Third-Party Authorization Endpoint unter einer dedizierten  
 615 URL bereitstellen und dort Authorization Requests und Authorization Codes eines  
 616 sektoralen Identity Provider annehmen. [**<=**]

617 **A\_22263 - Sitzungsmanagement des IDP-Dienstes zu einem sektoralen Identity  
 618 Provider**

619 Der IDP-Dienst MUSS für Anfragen zur Authentisierung an einem sektoralen Identity  
 620 Provider die folgenden Daten zur späteren Korrelation der Anfragen in einer Sitzung  
 621 speichern:

Quelle	Parameter	Erläuterung
E-Rezept-FdV/Daten aus dem Authorization Request des E-Rezept-FdV	client_id	Dies ist die client-id des Anwendungsfrontend.
	nonce_erp	Dies ist die Nonce für das ID-Token, das zum Anwendungsfrontend gesendet werden soll.
	state_erp	state-Parameter des Anwendungsfrontend
	code_challenge	code_challenge des Anwendungsfrontend
IDP-Dienst/Daten des Authorization Request des IDP-Dienstes an den sektoralen Identity Provider	nonce_idp	Nonce für das ID-Token des sektoralen Identity Provider
	code_verifier	Code-Verifier des IDP-Dienstes zur Abfrage des ID-Token
	kk_app_id	Identifizier für das zu nutzende Authenticator-Modul des angefragten sektoralen Identity Provider
	state_idp	state-Parameter es IDP-Dienstes zur Abfrage des ID-Tokenf Über diesen Wert wird die Sitzung anschließend referenziert.

622 Der IDP-Dienst MUSS diese Daten über den von ihm generierten state-Parameter  
 623 referenzieren und in den späteren Anwendungsfällen dereferenzieren können. [**<=**]

624 **3.3.2.1 Authorization-Endpoint Eingangsdaten**

625 **A\_22264 - Authorization-Request des IDP-Dienstes an sektorale Identity**  
 626 **Provider**

627 Wenn der Authorization Request einen Parameter "kk\_app\_id" mit dem Identifikator  
 628 eines sektoralen Authenticator-Moduls enthält, MUSS der IDP-Dienst selbst einen  
 629 Authorization Request als Client an den zugehörigen sektoralen Identity Provider stellen.  
 630 Der Request wird in Form eines HTTP-302-redirect als Antwort auf dessen  
 631 Authorisierungs-Request zurück an das Authenticator-Modul gesendet. Die "target\_url"  
 632 des "redirect" ist dabei die URL des Authenticator-Moduls des sektoralen Identity  
 633 Provider, welches durch den Parameter "kk\_app\_id" gewählt wurde. Hierbei sind die  
 634 folgenden Parameter zu verwenden:

Parameter	Wert	Anmerkung
client_id	"zentraler idp-dienst"	
state	dynamisch und zufällig zu erzeugen	Diesen State verwendet der IDP-Dienst, um die später erhaltene Antwort zuzuordnen.
redirect_uri	die Adresse des Authenticator-Moduls des IDP-Dienstes	Diese wird aus der ursprünglichen Anfrage übernommen.
code_challenge	mit der Methode "S256" erzeugter Hash des Code-Verifier	
code_challenge_method	"S256"	
response_type	code	
nonce	dynamisch und zufällig zu erzeugen	Nonce für das vom sektoralen IDP-Dienst zu erzeugende ID-Token
scope	"erp_sek_auth+openid"	

635 **[<=]**

636 Der Request geht als Antwort in Form eines HTTP-302-redirect auf den Authorisierungs-  
 637 Request zurück an das Authenticator-Modul (vergleiche Schritt 2 in ~~ML-122072~~  
 638 ~~Missing cross-reference~~ ). Die "target\_url" des redirect ist dabei die URL des  
 639 Authenticator-Moduls des sektoralen Identity Provider, welches durch den Parameter  
 640 "kk\_app\_id" gewählt wurde.

641 Auf einen "claims"-Parameter wird verzichtet.

642

643

644 **3.3.2.2 Authorization-Endpoint Ausgangsdaten**

645 **A\_22265 - Token Request des IDP-Dienstes an sektorale Identity Provider**

646 Bei eingehenden Authorization Requests am Third-Party Authorization Endpoint, die  
 647 anstelle eines Challenge-Token den AUTHORIZATION\_CODE\_IDP eines sektoralen  
 648 Identity Provider enthalten, MUSS der IDP-Dienst anhand des state-Parameters die  
 649 in A\_22263 definierten Sitzungsdaten rekonstruieren, selbst einen Token Request an den  
 650 sektoralen Identity Provider stellen und dabei als 'Confidential Client' agieren.

651  
 652 Der entsprechende sektorale Identity Provider ergibt sich dabei aus der gewählten  
 653 "kk\_app\_id" der Anfrage. Als "redirect\_uri" ist die übermittelte Adresse des  
 654 Authenticator-Moduls des sektoralen Identity Provider ("kk\_app\_redirect\_uri") zu  
 655 verwenden.

656  
 657 Hierbei sind die folgenden Inhalte zu verwenden:

Parameter	Wert	Anmerkung
grant_type	authorization_code	
code	AUTHORIZATION_CODE_IDP	Authorization_Code des sektoralen Identity Provider
code_verifier	<code_verifier des IDP-Dienstes>	aus den Sitzungsdaten
client_id	"zentraler-idp-dienst"	
redirect_uri	kk_app_redirect_uri	zusammen mit dem AUTHORIZATION_CODE übermittelte Adresse
client_assertion_type	"urn:ietf:params:oauth:client-assertion-type:jwt-bearer"	Authentisierung des confidential client entsprechend <a href="https://openid.net/specs/openid-connect-core-1_0.html#ClientAuthentication">https://openid.net/specs/openid-connect-core-1_0.html#ClientAuthentication</a> durch ein signiertes JWT
client_assertion	private_key_jwt	

659 [**<=**]

660 *Hinweis: Aufgrund der Speicherung und Referenzierung der Sitzungsdaten durch den*  
 661 *state-Parameter, reduziert sich die Prüfung auf Gleichheit zwischen übermittelten und*  
 662 *gespeicherten "state" auf die Prüfung des Vorhandensein einer unter dem übermittelten*  
 663 *"state" gespeicherten Sitzung.*

664 *Hinweis2: Der Timeout mit dem ein Request zum sektoralen Identity Provider*  
 665 *abgebrochen werden darf wird einheitlich für alle Abfragen (und analog zur Festlegung im*  
 666 *Kontext der OCSP Requests) auf 1100 ms festgelegt.*

667

668 **A\_22266 - Authentisierung des IDP-Dienstes gegenüber den sektoralen Identity**  
669 **Providern**

670 Der IDP-Dienst MUSS sich gegenüber dem Token-Endpunkt des sektoralen Identity  
671 Provider entsprechend [https://openid.net/specs/openid-connect-core-](https://openid.net/specs/openid-connect-core-1_0.html#ClientAuthentication)  
672 [1\\_0.html#ClientAuthentication](https://openid.net/specs/openid-connect-core-1_0.html#ClientAuthentication) als 'confidential client' mit einem "private\_key\_jwt"  
673 authentisieren.  
674 Dieses "private\_key\_jwt" hat eine maximale Gültigkeit von 3 Minuten und muss mit dem  
675 Schlüssel "PuK\_IDP\_SIG\_Sek" signiert werden. [ <= ]

676

677 **A\_22268 - Prüfung des ID-Token eines sektoralen Identity Provider**

678 Der IDP-Dienst MUSS empfangene ID-Token auf Authentizität gemäß  
679 [OpenID.Core#3.1.3.7] prüfen.  
680 Insbesondere MUSS die Signatur mit einem unter "jwks\_uri" referenzierter öffentlichen  
681 Schlüssel aus dem Discovery Document des sektoralen Identity Provider prüfbar sein.  
682 Dieser ist über die "kid" aus der Signatur des Token auszuwählen.  
683 Des Weiteren MUSS der IDP-Dienst prüfen, ob die im ID-Token enthaltene Nonce dem  
684 Wert "nonce\_idp" aus den Sitzungsdaten der Session entspricht. [ <= ]

685 **A\_22269 - Produktion eines Authorization Code nach Bestätigung des**  
686 **sektoralen Identity Provider**

687 Nach erfolgreicher Prüfung des ID-Token MUSS der IDP-Dienst auf Basis der  
688 Sitzungsdaten und der Inhalte der Claims einen Authorization Code wie in  
689 [gemSpec\_IDP#5.2.2] beschrieben produzieren und diesen zusammen mit dem  
690 gespeicherten 'State' und einem SSO\_TOKEN an das Anwendungsfrend  
691 übermitteln. [ <= ]

692 **A\_22270 - Löschung der Sitzungsdaten zum sektoralen Identity Provider**

693 Der IDP-Dienst MUSS nach erfolgter Ausstellung des Authorization Code oder Abbruch  
694 des Prozesses die unter dem vom ihm erzeugten 'State' gespeicherten Sitzungsdaten zur  
695 Anfrage an einen sektoralen Identity Provider löschen. [ <= ]

696 Der restliche Flow gestaltet sich wie in den Dokumenten [gemSpec\_IDP\_Dienst],  
697 [gemSpec\_IDP\_Frontend] und [gemSpec\_IDP\_Dienst] beschrieben. Dieses schließt die  
698 Produktion eines geeigneten ACCESS\_TOKEN durch den IDP-Dienst mit ein.

699

700 **3.3.3 Token-Endpunkt Ausgangsdaten**

701 **A\_22271 - Befüllen der Claims "given\_name", "family\_name",**  
702 **"organizationName", "professionOID", "idNummer", "acr" und "amr" nach**  
703 **Bestätigung durch einen sektoralen Identity Provider**

704 Der Token-Endpunkt MUSS benötigte Attribute in Claims für das  
705 auszustellende "ACCESS\_TOKEN" und das "ID\_TOKEN" ausschließlich aus den  
706 entsprechenden Claims des ID-Token des sektoralen Identity Provider beziehen.  
707 Der Claim "amr" MUSS entsprechend des ursprünglich zur Authentisierung verwendeten  
708 Authentisierungsmittels belegt werden.  
709

710 **Tabelle 7: TAB\_IDP\_DIENST\_000X Befüllung der Attribute nach Bestätigung durch einen**  
 711 **sektoralen Identity Provider**

Attribute	Versicherte
Attribute "given_name" (Claim)	Vorname (given_name)
Attribute "family_name" (Claim)	Nachname (family_name)
Attribute "organizationName" (Claim)	Herausgeber-ID (organization_number)
Attribute "professionOID"	1.2.276.0.76.4.49
Identifizier "idNummer" (Claim)	unveränderlicher Teil der KV-Nummer (idNummer)
Attribut "amr"	mfa
Attribut "acr"	gematik-ehealth-loa-high

712 [**<=**]

713

714 **3.4 [gemSpec\_IDP\_FD]**

715 **A\_20297-03 - Inhalte der Claims für Versicherte**

716 Fachdienste MÜSSEN bei ihrer Registrierung am IdP-Dienst sicherstellen, dass für  
 717 Versicherte mit einer eGK als Nutzer die fachlich benötigten Attribute aus der folgenden  
 718 Auswahl als Claims beantragt werden. Standardclaims sind mit "public", eigene Claims  
 719 mit "private" gekennzeichnet:  
 720

721 **Tabelle 8: TAB\_IDP\_FD\_0003 Inhalte der Claims für Versicherte**

Attribut	Inhalt
"iss" (public)	Beinhaltet die URL des IdP-Dienstes als HTTPS-Adresse mit Pfad und Angabe des Ports, wenn dieser vom Standard abweicht. Zusätzliche Query-Parameter sind nicht erlaubt.
"sub" (public)	Beinhaltet einen Identifikator. Es werden 3 Eingangswerte verwendet: der Fachdienstidentifizier (konfiguriert), ein

	<p>Fachdienst-spezifischer Salt (konfiguriert) und der Claim "idNummer".</p> <p>Diese Eingangswerte werden verkettet in der Reihenfolge: Fachdienstidentifizier, Claim "idNummer" und Fachdienst-spezifischer Salt. Dieser verkettete Text wird mit SHA-256 gehasht, das Ergebnis ist der Claim "sub".</p> <p>SHA256(fd_identifizier + idNummer + fd_salt)</p> <p>Dieser zusammengesetzte Wert wird nach der pairwise-Methode [ <a href="#">openid-connect-core-1_0 # PairwiseAlg</a>] vom IdP-Dienst zusammengestellt.</p>
"nonce" (public)	<p>Beinhaltet einen Zufallswert, welchen der IdP-Dienst nach den Vorgaben des Anwendungsfrontends befüllt und anhand dessen das Anwendungsfrend seine Vorgänge unterscheiden und zuordnen kann. (Dieser Claim ist nur in ID-Token enthalten.)</p>
"acr" (public)	<p>Authentication Context Class Reference gemäß [ <a href="#">openid-connect-core-1_0 # IDToken</a>] mit dem konkreten Wert "gematik-ehealth-loa-high".</p>
"amr" (public)	<p>Authentication Method Reference gemäß [ <a href="https://tools.ietf.org/html/rfc8176">https://tools.ietf.org/html/rfc8176</a>] und [ <a href="https://openid.net/specs/openid-connect-modrna-authentication-1_0.html">https://openid.net/specs/openid-connect-modrna-authentication-1_0.html</a>]</p>
"aud" (public)	<p>Hier sind gemäß [ <a href="#">RFC7519 # section-4.1.3</a>] entweder die URI des Fachdienstes oder ein entsprechender eindeutiger String eingetragen, die bzw. der den Fachdienst identifiziert.</p>
"professionOID" (private)	<p>Beinhaltet die professionOID des Versicherten gemäß [gemSpec_OID#Tab_PKI_402].</p>
"given_name" (public)	<p>Vorname des Versicherten: der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat oder dem ID-Token eines sektoralen Identity Provider aus.</p>
"family_name" (public)	<p>Nachname des Versicherten: der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat oder dem ID-Token eines sektoralen Identity Provider aus.</p>
"organizationName" (private)	<p>ID oder Name der bestätigende Stelle: der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat oder dem ID-Token eines sektoralen Identity Provider aus.</p>
"idNummer" (private)	<p>Beinhaltet die KVNR des Versicherten: der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat oder dem ID-Token eines sektoralen Identity Provider aus.</p>
"jti"	<p>ID des Token</p>

722 [**<=**]

723 *Hinweise:*

- 724 • Die Befüllung des Claim erfolgt grundsätzlich gemäß [ [rfc7519 # section-4](#)]
- 725 • Beispiel-Wert des Attributes "iss": "https://idp.zentral.idp.splitdns.ti-  
726 dienste.de"
- 727 • Das Attribut "iss" wird durch den IDP-Dienst befüllt.
- 728 • Das Attribut "aud" enthält die eindeutige URI des Fachdienstes oder einen beim  
729 IDP-Dienst ausschließlich diesem Fachdienst zugesprochenen Wert z. B. "E-  
730 Rezept" oder "eRp".
- 731 • Das Attribut "professionOID" des Versicherten wird durch den IDP-Dienst befüllt.
- 732 • Das Attribut "jti" kann als eindeutiger Identifikator für einen Replay-Schutz  
733 genutzt werden. Anhand des Attributs "jti" lassen sich "ID\_TOKEN"  
734 und "SSO\_TOKEN" einem bestimmten Vorgang zuordnen.

735 Die Aufbau von ACCESS\_TOKEN und ID\_TOKEN entspricht  
736 [gemSpec\_IDP\_Dienst#Kapitel 7.6 Token Response].

737

### 738 **3.5 [gemSpec\_FD\_eRp]**

#### 739 **A\_19439-01 - E-Rezept-Fachdienst - Authentifizierung Authentifizierungsstärke**

740 Der E-Rezept-Fachdienst MUSS die Authentifizierungsstärke des übergebenen IDP-Token  
741 anhand des Attributs "acr" im übergebenen IDP-Token im HTTP-Header "Authorization"  
742 auf dem Authentifizierungsniveau "hoch" feststellen und einen anderen Wert als bzw. ein  
743 Authentifizierungsniveau unterhalb von "gematik-ehealth-loa-high" mit dem HTTP-  
744 Status-Code 401 ablehnen.

745 [**<=**]

746