

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 Datenschutz- und Sicherheitsanforderungen der TI an Anbieter

Version: 1.12.0 CC
Revision: 199599238131
Stand: 18.12.201820.05.2020
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemSpec_DS_Anbieter

Dokumentinformationen

Änderungen zur Vorversion

Einarbeitung einer Änderung gemäß Änderungsliste [P17.1](#)[P21.3](#).

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.9.0	18.09.17		Initiale Erstellung	gematik
1.0.0	14.05.18		freigegeben	gematik
1.0.1	05.06.18	7.2.1	formale Anpassung	gematik
1.1.0	18.12.18	4.1, S. 20	Änderung gemäß Änderungsliste P17.1	gematik
1.1.2.0	18.12.18 20.05.20		freigegeben Anpassungen lt. Änderungsliste P21.3	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments	6
1.1 Zielsetzung	6
1.2 Zielgruppe	6
1.3 Geltungsbereich	6
1.4 Abgrenzungen	6
1.5 Methodik	7
2 Modularisierung	8
2.1 Zuordnung der Module zur Informationssicherheit	11
2.2 Zuordnung der Module zum Datenschutz	12
2.3 Regelungen im Anbietervertrag und Steckbriefen	14
3 Module der Informationssicherheit	15
3.1 Modul „Basis-IS“	15
3.2 Modul „Basis-ISMS“	16
3.3 Modul „Erweitertes ISMS“	19
3.4 Modul „TI-Sicherheitsbericht“	20
3.5 Modul „Erweiterter TI-Sicherheitsbericht“	21
4 Module des Datenschutzes	23
4.1 Modul „Basis-DS“	23
4.2 Modul „TI-Datenschutzbericht“	24
4.3 Modul „Erweiterter TI-Datenschutzbericht“	25
5 Spezifische Module	28
5.1 Module für weitere Anwendungen	28
5.1.1 Modul „Weitere Anwendungen (mit TI-Beeinträchtigung)“	29
5.1.2 Modul „Weitere Anwendungen (ohne TI-Beeinträchtigung)“	31
5.2 Modul „Schlüsselverwaltung“	31
5.3 Modul „Kartenherausgabe“	32
6 Anhang A – Verzeichnisse	34
6.1 Abkürzungen	34
6.2 Abbildungsverzeichnis	35
6.3 Tabellenverzeichnis	35
6.4 Referenzierte Dokumente	36

67	6.4.1 Dokumente der gematik.....	36
68	6.4.2 Weitere Dokumente.....	36
69	7 Anhang B – Modularisierungskonzept.....	38
70	7.1 Anordnung der Module.....	38
71	7.2 Kriterien der Modulzuordnung.....	40
72	7.2.1 Kriterium: Spezifikationshoheit der gematik.....	40
73	7.2.2 Kriterium: Beeinträchtigung der TI.....	43
74	8 Anhang C – Modulzuordnung bei Anwendbarkeit des § 274 Abs. 1 SGB V.....	48
76	1 Einordnung des Dokuments	6
77	1.1 Zielsetzung	6
78	1.2 Zielgruppe	6
79	1.3 Geltungsbereich	6
80	1.4 Abgrenzungen	6
81	1.5 Methodik	7
82	2 Modularisierung	8
83	2.1 Zuordnung der Module zur Informationssicherheit.....	11
84	2.2 Zuordnung der Module zum Datenschutz.....	12
85	2.3 Regelungen im Anbietervertrag und Steckbriefen	14
86	3 Module der Informationssicherheit.....	15
87	3.1 Modul „Basis-IS“	15
88	3.2 Modul „Basis-ISMS“	16
89	3.3 Modul „Erweitertes ISMS“	19
90	3.4 Modul „TI-Sicherheitsbericht“	20
91	3.5 Modul „Erweiterter TI-Sicherheitsbericht“	21
92	4 Module des Datenschutzes.....	23
93	4.1 Modul „Basis-DS“	23
94	4.2 Modul „TI-Datenschutzbericht“	24
95	4.3 Modul „Erweiterter TI-Datenschutzbericht“	25
96	5 Spezifische Module	28
97	5.1 Module für weitere Anwendungen	28
98	5.1.1 Modul „Weitere Anwendungen (mit TI-Beeinträchtigung)“	29
99	5.1.2 Modul „Weitere Anwendungen (ohne TI-Beeinträchtigung)“	31
100	5.2 Modul „Schlüsselverwaltung“	31

101	5.3 Modul „Kartenherausgabe“	32
102	6 Anhang A – Verzeichnisse	34
103	6.1 Abkürzungen	34
104	6.2 Abbildungsverzeichnis.....	35
105	6.3 Tabellenverzeichnis	35
106	6.4 Referenzierte Dokumente.....	36
107	6.4.1 Dokumente der gematik.....	36
108	6.4.2 Weitere Dokumente.....	36
109	7 Anhang B – Modularisierungskonzept.....	38
110	7.1 Anordnung der Module	38
111	7.2 Kriterien der Modulzuordnung.....	40
112	7.2.1 Kriterium: Spezifikationshoheit der gematik.....	40
113	7.2.2 Kriterium: Beeinträchtigung der TI	43
114	8 Anhang C – Modulzuordnung bei Anwendbarkeit des § 274 Abs. 1	
115	SGB V.....	48
116		
117		

1 Einordnung des Dokuments

1.1 Zielsetzung

Das Dokument definiert übergreifende Sicherheits- und Datenschutzanforderungen für Anbieter von Diensten der Telematikinfrastruktur (TI), Anbieter von Fachdiensten VSDM gemäß § 291 Abs. 2b SGB V, Anbieter von Rechenzentrums-Consumern (RZ-Consumer) sowie Anbieter weiterer Anwendungen gemäß § 291a Abs. 7 Satz 3 SGB V.

1.2 Zielgruppe

Das Dokument richtet sich an Anbieter von Diensten der Telematikinfrastruktur, Anbieter von Fachdiensten VSDM gemäß § 291 Abs. 2b SGB V, Anbieter von Rechenzentrums-Consumern (RZ-Consumer) sowie Anbieter weiterer Anwendungen gemäß § 291a Abs. 7 Satz 3 SGB V.

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 GmbH in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Wichtiger 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

Spezifische Datenschutz- und Sicherheitsanforderungen für einzelne Produkttypen sind in den jeweiligen Spezifikationen und Konzepten des Produkttyps festgelegt.

Übergreifende Anforderungen an die Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur sind in [gemSpec_Krypt] festgelegt.

Dieses Dokument enthält keine Anforderungen an Hersteller von Produkten der Telematikinfrastruktur. Diese sind in [gemSpec_DS_Hersteller] festgelegt.

151 **1.5 Methodik**

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

156 Sie werden im Dokument wie folgt dargestellt:

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

158 Text / Beschreibung

159 [**<=**]

160

161 Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

ENTWURF

162

2 Modularisierung

163 Dieses Dokument enthält übergreifende Datenschutz- und Sicherheitsanforderungen an
164 Anbieter von Diensten der TI, Anbieter von Fachdiensten VSDM gemäß § 291 Abs. 2b
165 SGB V, Anbieter von Rechenzentrums-Consumern (RZ-Consumer) gemäß
166 [gemKPT_Arch_TIP] sowie an Anbieter weiterer Anwendungen gemäß § 291a Abs. 7 S. 3
167 SGB V.

168 Der Begriff „Dienste der TI“ umfasst dabei Dienste der TI-Plattform, Dienste der
169 gesetzlichen Anwendungen der eGK nach § 291a Abs. 2 und Abs. 3 SGB V sowie Dienste
170 der sicheren Übermittlungsverfahren nach § 291b Abs. 1e SGB V.

171 Im Gegensatz zu den Diensten der TI fallen die Fachdienste VSDM nicht in den
172 gesetzlichen Aufgabenbereich der gematik gemäß § 291b Abs. 1 SGB V. Die Fachdienste
173 VSDM sind Fachdienste der Krankenkassen. Hieraus resultiert für die Fachdienste VSDM
174 eine gesonderte Anforderungszuordnung und sie werden daher auch nicht unter dem
175 Begriff „Dienste der TI“ subsummiert.

176 Ein RZ-Consumer ist ein in einem Rechenzentrum betriebener Produkttyp einer
177 Fachanwendung der TI, der als Consumer mit der TI interagiert und dabei sowohl Anteile
178 der TI-Plattform als auch Anteile der Fachanwendung enthält. Der Produkttyp KTR-AdV
179 ist ein Beispiel eines RZ-Consumers [gemSysL_AdV].

180 Alle Anforderungen sind in Module unterteilt. Jede Anforderung ist dabei genau einem
181 Modul zugeteilt. Diese Module werden anschließend Anbietern zugeordnet (siehe
182 Abbildung 1). Ist ein Modul einem Anbieter zugeordnet, muss dieser alle Anforderungen
183 des Moduls umsetzen.

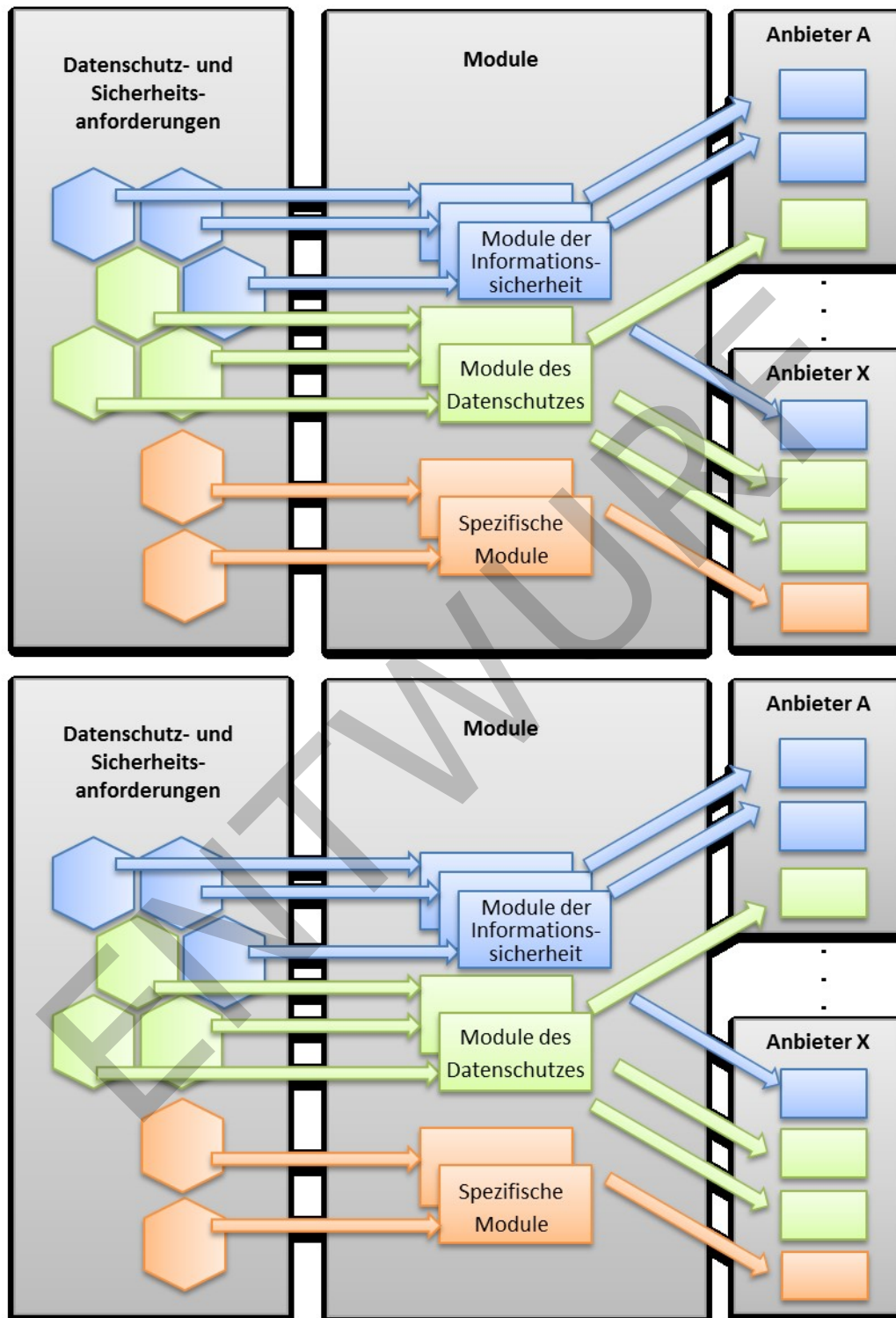
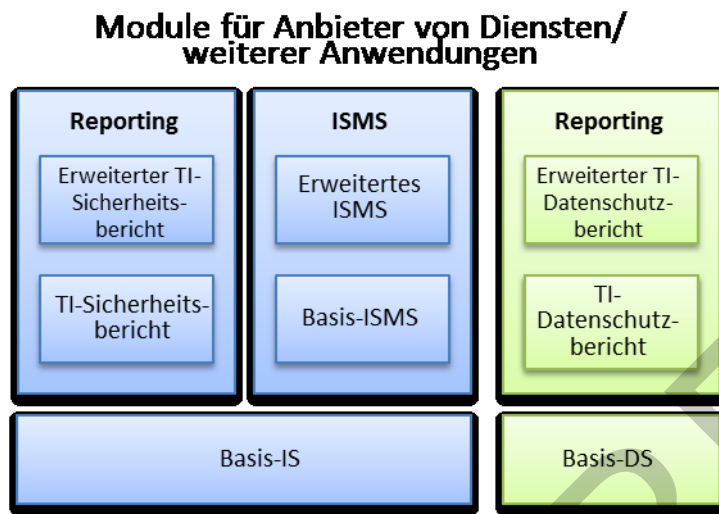
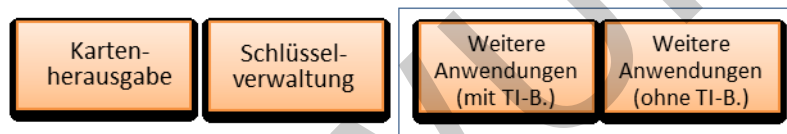


Abbildung 1 – Anforderungen, Module und Anbieter

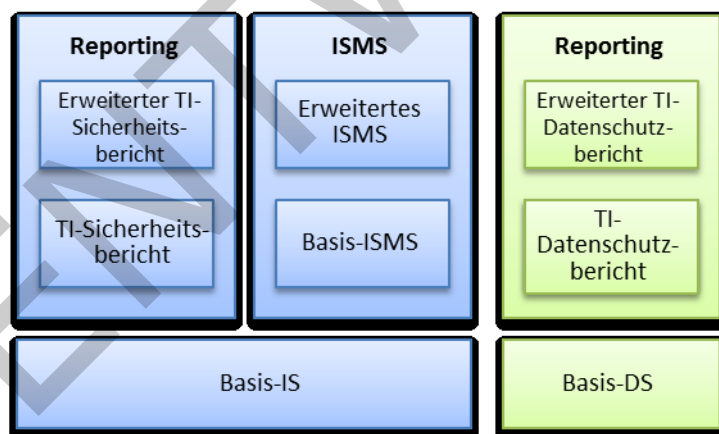
Abbildung 2 zeigt die Module im Überblick; unterteilt in Module zur Informationssicherheit (blau), zum Datenschutz (grün) sowie spezifische Module (rot). Die Anforderungen der Module sind in den Kapiteln 3, 4 und 5 beschrieben.



Spezifische Module



Module für Anbieter von Diensten/ weiterer Anwendungen



Spezifische Module

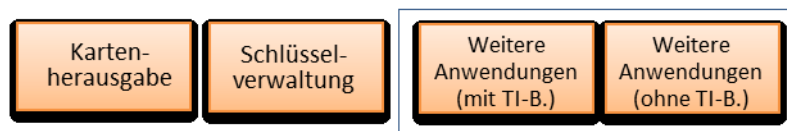


Abbildung 2 – Modulübersicht für Anbietermodule

Die Module zur Informationssicherheit (blau) und zum Datenschutz (grün) sind anbieter-
übergreifend, d. h. unabhängig von einer speziellen Rolle des Anbieters.

197 Darüber hinaus gibt es spezifische Module für Kartenherausgeber, Anbieter von
198 Schlüsselverwaltungen sowie Anbieter weiterer Anwendungen nach § 291a Abs. 7 S. 3
199 SGB V (unterteilt in weitere Anwendungen mit möglicher TI-Beeinträchtigung und weitere
200 Anwendungen, bei denen eine TI-Beeinträchtigung technisch ausgeschlossen ist). Diese
201 Module enthalten Sicherheitsanforderungen, die nur von Anbietern in diesen Rollen zu
202 erfüllen sind.

203 Im Folgenden bezeichnet der Begriff „weitere Anwendungen“ immer weitere
204 Anwendungen nach § 291a Abs. 7 S. 3 SGB V.

205 **2.1 Zuordnung der Module zur Informationssicherheit**

206 In diesem Abschnitt werden die anbieterübergreifenden Module zur
207 Informationssicherheit Anbietern von Diensten der TI, Anbietern der Fachdienste VSDM,
208 Anbietern von Rechenzentrums-Consumern (RZ-Consumer) und Anbietern weiterer
209 Anwendungen zugeordnet (Abbildung 3).

210 Bei den Fachdiensten VSDM und weiteren Anwendungen wird unterschieden, ob der
211 Verlust der Sicherheit des Dienstes die Sicherheit oder den Datenschutz der TI
212 beeinträchtigen könnte oder ob dies technisch ausgeschlossen ist. Dies ist abhängig vom
213 technischen Anschlusstyp des Dienstes an die TI.


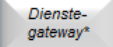

214 Die aktuell verfügbaren Anschlusstypen sind der Sichere Zentrale Zugangspunkt (SZZP)
215 und das Sicherheitsgateway Bestandsnetze (SG-BNet). Beim Sicherheitsgateway
216 Bestandsnetze kann eine Beeinträchtigung der TI technisch ausgeschlossen werden, da
217 darüber keine Dienste der TI erreichbar sind. Beim Verlust der Sicherheit eines über
218 einen SZZP an die TI angeschlossenen Dienstes hingegen ist eine Beeinträchtigung der TI
219 technisch nicht ausgeschlossen.

220 Derzeit werden die Fachdienste VSDM mittels SZZP an die TI angeschlossen. Daher
221 werden den Fachdiensten VSDM die Module der Zeile „Beeinträchtigt TI“ zugeordnet. Die
222 Zuordnung der Module zu den Fachdiensten VSDM berücksichtigt die Anwendbarkeit des
223 § 274 Abs. 1 SGB V (vgl. Anhang C).

224 Die gematik prüft, ob ein technischer Anschlusstyp zur Verfügung gestellt werden kann,
225 über den die Fachdienste VSDM und die weiteren Anwendungen ein Zugriff auf Dienste
226 der TI ermöglicht wird und der gleichzeitig die TI vor Angriffen schützt, um so
227 Sicherheitsanforderungen auf Seiten des Anbieters derart entbehrlich zu machen, dass
228 bestimmte Module zur Sicherheit für den Anbieter entfallen. In den Abbildungen ist dieser
229 intendierte technische Anschlusstyp als „Dienstegateway“ aufgenommen, um das Ziel zu
230 verdeutlichen, welche Module mit dem Dienstegateway im Gegensatz zum Anschluss
231 mittels SZZP entfallen sollen.

232 Für Dienste der TI-Plattform, der § 291a-eGK-Anwendungen und der sicheren
233 Übermittlungsverfahren sowie der KTR-AdV als RZ-Consumer ist die Zuordnung der
234 Module unabhängig vom Anschlusstyp. Der Verlust der Sicherheit der Dienste der TI
235 (selbst wenn sie nicht an das zentrale Netz der TI angeschlossen sind) und der KTR-AdV,
236 ist sofort auch eine Beeinträchtigung der Sicherheit der TI, da diese Produkttypen selbst
237 ein integraler Bestandteil der TI sind (daher „nicht anwendbar“ in der Abbildung). Zum
238 Beispiel könnte bei einer kompromittierten CVC-Root-CA (als Dienst der TI-Plattform)
239 CV-Schlüsselmateriale unautorisiert ausgestellt werden, das einen Zugriff auf medizinische
240 Daten von eGKs ermöglicht.

241 Die Produkttypen der TI-Plattform sind in [gemKPT_Arch_TIP] festgelegt.


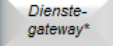

	TI-Plattform/ KTR-AdV	§291a-eGK- Anwendung/ SÜV	Fachdienste VSDM**	Weitere Anwendungen (§ 291a Abs. 7 S. 3 SGB V)
Beeinträch- tigt TI nicht  	nicht anwendbar	nicht anwendbar	In diesem Fall werden keine Module zugeordnet.	Basis-IS
Beeinträch- tigt TI 	<div>Erweiterter TI- Sicherheits- bericht</div> <div>Erweitertes ISMS</div> <div>TI-Sicherheits- bericht</div> <div>Basis- ISMS</div> <div>Basis-IS</div>	<div>Erweiterter TI- Sicherheits- bericht</div> <div>TI-Sicherheits- bericht</div> <div>Basis- ISMS</div> <div>Basis-IS</div>	<div>Basis-ISMS</div> <div>Basis-IS</div>	<div>TI-Sicherheits- bericht</div> <div>Basis- ISMS</div> <div>Basis-IS</div>

* in Planung (Arbeitstitel)
 ** Bei Fachdiensten VSDM gehören nur die Schnittstellen zur TI.

SG-BNet
 SZZP
 SÜV

= Sicherheitsgateway Bestandsnetze
 = Sicherer Zentraler Zugangspunkt
 = Sicheres Übermittlungsverfahren nach § 291b Abs. 1e SGB V

242

	TI-Plattform/ KTR-AdV	§291a-eGK- Anwendung/ SÜV	Fachdienste VSDM**	Weitere Anwendungen (§ 291a Abs. 7 S. 3 SGB V)
Beeinträch- tigt TI nicht  	nicht anwendbar	nicht anwendbar	In diesem Fall werden keine Module zugeordnet.	Basis-IS
Beeinträch- tigt TI 	<div>Erweiterter TI- Sicherheits- bericht</div> <div>Erweitertes ISMS</div> <div>TI-Sicherheits- bericht</div> <div>Basis- ISMS</div> <div>Basis-IS</div>	<div>Erweiterter TI- Sicherheits- bericht</div> <div>TI-Sicherheits- bericht</div> <div>Basis- ISMS</div> <div>Basis-IS</div>	<div>Basis-ISMS</div> <div>Basis-IS</div>	<div>TI-Sicherheits- bericht</div> <div>Basis- ISMS</div> <div>Basis-IS</div>

* in Planung (Arbeitstitel)
 ** Bei Fachdiensten VSDM gehören nur die Schnittstellen zur TI.

SG-BNet
 SZZP
 SÜV

= Sicherheitsgateway Bestandsnetze
 = Sicherer Zentraler Zugangspunkt
 = Sicheres Übermittlungsverfahren nach § 291b Abs. 1e SGB V

243

244 **Abbildung 3 – Zuordnung der Module der Informationssicherheit**

245 2.2 Zuordnung der Module zum Datenschutz

246 Abbildung 4 zeigt die Zuordnung der anbieterübergreifenden Module zum Datenschutz.

247 Anbietern werden Module zum Datenschutz nur zugeordnet, falls personenbezogene

248 Daten in ihren Diensten verarbeitet werden.

Die Anforderungen der gematik zum Datenschutz konkretisieren die bestehenden Vorschriften zum Datenschutz um TI-spezifische Vorgaben, die aus Sicht der gematik notwendig sind, ihren gesetzlichen Auftrag nach § 291b Abs. 1 SGB V zu erfüllen. Die Anforderungen der gematik ersetzen die bestehenden Vorschriften zum Datenschutz nicht. Diese sind weiterhin von den Anbietern in ihrer eigenen Verantwortung einzuhalten.

	TI-Plattform/ KTR-AdV	§291a-eGK- Anwendung/SÜV	Fachdienste VSDM**	Weitere Anwendungen (§ 291a Abs. 7 S. 3 SGB V)
Beeinträchtigt TI nicht 	nicht anwendbar	nicht anwendbar	In diesem Fall werden keine Module zugeordnet	Basis-DS
Beeinträchtigt TI 	 	 		

* in Planung (Arbeitstitel)

** Bei Fachdiensten VSDM gehören nur die Schnittstellen zur TI.

SG-BNet
SZZP
SÜV

= Sicherheitgateway Bestandsnetze

= Sicherer Zentraler Zugangspunkt

= Sicheres Übermittlungsverfahren nach § 291b Abs. 1e SGB V

	TI-Plattform/ KTR-AdV	§291a-eGK- Anwendung/SÜV	Fachdienste VSDM**	Weitere Anwendungen (§ 291a Abs. 7 S. 3 SGB V)
Beeinträchtigt TI nicht 	nicht anwendbar	nicht anwendbar	In diesem Fall werden keine Module zugeordnet	Basis-DS
Beeinträchtigt TI 	 	 		

* in Planung (Arbeitstitel)

** Bei Fachdiensten VSDM gehören nur die Schnittstellen zur TI.

SG-BNet
SZZP
SÜV

= Sicherheitgateway Bestandsnetze

= Sicherer Zentraler Zugangspunkt

= Sicheres Übermittlungsverfahren nach § 291b Abs. 1e SGB V

Abbildung 4 – Zuordnung der Module zum Datenschutz

259 **2.3 Regelungen im Anbietervertrag und Steckbriefen**

260 Neben den Anforderungen des Datenschutzes und der Informationssicherheit dieses
261 Dokumentes können sich für Anbieter weitere vertragliche Pflichten bzgl. Datenschutz
262 und Informationssicherheit ergeben.

263 Hierzu gehören insbesondere Festlegungen, ob bei Zuordnung des Moduls „Erweitertes
264 ISMS“ zusätzlich eine ISO27001-Zertifizierung gefordert wird.

265 Die Art des Nachweises der Anforderungen (Sicherheitsgutachten, Anbietererklärungen)
266 ergibt sich aus dem Steckbrief des Zulassungs- bzw. Bestätigungsobjekts.

ENTWURF

3 Module der Informationssicherheit

Dieses Kapitel beschreibt die Anforderungen der Module zur Informationssicherheit.

3.1 Modul „Basis-IS“

Die Anforderungen dieses Moduls fordern ein grundlegendes Informationssicherheitsmanagement. Vorgaben zu dessen konkreter Ausgestaltung erfolgen jedoch nicht.

GS-A_5551 - Betriebsumgebung in einem Mitgliedstaat der EU bzw. des EWR

Der Anbieter MUSS sicherstellen, dass sich die Betriebsumgebung/en der mittels der TI erreichbaren Dienste auf dem Gebiet eines Mitgliedstaates der EU bzw. des EWR befindet/befinden. [<=]

Hinweis: Anbietern von Fachdiensten VSDM wird die Anforderung GS-A_5551 aufgrund gesetzlicher Regelungen im SGB X nicht zugeordnet.

GS-A_5552 - Angemessene Sicherheitsmaßnahmen

Der Anbieter MUSS die erforderlichen technischen Maßnahmen treffen, um die Anforderungen an die Sicherheit des Dienstes der TI, des RZ-Consumers, der Fachdienste VSDM bzw. der weiteren Anwendung im Hinblick auf die Schutzbedürftigkeit der dort verarbeiteten Daten zu gewährleisten. [<=]

GS-A_5553 - Sicherheitskonzept

Der Anbieter MUSS eine aktuelle und nachvollziehbare Dokumentation besitzen, in der der Schutzbedarf der Daten und die technischen Maßnahmen beschrieben werden, die getroffen wurden, um die Anforderungen an die Sicherheit des Dienstes der TI, des RZ-Consumers, der Fachdienste VSDM bzw. der weiteren Anwendung im Hinblick auf die Schutzbedürftigkeit der dort verarbeiteten Daten zu gewährleisten. Es sind zudem die Wirksamkeit der Sicherheitsmaßnahmen hinsichtlich des Schutzbedarfs der verarbeiteten Daten, die Restrisiken, ein Netzstrukturplan und die Maßnahmen zum Notfallmanagement zu dokumentieren. [<=]

GS-A_5554 - Aufrechterhaltung der Informationssicherheit

Der Anbieter MUSS Prozesse zur Gewährleistung der Informationssicherheit aufbauen und kontinuierlich verbessern. [<=]

GS-A_4523-01 - Bereitstellung Kontaktinformationen für Informationssicherheit

Der Anbieter MUSS im Rahmen des Informationssicherheitsmanagements eine Kommunikationsschnittstelle direkt der gematik mitteilen (übliche Kontaktinformationen wie Name eines Ansprechpartners, Stellvertreter, E-Mailadresse, Telefon, Fax, Anschrift, ...). [<=]

GS-A_4524-01 - Meldung von Änderungen der Kontaktinformationen für Informationssicherheit

Der Anbieter MUSS Änderungen an der Kommunikationsschnittstelle seines Informations-sicherheits-managements der gematik unverzüglich direkt melden. [<=]

GS-A_5555 - Unverzügliche Meldung von erheblichen Sicherheitsvorfällen und -notfällen

Der Anbieter MUSS erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit, die zum Ausfall oder zur Beeinträchtigung der Sicherheit oder

309 Funktionsfähigkeit des Dienstes der TI, des RZ-Consumers, der Fachdienste VSDM bzw.
310 der weiteren Anwendung oder zum Ausfall oder zur Beeinträchtigung der Sicherheit oder
311 Funktionsfähigkeit der Telematikinfrastruktur führen können oder bereits geführt haben,
312 unverzüglich nach bekannt werden direkt der gematik melden. [≤]

313 **GS-A_5556 - Unverzügliche Behebung von erheblichen Sicherheitsvorfällen und**
314 **-notfällen**

315 Der Anbieter MUSS bei erheblichen Sicherheitsvorfällen oder Sicherheitsnotfällen, die
316 Dienste der TI, RZ-Consumer, Fachdienste VSDM bzw. weitere Anwendungen betreffen,
317 unverzüglich Maßnahmen zur Behebung des Vorfalls bzw. Notfalls umsetzen und den
318 erfolgreichen Abschluss direkt an die gematik melden. [≤]

319 Hinweis: TI-ITSM-Teilnehmer melden die erfolgreiche Behebung eines Vorfalls gemäß den
320 Vorgaben des Incident Managements (vgl. [gemRL_Betr_TI]).

321 **3.2 Modul „Basis-ISMS“**

322 Die Anforderungen dieses Moduls richten sich an die Ausgestaltung des ISMS beim
323 Anbieter.

324 **GS-A_4980-01 - Umsetzung der Norm ISO/IEC 27001**

325 Der Anbieter MUSS für mindestens genau die Umgebungen, in denen die Dienste der TI,
326 RZ-Consumer, der Fachdienste VSDM bzw. die weiteren Anwendungen betrieben werden,
327 die internationale Norm ISO/IEC 27001 umsetzen. [≤]

328 Hinweis: Falls Anbieter direkt von der gematik beauftragt werden, wird zusätzlich eine
329 ISO 27001-Zertifizierung mit einem Geltungs-bereich, der den betriebenen Dienst der TI
330 und die unterstützenden Systeme umfasst, gefordert.

331 **GS-A_4981-01 - Erreichen der Ziele der Norm ISO/IEC 27001 Annex A**

332 Der Anbieter MUSS für mindestens genau die Umgebungen, in denen die Dienste der TI,
333 RZ-Consumer, der Fachdienste VSDM bzw. die weiteren Anwendungen betrieben werden,
334 zu allen gemäß der Erklärung der Anwendbarkeit (engl. „Statement of Applicability“)
335 anwendbaren Maßnahmen (engl. „controls“) der internationalen Norm ISO/IEC 27001
336 ergreifen und die dort angegebenen Ziele (engl. „objectives“) erreichen. [≤]

337 **GS-A_4982-01 - Umsetzung der Maßnahmen der Norm ISO/IEC 27002**

338 Der Anbieter SOLL für mindestens genau die Umgebungen, in denen die Dienste der TI,
339 RZ-Consumer, der Fachdienste VSDM bzw. die weiteren Anwendungen betrieben werden,
340 beim Ergreifen der Maßnahmen (engl. „controls“) aus der internationalen Norm ISO/IEC
341 27002 die dort angegebene „Anleitung zur Umsetzung“ (engl. „implementation
342 guidance“) und die dort angegebenen „Weiteren Informationen“ (engl. „other
343 information“) befolgen. [≤]

344 Hinweis: Der Nachweis der Umsetzung der Anforderungen GS-A_4980-01, GS-A_4981-
345 01 und GS-A_4982-01 kann durch Vorlage eines ISO27001-Zertifikats, welches den
346 Geltungsbereich des Dienstes der TI, RZ-Consumers, der Fachdienste VSDM bzw. der
347 weiteren Anwendung und der unterstützenden Systeme umfasst, erfolgen.

348 **GS-A_4983-01 - Umsetzung der Maßnahmen aus dem BSI-Grundschutz**

349 Der Anbieter SOLL für mindestens genau die Umgebungen, in denen die Dienste der TI,
350 der RZ-Consumer, die Fachdienste VSDM bzw. die weiteren Anwendungen betrieben
351 werden, bei der Umsetzung der inter-nationalen Normen ISO/IEC 27001 und ISO/IEC
352 27002 die anwendbaren Anforderungen des BSI-Grundschutzkompendiums oder

entsprechende Maßnahmen, die ein vergleichbares Sicherheitsniveau gewährleisten,
umsetzen. [≤]

Hinweis: Der Anbieter muss aufgrund der Anforderung GS-A_4983-01 neben der nativen
ISO 27001-Vorgehensweise nicht die Grundsatzvorgehensweise (BSI Standard 200-X)
umsetzen. Eine zusätzliche Dokumentation ist aufgrund der Anforderung nicht
erforderlich. Das BSI-Grundsatzkompodium beschreibt zu erreichende
Sicherheitsanforderungen detaillierter als die Normen ISO 27001 und ISO 27002.
Hierdurch soll eine gemeinsame Baseline anhand des BSI-Grundsatzkompodiums
über das erforderliche Sicherheitsniveau und die Angemessenheit von Maßnahmen
erlangt werden. Beispielsweise wird es einem Sicherheitsgutachter hierdurch erleichtert,
die Angemessenheit von getroffenen Sicherheitsmaßnahmen besser einzuschätzen.

GS-A_3737-01 - Sicherheitskonzept

Der Anbieter MUSS die von ihm betriebenen Dienste der TI, RZ-Consumer, die
Fachdienste VSDM bzw. weiteren Anwendungen in seine bestehende
Sicherheitskonzeption einbinden oder ein betreiberspezifisches Sicherheitskonzept
erstellen. Folgende Inhalte MÜSSEN vom Anbieter mindestens dokumentiert werden:

- Beschreibung des Dienstes der TI, RZ-Consumers, der Fachdienste VSDM bzw. der
weiteren Anwendung bzgl. der Informationssicherheitsaspekte,
- Schutzbedarf der Daten,
- Bedrohungsanalyse,
- Dokumentation der Erfüllung der Sicherheitsanforderungen der gematik,
- Sicherheitsanalyse (Verifikation der Wirksamkeit der Sicherheitsmaßnahmen),
- Erstellung einer Restrisikoabschätzung.

[≤]

GS-A_3753-01 - Notfallkonzept

Der Anbieter MUSS die von ihm betriebenen Dienste der TI, RZ-Consumer, Fachdienste
VSDM bzw. weiteren Anwendungen in seine bestehende Notfallkonzeption einbinden oder
ein betreiberspezifisches Notfallkonzept erstellen. Folgende Inhalte MÜSSEN mindestens
dokumentiert werden:

- übergeordnete Notfallstrategie und Einordnung der Dienste der TI, RZ-Consumer,
der Fachdienste VSDM bzw. weiteren Anwendungen,
- gesetzliche und vertragliche Anforderungen,
- Rollen und Verantwortliche in Bezug auf das Notfall-Management,
- Dokumentation zur Notfallvorsorge inkl. durchgeführter Auswirkungsanalyse (BIA
oder vergleichbar),
- szenariounabhängige Notfallbewältigungsstrategie (Hierbei ist insbesondere auch
die TI-spezifische Eskalation zu weiteren Anbietern und zur gematik zu
beschreiben.),
- Dokumentation der szenariospezifischen Notfallpläne (Hierbei sind neben
allgemeinen Notfallplänen für Brand und Wassereinbruch etc. insbesondere auch
TI-spezifische Notfallszenarien wie der Ausfall verfügbarkeitskritischer TI-
Produkte, Schwächung oder Kompromittierung von kryptographischen
Schlüsselmaterial etc. zu dokumentieren.)
- Nachbereitung von Notfällen,

- Prävention und Vorbeugung von Notfällen, inklusive Fachkunde und Schulungen.

[<=]

GS-A_3772-01 - Notfallkonzept: Der Dienstanbieter soll dem BSI-Standard 100-4 folgen

Der Anbieter SOLL bei der Erstellung seines Notfallkonzeptes den inhaltlichen Vorgaben des Dokuments BSI-Standard 100-4 „Notfallmanagement“ [BSI 100-4] folgen.[<=]

GS-A_2328-01 - Pflege und Fortschreibung des Sicherheitskonzeptes und Notfallkonzeptes

Der Anbieter MUSS die Pflege und Fortschreibung der Sicherheits- und Notfallkonzepte für die von ihm betriebenen Dienste der TI, RZ-Consumer, Fachdienste VSDM bzw. weiteren Anwendungen durchführen.[<=]

GS-A_2329-01 - Umsetzung der Sicherheitskonzepte

Der Anbieter MUSS die Maßnahmen zur Sicherheit des Personals, der Organisation, der Infrastruktur und der eingesetzten Technologien entsprechend der erstellten Sicherheitskonzepte umsetzen und dokumentieren; wozu insbesondere die Implementierung und Einhaltung von organisatorischen und technischen Sicherheitsmaßnahmen und die Kommunikation sowie Durchführung von Sensibilisierungen für den Themenbereich „Informationssicherheit“ und Schulungen gehören.[<=]

GS-A_2345-01 - regelmäßige Reviews

Der Anbieter MUSS regelmäßige Reviews seiner bestehenden Sicherheitskonzepte inkl. der organisatorischen und technischen Sicherheitsmaßnahmen durchführen und die sich daraus ergebenden Verbesserungspotenziale umsetzen.[<=]

GS-A_2158-01 - Trennung von kryptographischen Identitäten und Schlüsseln in Produktiv- und Testumgebungen

Der Anbieter MUSS sicherstellen, dass kryptographische Identitäten bzw. Schlüssel der Produktivumgebung der TI des Anbieters (Umgebungen mit Echtdaten) nicht in Testumgebungen und dass keine kryptographischen Identitäten bzw. Schlüssel aus Testumgebungen in der Produktivumgebung der TI genutzt werden.[<=]

GS-A_4984-01 - Befolgen von herstellereigenen Vorgaben

Der Anbieter SOLL für die von ihm betriebenen Dienste der TI, RZ-Consumer, Fachdienste VSDM bzw. weiteren Anwendungen herstellereigene Sicherheitsvorgaben und -empfehlungen befolgen.[<=]

GS-A_2331-01 - Sicherheitsvorfalls-Management

Der Anbieter MUSS Sicherheitsvorfälle („security incidents“) wirksam vorbeugen, diese aufdecken und unterbinden.[<=]

GS-A_2355-01 - Meldung von erheblichen Schwachstellen und Bedrohungen

Der Anbieter MUSS erhebliche Schwachstellen und erhebliche Bedrohungen, die Dienste der TI, RZ-Consumer, Fachdienste VSDM bzw. weiteren Anwendungen betreffen, unverzüglich nach bekannt werden und direkt an die gematik melden.[<=]

GS-A_2332-01 - Notfallmanagement

Der Anbieter MUSS die durch Notfälle aufgetretenen Schäden zeitnah durch entsprechende Maßnahmen seines Notfallmanagements korrigieren.[<=]

A_19174 - Bereitstellung Übersicht Internet-Schnittstellen der TI

Der Anbieter MUSS der gematik halbjährlich und bei Änderungen eine Übersicht über die Außenschnittstellen der Telematikinfrastruktur (IP Adresse bzw. FQDN), die über das Internet hin erreichbar sind, zur Verfügung zu stellen.[<=]

A_19175 - Zustimmung zu regelmäßigen Schwachstellenscans durch die gematik

Der Anbieter MUSS zustimmen, dass die gematik monatliche nicht-invasive Schwachstellenscans auf die Außenschnittstellen ihrer TI-Produkte durchführen darf. [<=]

Spezialisierung von Anforderungen des Moduls Basis-IS

Das Modul Basis-ISMS spezialisiert die Anforderungen GS-A_5552, GS-A_5553 und GS-A_5554 des Moduls Basis-IS. Werden die Anforderungen des Moduls Basis-ISMS umgesetzt, so auch diese Anforderungen des Moduls Basis-IS. Daher werden die Anforderungen GS-A_5552, GS-A_5553 und GS-A_5554 nicht den Anbietern zugeordnet, denen das Modul Basis-ISMS zugeordnet ist.

3.3 Modul „Erweitertes ISMS“

Von Anbietern, denen das Modul „Erweitertes ISMS“ zugeordnet ist, wird eine enge Zusammenarbeit mit dem CERT der gematik hinsichtlich der Erkennung, Analyse, Bewertung und dem Umgang von Sicherheitsvorfällen, Schwachstellen, Bedrohungen und Risiken erwartet. Die folgenden Anforderungen konkretisieren diese Notwendigkeit.

GS-A_5557 - Security Monitoring

Der Anbieter MUSS im Rahmen eines Security Monitoring präventive Maßnahmen zur Erkennung und Analyse von Bedrohungen (z. B. über Korrelation und Auswertung von Log-Daten) durchführen. [<=]

Hinweis: Die durch den Anbieter auszuwertenden Informationen (z. B. Log-Daten der Kommunikationsverbindungen und anwendungsnaher Dienste) sind mit der gematik vor Betriebsaufnahme und im Rahmen der Einführung neuer Produkte und bei Änderungen an bestehenden Produkten abzustimmen. Die Anforderung GS-A_5557 gibt dabei bewusst nicht die einzusetzende Überwachungstechnologie bzw. Auswertungsmethode (z. B. IDS, SIEM) vor, sondern lässt den Anbietern die Freiheit bereits etablierte Technologien und Verfahren zu nutzen.

GS-A_5558 - Aktive Schwachstellenscans

Der Anbieter MUSS im Rahmen seines Schwachstellenmanagements mindestens monatliche Schwachstellenscans oder vergleichbare Maßnahmen zur Erkennung und Analyse von tech-nischen Schwachstellen („vulnerabilities“) in den vom ihm betriebenen Dienst der TI bzw. RZ-Consumer durchführen. [<=]

Hinweis: Als vergleichbar werden Maßnahmen angesehen, die eine kontinuierliche technisch unterstützte Erkennung von Schwachstellen gewährleisten (z.B. durch Inventarisierung der auf Systemen laufenden Dienste und Abgleich gegen aktuelle Schwachstelleninformationen). Schwachstellenscans dienen auch dazu, Veränderungen an IT-Systemen durch bereits erfolgte Kompromittierungen aufzudecken. Dieses Ziel kann alternativ auch durch eine automatisierte Integritätsüberwachung erreicht werden.

GS-A_5559 - Bereitstellung Ergebnisse von Schwachstellenscans

Der Anbieter MUSS der gematik die Ergebnisse von durchgeführten Schwachstellenscans oder der vergleichbaren Maßnahmen zur Erkennung und Analyse von technischen Schwachstellen monatlich zur Verfügung stellen. [<=]

Hinweis: Der genaue Detailgrad, das zu verwendende Format und die einzuhaltenden Sicherheitsmaßnahmen für die Übergabe der bereitzustellenden Ergebnisse sind vor

Betriebsaufnahme und im Rahmen der Einführung neuer Produkte und bei Änderungen an bestehenden Produkten mit der gematik abzustimmen.

GS-A_5017-01 - Meldung und Behandlung von Schwachstellen

Der Anbieter MUSS die gematik unverzüglich und direkt über Schwachstellen in den von ihnen betriebenen Diensten der TI bzw. RZ-Consumern informieren und sich mit der gematik anhand einer Einzelfall-betrachtung und -bewertung der Schwachstelle hinsichtlich der einzuleitenden Maßnahmen und der Behebungszeit abstimmen. [<=]

Hinweis: Die erforderliche Abstimmung ist durch den Change-Prozess gemäß [gemRL_Betr_TI] abgedeckt. Sofern durch die Schwachstelle eine unmittelbare Gefahr im Verzug besteht, ist der Anbieter angehalten, auch vor Abstimmung mit der gematik Sofortmaßnahmen zur Gefahrenabwehr einzuleiten.

GS-A_5560 - Entgegennahme und Prüfung von Meldungen der gematik

Der Anbieter MUSS von der gematik übermittelte Meldungen zu Schwachstellen, Bedrohungen und Sicherheitsvorfällen annehmen, bewerten und die erforderlichen Maßnahmen mit der gematik abstimmen und umsetzen. [<=]

Hinweis: Sofern der Anbieter als Verpflichteter gemäß BSI-Gesetz Meldungen aus dem Lagezentrum des BSI erhält, wird die gematik diese Meldungen in der Regel nicht nochmals an die Anbieter zur Bewertung weiterleiten.

GS-A_5561 - Bereitstellung 24/7-Kontaktpunkt

Der Anbieter MUSS der gematik einen Kontaktpunkt benennen, über den der Anbieter jederzeit sicherheitsrelevante Meldungen der gematik entgegennehmen kann, um eine unverzügliche Bearbeitung und Reaktion zu gewährleisten. [<=]

Hinweis: Sofern der Anbieter aufgrund gesetzlicher Anforderungen bereits eine Kontaktstelle zum BSI eingerichtet hat, kann der Anbieter diese auch für den Kontakt zur gematik nutzen.

GS-A_5562 - Bereitstellung Produktinformationen

Der Anbieter MUSS der gematik halbjährlich eine aktuelle Liste der zur Leistungserbringung von Diensten der TI bzw. RZ-Consumern verwendeten Hard- und Softwareprodukte sowie dem zugehörigen TI-Produkttyp übermitteln. [<=]

Hinweis: Die zur Verfügung gestellten Produktinformationen (z.B. Betriebssystem, eingesetzte Webserver, Datenbanken, Netzwerkkomponenten inkl. jeweils aktueller Version) dienen dazu, bei Schwachstellen und Sicherheitsvorfällen die Sicherheitslage der TI besser einschätzen zu können und mit Anbietern gezielt Maßnahmen zur Beseitigung der Schwachstellen zeitnah abstimmen zu können. Von Interesse sind hierbei insbesondere exponierte Systeme der TI und Spezialkomponenten, die für die Sicherheit der TI eine besondere Bedeutung haben.

Der Detailgrad und das zu verwendende Format der bereitzustellenden Liste der Produktinformationen sind vor Betriebsaufnahme und im Rahmen der Einführung neuer Produkte und bei Änderungen an bestehenden Produkten mit der gematik abzustimmen.

3.4 Modul „TI-Sicherheitsbericht“

GS-A_5563 - Jahressicherheitsbericht

Der Anbieter MUSS sicherstellen, dass der gematik jährlich ein Sicherheitsbericht vorliegt (spätestens bis Ende März des Folgejahres), der mindestens folgende Inhalte hat:

- allgemeiner Überblick des Sicherheitsstatus der vom Anbieter betriebenen Dienste der TI, RZ-Consumer bzw. weiteren Anwendungen (einschl. sicherheitsrelevanter Erkenntnisse aufgrund gesetzlicher Änderungen, des technischen Fortschritts oder veränderter Bedrohungslage)
- Übersicht der im Jahreszeitraum eigenverantwortlich durchgeführten Audits (Management Summary)
- Handlungsempfehlungen und Entscheidungsbedarf auf Seiten der gematik.

[<=]

GS-A_4530-01 - Maßnahmen zur Behebung von erheblichen Sicherheitsvorfällen und Notfällen

Der Anbieter MUSS sich bei erheblichen Sicherheitsvorfällen und Notfällen mit der gematik hinsichtlich der Maßnahmen und deren Umsetzung abstimmen sowie deren erfolgreichen Abschluss direkt der gematik melden. [<=]

Hinweis: Die erforderliche Abstimmung ist durch den Change-Prozess gemäß [gemRL_Betr_TI] abgedeckt. Der Anbieter ist bei erheblichen Sicherheitsvorfällen und Notfällen angehalten, auch vor Abstimmung mit der gematik Sofortmaßnahmen zur Gefahrenabwehr einzuleiten.

GS-A_4532-01 - Nachweis der Umsetzung von Maßnahmen in Folge eines erheblichen Sicherheitsvorfalls oder Notfalls

Der Anbieter MUSS der gematik auf Anfrage die Umsetzung der Maßnahmen zur Behebung eines erheblichen Sicherheitsvorfalls oder Notfalls, z. B. in Form von zur Verfügung gestellten Dokumentationen, neuen Regelungen oder Prozessen sowie anhand von Auszügen aus der Konfiguration oder Logdaten, nachweisen. [<=]

Hinweis: Die Nachweise der Umsetzung der Maßnahmen in Folge eines erheblichen Sicherheitsvorfalls oder Notfalls kann über den Changemanagement-Prozess erfolgen. Sofern einzelne Nachweise aufgrund von Vertraulichkeitsbeschränkungen der gematik nicht übermittelt werden dürfen, kann die Anforderung auch durch Einsichtnahme der gematik vor Ort beim Anbieter im Rahmen eines anlassbezogenen Audits erfüllt werden.

GS-A_5324-01 - Teilnahme des Anbieters an Sitzungen des kISMS

Der Anbieter MUSS der gematik zusichern, dass der Anbieter das koordinierende Informationssicherheitsmanagementsystem (kISMS) der gematik unterstützt, indem auf Einladung der gematik ein Sicherheitsbeauftragter des Anbieters am Arbeitskreis Datenschutz und Informationssicherheit (AK DIS) teilnimmt, der sich im Rahmen seiner beruflichen Tätigkeit mit dem operativen Betrieb der vom Anbieter betriebenen Dienste befasst. [<=]

Hinweis: Sofern die Ziele des AK DIS durch die Teilnahme des Anbieters in anderen Gremien der gematik erreicht werden können, kann die gematik auf die Einladung des Anbieters zur Teilnahme am AK DIS verzichten.

3.5 Modul „Erweiterter TI-Sicherheitsbericht“

GS-A_5624 - Auditrechte der gematik zur Informationssicherheit

Der Anbieter MUSS zusichern, dass die gematik oder ein von ihr zur Geheimhaltung verpflichteter Bevollmächtigter berechtigt sind,

- pro Kalenderjahr maximal ein Regelaudit durchzuführen. Hiervon unbenommen ist das Recht der gematik, anlassbezogene Audits durchzuführen,

- im Rahmen eines Audits beim Anbieter die konkrete Umsetzung der an den Anbieter gestellten Anforderungen der TI zur Informationssicherheit zu überprüfen,
- im Rahmen eines Audits während der üblichen Geschäftszeiten die Geschäftsräume des Anbieters zu betreten,
- im Rahmen eines Audits alle für das Audit benötigten Informationen zur Verfügung gestellt zu bekommen und insbesondere die erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte zu erhalten.

Dies hat der Anbieter im gleichen Maße für Unterauftragnehmer zuzusichern. Die Kosten, die dem Anbieter durch diese Mitwirkungspflichten entstehen, trägt der Anbieter selbst. [≤]

Hinweis: Die gematik verfolgt mit der Durchführung der Audits das Ziel, gemeinsam mit den Anbietern in einem kooperativen Ansatz die Aufrechterhaltung des erforderlichen Sicherheitsniveaus nachzuweisen. Die gematik wird ein Regelaudit in der Regel drei Monate vor der Durchführung beim Anbieter ankündigen. Die Terminvereinbarung erfolgt im Einvernehmen mit dem Anbieter. Die gematik erstellt im Vorfeld einen Auditplan, aus dem der Umfang und die zu betrachtenden Themenbereiche festgelegt sind und stimmt den Auditplan mit dem Anbieter ab. Die gematik muss das Auditrecht nicht notwendigerweise jedes Jahr wahrnehmen.

GS-A_4526-01 - Aufbewahrungsvorgaben an die Nachweise zu Sicherheitsmeldungen

Der Anbieter MUSS geeignete Nachweise zu den an die gematik übermittelten Sicherheitsmeldungen mindestens ein Jahr, nachdem diese bei der gematik eingegangen sind, vorhalten, um bei einem Informationssicherheitsaudit die Nachvollziehbarkeit der gemachten Meldungen zu ermöglichen. [≤]

4 Module des Datenschutzes

Dieses Kapitel beschreibt die Anforderungen der Module zum Datenschutz.

4.1 Modul „Basis-DS“

GS-A_2076-01 - kDSM: Datenschutzmanagement nach BSI

Der Anbieter MUSS ein Datenschutzmanagement nach Baustein CON.2 des IT-Grundschutzkompendiums umsetzen[<=]

GS-A_5564 - kDSM: Ansprechpartner für Datenschutz

Der Anbieter MUSS der gematik eine Kommunikationsschnittstelle für Datenschutz (übliche Kontaktinformationen, wie Name eines Ansprechpartners, Stellvertreter, E-Mail-Adresse, Telefon, Fax, Anschrift, ...) sowie die für den Anbieter zuständige datenschutzrechtliche Aufsichtsbehörde mitteilen.[<=]

Hinweis: Bei der in GS-A_5564 geforderten Kommunikationsschnittstelle muss es sich nicht notwendigerweise um den betrieblichen Datenschutzbeauftragten handeln.

GS-A_4479-01 - kDSM: Meldung von Änderungen der Kontaktinformationen zum Datenschutzmanagement

Der Anbieter MUSS der gematik Änderungen der Kontaktinformationen seines Datenschutzmanagements unverzüglich mitteilen.[<=]

GS-A_4473-01 - kDSM: Unverzügliche Benachrichtigung bei Verstößen gemäß Art. 34 DSGVO

Der Anbieter MUSS jeden Datenschutzverstoß, der die Voraussetzungen für eine Benachrichtigung der Betroffenen nach Art. 34 DSGVO erfüllt und der sich auf die vom Anbieter betriebenen Dienste der TI, RZ-Consumer, Fachdienste VSDM bzw. die weiteren Anwendungen bezieht, unverzüglich nach bekannt werden der gematik zusammen mit folgenden Informationen melden:

- Die nach Art. 33 Abs. 3 DSGVO geforderten Informationen.
- Eine Information darüber, ob der Verstoß bei einem Auftragsverarbeiter erfolgte.

[<=]

Hinweis: Die vorstehende Anforderung knüpft an den Inhalt der DSGVO unabhängig von deren Anwendbarkeit an. Gleiches gilt für nachstehende Anforderungen, in denen auf Voraussetzungen der DSGVO verwiesen wird.

GS-A_5565 - kDSM: Unverzügliche Behebung von Verstößen gemäß Art. 34 DSGVO

Der Anbieter MUSS im Fall von Datenschutzverstößen, die die Voraussetzungen für eine Benachrichtigung der Betroffenen nach Art. 34 DSGVO erfüllen und die sich auf die vom Anbieter betriebenen Dienste der TI, RZ-Consumer, Fachdienste VSDM bzw. die weiteren Anwendungen beziehen, unverzüglich Maßnahmen zur Behebung des Verstoßes umsetzen und den erfolgreichen Abschluss unverzüglich an die gematik melden.[<=]

Hinweis: TI-ITSM-Teilnehmer melden die erfolgreiche Behebung eines Verstoßes gemäß den Vorgaben des Incident Managements (vgl. [gemRL_Betr_TI]).

GS-A_5626 - kDSM: Auftragsverarbeitung

Falls ein Anbieter als Auftragsverarbeiter i. S. des Art. 4 Nr. 8 DSGVO tätig ist, MUSS dieser mit dem Auftraggeber als Verantwortlichen i. S. des Art. 4 Nr. 7 DSGVO verbindlich regeln, wie die Pflichten des Anbieters gegenüber der gematik, die sich aus den Sicherheits- und Datenschutzanforderungen der gematik ergeben, erfüllt werden.[<=]

Hinweis: Die Ausgestaltung der Regelung obliegt den Vertragsparteien der Auftragsverarbeitung.

4.2 Modul „TI-Datenschutzbericht“

Ist einem Anbieter der jährliche Datenschutzbericht des Moduls „Erweiterter TI-Datenschutzbericht“ (s. Afo GS-A_4468-02) zugeordnet, entfällt der in GS-A_4468-01 geforderte jährliche Datenschutzbericht (kurz).

GS-A_4468-01 - kDSM: Jährlicher Datenschutzbericht (kurz)

Der Anbieter MUSS gewährleisten, dass der gematik jährlich (spätestens bis Ende März des Folgejahres) ein Jahresdatenschutzreport bzgl. der vom Anbieter angebotenen Dienste der TI, RZ-Consumer bzw. die weiteren Anwendungen vorliegt, der mindestens folgende Inhalte enthält:

- eine Übersicht über die Anzahl der aufgetretenen Datenschutzverstöße, die die Voraussetzungen nach Art. 83 Abs. 4, 5 und 6 DSGVO erfüllen, bei denen Dienste der TI, RZ-Consumer bzw. weitere Anwendungen betroffen waren; hierbei ist jeweils anzugeben, gegen welche Bestimmung verstoßen wurde,
- eine Übersicht über die Anzahl der aufgetretenen Verletzungen des Schutzes personenbezogener Daten, die die Voraussetzungen gemäß Art. 33 und 34 DSGVO erfüllen, bei denen Dienste der TI, RZ-Consumer bzw. weitere Anwendungen betroffen waren,
- eine Übersicht über die Anzahl der von Betroffenen gestellten Anfragen zur Wahrnehmung der Betroffenenrechte aufgeschlüsselt nach Art. 15 (Auskunft), Art. 16 (Berichtigung), Art. 17 (Löschung), Art. 18 (Einschränkung), Art. 20 (Datenübertragbarkeit) und Art. 21 (Widerspruch) DSGVO, bezogen auf Dienste der TI, RZ-Consumer bzw. weitere Anwendungen. Sofern die DSGVO nicht anwendbar ist, sind die vorstehenden Angaben entsprechend bereitzustellen,
- eine Übersicht über die Anzahl der von Betroffenen bei der Aufsichtsbehörde eingereichten Beschwerden gem. Art. 77 DSGVO, die den Anbieter als Betreiber eines Dienstes der TI, RZ-Consumers bzw. einer weiteren Anwendung betreffen.

Bei der KTR-AdV sind Angaben im Bericht nur insoweit zu machen, sofern sie nicht die Versichertenstammdaten nach § 291 SGB V betreffen.[<=]

Hinweis: Im jährlichen Datenschutzbericht der TI ist jeweils nur die Anzahl der Datenschutzverstöße, Anfragen bzw. Beschwerden zu nennen, nicht jedoch deren Inhalte.

Hinweis: Der KTR-AdV wird die Anforderung GS-A_4468-01 nicht zugeordnet, da in der aktuellen Ausbaustufe der TI in der KTR-AdV keine medizinischen Daten nach § 291a Abs. 3 SGB V verarbeitet werden. Beim Ausbau der TI ist zu prüfen, ob diese Bedingung dann weiterhin erfüllt ist und die Zuordnung der Anforderung GS-A_4468-01 erfolgen muss.

Neben dem Jahresdatenschutzreport ist im Falle gravierender Datenschutzverstöße die erfolgreiche Umsetzung der Maßnahmen zur Behebung des Verstoßes der gematik zu melden.

GS-A_4478-01 - kDSM: Nachweis der Umsetzung von Maßnahmen in Folge eines gravierenden Datenschutzverstößes

Der Anbieter MUSS der gematik auf Anfrage die Umsetzung der Maßnahmen zur Behebung eines Datenschutzverstößes, der die Voraussetzungen für eine Benachrichtigung der Betroffenen nach Art. 34 DSGVO erfüllt und der sich auf die vom Anbieter betriebenen Dienste der TI, RZ-Consumer bzw. weitere Anwendungen bezieht, unter zur Verfügungsstellung einer Dokumentation mit den in Art. 33 Abs. 5 DSGVO geforderten Inhalten nachweisen.

Bei der KTR-AdV sind Nachweise zur Umsetzung von Maßnahmen nur insoweit zu machen, sofern sie nicht die Versichertenstammdaten nach § 291 SGB V betreffen. [≤]

GS-A_5324-02 - kDSM: Teilnahme des Anbieters an Sitzungen des kDSM

Der Anbieter MUSS der gematik zusichern, dass der Anbieter das koordinierende Datenschutzmanagementsystem der gematik unterstützt, indem auf Einladung der gematik ein sachkundiger Ansprechpartner für Datenschutz des Anbieters am Arbeitskreis Datenschutz und Informationssicherheit (AK DIS) teilnimmt, der sich im Rahmen seiner beruflichen Tätigkeit mit dem operativen Betrieb der vom Anbieter betriebenen Dienste befasst. [≤]

Hinweis: Sofern die Ziele des AK DIS durch die Teilnahme des Anbieters in anderen Gremien der gematik erreicht werden können, kann die gematik auf die Einladung des Anbieters zur Teilnahme am AK DIS verzichten.

4.3 Modul „Erweiterter TI-Datenschutzbericht“

Ist einem Anbieter der jährliche Datenschutzbericht (GS-A_4468-02) zugeordnet, entfällt der in GS-A_4468-01 geforderte jährliche Datenschutzbericht (kurz) des Moduls „TI-Datenschutzbericht“.

GS-A_4468-02 - kDSM: Jährlicher Datenschutzbericht der TI

Der Anbieter MUSS gewährleisten, dass der gematik jährlich (spätestens bis Ende März des Folgejahres) ein Jahresdatenschutzreport bzgl. der vom Anbieter angebotenen Dienste der TI bzw. RZ-Consumer vorliegt, der mindestens folgende Inhalte enthält:

- eine Liste der Verarbeitungsvorgänge nach Art. 35 Abs. 4 DSGVO mit Bezug zu Diensten der TI bzw. RZ-Consumern, für die eine Datenschutz-Folgenabschätzung durchgeführt wurde inkl. der Bewertung der Risiken gemäß Art. 35 Abs. 7 Buchstabe c) DSGVO,
- eine Übersicht über die getroffenen technischen und organisatorischen Maßnahmen zur Umsetzung der Grundsätze für die Verarbeitung personenbezogener Daten entsprechend Art. 5 DSGVO,
- eine Übersicht über die Umsetzung der technischen und organisatorischen Maßnahmen entsprechend Art. 32 DSGVO zum Schutz der personenbezogenen Daten in den Diensten der TI bzw. RZ-Consumern,
- eine Übersicht der durchgeführten Audits mit thematischem Inhalt, bei denen Dienste der TI bzw. RZ-Consumer betroffen waren,

- eine Übersicht über die Anzahl der aufgetretenen Datenschutzverstöße, die die Voraussetzungen nach Art. 83 Abs. 4, 5 und 6 DSGVO erfüllen, bei denen Dienste der TI bzw. RZ-Consumer betroffen waren; hierbei ist jeweils anzugeben, gegen welche Bestimmung verstoßen wurde,
- eine Übersicht über die Anzahl der aufgetretenen Verletzungen des Schutzes personenbezogener Daten, die die Voraussetzungen gemäß Art. 33 und 34 DSGVO erfüllen, bei denen Dienste der TI bzw. RZ-Consumer betroffen waren,
- eine Übersicht über die Anzahl der von Betroffenen gestellten Anfragen zur Wahrnehmung der Betroffenenrechte aufgeschlüsselt nach Art. 15 (Auskunft), Art. 16 (Berichtigung), Art. 17 (Löschung), Art. 18 (Einschränkung), Art. 20 (Datenübertragbarkeit) und Art. 21 (Widerspruch) DSGVO, bezogen auf Dienste der TI bzw. RZ-Consumer. Sofern die DSGVO nicht anwendbar ist, sind die vorstehenden Angaben entsprechend bereitzustellen,
- den Anteil der fehlerhaft adressierten Datenschutz-Anfragen (d. h. Anfragen, für die der Anbieter nicht Verantwortlicher ist) im Verhältnis zur Gesamtzahl der Datenschutz-Anfragen bzgl. der im Verantwortungsbereich des Anbieters liegenden Dienste der TI bzw. RZ-Consumer,
- eine Übersicht über die durchschnittliche Bearbeitungszeit von korrekt an den Anbieter im Berichtszeitraum adressierten Datenschutz-Anfragen bzgl. der Dienste der TI bzw. RZ-Consumer (Zeitspanne vom Eingang der Anfrage beim Anbieter bis zum Abschluss des Vorgangs beim Anbieter),
- eine Übersicht über die Anzahl der gemäß Art. 14 und Art. 19 DSGVO erteilten Auskünfte ggü. Betroffenen bezogen auf Dienste der TI bzw. RZ-Consumer. Sofern die DSGVO nicht anwendbar ist, sind die vorstehenden Angaben entsprechend bereitzustellen,
- eine Übersicht über die Anzahl der von Betroffenen eingereichten Beschwerden gem. Art. 77 DSGVO, die den Anbieter als Betreiber eines Dienstes der TI bzw. RZ-Consumers betreffen,
- eine Liste der Auftragsverarbeiter, die Dienste der TI bzw. RZ-Consumer betreiben; zusätzlich ggf. für jeden Auftragsverarbeiter die von ihm beauftragten weiteren Auftragsverarbeiter,
- eine Übersicht der durchgeführten Schulungen der Mitarbeiter zum Datenschutz (Dauer, thematische Inhalte),
- eine Selbsteinschätzung, ob es Umsetzungsprobleme mit den Anforderungen des Datenschutzes der TI bzgl. der vom Anbieter betriebenen Dienste der TI bzw. RZ-Consumer gibt.

Bei der KTR-AdV sind Angaben im Bericht nur insoweit zu machen, sofern sie nicht die Versichertenstammdaten nach § 291 SGB V betreffen.【<=】

Hinweis: Der KTR-AdV wird die Anforderung GS-A_4468-02 nicht zugeordnet, da in der aktuellen Ausbaustufe der TI in der KTR-AdV keine medizinischen Daten nach § 291a Abs. 3 SGB V verarbeitet werden. Beim Ausbau der TI ist zu prüfen, ob diese Bedingung dann weiterhin erfüllt ist und die Zuordnung der Anforderung GS-A_4468-02 erfolgen muss.

Die im Datenschutzreport genannten Auftragsverarbeiter sind jährlich vom Anbieter zu kontrollieren.

GS-A_2214-01 - kDSM: Anbieter müssen jährlich die Auftragsverarbeiter kontrollieren

Falls der Anbieter Auftragsverarbeiter i.S. des Art. 4 Nr. 8 DSGVO beauftragt hat, MUSS er sich jährlich bei den beauftragten Auftragsverarbeitern von der Einhaltung der von den Auftragsverarbeitern getroffenen Maßnahmen überzeugen. [<=]

GS-A_5566 - kDSM: Sicherstellung der Datenschutzerfordernissen in Unterbeauftragungsverhältnissen

Der Anbieter MUSS im Falle von Unterbeauftragungen einzelner oder mehrerer Leistungen an Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO in den Unterbeauftragungsverträgen sicherstellen, dass die datenschutzrechtlichen Pflichten, die er zu beachten hat, im gleichen Maße von den Unterauftragnehmern erfüllt werden. Dies gilt gleichermaßen für weitere Unterbeauftragungsverhältnisse. [<=]

GS-A_5625 - kDSM: Auditrechte der gematik zum Datenschutz

Der Anbieter MUSS zusichern, dass die gematik oder ein von ihr zur Geheimhaltung verpflichteter Bevollmächtigter berechtigt sind,

- pro Kalenderjahr maximal ein Regelaudit durchzuführen. Hiervon unbenommen ist das Recht der gematik, anlassbezogene Audits durchzuführen,
- im Rahmen eines Audits beim Anbieter die konkrete Umsetzung der an den Anbieter gestellten Anforderungen der TI zum Datenschutz zu überprüfen,
- im Rahmen eines Audits während der üblichen Geschäftszeiten die Geschäftsräume des Anbieters zu betreten,
- im Rahmen eines Audits alle für das Audit benötigten Informationen zur Verfügung gestellt zu bekommen und insbesondere die erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte zu erhalten.

Dies hat der Anbieter im gleichen Maße für Unterauftragnehmer zuzusichern. Die Kosten, die dem Anbieter durch diese Mitwirkungspflichten entstehen, trägt der Anbieter selbst. [<=]

Hinweis: Die gematik verfolgt mit der Durchführung der Audits das Ziel, gemeinsam mit den Anbietern in einem kooperativen Ansatz die Aufrechterhaltung des erforderlichen Datenschutzniveaus nachzuweisen. Die gematik wird ein Regelaudit in der Regel drei Monate vor der Durchführung beim Anbieter ankündigen. Die Terminvereinbarung erfolgt im Einvernehmen mit dem Anbieter. Die gematik erstellt im Vorfeld einen Auditplan, aus dem der Umfang und die zu betrachtenden Themenbereiche festgelegt sind und stimmt den Auditplan mit dem Anbieter ab. Die gematik muss das Auditrecht nicht notwendigerweise jedes Jahr wahrnehmen.

806

5 Spezifische Module

807 Kapitel 3 und 4 enthalten anbieterübergreifende Module, die unabhängig von einer
808 speziellen Rolle des Anbieters sind. Dieses Kapitel beschreibt die Module für Anbieter in
809 spezifischen Rollen (vgl. spezifische Module (rot) in Abbildung 2). Die spezifischen Module
810 werden Anbietern zusätzlich zu den anbieterübergreifenden Modulen zugeordnet.

5.1 Module für weitere Anwendungen

812 Anbietern weiterer Anwendungen nach § 291a Abs. 7 S. 3 SGB V wird neben den
813 anbieterübergreifenden Modulen der Informationssicherheit aus Kapitel 3 und des
814 Datenschutzes aus Kapitel 4 auch das spezifische Modul „Weitere Anwendungen (ohne
815 TI-Beeinträchtigung)“ bzw. das Modul „Weitere Anwendungen (mit TI-Beeinträchtigung)“
816 zugeordnet.

817 Das Modul „Weitere Anwendungen (ohne TI-Beeinträchtigung)“ ist für Anbieter relevant,
818 bei denen technisch ausgeschlossen ist, dass der Verlust der Sicherheit ihrer Dienste die
819 Sicherheit der TI beeinträchtigen können.

820 Das Modul „Weitere Anwendungen (mit TI-Beeinträchtigung)“ ist für Anbieter relevant,
821 bei denen technisch nicht ausgeschlossen werden kann, dass sie die Sicherheit der TI
822 beeinträchtigen könnten.

823 Die Richtlinie für weitere Anwendungen [gemRL_NvTIwA] unterscheidet die folgenden
824 Anwendungskategorien für weitere Anwendungen:

- 825 • Andere Anwendungen des Gesundheitswesens (aAdG),
- 826 • Andere Anwendungen des Gesundheitswesens mit Zugriff auf Dienste der TI aus
827 angeschlossenen Netzen des Gesundheitswesens (aAdG-NetG-TI),
- 828 • Andere Anwendungen des Gesundheitswesens ohne Zugriff auf Dienste der TI in
829 angeschlossenen Netzen des Gesundheitswesens (aAdG-NetG).

830 Die aAdG und aAdG-NetG-TI könnten die TI, aufgrund der Anbindungstechnik ihrer
831 Dienste an die TI, beeinträchtigen. Bei den aAdG-NetG ist eine Beeinträchtigung
832 aufgrund der Anbindungstechnik an die TI technisch ausgeschlossen.

833 Anbieter von aAdG und aAdG-NetG-TI sind daher „Anbieter weiterer Anwendungen mit
834 Beeinträchtigung der TI“ und ihnen wird das Modul „Weitere Anwendungen (mit TI-
835 Beeinträchtigung)“ zugeordnet. Anbieter von aAdG-NetG sind „Anbieter weiterer
836 Anwendungen ohne Beeinträchtigung der TI“, denen das Modul „Weitere Anwendungen
837 (ohne TI-Beeinträchtigung)“ zugeordnet wird. Die Art der Anbindungstechnik für weitere
838 Anwendungen an die TI wird von der gematik geprüft, mit dem Ziel, die Anbindung für
839 weitere Anwendungen zu vereinfachen und die Sicherheitsanforderungen an die Anbieter
840 zu reduzieren. Ziel ist es, dass auch den aAdG und aAdG-NetG-TI das Modul „Weitere
841 Anwendungen (ohne TI-Beeinträchtigung)“ zugeordnet werden kann.

842 Abbildung 5 zeigt alle Module der Informationssicherheit für weitere Anwendungen im
843 Überblick.

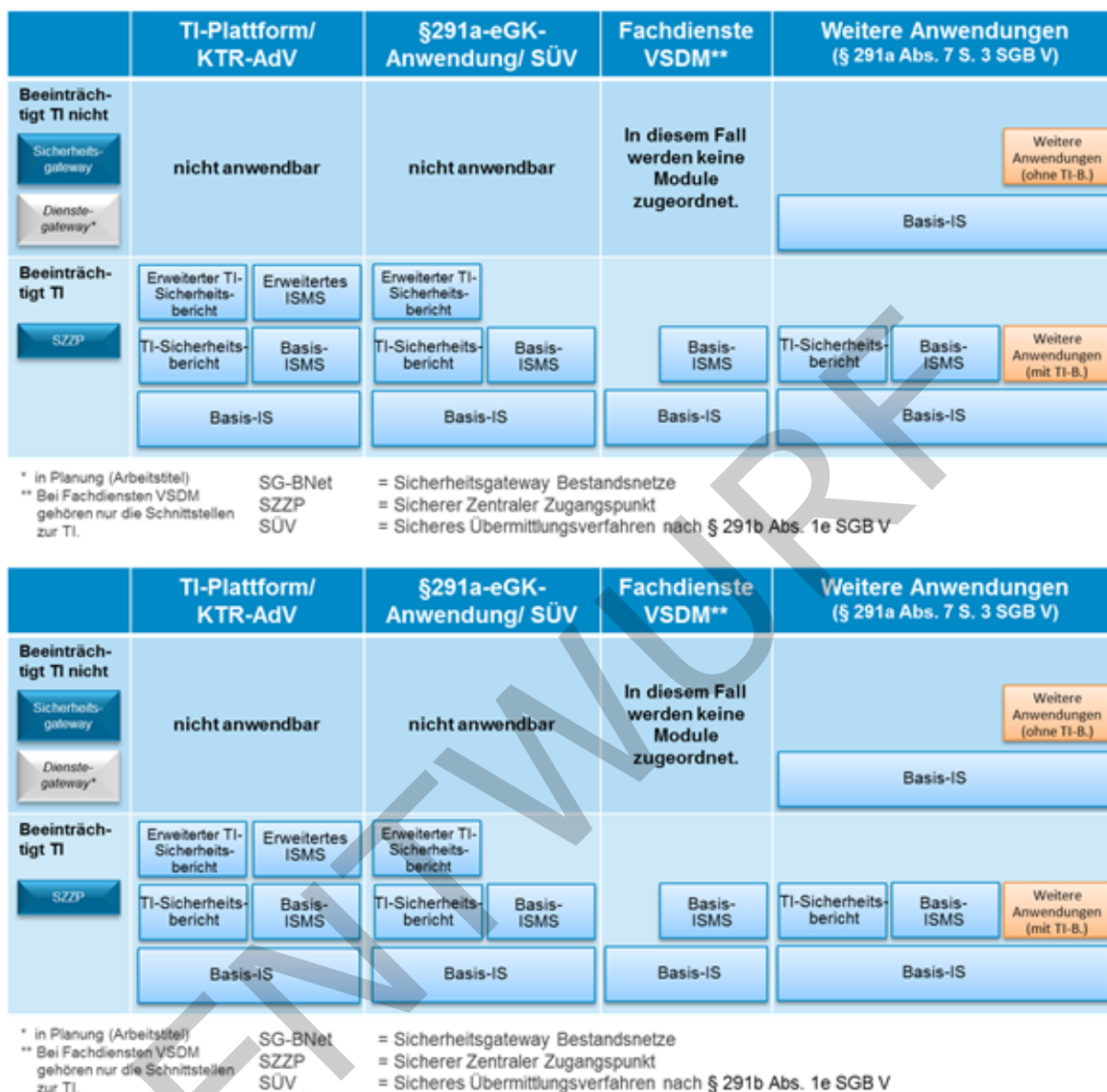


Abbildung 5 – Module für weitere Anwendungen

5.1.1 Modul „Weitere Anwendungen (mit TI-Beeinträchtigung)“

Die Anforderungen des spezifischen Moduls „Weitere Anwendungen (mit TI-Beeinträchtigung)“ gewährleisten eine zulässige Nutzung der Zentralen Dienste der TI durch die weiteren Anwendungen.

GS-A_5567 - Nutzung Zentraler Dienste der TI nur durch bestätigte Anwendungen

Ein Anbieter weiterer Anwendungen mit Beeinträchtigung der TI MUSS durch technisch-organisatorische Maßnahmen gewährleisten, dass ausschließlich die bestätigten Anwendungen bestimmte, festgelegte Zentrale Dienste der TI nutzen können. [<=]

Hinweis: Die Anforderung GS-A_5567 verbietet insbesondere auch eine reine Proxyfunktion im Sinne der Zurverfügungstellung der Schnittstellen zu den Diensten der

858 TI-Plattform für Dienste, die nicht im Bestätigungs- bzw. Zulassungsumfang enthalten
859 sind.

860 **GS-A_5568 - Keine Weitergabe von Daten Zentraler Dienste der TI an nicht**
861 **bestätigte oder zugelassene Anwendungen**

862 Der Anbieter weiterer Anwendungen mit Beeinträchtigung der TI MUSS durch technisch-
863 organisatorische Maßnahmen gewährleisten, dass von Zentralen Diensten der TI zur
864 Verfügung gestellte personenbezogene Daten weder unverändert noch geändert an nicht
865 bestätigte oder nicht zugelassene Anwendungen weitergegeben werden. [<=]

866 **GS-A_5569 - Sicherung der Netzgrenzen**

867 Der Anbieter weiterer Anwendungen mit Beeinträchtigung der TI MUSS ggf. vorhandene
868 Netzgrenzen derart sichern, dass außerhalb der Netzgrenzen nicht auf die TI zugegriffen
869 werden kann. [<=]

870 **GS-A_5570 - Kein Zugriff auf gekoppelte Netze**

871 Der Anbieter weiterer Anwendungen mit Beeinträchtigung der TI MUSS durch technisch-
872 organisatorische Maßnahmen gewährleisten, dass ggf. an die Netzgrenzen des
873 Bestätigungsumfangs gekoppelte Netze nicht von Nutzern der TI erreichbar sind. [<=]

874 **GS-A_5571 - keine Fälschung von IP-Adressen**

875 Der Anbieter weiterer Anwendungen mit Beeinträchtigung der TI MUSS sicherstellen,
876 dass in allen Netzsegmenten, die zur Verbindung der bestätigten oder zugelassenen
877 Dienste mit dem Netzübergang zur Telematikinfrastruktur genutzt werden,
878 Adressinformationen in IP-Paketen unverändert bleiben und es nicht möglich ist, IP-
879 Pakete mit falschen Adressinformationen einzuschleusen. [<=]

880 Hinweis: Die Anforderung GS-A_5571 soll unter anderem IP-Spoofing verhindern.

881 **GS-A_5572 - Sichere Speicherung privater Schlüssel für TI-Identitäten**

882 Der Anbieter weiterer Anwendungen mit Beeinträchtigung der TI MUSS die ihm
883 zugeordneten privaten asymmetrischen Schlüssel von Identitäten der
884 Telematikinfrastruktur sicher speichern, so dass der Schlüssel während der Speicherung
885 insbesondere nicht unautorisiert ausgelesen, unautorisiert verändert, unautorisiert
886 ersetzt oder in anderer Weise unautorisiert benutzt werden kann. [<=]

887 **GS-A_5573 - Qualität der X.509-Identität des Dienstes der Anwendung**

888 Der Anbieter weiterer Anwendungen mit Beeinträchtigung der TI MUSS sicherstellen,
889 dass die zum Komponentenzertifikat gehörende X.509-Identität des Dienstes der
890 weiteren Anwendung die Vorgaben für X.509-Identitäten aus [gemSpec_Krypt]
891 erfüllt. [<=]

892 **GS-A_5574 - Kryptographische Verfahren bei Anbietern mit Beeinträchtigung**
893 **der TI**

894 Falls der Anbieter weiterer Anwendungen mit Beeinträchtigung der TI kryptographische
895 Verfahren zum Schutz personenbezogener medizinischer Daten verwendet, MÜSSEN die
896 Vorgaben aus [gemSpec_Krypt] eingehalten werden. [<=]

897 Die folgende Anforderung legt die Auditrechte der gematik für Anbieter weiterer
898 Anwendungen mit Beeinträchtigung der TI fest. Sie entspricht inhaltlich den vertraglich
899 festgelegten Auditrechten der gematik bei Anbietern von Diensten der TI.

900 **GS-A_5575 - Auditrechte der gematik bei weiteren Anwendungen**

901 Der Anbieter weiterer Anwendungen mit Beeinträchtigung der TI MUSS zusichern, dass
902 die gematik oder ein von ihr zur Geheimhaltung verpflichteter Bevollmächtigter
903 berechtigt sind,

- 904 • pro Kalenderjahr maximal ein Regelaudit durchzuführen. Hiervon unbenommen ist
905 das Recht der gematik, anlassbezogene Audits durchzuführen,
- 906 • im Rahmen eines Audits beim Anbieter die konkrete Umsetzung der an den
907 Anbieter gestellten Anforderungen der TI zum Datenschutz und der
908 Informationssicherheit zu überprüfen,
- 909 • im Rahmen eines Audits während der üblichen Geschäftszeiten die
910 Geschäftsräume des Anbieters zu betreten,
- 911 • im Rahmen eines Audits alle für das Audit benötigten Informationen zur
912 Verfügung gestellt zu bekommen und insbesondere die erforderlichen Zugangs-,
913 Auskunfts- und Einsichtsrechte zu erhalten.
- 914 Dies hat der Anbieter im gleichen Maße für Unterauftragnehmer zuzusichern. Die Kosten,
915 die dem Anbieter durch diese Mitwirkungspflichten entstehen, trägt der Anbieter selbst.
916 [\leq]

917 **5.1.2 Modul „Weitere Anwendungen (ohne TI-Beeinträchtigung)“**

918 Das spezifische Modul „Weitere Anwendungen (ohne TI-Beeinträchtigung)“ enthält
919 folgende Anforderungen.

920 **GS-A_5576 - Regelmäßiger Nachweis von Datenschutz- und Sicherheit**

921 Der Anbieter weiterer Anwendungen ohne Beeinträchtigung der TI MUSS der
922 Zulassungsstelle der gematik alle drei Jahre schriftlich mitteilen, dass in allen
923 Anwendungen des Anbieters, die mittels der TI nutzbar sind, die Datenschutz- und
924 Sicherheitsanforderungen des für die Anwendungen geltenden Produktsteckbriefes
925 umgesetzt sind, die Vorschriften zum Datenschutz eingehalten werden und die
926 Anforderungen an die Sicherheit der Anwendungen gewährleistet ist. [\leq]

927 **GS-A_5577 - Erklärung bei Änderungen am Bestätigungsobjekt**

928 Der Anbieter weiterer Anwendungen ohne Beeinträchtigung der TI MUSS bei Änderungen
929 am Objekt der Bestätigung, die der Zulassungsstelle der gematik angezeigt werden
930 müssen, schriftlich mitteilen, dass durch die Änderungen weiterhin die Vorschriften zum
931 Datenschutz eingehalten werden und die Anforderungen an die Sicherheit gewährleistet
932 sind. [\leq]

933 **GS-A_5578 - Kryptographische Verfahren bei Anbietern ohne Beeinträchtigung 934 der TI**

935 Falls der Anbieter weiterer Anwendungen ohne Beeinträchtigung der TI kryptographische
936 Verfahren zum Schutz personenbezogener medizinischer Daten verwendet, MÜSSEN die
937 Vorgaben aus [gemSpec_Krypt] eingehalten werden [\leq]

938 **5.2 Modul „Schlüsselverwaltung“**

939 Dieses Modul ist nur von Anbietern umzusetzen, die eine Schlüsselverwaltung anbieten.

940 Hinweis: Die betroffenen zentralen Produkttypen sind CVC-Root, gematik Root-CA,
941 Intermediär VSDM, Namensdienst, TSP CVC, TSP X.509 nonQES (HBA, SMC-B, gSMC,
942 FD, ZD), TLS-Dienst, Fachdienst KOM-LE.

**GS-A_3078 - Anbieter einer Schlüsselverwaltung: verpflichtende
Migrationsstrategie bei Schwächung kryptographischer Primitive**

Der Anbieter einer Schlüsselverwaltung innerhalb der TI MUSS in seinem Sicherheitskonzept notwendige Umstellungsprozesse bei Schwächung von kryptographischen Primitiven beschreiben und die Wirksamkeit der getroffenen Maßnahmen ist nachzuweisen (z.B. durch dokumentierte Notfallübungen, Ablaufprotokolle von abgewickelten Vorfällen).[<=]

GS-A_3125 - Schlüsselinstallation und Verteilung: Dokumentation gemäß Minimalitätsprinzip

Der Anbieter einer Schlüsselverwaltung MUSS in seinem Sicherheitskonzept dokumentieren, welcher Schlüssel in welcher Phase seines Lebenszyklus in welcher Systemkomponente transportiert wird. Es MUSS dabei sichergestellt werden, dass die Schlüssel nur an diejenigen Systemkomponenten verteilt werden, in denen ihr Aufenthalt vorgesehen ist und wo sie hinreichend geschützt sind.[<=]

GS-A_3130 - Krypto_Schlüssel_Installation: Dokumentation der Schlüsselinstallation gemäß Minimalitätsprinzip

Der Anbieter einer Schlüsselverwaltung MUSS in seinem Sicherheitskonzept dokumentieren, welcher Schlüssel in welcher Systemkomponente installiert wird. Es MUSS dabei sichergestellt werden, dass die Schlüssel in Systemkomponenten installiert werden, in denen ihr Aufenthalt vorgesehen ist und wo sie hinreichend geschützt sind.[<=]

GS-A_3139 - Krypto_Schlüssel: Dienst Schlüsselableitung

Der Anbieter einer Schlüsselverwaltung MUSS sicherstellen, dass der Ableitungsprozess unumkehrbar und nicht vorhersehbar ist (die Kompromittierung eines abgeleiteten Schlüssels darf nicht den Ableitungsschlüssel oder andere abgeleitete Schlüssel kompromittieren).[<=]

GS-A_3141 - Krypto_Schlüssel_Ableitung: Maßnahmen bei Bekanntwerden von Schwächen in der Schlüsselableitungsfunktion

Der Anbieter einer Schlüsselverwaltung MUSS im Falle des Einsatzes einer Schlüsselableitung (nach [ISO11770]) in seinem Sicherheitskonzept Maßnahmen für das Bekanntwerden von Schwächen des kryptographischen Verfahrens, welche die Grundlage der Schlüsselableitung ist, darlegen.[<=]

GS-A_3149 - Krypto_Schlüssel_Archivierung: Dokumentation der Schlüsselarchivierung gemäß Minimalitätsprinzip

Der Anbieter einer Schlüsselverwaltung MUSS, falls er kryptographische Schlüssel archiviert, in seinem spezifischen Sicherheitskonzept beschreiben, welcher Schlüssel in welcher Phase in welcher Systemkomponente archiviert wird. Er MUSS sicherstellen, dass die Schlüssel nur an diejenigen Systemkomponenten verteilt werden, in denen ihr Aufenthalt vorgesehen ist und wo sie hinreichend geschützt sind.[<=]

5.3 Modul „Kartenherausgabe“

Dieses Modul ist von Anbietern umzusetzen, die Karten herausgeben, die Produkttypen der TI-Plattform gemäß [gemKPT_Arch_TIP] sind. Dies sind die Karten eGK, HBA, SMC-B, gSMC-K und gSMC-KT.

Das Modul enthält alle Anforderungen aus [gemSpec_PINPUK_TI], [gemSpec_CAN_TI] für die sichere Verarbeitung von PIN/PUK und CAN. Diese Anforderungen werden einer Karte zugeordnet, falls diese eine PIN/PUK bzw. eine CAN besitzt.

989 Zudem hat der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit
990 der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer, für die
991 Kartenpersonalisierung jene Module zur Informationssicherheit und, im Falle von
992 personenbezogenen Kartendaten, jene Module zum Datenschutz umzusetzen, welche
993 Produkttypen der TI-Plattform zugeordnet werden (vgl. Abbildung 3 und Abbildung 4).
994 Kartenherausgeber der gSMC-K sind die Hersteller der Konnektoren. Kartenherausgeber
995 der gSMC-KT sind die Hersteller der Kartenterminals.

ENTWURF

996

6 Anhang A – Verzeichnisse

997

6.1 Abkürzungen

Kürzel	Erläuterung
aAdG	Andere Anwendungen des Gesundheitswesens
aAdG-NetG	Andere Anwendungen des Gesundheitswesens ohne Zugriff auf Dienste der TI in angeschlossenen Netzen des Gesundheitswesens
aAdG-NetG-TI	Andere Anwendungen des Gesundheitswesens mit Zugriff auf Dienste der TI aus angeschlossenen Netzen des Gesundheitswesens
AdV	Anwendungen des Versicherten
BIA	Business Impact Analyse
DS	Datenschutz
DSMS	Datenschutzmanagementsystem
eGK	elektronische Gesundheitskarte
EU	Europäische Union
EWK	Europäischer Wirtschaftsraum
IS	Informationssicherheit
ISMS	Informationssicherheitsmanagementsystem
kDSM	koordinierendes Datenschutzmanagementsystem
KTR	Kostenträger
RU	Referenzumgebung
SGB	Sozialgesetzbuch

SG-BNet	Sicherheitsgateway Bestandsnetze
sÜv	sicheres Übermittlungsverfahren
TI	Telematikinfrastuktur
TU	Testumgebung

998

999 **6.2 Abbildungsverzeichnis**

1000	Abbildung 1 – Anforderungen, Module und Anbieter	9
1001	Abbildung 2 – Modulübersicht für Anbietermodule	10
1002	Abbildung 3 – Zuordnung der Module der Informationssicherheit	12
1003	Abbildung 4 – Zuordnung der Module zum Datenschutz	13
1004	Abbildung 5 – Module für weitere Anwendungen	29
1005	Abbildung 6 – Modulübersicht für Anbietermodule	39
1006	Abbildung 7 – Auswirkungen des § 274 SGB V auf die Modulzuordnung (grau = entfällt)	48
1007	48
1008	Abbildung 1 – Anforderungen, Module und Anbieter	9
1009	Abbildung 2 – Modulübersicht für Anbietermodule	10
1010	Abbildung 3 – Zuordnung der Module der Informationssicherheit	12
1011	Abbildung 4 – Zuordnung der Module zum Datenschutz	13
1012	Abbildung 5 – Module für weitere Anwendungen	29
1013	Abbildung 6 – Modulübersicht für Anbietermodule	39
1014	Abbildung 7 – Auswirkungen des § 274 SGB V auf die Modulzuordnung (grau = entfällt)	48
1015	48
1016		
1017		

1018 **6.3 Tabellenverzeichnis**

1019	Tabelle 1 – Modulzuordnung bzgl. der Spezifikationshoheit der gematik	40
1020	Tabelle 2 – Modulzuordnung bzgl. der Möglichkeit, die TI zu beeinträchtigen	44
1021	Tabelle 1 – Modulzuordnung bzgl. der Spezifikationshoheit der gematik	40
1022	Tabelle 2 – Modulzuordnung bzgl. der Möglichkeit, die TI zu beeinträchtigen	44
1023		

1024

1025 **6.4 Referenzierte Dokumente**

1026 **6.4.1 Dokumente der gematik**

1027 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument
1028 referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der
1029 vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und
1030 Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und
1031 Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht
1032 aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in
1033 der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der
1034 die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemRL_Betr_TI]	gematik: Übergreifende Richtlinien zum Betrieb der TI
[gemRL_NvTIWA]	gematik: Richtlinie – Nutzungsvoraussetzungen der TI für weitere Anwendungen des Gesundheitswesens sowie für die Gesundheitsforschung
[gemSpec_CAN_TI]	gematik: Übergreifende Spezifikation CAN-Policy
[gemSpec_Hersteller_SI]	gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen an Hersteller
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_PINPUK_TI]	gematik: Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur

1035 **6.4.2 Weitere Dokumente**

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ISO11770]	ISO/IEC 11770: 1996 Information technology – Security techniques – Key management Part 3: Mechanisms using asymmetric techniques

[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://tools.ietf.org/html/rfc2109
-----------	--

ENTWURF

1036

7 Anhang B – Modularisierungskonzept

1037 Kapitel 3 und 4 ordnen die anbieterübergreifenden Module den Anbietern von Diensten
1038 der TI, Anbietern von Fachdiensten VSDM gemäß § 291 Abs. 2b SGB V, Anbietern von
1039 Rechenzentrums-Consumern (RZ-Consumer) sowie Anbietern weiterer Anwendungen
1040 gemäß § 291a Abs. 7 Satz 3 SGB V zu. In diesem Anhang wird dargestellt, nach welchem
1041 Schema die Module angeordnet sind und nach welchen Kriterien die Zuordnung der
1042 Module zu den Anbietern erfolgt.

7.1 Anordnung der Module

1044 Die Module zur Informationssicherheit und zum Datenschutz sind jeweils in Säulen
1045 angeordnet, die auf einem Basis-Modul („Basis-IS“ für Informationssicherheit, „Basis-DS“
1046 für Datenschutz) aufsetzen.

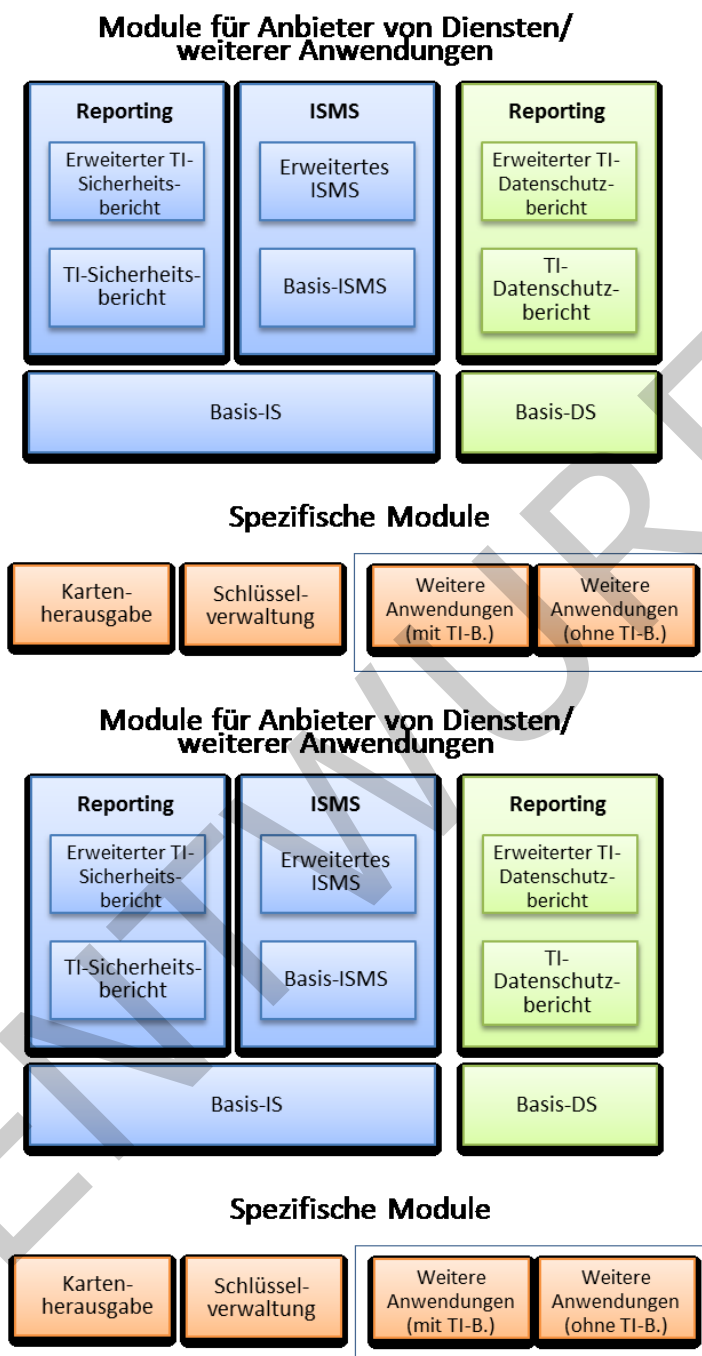


Abbildung 6 – Modulübersicht für Anbietermodule

Wird einem Anbieter ein Modul einer Säule zugeordnet, so gelten für ihn auch alle darunter liegenden Module der Säule. Wird einem Anbieter beispielsweise das Modul „Erweitertes ISMS“ zugeordnet, so gelten für ihn auch die darunter liegenden Module „Basis-ISMS“ und „Basis-IS“.

Für die Informationssicherheit gibt es eine Säule zur Etablierung eines Informationssicherheitsmanagementsystems und eine Säule zum Reporting an die gematik. Für den Datenschutz gibt es nur die Säule zum Reporting. Die Basis-Module

1057 enthalten jeweils die Minimalanforderungen zum Managementsystem und zu
1058 Meldepflichten.

1059 **7.2 Kriterien der Modulzuordnung**

1060 Die Zuordnung der anbieterübergreifenden Module zur Informationssicherheit und des
1061 Datenschutzes in Abbildung 3 und Abbildung 4 erfolgt anhand der beiden folgenden
1062 Kriterien.

- 1063 • **Spezifikationshoheit der gematik**, d. h., ist die gematik gesetzlich
1064 verantwortlich für die Spezifikation?
- 1065 • **Beeinträchtigung des Datenschutzes oder der Sicherheit der TI**, d. h., kann
1066 der Verlust der Sicherheit oder des Datenschutzes des Dienstes den Datenschutz
1067 oder die Sicherheit der TI beeinträchtigen?

1068 Es werden einem Anbieter alle anbieterübergreifenden Module zur Informationssicherheit
1069 und zum Datenschutz zugeordnet, die sich für ihn aus diesen beiden Kriterien ergeben.

1070 **7.2.1 Kriterium: Spezifikationshoheit der gematik**

1071 Die Spezifikationshoheit der gematik unterscheidet sich bei Diensten der TI, der KTR-AdV
1072 als aktuell einzig spezifizierten RZ-Consumer, den Fachdiensten VSDM und weiteren
1073 Anwendungen nach § 291a Abs. 7 S.3 SGB V. Tabelle 2 zeigt die Zuordnung der Module
1074 der Informationssicherheit und des Datenschutzes anhand dieses Kriteriums.

1075

1076 **Tabelle 1 – Modulzuordnung bzgl. der Spezifikationshoheit der gematik**

Anbieter			Module
gematik-Spezifikationshoheit (Dienste der TI)	zentrale TI-Plattform	Der Anbieter betreibt einen Dienst der zentralen TI-Plattform.	Module Informationssicherheit : x Basis-IS x Basis-ISMS o Erweitertes ISMS x TI-Sicherheitsbericht x Erweiterter TI-Sicherheitsbericht
		Die Dienste der zentralen TI-Plattform werden von der gematik spezifiziert.	Module Datenschutz: x Basis-DS x TI-Datenschutzbericht x Erweiterter TI-Datenschutzbericht

	KTR-AdV	<p>Der Anbieter betreibt die im Rechenzentrum zu betreibenden Anteile der KTR-AdV.</p> <p>Die KTR-AdV wird von der gematik spezifiziert.</p>	<p>Module Informationssicherheit :</p> <ul style="list-style-type: none"> x Basis-IS x Basis-ISMS o Erweitertes ISMS x TI-Sicherheitsbericht x Erweiterter TI-Sicherheitsbericht
			<p>Module</p> <p>Datenschutz:</p> <ul style="list-style-type: none"> x Basis-DS x TI-Datenschutzbericht x Erweiterter TI-Datenschutzbericht
	eGK-Anwendung/sÜv	<p>Der Anbieter betreibt einen Dienst einer eGK-Anwendung oder eines sicheren Übermittlungsverfahrens (sÜv).</p> <p>Dienste der eGK-Anwendungen und der sÜv werden von der gematik spezifiziert.</p>	<p>Module Informationssicherheit :</p> <ul style="list-style-type: none"> x Basis-IS x Basis-ISMS o Erweitertes ISMS x TI-Sicherheitsbericht x Erweiterter TI-Sicherheitsbericht
			<p>Module</p> <p>Datenschutz:</p> <ul style="list-style-type: none"> x Basis-DS x TI-Datenschutzbericht x Erweiterter TI-Datenschutzbericht
keine gematik-Spezifikationshoheit	Fachdienste VSDM	<p>Der Anbieter betreibt einen Fachdienst VSDM gemäß § 291 Abs. 2b SGB V.</p> <p>Die Fachdienste VSDM und deren Spezifikation fallen nicht in den gesetzlichen Aufgabenbereich der gematik gemäß § 291b Abs. 1 SGB V.</p>	<p>Module Informationssicherheit :</p> <ul style="list-style-type: none"> o Basis-IS o Basis-ISMS o Erweitertes ISMS o TI-Sicherheitsbericht o Erweiterter TI-Sicherheitsbericht
			<p>Module</p> <p>Datenschutz:</p> <ul style="list-style-type: none"> o Basis-DS o TI-Datenschutzbericht o Erweiterter TI-Datenschutzbericht

	weitere Anwendunge n	Der Anbieter betreibt eine weitere Anwendung gemäß § 291a Abs. 7 Satz 3 SGB V. Weitere Anwendungen werden nicht von der gematik spezifiziert.	Module Informationssicherheit : x Basis-IS o Basis-ISMS o Erweitertes ISMS o TI-Sicherheitsbericht o Erweiterter TI-Sicherheitsbericht Module Datenschutz: x Basis-DS o TI- Datenschutzbericht o Erweiterter TI- Datenschutzbericht
--	-------------------------------------	--	---

1077

1078

1079 **Dienste der TI**

1080 Für Dienste der TI erstellt die gematik die funktionalen und technischen Vorgaben, legt
1081 den Inhalt und die Struktur der Datensätze für deren Bereitstellung und Nutzung fest,
1082 erstellt die Vorgaben für einen sicheren Betrieb der TI und überwacht ihre Umsetzung
1083 (§ 291b Abs. 1 SGB V).

1084 Die gematik spezifiziert für Dienste der TI insbesondere die Maßnahmen, mit denen der
1085 Datenschutz und die Informationssicherheit gewährleistet werden. Die korrekte
1086 Umsetzung dieser Maßnahmen durch den Anbieter stellt sicher, dass in der TI die
1087 Vorschriften zum Datenschutz eingehalten und ein angemessenes Sicherheitsniveau in
1088 den Diensten der TI gewährleistet wird (vgl. § 291b Abs. 1 SGB V).

1089 Anbietern von Diensten der TI werden sämtliche Module des Datenschutzes und, mit
1090 Ausnahme des Moduls „Erweitertes ISMS“, sämtliche Module der Informationssicherheit
1091 zugeordnet. Diese Module gewährleisten eine sichere Betriebsumgebung beim Anbieter.

1092 **KTR-AdV**

1093 Der im Rechenzentrum betriebene Anteil der KTR-AdV (AdV-Server) stellt die
1094 Funktionalitäten zur Verfügung, die eine AdV-App benötigt, um mit den Diensten der
1095 zentralen Telematikinfrastruktur und den Fachdiensten in der TI zu kommunizieren. Es
1096 handelt sich beim AdV-Server um einen Teil der TI. § 291b Absatz 1 Satz 1 Nummer 1
1097 SGB V weist der gematik die Aufgabe zu, die funktionalen und technischen Vorgaben
1098 einschließlich eines Sicherheitskonzepts zu erstellen sowie nach § 291b Absatz 1 Satz 1
1099 Nummer 3 auch Vorgaben für den sicheren Betrieb der TI zu erstellen und ihre
1100 Umsetzung zu überwachen. Um die Sicherheit der AdV konsistent über alle Daten bzw.
1101 Anwendungen hinweg zu gewährleisten, unterliegt die AdV einschließlich des AdV-Servers
1102 der betrieblichen Überprüfung der gematik.^[SEP]

1103 Anbietern der KTR-AdV werden nach dem Kriterium der Spezifikationshoheit der gematik
1104 sämtliche Module des Datenschutzes und, mit Ausnahme des Moduls „Erweitertes ISMS“,
1105 sämtliche Module der Informationssicherheit zugeordnet.

1106 **Fachdienste VSDM**

1107 Die Fachdienste VSDM und deren Spezifikation fallen nicht in den gesetzlichen
1108 Aufgabenbereich der gematik gemäß § 291b Abs. 1 SGB V. Die gematik ist insbesondere
1109 nicht gesetzlich damit beauftragt – anders als bei den weiteren Anwendungen in § 291a
1110 Abs. 7 Satz 3 Nr. 2 SGB V – die Einhaltung der Vorschriften des Datenschutzes und ein
1111 angemessenes Sicherheitsniveau im Hinblick auf die Schutzbedürftigkeit der in den
1112 Fachdiensten VSDM verarbeiteten Daten zu gewährleisten. Die Fachdienste VSDM
1113 gehören nicht zur TI. Lediglich die Schnittstellen der Fachdienste VSDM sind Teil der TI.

1114 Anbietern von Fachdiensten VSDM werden daher aufgrund des Kriteriums der
1115 „Spezifikationshoheit der gematik“ keine Module der Informationssicherheit oder des
1116 Datenschutzes zugeordnet.

1117 **Weitere Anwendungen**

1118 Weitere Anwendungen nach § 291a Abs. 7 Satz 3 SGB V werden nicht von der gematik
1119 spezifiziert. Der gesetzliche Auftrag der gematik beschränkt sich bzgl. der Spezifikation
1120 darauf, zu gewährleisten, dass nur weitere Anwendungen die TI nutzen, die die
1121 Vorschriften zum Datenschutz einhalten und ein angemessenes Sicherheitsniveau bzgl.
1122 ihrer Anwendung bieten (vgl. § 291a Abs. 7 Satz 3 Nr. 2 SGB V). Insbesondere
1123 spezifiziert die gematik keine Maßnahmen des Datenschutzes und der
1124 Informationssicherheit zum Schutz der Anwendungsdaten.

1125 Es werden die Module „Basis-IS“ und „Basis-DS“ zugeordnet, um gemäß § 291a Abs. 7
1126 Satz 3 Nr. 2 SGB V sicherzustellen, dass die Anbieter die Vorschriften zum Datenschutz
1127 und die Anforderungen der Informationssicherheit in ihrer weiteren Anwendung
1128 einhalten.

1129 **7.2.2 Kriterium: Beeinträchtigung der TI**

1130 Dieses Kriterium unterscheidet die Anbieter danach, ob der Verlust der Sicherheit ihres
1131 Dienstes den Datenschutz oder die Sicherheit der TI beeinträchtigen kann. Tabelle 3 zeigt
1132 die Zuordnung der Module nach diesem Kriterium.

1133 Es werden einem Anbieter nach diesem Kriterium keine Module zugeordnet, falls die
1134 Dienste des Anbieters so an die TI angeschlossen werden, dass eine Beeinträchtigung der
1135 Sicherheit der TI durch den Verlust der Sicherheit des Dienstes technisch ausgeschlossen
1136 ist.

1137 Diensten der TI werden alle Module des Datenschutzes und der Informationssicherheit,
1138 mit Ausnahme des Moduls „Erweitertes ISMS“, zugeordnet, da der Verlust der Sicherheit
1139 eines Dienstes der TI die Sicherheit der TI per Definition beeinträchtigt.

1140 Das Modul „Erweitertes ISMS“ ist von Anbietern der Dienste der zentralen TI-Plattform
1141 umzusetzen, da die Aufrechterhaltung von Sicherheit und Datenschutz bei diesen
1142 Diensten von besonderer Bedeutung für alle Teilnehmer der TI ist. Sie werden daher
1143 gemäß dem Modul „Erweitertes ISMS“ stärker bzgl. der Sicherheit kontrolliert.

1144 Dem Anbieter einer KTR-AdV werden alle Module des Datenschutzes und der
1145 Informationssicherheit inkl. des Moduls „Erweitertes ISMS“ zugeordnet, da der Verlust
1146 der Sicherheit der KTR-AdV als integraler Bestandteil der TI die Sicherheit der TI per
1147 Definition beeinträchtigt. Zudem ergibt sich aufgrund der Erreichbarkeit des AdV-Servers
1148 (Teil der KTR-AdV) über das Internet zusammen mit der Möglichkeit, auf eine
1149 freigeschaltete eGK zuzugreifen, ein höheres Bedrohungspotential zur Beeinträchtigung
1150 der TI, so dass eine intensivere betriebliche Überprüfung erfolgt.

Kann für einen Dienst einer weiteren Anwendung eine Beeinträchtigung der TI nicht technisch ausgeschlossen werden, so werden auch dem Anbieter der weiteren Anwendung alle Module zugeordnet, mit Ausnahme der Module „Erweitertes ISMS“, „Erweiterter TI-Sicherheitsbericht“ und „Erweiterter TI-Datenschutzbericht“. Das Modul „Erweitertes ISMS“ wird nicht zugeordnet, da die Dienste der weiteren Anwendung, anders als Dienste der TI-Plattform, nicht von allen Teilnehmern der TI genutzt werden. Für weitere Anwendungen sind die Berichte der Module „TI-Sicherheitsbericht“ und „TI-Datenschutzbericht“ ausreichend zur Erfüllung des gesetzlichen Auftrags der gematik.

Bei den Fachdiensten VSDM wird – analog zu den Diensten der weiteren Anwendungen – bei der Zuordnung der Module berücksichtigt, ob eine Beeinträchtigung der Sicherheit und des Datenschutzes der TI bei Verlust der Sicherheit oder des Datenschutzes eines Fachdienstes VSDM technisch ausgeschlossen werden kann. Ist eine Beeinträchtigung der TI technisch ausgeschlossen, so werden keine Module zugeordnet. Ist eine Beeinträchtigung der TI nicht ausgeschlossen, werden die Module „Basis-IS“ und „Basis-ISMS“ sowie „Basis-DS“ zugeordnet. Zusammen mit der Prüfung der Fachdienste gemäß § 274 Abs. 1 SGB V (vgl. Anhang C) wird so der gesetzliche Auftrag der gematik gemäß § 291b Abs. 1 SGB V zur Gewährleistung eines sichereren Betriebs der TI und zur Sicherstellung der Einhaltung der Vorschriften zum Datenschutz in der TI umgesetzt.

In der derzeitigen Form des Anschlusses der Fachdienste VSDM an die TI ist eine Beeinträchtigung der Sicherheit und des Datenschutzes der TI bei Verlust der Sicherheit oder des Datenschutzes eines Fachdienstes VSDM technisch nicht ausgeschlossen.

Tabelle 2 – Modulzuordnung bzgl. der Möglichkeit, die TI zu beeinträchtigen

Grad der möglichen Beeinträchtigung der TI	Anbieter	Beschreibung	Module
keine Beeinträchtigung möglich	weitere Anwendungen	Die Sicherheit der Betriebsumgebung des Dienstes der weiteren Anwendung hat keinen Einfluss auf die Sicherheit der TI.	Module Informationssicherheit: o Basis-IS o Basis-ISMS o Erweitertes ISMS o TI-Sicherheitsbericht o Erweiterter TI-Sicherheitsbericht
			Module Datenschutz: o Basis-DS o TI-Datenschutzbericht o Erweiterter TI-Datenschutzbericht

Beeinträchtigung möglich	Fachdienste VSDM	<p>Die Sicherheit der Betriebsumgebung des Fachdienstes VSDM hat keinen Einfluss auf die Sicherheit der TI.</p> <p>Hinweis: In der derzeitigen Form des Anschlusses der Fachdienste VSDM an die TI ist dies nicht gegeben</p>	<p>Module</p> <p>Informationssicherheit:</p> <ul style="list-style-type: none"> o Basis-IS o Basis-ISMS o Erweitertes ISMS o TI-Sicherheitsbericht o Erweiterter TI-Sicherheitsbericht
	zentrale TI-Plattform	<p>Die Sicherheit der Betriebsumgebung des Dienstes der TI hat einen Einfluss auf die Sicherheit der TI.</p> <p>Die Aufrechterhaltung von Informationssicherheit und Datenschutz bei Diensten der zentralen TI-Plattform ist von besonderer Bedeutung, da sie von allen Teilnehmern der TI genutzt werden.</p>	<p>Module</p> <p>Informationssicherheit:</p> <ul style="list-style-type: none"> x Basis-IS x Basis-ISMS x Erweitertes ISMS x TI-Sicherheitsbericht x Erweiterter TI-Sicherheitsbericht
	KTR-Adv	<p>Die Sicherheit der im Rechenzentrum betriebenen Anteile der KTR-Adv hat einen Einfluss auf die Sicherheit der TI</p> <p>Die Aufrechterhaltung von Informationssicherheit und Datenschutz ist von besonderer Bedeutung, da auf freigeschaltete eGKs von Versicherten zugegriffen werden kann und damit</p>	<p>Module</p> <p>Informationssicherheit:</p> <ul style="list-style-type: none"> x Basis-IS x Basis-ISMS x Erweitertes ISMS x TI-Sicherheitsbericht x Erweiterter TI-Sicherheitsbericht

		missbräuchliche Zugriffe auf schützenswerte Daten der Versicherten möglich wären.	Module Datenschutz: x Basis-DS x TI-Datenschutzbericht x Erweiterter TI-Datenschutzbericht
	eGK-Anwendung/süv	Die Sicherheit der Betriebsumgebung des Dienstes der TI hat einen Einfluss auf die Sicherheit der TI.	Module Informationssicherheit: x Basis-IS x Basis-ISMS o Erweitertes ISMS x TI-Sicherheitsbericht x Erweiterter TI-Sicherheitsbericht Module Datenschutz: x Basis-DS x TI-Datenschutzbericht x Erweiterter TI-Datenschutzbericht
	Fachdienste VSDM	Die Sicherheit der Betriebsumgebung des Fachdienstes VSDM hat einen Einfluss auf die Sicherheit der TI.	Module Informationssicherheit: x Basis-IS x Basis-ISMS o Erweitertes ISMS o TI-Sicherheitsbericht o Erweiterter TI-Sicherheitsbericht Module Datenschutz: x Basis-DS o TI-Datenschutzbericht o Erweiterter TI-Datenschutzbericht
	weitere Anwendungen	Die Sicherheit der Betriebsumgebung des Dienstes der weiteren Anwendung hat einen Einfluss auf die Sicherheit der TI.	Module Informationssicherheit: x Basis-IS x Basis-ISMS o Erweitertes ISMS x TI-Sicherheitsbericht o Erweiterter TI-Sicherheitsbericht Module Datenschutz: x Basis-DS x TI-Datenschutzbericht

			o Erweiterter TI- Datenschutzbericht
--	--	--	---

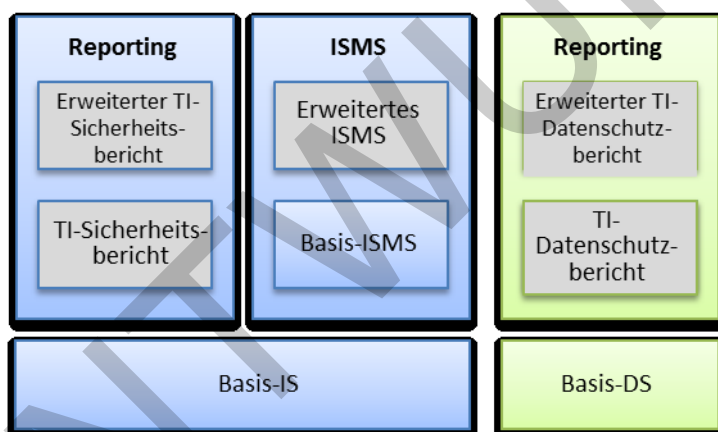
ENTWURF

8 Anhang C – Modulzuordnung bei Anwendbarkeit des § 274 Abs. 1 SGB V

Für ausgewählte Anbieter legt der § 274 Abs. 1 SGB V eine Aufsichtsbehörde und einen Prüfzyklus fest, nach dem die dort benannte Aufsichtsbehörde die Geschäfts-, Rechnungs- und Betriebsführung beim Anbieter prüft. Die Prüfung erstreckt sich auf den gesamten Geschäftsbetrieb des Anbieters und umfasst die Prüfung seiner Gesetzmäßigkeit und Wirtschaftlichkeit. Die Prüfung beinhaltet die Einhaltung der Vorschriften des Datenschutzes und die Maßnahmen zur Informationssicherheit.

Da die Prüfung des Datenschutzes und der Informationssicherheit inklusive Prüfzyklus gesetzlich geregelt ist, entfallen die Module zum Reporting und das Modul „Erweitertes ISMS“ für Anbieter der Fachdienste VSDM und Anbieter weiterer Anwendungen, für die der § 274 Abs. 1 SGB V anwendbar ist (siehe Abbildung 7).

Module für Anbieter von Diensten/ weiterer Anwendungen



Module für Anbieter von Diensten/ weiterer Anwendungen

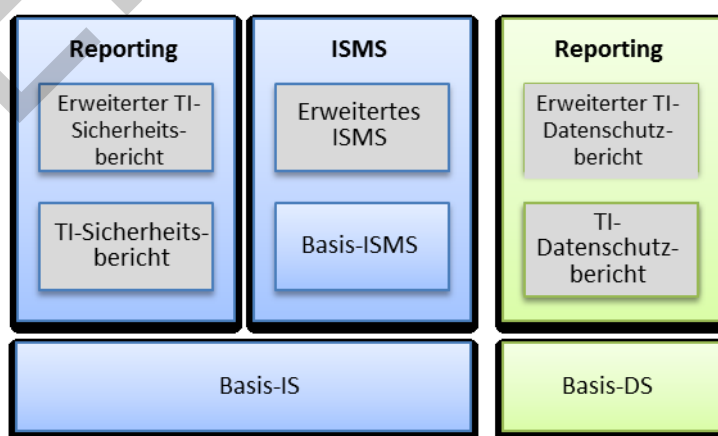


Abbildung 7 – Auswirkungen des § 274 SGB V auf die Modulzuordnung (grau = entfällt)