

Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

## Elektronische Gesundheitskarte und Telematikinfrastruktur

# Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller

Version: 1.2.0 [CC](#)  
Revision: [246940269968](#)  
Stand: [30.0617.08.2020](#)  
Status: [zur Abstimmung](#) freigegeben  
Klassifizierung: öffentlich\_Entwurf  
Referenzierung: gemSpec\_DS\_Hersteller

## Dokumentinformationen

### Änderungen zur Vorversion

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

### Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	14.05.18		freigegeben	gematik
1.1.0	15.05.19		Änderungsliste P18.1	gematik
1.2.0	30.06.20		Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0	gematik
<a href="#">1.3.0 CC</a>	<a href="#">17.08.20</a>		<a href="#">Einarbeitung Scope-Themen zu R4.0.1 zur Abstimmung freigegeben</a>	<a href="#">gematik</a>

## Inhaltsverzeichnis

<b>1 Einordnung des Dokuments</b>	<b>5</b>
1.1 Zielsetzung	5
1.2 Zielgruppe	5
1.3 Geltungsbereich	5
1.4 Abgrenzungen	5
1.5 Methodik	6
<b>2 Anforderungen der Informationssicherheit an Hersteller</b>	<b>7</b>
2.1 Basis-Anforderungen	7
2.2 Sicherer Softwareentwicklungsprozess	9
2.3 Unterstützung von Audits	11
<b>3 Anhang A – Verzeichnisse</b>	<b>13</b>
3.1 Abkürzungen	13
3.2 Abbildungsverzeichnis	13
3.3 Referenzierte Dokumente	13
3.3.1 Dokumente der gematik	13
3.3.2 Weitere Dokumente	14
<b>1 Einordnung des Dokuments</b>	<b>5</b>
1.1 Zielsetzung	5
1.2 Zielgruppe	5
1.3 Geltungsbereich	5
1.4 Abgrenzungen	5
1.5 Methodik	6
<b>2 Anforderungen der Informationssicherheit an Hersteller</b>	<b>7</b>
2.1 Basis-Anforderungen	7
2.2 Sicherer Softwareentwicklungsprozess	9
2.3 Unterstützung von Audits	11
<b>3 Anhang A – Verzeichnisse</b>	<b>13</b>
3.1 Abkürzungen	13
3.2 Abbildungsverzeichnis	13
3.3 Referenzierte Dokumente	13
3.3.1 Dokumente der gematik	13

68	<a href="#">3.3.2 Weitere Dokumente.....</a>	14
69		

ENTWURF

---

## **1 Einordnung des Dokuments**

---

### **1.1 Zielsetzung**

Das vorliegende Dokument definiert übergreifende Sicherheits- und  
Datenschutzanforderungen für Hersteller von Produkten der Telematikinfrastruktur (TI),  
für die eine Produktzulassung vorgesehen ist.

### **1.2 Zielgruppe**

Das vorliegende Dokument richtet sich an Hersteller von Produkten der  
Telematikinfrastruktur, für die eine Produktzulassung vorgesehen ist.

### **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**

Die Anforderungen dieses Dokumentes richten sich nicht an Anbieter betrieblicher  
Leistungen von Produkten der TI oder weiterer Anwendungen.

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

Übergreifende Anforderungen an die Verwendung kryptographischer Algorithmen in der  
Telematikinfrastruktur sind in [gemSpec\_Krypt] festgelegt.

100 **1.5 Methodik**

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

105 Sie werden im Dokument wie folgt dargestellt:

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

107 Text / Beschreibung

108 [**<=**]

109

110 Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und Textmarke angeführten  
111 Inhalte.

ENTWURF

## 2 Anforderungen der Informationssicherheit an Hersteller

Dieses Dokument enthält Sicherheitsanforderungen an Produkttypen der TI (vgl. [gemKPT\_Arch\_TIP]). Bei Smartcards (z.B. eGK) sind die Anforderungen nur dem COS zugeordnet, nicht dem Objektsystem.

### 2.1 Basis-Anforderungen

#### ~~GS-A\_2524-01 – Produktunterstützung: Nutzung des Problem-Management-Prozesses~~

~~Hersteller von dezentralen Produkten der TI MÜSSEN im Rahmen der Produktunterstützung den in den „Übergreifenden Richtlinien zum Betrieb der TI“ [gemRL\_Betr\_TI] fest ge- legten Problem-Management-Prozess nutzen, um Schwachstellen an die gematik zu melden. [<=]~~

#### **GS-A\_2330-02 - Hersteller: Schwachstellen-Management**

Hersteller von dezentralen Produkten der TI MÜSSEN präventive Maßnahmen zur Erkennung und Analyse von technischen Hard- oder Softwareschwachstellen („vulnerabilities“) ihres Produktes wie auch zur Bewertung und Implementierung von Sicherheitsupdates durchführen. Hierzu gehört insbesondere auch, dass sich der Hersteller aktiv und kontinuierlich über Schwachstellen in eingesetzten Hard- und Softwarekomponenten von Dritten informiert. Dies ist auch für Anteile des Produktes sicherzustellen, die von Drittherstellern stammen. [<=]

#### **GS-A\_2525-01 - Hersteller: Schließen von Schwachstellen**

Hersteller von dezentralen Produkten der TI MÜSSEN die gematik direkt und unverzüglich über neu gemeldete Software- oder Hardware-Schwachstellen in ihren Produkten informieren und das weitere Vorgehen mit der gematik abstimmen, um die Auswirkungen unverzüglich auf das mögliche Minimum zu reduzieren und die Schwachstelle schnellstmöglich komplett zu schließen.  
[<=]

#### **GS-A\_2354-01 - Produktunterstützung mit geeigneten Sicherheitstechnologien**

Hersteller von dezentralen Produkten der TI MÜSSEN eine vom koordinierenden ISM freigegebene Technologie zur Wahrung der Integrität, Authentizität und (wo nötig) Vertraulichkeit der Informationen zur Produktunterstützung und Schwachstellenmeldung einsetzen.  
[<=]

#### **GS-A\_2350-01 - Produktunterstützung der Hersteller**

Hersteller von dezentralen Produkten der TI MÜSSEN der gematik Supportinformationen sowie Informationen zu Softwareupdates als Produktunterstützung für von ihnen entwickelte Produkte der TI zur Konsolidierung und Weiterleitung an die ISM der Beteiligten zur Verfügung stellen.  
[<=]

#### **GS-A\_4944-01 - Produktentwicklung: Behebung von Sicherheitsmängeln**

Hersteller von dezentralen Produkten der TI MÜSSEN für die von ihnen angebotenen Produkte der TI gewährleisten, dass technisch-organisatorische Verfahren zur Behebung von Sicherheitsmängeln in den Produkten während der Zeit des Einsatzes in der TI vorgehalten werden. Dies beinhaltet das kontinuierliche Aufspüren (bug tracking) und

155 Nachbessern (bug fixing) von Sicherheitsmängeln (security bugs) und das zur Verfügung  
156 stellen von Updates (security updates).[<=]

157 Hinweis: In Anforderung GS-A\_4944-01 bezeichnet die „Zeit des Einsatzes in der TI“ die  
158 Zeitspanne, für die das Produkt für die TI zugelassen ist.

159 **GS-A\_4945-01 - Produktentwicklung: Qualitätssicherung**

160 Hersteller von dezentralen Produkten der TI MÜSSEN für die von ihnen angebotenen  
161 Produkte der TI gewährleisten, dass bei der Entwicklung der Produkte technisch-  
162 organisatorische Verfahren der Qualitätssicherung angewendet werden (bspw. fuzz  
163 (robustness) testing bzw. penetration testing und source code review).[<=]

164 **GS-A\_4946-01 - Produktentwicklung: sichere Programmierung**

165 Hersteller von dezentralen Produkten der TI MÜSSEN für die von ihnen angebotenen  
166 Produkte der TI gewährleisten, dass bei der Entwicklung der Produkte Secure Coding  
167 Guidelines angewendet werden; d. h., in einschlägigen Fachkreisen anerkannte, erprobte  
168 und bewährte Regeln sicherer Programmierung befolgt wurden.[<=]

169 **GS-A\_4947-01 - Produktentwicklung: Schutz der Vertraulichkeit und Integrität**

170 Hersteller von dezentralen Produkten der TI MÜSSEN für die von ihnen angebotenen  
171 Produkte der TI gewährleisten, dass sie in einer Entwicklungsumgebung entwickelt  
172 werden, für die technische und organisatorische Maßnahmen zum Schutz der  
173 Vertraulichkeit und Integrität der Produkte getroffen werden.[<=]

174 **A\_17178 - Produktentwicklung: Basisschutz gegen OWASP Top 10 Risiken**

175 Hersteller von dezentralen Produkten der TI MÜSSEN für die von ihnen angebotenen  
176 Produkte der TI gewährleisten, dass das Produkt resistent bezüglich der im aktuellen und  
177 den beiden vorherigen OWASP Top 10 Report(s) ausgewiesenen Risiken ist.[<=]

178 Hinweis: Die Nichtanwendbarkeit eines Risikos für das Produkt ist zu begründen. Für  
179 Informationen zum Umgang mit den OWASP Top 10 Risiken wird auf den aktuellen  
180 [OWASP Top 10 Report] und die darin enthaltenen Vorgehensweisen für z. B. Entwickler  
181 und Tester verwiesen.

182 **A\_17179 - Auslieferung aktueller zusätzlicher Softwarekomponenten**

183 Hersteller von dezentralen Produkten der TI, die zu ihrem Produkt ein Installationspaket  
184 mit zusätzlichen Softwarekomponenten ausliefern, MÜSSEN im Falle von  
185 Sicherheitsaktualisierungen dieser zusätzlichen Softwarekomponenten unverzüglich die  
186 gepatchten Softwareversionen als Aktualisierung an die Nutzer des Produktes  
187 ausliefern.[<=]

188 Hinweis: Hierunter fallen Softwarekomponenten von Dritten, die nicht von der gematik  
189 zugelassen werden und somit auch nicht Teil des Sicherheitsnachweises im Rahmen der  
190 Zulassung sind, bspw. Bibliotheken zur Laufzeitumgebung (Java-Bibliotheken etc.). Im  
191 Kontext dieser Anforderung beinhaltet „unverzüglich“ auch, dass der Hersteller sein  
192 Produkt im Zusammenhang mit den neuen Versionen der zusätzlichen  
193 Softwarekomponenten testet, bevor er diese an die Nutzer ausliefert. Ansonsten gilt,  
194 dass er die zusätzlichen Softwarekomponenten ohne schuldhaftes Zögern so schnell als  
195 möglich ausliefert. Sollte der Hersteller feststellen, dass die Sicherheitseigenschaften  
196 seines Produkts von der Aktualisierungen der zusätzlichen Softwarekomponenten  
197 beeinträchtigt sind, so muss er das Produkt erneut bei der gematik zur Zulassung  
198 einreichen – unabhängig davon, ob er sein Produkt verändert hat oder nicht.



## 199 **2.2 Sicherer Softwareentwicklungsprozess**

### 200 **A\_19148 - Sicherheits- und Datenschutzkonzept**

201 Der Hersteller eines Produktes MUSS die Sicherheits- und Datenschutzmaßnahmen für  
202 sein Produkt in einem Sicherheits- und Datenschutzkonzept dokumentieren und auf  
203 Verlangen der gematik zur Verfügung stellen.[<=]

204 Hinweis: Das Sicherheitskonzept muss die folgenden Punkte umfassen:

- 205 • Beschreibung des Produkts bzgl. allgemeiner Informationssicherheitsaspekte,
- 206 • Sicherheitsanforderungen der gematik,
- 207 • Schutzbedarfsfeststellung,
- 208 • Bedrohungsanalyse,
- 209 • Sicherheitsanalyse (Verifikation der Wirksamkeit der Sicherheitsmaßnahmen),
- 210 • Erstellung einer Restrisikoabschätzung.

211 Hinweis: Das Datenschutzkonzept muss die folgenden Punkte umfassen:

- 212 • Beschreibung des Produkts bzgl. Datenschutzaspekten,
- 213 • Identifikation der Rahmenbedingungen des Datenschutzes,
- 214 • Identifikation der personenbezogenen Daten und Anwendungsprozesse,
- 215 • Umsetzung der Grundsätze für die Verarbeitung personenbezogener Daten -
- 216 Datenschutz-Risiken und Datenschutz-Hinweise.

### 217 **A\_19147 - Sicherheitstestplan**

218 Der Hersteller eines Produktes MUSS einen Testplan für Sicherheitstests erstellen und auf  
219 Verlangen der gematik zur Verfügung stellen.[<=]

220 Hinweis: Der Testplan umfasst alle Sicherheitstests während der Phasen der  
221 Produktentwicklung sowie regelmäßige Sicherheitsprüfungen (Pentest) durch  
222 unabhängige Sicherheitsexperten. Der Umfang des Testplans hängt von der Zielplattform  
223 sowie den Funktionalitäten des Produktes ab und muss zwingend das Testvorgehen zu  
224 den Sicherheitsvorgaben der gematik beinhalten.

225 Orientierungen zu den Inhalten eines Testplanes sind z.B. imOWASP Mobile Security  
226 Testing Guide [MSTG] und im OWASP Mobile Application Security Verification Standard  
227 [MASVS] beschrieben. Der Testplan muss einen ähnlichen Detaillierungsgrad haben wie  
228 in den beiden OWASP-Referenzen.

### 229 **A\_19150 - Umsetzung Sicherheitstestplan**

230 Der Hersteller eines Produktes MUSS seinen Testplan für Sicherheitstests umsetzen und  
231 der gematik bei jeder Veröffentlichung einer neuen Produktversion einen Testbericht zur  
232 Verfügung stellen.[<=]

### 233 **A\_19151 - Implementierungsspezifische Sicherheitsanforderungen**

234 Der Hersteller eines Produktes MUSS während der Entwicklung des Produktes  
235 implementierungsspezifische Sicherheitsanforderungen dokumentieren und  
236 umsetzen.[<=]

237 Hinweis: Der Testbericht muss zwingend Testauswertungen zu den Sicherheitsvorgaben  
238 der gematik beinhalten.

**A\_19152 - Verwendung eines sicheren Produktlebenszyklus**

Der Hersteller eines Produktes MUSS innerhalb des Produktlebenszyklus (Entwicklung, Betrieb, Außerbetriebnahme) seines Produktes Sicherheitsaktivitäten integrieren und anwenden, d. h. in einschlägigen Fachkreisen anerkannte, erprobte und bewährte Regeln anwenden. [ <= ]

Hinweis: Ein Beispiel für Sicherheitsaktivitäten in einem Produktlebenszyklus ist der Microsoft Security Development Lifecycle. Für weitere Informationen siehe [OWASP SAMM Project] oder den durch das BSI bereitgestellten "Leitfaden zur Entwicklung sicherer Webanwendungen - Empfehlungen und Anforderungen an die Auftragnehmer" (insbesondere Kapitel 4).

**A\_19153 - Sicherheitsrelevanter Softwarearchitektur-Review**

Der Hersteller eines Produktes MUSS einen sicherheitsrelevanten Softwarearchitektur-Review durchführen und identifizierte Architekturschwachstellen beheben. [ <= ]

**A\_19154 - Durchführung einer Bedrohungsanalyse**

Der Hersteller eines Produktes MUSS eine Bedrohungsanalyse durchführen und Maßnahmen gegen die identifizierten Bedrohungen implementieren. [ <= ]

**A\_19155 - Durchführung sicherheitsrelevanter Quellcode-Reviews**

Der Hersteller eines Produktes MUSS während der Entwicklung des Produktes sicherheitsrelevante Quellcode-Reviews oder automatisierte sicherheitsrelevante Quellcode-Scans durchführen. [ <= ]

**A\_19156 - Durchführung automatisierter Sicherheitstests**

Der Hersteller eines Produktes MUSS während der Entwicklung des Produktes automatisierte Sicherheitstests durchführen. [ <= ]

**A\_19157 - Dokumentierter Plan zur Sicherheitsschulung für Entwickler**

Der Hersteller eines Produktes MUSS einen Schulungsplan zur regelmäßigen Schulung von Entwicklern in sicherer Entwicklung und Secure-Coding-Techniken dokumentieren und umsetzen. [ <= ]

**A\_19158 - Sicherheitsschulung für Entwickler**

Der Hersteller eines Produktes MUSS alle Entwickler des Produktes in sicherer Entwicklung und Secure-Coding-Techniken schulen. [ <= ]

**A\_19159 - Dokumentation des sicheren Produktlebenszyklus**

Der Hersteller eines Produktes MUSS den verwendeten sicheren Produktlebenszyklus und dessen Teilprozesse dokumentieren und auf Nachfrage der gematik zur Verfügung stellen. Die Dokumentation soll mindestens die folgenden Sicherheitsaktivitäten beschreiben:

- Erfassen und Umsetzen von implementierungsspezifischen Sicherheitsanforderungen für das Produkt und von Best-Practice-Sicherheitsanforderungen,
- Durchführen von sicherheitsrelevanten Architektur- und Design-Reviews,
- Durchführen von Bedrohungsanalysen,
- Durchführen von sicherheitsrelevanten Quellcode-Reviews,
- Durchführen von Sicherheitstests während der Qualitätssicherungsphase,
- Etablieren von Quality Gates, die eine Veröffentlichung des Produkts mit 'Mittel' oder 'Hoch' bewerteten Sicherheitsfehlern verhindern,
- Änderungs- und Konfigurationsmanagement,

- Schwachstellen-Management.

[<=]

#### **A\_19160 - Änderungs- und Konfigurationsmanagementprozess**

Der Hersteller eines Produktes MUSS während der Entwicklung des Produktes einen Änderungs- und Konfigurationsmanagementprozess verwenden. Das Änderungsmanagement umfasst mindestens den Entscheidungsprozess über vorgeschlagene Änderungen und die Autorisierung der Änderungen. Das Konfigurationsmanagement liefert mindestens zu jedem Zeitpunkt die eindeutige Zusammensetzung des Produktes bezüglich seiner eindeutigen Komponenten (Dritt-Software wie Bibliotheken, Frameworks) und den vorgenommenen Änderungen an eigenen Komponenten.[<=]

#### **A\_19161 - Verifizierung der Einhaltung sicherheitstechnische Eignung durch Datenschutzbeauftragten**

Der Hersteller eines Produktes MUSS bei Veröffentlichung einer neuen Produktversion des Produktes die Einhaltung der Herstellererklärung "sicherheitstechnische Eignung" durch seinen Datenschutzbeauftragten verifizieren lassen.[<=]

Hinweis: Falls es keinen Datenschutzbeauftragten beim Hersteller gibt, kann eine alternative Rolle die sicherheitstechnische Eignung verifizieren, z.B. der Sicherheitsbeauftragte. Diese Rolle darf nicht an der Entwicklung des Produktes teilnehmen und muss direkt an die Geschäftsführung des Herstellers berichten.

#### **A\_19162 - Informationspflicht bei Veröffentlichung neue Produktversion**

Der Hersteller eines Produktes MUSS die gematik bei Veröffentlichung einer neuen Produktversion informieren.[<=]

### **2.3 Unterstützung von Audits**

#### **A\_19163 - Rechte der gematik zur sicherheitstechnischen Prüfung des Produktes**

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

- Sicherheitsprüfungen (z.B. Whitebox oder Blackbox Pentest) seines Produktes durchzuführen (hiervon unbenommen ist das Recht der gematik, eine anlasslose Sicherheitsprüfung durchzuführen),
- im Rahmen einer Sicherheitsprüfung die konkrete Umsetzung der an das Produkt gestellten Anforderungen zu überprüfen.

Der Hersteller MUSS dies im gleichen Maße für Unterauftragnehmer zusichern. Die Kosten, die dem Hersteller durch diese Mitwirkungspflichten entstehen, trägt der Hersteller selbst.[<=]

#### **A\_19164 - Mitwirkungspflicht bei Sicherheitsprüfung**

Der Hersteller eines Produktes MUSS Sicherheitsprüfungen (z.B. Pentest) der gematik unterstützen.[<=]

Hinweis: Unterstützen bedeutet beispielsweise das Bereitstellen einer Release- oder Beta-Version des Produkts, das Bereitstellen eines Testsystems inkl. Test-Accounts, kleine Anpassungen des Produktes, die eine Beschleunigung des Tests ermöglichen (z.B. Entfernung von Certificate Pinning, Code Obfuscation) und Unterstützung bei Rückfragen.

**A\_19165 - Auditrechte der gematik zur Prüfung der Herstellerbestätigung**

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

- Audits durchzuführen (hiervon unbenommen ist das Recht der gematik, anlasslose Audits durchzuführen),
- im Rahmen eines Audits beim Hersteller die konkrete Umsetzung der an den Hersteller gestellten Anforderungen zu überprüfen,
- im Rahmen eines Audits während der üblichen Geschäftszeiten die Geschäftsräume des Herstellers 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.

Der Hersteller MUSS dies im gleichen Maße für Unterauftragnehmer zusichern. Die Kosten, die dem Hersteller durch diese Mitwirkungspflichten entstehen, trägt der Hersteller selbst. [≤]

## 3 Anhang A – Verzeichnisse

### 3.1 Abkürzungen

Kürzel	Erläuterung
ISM	Informationssicherheitsmanagement
SGB V	Sozialgesetzbuch
TI	Telematikinfrastruktur

### 3.2 Abbildungsverzeichnis

Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

### 3.3 Referenzierte Dokumente

#### 3.3.1 Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemRL_Betr_TI]	gematik: Übergreifende Richtlinien zum Betrieb der TI
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur

358 **3.3.2 Weitere Dokumente**

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[OWASP Top 10 Report]	OWASP Foundation, OWASP Top Ten Project: "OWASP Top 10 The Ten Most Critical Web Application Security Risks", <a href="https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project">https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project</a> (üblicherweise im PDF Format)

359