

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# **Richtlinie zur Prüfung der Sicherheitseignung**

Version:	3.0.0
Revision:	1197553
Stand:	14.04.2025
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemRL_PruefSichEig_DS

---

## Dokumentinformationen

---

### Änderungen zur Vorversion

Einfügen des Produktgutachtens/Produktgutachters sowie grundlegende Anpassung des gesamten Dokuments. Die Änderungen zur Vorversion sind auf Grund der grundsätzlichen Überarbeitung und entsprechenden Vielzahl von Änderungen nicht markiert.

### Dokumentenhistorie

Version	Datum	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.5.0	03.07.12		zur Abstimmung freigegeben	PL P77
1.0.0	15.10.12		Einarbeitung Kommentare	P77
1.1.0	06.06.13		Einarbeitung Kommentare LA	P77
1.2.0	15.08.13	Kap. 3.9	Anpassung der Formulierung bezüglich zu prüfender Anforderungen aus den Produkttypsteckbriefen (vorher Checklisten), Änderungsliste vom 08.08.13	P77
1.2.1	25.01.17	Kap. 3.8.1, Kap. 8.2	Anpassung zum 4-Augen-Prinzip bei der Erstellung von Gutachten sowie Streichung des Kap. 3.8.1 „Bestätigung nach SigG“	gematik
2.0.0	26.11.18	alle	Einführung Produktgutachten; grundlegende Anpassung	gematik
2.1.0	27.04.2020	2.3	Qualifikation Produktgutachter, Definition Delta-Gutachten	gematik
2.2.0	28.02.2023	Kap. 2  6.8 - 6.10	Geändertes Verfahren für Produktgutachten Präzisierungen zu bestehenden Prüfmethoden des Produktgutachtens und Aufnahme Prüfung physischer Schutzmaßnahmen	gematik

3.0.0	14.04.2025	alle	grundlegende Überarbeitung der gesamten Richtlinie	gematik
-------	------------	------	---	---------

---

## Inhaltsverzeichnis

---

<b>1 Einordnung des Dokumentes.....</b>	<b>7</b>
1.1 Zielsetzung.....	7
1.2 Zielgruppe.....	7
1.3 Geltungsbereich.....	7
1.4 Abgrenzung des Dokumentes.....	8
1.5 Methodik.....	8
<b>2 Gutachten-Typen.....</b>	<b>9</b>
2.1 Sicherheitsgutachten.....	9
2.2 Produktgutachten.....	10
2.3 Delta-Gutachten.....	10
<b>3 Prüfauftrag.....</b>	<b>11</b>
<b>4 Prüfumfang und -grundlage.....</b>	<b>12</b>
<b>5 Prüfkriterien und Bewertungsschema.....</b>	<b>13</b>
5.1 Aktualität.....	13
5.2 Angemessenheit.....	13
5.3 Vollständigkeit der Maßnahmen.....	13
5.4 Umsetzung der Anforderungen.....	14
5.4.1 Umgesetzt.....	14
5.4.2 Teilweise umgesetzt.....	14
5.4.3 Nicht umgesetzt.....	14
5.4.4 Nicht anwendbar.....	15
5.5 Sicherheitsbewertung.....	15
5.5.1 Kein Sicherheitsmangel (OK).....	15
5.5.2 Schwerwiegender Sicherheitsmangel (NC-A).....	16
5.5.3 Sicherheitsmangel (NC-B).....	16
5.5.4 Sicherheitsempfehlung (PI).....	16
<b>6 Prüfmethoden.....</b>	<b>17</b>
<b>6.1 Gutachten-Typ-spezifische Festlegungen.....</b>	<b>17</b>
6.1.1 Sicherheitsgutachten.....	17
6.1.2 Produktgutachten.....	17
<b>6.2 Aktenanalyse (DOK).....</b>	<b>18</b>
<b>6.3 Datenanalyse (DA).....</b>	<b>18</b>
<b>6.4 Quellcode-Analyse (SCA).....</b>	<b>18</b>
<b>6.5 Befragung (BE).....</b>	<b>18</b>

6.5.1 Mündliche Befragungen.....	19
6.5.2 Schriftliche Befragungen.....	19
<b>6.6 Inaugenscheinnahme und Beobachtung (IB).....</b>	<b>19</b>
6.6.1 Inaugenscheinnahme.....	20
6.6.2 Beobachtung.....	20
<b>6.7 Prüfung physischer Schutzmaßnahmen (INF).....</b>	<b>20</b>
<b>6.8 Technische Prüfung ohne eigenen Systemzugriff (TP).....</b>	<b>21</b>
<b>6.9 Technische Prüfung mit Systemzugriff (TP+).....</b>	<b>21</b>
<b>6.10 Penetrationstest (PEN).....</b>	<b>21</b>
<b>6.11 Verwendung bestehender Nachweise (ZER).....</b>	<b>22</b>
<b>7 Prüfplan.....</b>	<b>24</b>
7.1 Festlegung anzuwendender Prüfmethoden.....	24
<b>8 Gutachten.....</b>	<b>25</b>
8.1 Gutachten-Beurteilung & Nachforderungen.....	25
8.2 Bestätigung durch die Zulassungsstelle.....	26
<b>9 Gutachter-Kompetenz.....</b>	<b>27</b>
<b>9.1 Sicherheitsgutachter.....</b>	<b>27</b>
9.1.1 Basisqualifikation.....	27
9.1.2 Zusatzqualifikation „Sicherheitsgutachter TI“.....	28
9.1.3 Aufrechterhaltung der Sicherheitsgutachter-Akkreditierung.....	28
<b>9.2 Produktgutachter.....</b>	<b>29</b>
9.2.1 Basisqualifikation.....	29
9.2.2 Zusatzqualifikation „Sicherheitsgutachter TI“.....	29
9.2.3 Begutachtung von Frontends des Versicherten.....	30
<b>9.3 Fachexperten.....</b>	<b>30</b>
<b>9.4 Vier-Augen-Prinzip.....</b>	<b>30</b>
9.4.1 Allgemeines.....	30
9.4.2 Sicherheitsgutachten.....	31
9.4.3 Produktgutachten.....	31
<b>9.5 Unabhängigkeit und Objektivität.....</b>	<b>31</b>
<b>10 Anhang A - Verzeichnisse.....</b>	<b>32</b>
<b>10.1 A1 - Abkürzungen.....</b>	<b>32</b>
<b>10.2 A2 - Referenzierte Dokumente.....</b>	<b>32</b>
<b>10.3 A3 - Muster Gutachten Kapitelstruktur.....</b>	<b>33</b>
10.3.1 Deckblatt.....	33
10.3.2 Dokumentenhistorie.....	33
10.3.3 Kontaktdaten des Antragsstellers.....	34
10.3.4 Kontaktdaten der Gutachter / Fachexperten.....	34
10.3.5 Management Summary.....	35
10.3.6 Grundlagen der Prüfung.....	35
10.3.7 detaillierte Beschreibung der Prüfung.....	36
10.3.7.1 Beschreibung des Prüfgegenstandes.....	36

10.3.7.2 Standorte des Prüfgegenstandes.....	36
10.3.7.3 Liste der Dienstleister.....	36
10.3.7.4 Beschreibung des Prüfplans.....	36
10.3.7.5 Absprachen.....	37
10.3.7.6 Beschreibung bei Vor-Ort-Prüfungen.....	37
10.3.8 Dokumentation der Prüfergebnisse.....	38
10.3.9 Eigenerklärung der Gutachter / Fachexperten.....	39
10.3.10 Anhang.....	39

---

## **1 Einordnung des Dokumentes**

---

### **1.1 Zielsetzung**

Im Rahmen der Zulassungs- und Bestätigungsverfahren (im Folgenden „Zulassung“ genannt) der gematik für zentrale Dienste, Fachdienste, Dienste der sicheren Übermittlungsverfahren, Anbieter dieser Dienste der Telematikinfrastruktur (im Folgenden „TI“ genannt) sowie für weitere Anwendungen, die die TI beeinflussen können, ist die Bewertung der Sicherheitseignung erforderlich. Hierzu werden vom Zulassungsnehmer Prüfaufträge an externe Gutachter vergeben. Diese bewerten in von ihnen erstellten Sicherheits- oder Produktgutachten (im Folgenden zusammenfassend „Gutachten“ genannt) die sicherheitstechnischen Eigenschaften des Prüfgegenstandes. Die formalen und fachlichen Anforderungen an die Gutachter werden durch die vorliegende Richtlinie [gemRL\_PruefSichEig\_DS] sowie durch die spezifischen Produkttyp-, Anbietertyp- und Anwendungssteckbriefe (im Folgenden zusammenfassend „Steckbriefe“ genannt) festgelegt. Im Rahmen der Gutachtertätigkeit werden die konkreten Umsetzungen und Implementierungen der jeweiligen Maßnahmen zur Gewährleistung der Informationssicherheit und des Datenschutzes validiert und dokumentiert. Diese Gutachten bilden eine Grundlage für die nachgelagerte Bewertung der Zulassungsfähigkeit durch die gematik.

Die innerhalb der Gutachtertätigkeit gewählte Prüfmethodik orientiert sich am BSI-Leitfaden für die Informationssicherheitsrevision [BSIInfRev]. Das Ziel ist die Nachvollziehbarkeit der Prüftätigkeiten sowie der gutachterlichen Bewertungen zum Umsetzungsstand der sicherheitstechnischen Anforderungen. Besonderer Wert wird dabei auf die Auswertbarkeit, Vergleichbarkeit und Nachnutzbarkeit der Gutachten gelegt, da diese einen wesentlichen Baustein in den Zulassungsprozessen der gematik darstellen.

### **1.2 Zielgruppe**

Das Dokument richtet sich an Organisationen und Personen, die mit der Prüfung der Sicherheitseignung von Produkten und Anbietern der TI beauftragt sind.

### **1.3 Geltungsbereich**

Dieses Dokument enthält normative Festlegungen für die Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren werden von der gematik in gesonderten Dokumenten (z. B. Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Das Dokument ist verbindlich für die Erstellung und Prüfung von Gutachten, die im Rahmen der Zulassung von Anbietern und Produkten der TI vorzulegen sind.

## **1.4 Abgrenzung des Dokumentes**

Das Dokument definiert keine neuen Anforderungen an die Prüfgegenstände. Es werden lediglich Anforderungen an die Prüfprozesse im Rahmen der Begutachtung sowie an die Gutachter selbst definiert.

## **1.5 Methodik**

Die in diesem Dokument definierten Anforderungen an Gutachten und Gutachter sind **nicht** durch eine eindeutige ID und **nicht** durch die in Großbuchstaben geschriebenen deutschen Schlüsselwörter MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN entsprechend RFC 2119 [RFC2119] gekennzeichnet.



---

## 2 Gutachten-Typen

---

Für den Nachweis der Sicherheitseignung von TI Diensten gibt es zwei Arten von Gutachten: Das Sicherheitsgutachten und das Produktgutachten. Im Folgenden sind häufig beide Arten gemeint, weshalb zusammenfassend von „Gutachten“ gesprochen wird. An den entsprechenden Stellen wird jedoch explizit auf die Besonderheiten der jeweiligen Gutachtenart eingegangen. Ein Gutachten wird als Vollgutachten bezeichnet, wenn der Prüfumfang alle Anforderungen des Steckbriefs umfasst. Ein Gutachten, in dem nur ein Teil der Anforderungen geprüft wird, wird als Delta-Gutachten bezeichnet.

Sowohl Sicherheits- als auch Produktgutachten haben in den jeweiligen Zulassungsverfahren eine Gültigkeit von maximal drei Jahren und müssen entsprechend erneuert werden, um die Aussage über die sicherheitstechnische Eignung aufrecht zu erhalten.

Die Dienste der TI werden zusätzlich in einer Referenz- und einer Testumgebung betrieben. Die Referenzumgebung (RU) steht den Betreibern / Anbietern / Herstellern, die Testumgebung (TU) der gematik für Tests zur Verfügung. Innerhalb der RU und TU ist ausschließlich die Nutzung von Testdaten zulässig. Die Nutzung und der Betrieb von Echtdaten ist nur in der Produktivumgebung (PU) zulässig.

Etwaige Prüfungen von Anforderungen in der RU / TU sind im Gutachten nachvollziehbar zu begründen. Produktgutachten müssen nachvollziehbar darlegen, wie sichergestellt wird, dass das geprüfte Produkt auch in der PU so eingesetzt wird.

### **Hinweis:**

*Insbesondere bei neuen Produkten ist bei Sicherheitsgutachten eine teilweise Begutachtung in der RU/TU zulässig, da vor der Zulassung kein Betrieb in der PU zulässig ist. Gegebenenfalls kann eine Überprüfung in der PU nach Erteilung der Zulassung gefordert werden.*

### **2.1 Sicherheitsgutachten**

Der inhaltliche Schwerpunkt von Sicherheitsgutachten liegt in der Überprüfung der definierten Anforderungen an eine sichere Betriebsumgebung (z. B. Rechenzentren, Entwicklungsstandorte etc.) und insbesondere an die Prozesse zur Einhaltung der Informationssicherheit. Sekundär umfassen Sicherheitsgutachten zum Teil auch eine Überprüfung der Hard- und Software im Hinblick auf die konkret umgesetzten technischen und organisatorischen Maßnahmen.

Da Sicherheitsgutachten die allgemeinen und grundlegenden Sicherheitsprozesse von Anbietern/Betreibern/Herstellern bewerten und deren Vorgaben und Umsetzungen in der Regel längerfristig Bestand haben, ist innerhalb der dreijährigen Gültigkeitsdauer des Sicherheitsgutachtens die Vorlage eines Deltagutachtens nach dem ersten bzw. zweiten Jahr nicht erforderlich, sofern die im ursprünglichen Vollgutachten bescheinigten Maßnahmenumsetzungen weiterhin gültig sind.

## **2.2 Produktgutachten**

Der inhaltliche Schwerpunkt von Produktgutachten liegt in der vertieften sicherheitstechnischen Prüfung einer konkreten IT-Lösung und umfasst neben der Quellcode-Analyse auch die Durchführung von Penetrationstests, um sowohl die tatsächliche technische Umsetzung der definierten Anforderungen als auch die Resilienz des Prüfgegenstandes gegenüber verschiedenen Angriffsvektoren zu validieren. Darüber hinaus ist die Überprüfung der umgebenden technischen und organisatorischen Maßnahmen zur Einhaltung der Sicherheitsprozesse flankierend zur Sicherheitsüberprüfung ein untergeordneter Bestandteil der Produktgutachten.

Für das jeweilige Produkt ist jährlich ein Voll- bzw. Deltagutachten einzureichen.

- Für das erste Produktrelease ist ein Vollgutachten erforderlich, das vor dem Einsatz des Produktes in der Produktivumgebung (PU) zu erstellen und der gematik für das Zulassungsverfahren vorzulegen ist. Spätestens nach drei Jahren ist ein neues Vollgutachten auf Basis der aktuellen Anforderungssituation zu erstellen und einzureichen.
- Während der dreijährigen Gültigkeit des Vollgutachtens ist jährlich ein Delta-Gutachten zu erstellen, sofern sicherheits- oder datenschutzrelevante Änderungen am Produkt vorgenommen wurden, die im letzten Gutachten noch nicht geprüft wurden.

## **2.3 Delta-Gutachten**

Bei wesentlichen Änderungen (z. B. bei technischen, organisatorischen oder baulichen Änderungen mit Einfluss auf Anforderungen des Steckbriefes) an einem sicherheits- oder produktgutachterlich geprüften Produkt ist der Sicherheitsgutachter durch den Anbieter bzw. Hersteller stets einzubeziehen, sofern nicht bereits produkttypspezifische Regelungen festlegen, wann eine erneute Begutachtung erforderlich ist. Ist dies nicht der Fall, entscheidet der Sicherheitsgutachter (bei Produktgutachten ggf. gemeinsam mit dem Produktgutachter), ob die Änderungen für den Datenschutz und die Informationssicherheit so relevant sind, dass sie vor der Inbetriebnahme erneut begutachtet werden müssen und ob das Sicherheits- bzw. Produktgutachten angepasst werden muss. Bei einer Anpassung des Gutachtens muss nur der Teil des Gutachtens neu beschrieben und bewertet werden, der sich auf die Änderung bezieht. Der übrige Inhalt kann unverändert bleiben, sofern die vorgenommenen Änderungen keinen Einfluss auf andere Teile des Produkts (oder im Extremfall auf das gesamte Produkt) haben. Die neue Version des Gutachtens ist dann ein sogenanntes „Delta-Gutachten“. Dabei ist zu beachten, dass die zeitliche Gültigkeit des ursprünglichen (vollständigen) Sicherheits- bzw. Produktgutachtens bestehen bleibt, also durch ein Delta-Gutachten nicht verlängert wird.

Das Delta-Gutachten ist somit kein eigener Gutachtentyp, sondern ein Sonderfall des Sicherheits- bzw. Produktgutachtens bei wesentlichen Änderungen, die nur einen kleinen Teil des Produktes betreffen und daher keine vollständige Neubewertung erfordern.

Die Beschreibungen und Bewertungen im Rahmen des Delta-Gutachtens sind immer im ursprünglichen Vollgutachten festzuhalten, wobei die Änderungen kenntlich zu machen sind (z. B. durch farbliche Markierung). Ziel ist es, einerseits einen Gesamtüberblick über den Prüfgegenstand zu erhalten und andererseits die Änderungen gegenüber dem ursprünglichen Vollgutachten kenntlich zu machen.

---

### **3 Prüfauftrag**

---

Der Prüfauftrag ist Bestandteil der Vereinbarung zwischen dem Auftraggeber (Zulassungsnehmer) und dem Sicherheitsgutachter. Der Prüfauftrag muss sich eindeutig auf die Anforderungen der gematik beziehen.

Der Gutachter hat im Rahmen der Gutachtenerstellung die ihm benannten Prüfgegenstände explizit anhand der in diesem Dokument [gemRL\_PruefSichEig\_DS] normierten Verfahren sowie anhand der Vorgaben der gematik (Steckbrief) zu prüfen und zu bewerten. Der Gutachter muss im Rahmen der Gutachtenerstellung das aktuelle Sicherheitsniveau der Prüfgegenstände sowie die Einhaltung der Vorschriften zum Schutz personenbezogener Daten feststellen und anhand der Vorgaben der gematik bewerten. Im Ergebnis soll durch den Gutachter eine belastbare Aussage über die Gesamtsicherheit des Prüfgegenstandes getroffen werden.

Insbesondere sind seitens des Gutachters im Rahmen der Gutachtenerstellung festgestellte Sicherheitslücken und Mängel, die das Erreichen des von der gematik geforderten Datenschutz- und Sicherheitsniveaus oder die Einhaltung der Vorschriften zum Schutz personenbezogener Daten verhindern, nachvollziehbar und eindeutig zu dokumentieren.

---

## **4 Prüfumfang und -grundlage**

---

Als Prüfgrundlage hat der Gutachter die zum Zeitpunkt des Beginns seiner Prüftätigkeit aktuellste von der gematik veröffentlichte zulassungsfähige Version des Produkttyps, des Anbietertyps bzw. der Anwendung und die zugehörige Spezifikation zu verwenden. Die Definition der zulassungsfähigen Versionen wird über den Online-Reader der gematik [gemSpecPages] zur Verfügung gestellt.

Aufgrund der Zeitspanne zwischen der Einreichung des Zulassungsantrages und dem Beginn der Prüfung durch das Gutachterteam ergibt sich für die Hersteller / Anbieter die Herausforderung des „Moving Target“ während der Entwicklung:

- Zulassungsantrag für eine bestimmte Produkttypversion / Anbietertypversion
- Anpassung der Spezifikationen durch die gematik während der Entwicklung
- Gutachten-Prüfhandlungen basieren auf neue Produkttypversion / Anbietertypversion mit ggf. neuen / geänderten Anforderungen

Seitens des Erstgutachters ist daher vor Beginn der Prüftätigkeiten zu beurteilen, ob und inwieweit der Anforderungsumfang des Gutachtens von etwaigen Neuerungen/Änderungen betroffen ist. Bei Unklarheiten über das weitere Vorgehen ist Rücksprache mit der gematik zu halten.

Bei Wiederholungsbegutachtungen - insbesondere bei der erneuten Vollbegutachtung (Folgegutachten) nach drei Jahren (siehe Kapitel 2) - wird daher in der Regel eine neuere Version des Steckbriefs verwendet als dies bei der eigentlichen Zulassung des Produkts, des Anbieters oder der Anwendung der Fall war. Bei Abweichungen hiervon - z. B. bei Delta-Begutachtungen - ist frühzeitig eine Abstimmung mit der gematik herbeizuführen, um zu klären, ob das beabsichtigte Vorgehen zulässig ist.

Der Gutachter hat die Konformität des Prüfgegenstandes mit den Anforderungen des verwendeten Steckbriefes zu prüfen und zu bewerten. Relevant sind dabei die Anforderungen, die im Steckbrief bei der Aufzählung der Anforderungen an die sicherheitstechnische Eignung in den Unterabschnitten „Sicherheitsgutachten“ bzw. „Produktgutachten“ aufgeführt sind.

Werden von einem Gutachter mehrere Produkte, Anbieter oder Anwendungen begutachtet, so ist es zulässig, diese in einem Gutachten zusammenzufassen, wobei sich das Votum ausdrücklich auf alle begutachteten Prüfgegenstände beziehen muss oder für jeden Prüfgegenstand ein dediziertes Votum zu erstellen ist.

---

## **5 Prüfkriterien und Bewertungsschema**

---

Ziel der Prüftätigkeiten im Gutachtenwesen ist die Bewertung des Datenschutz- und Informationssicherheitsniveaus. Das Gutachten zeigt dem Auftraggeber in strukturierter Form den Umsetzungsstand sowie das erreichte Sicherheitsniveau und ggf. den Handlungsbedarf aufgrund bestehender Sicherheitsdefizite, die durch fehlende oder unzureichend umgesetzte Anforderungen verursacht werden. Das Gutachten dient damit auch als Hilfestellung für den weiteren Optimierungsprozess. Dem Gutachten sind die in diesem Kapitel dokumentierten Bewertungsschemata zugrunde zu legen.

### **5.1 Aktualität**

Es ist zu bewerten, ob die getroffenen Sicherheitsmaßnahmen dem Stand der Technik entsprechen.

### **5.2 Angemessenheit**

Die Prüfung der Angemessenheit der Umsetzung von Anforderungen durch Maßnahmen beinhaltet die Bewertung hinsichtlich ihrer Wirksamkeit. Um die Angemessenheit einer Maßnahme zu beurteilen, sollten die Antworten auf die folgenden Fragen bewertet werden:

- Welches Risiko soll durch die Umsetzung der Maßnahme reduziert werden?
- Welches Restrisiko verbleibt und ist dieses Restrisiko aus heutiger Sicht akzeptabel?
- Ist die Maßnahme geeignet und praktikabel?
- Ist die Maßnahme anwendbar, leicht verständlich und wenig fehleranfällig?
- Steht die getroffene Maßnahme in einem angemessenen Verhältnis zur angestrebten Risikominderung?

Bei der Prüfung der Angemessenheit werden folgende Aspekte berücksichtigt

- Risiken, die durch die Maßnahme reduziert werden sollen;
- verbleibendes Restrisiko und Bewertung der Akzeptanz;
- Eignung und Umsetzbarkeit der Maßnahme;
- Anwendbarkeit, Verständlichkeit und Fehleranfälligkeit der Maßnahme.

### **5.3 Vollständigkeit der Maßnahmen**

Im Hinblick auf die Vollständigkeit der den Anforderungen gegenübergestellten Maßnahmen ist zu prüfen, ob alle Aspekte der Anforderung durch die Maßnahmen abgedeckt sind.

## **5.4 Umsetzung der Anforderungen**

Es ist zu prüfen, ob die Anforderungen des Steckbriefs durch wirksame Maßnahmen umgesetzt werden.

Die den jeweiligen Steckbriefen zugeordneten Anforderungen sind mit Schlüsselwörtern gemäß [RFC2119] versehen. Eine Umsetzung der mit dem Schlüsselwort „SOLL“ definierten Teilanforderungen ist optional. Es ist jedoch zu prüfen, ob und inwieweit sich der Anbieter / Hersteller dennoch nachvollziehbar inhaltlich mit diesen Anforderungen auseinandergesetzt hat und ob bei einer eventuellen Nichtumsetzung dieser Anforderungen eine dokumentierte Begründung vorliegt. Ein grundsätzliches „Ignorieren“ von SOLL-Anforderungen ohne transparente Begründung seitens des Anbieters / Herstellers ist nicht zulässig.

Im Hinblick auf die Vollständigkeit der Maßnahmen, die den Anforderungen gegenübergestellt werden, ist zu prüfen, ob alle Aspekte der Anforderung durch die Maßnahmen abgedeckt sind.

Der jeweilige Umsetzungsstatus ist für jede Anforderung durch den Gutachter zu erfassen und sowie nachvollziehbar begründet zu dokumentieren. Dabei ist für jede Anforderung eine der folgenden Varianten des Umsetzungsstatus durch den Gutachter festzulegen:

### **5.4.1 Umgesetzt**

Alle Maßnahmen zur Erfüllung der Anforderung sind vollständig, wirksam und angemessen umgesetzt. Die umgesetzten Maßnahmen reduzieren das Risiko in ausreichendem Maße. Sofern der Status „Umgesetzt“ nicht erreicht wird, sind notwendige Folgemaßnahmen zur Erfüllung der Anforderungen durch den Gutachter zu beschreiben.

#### **Hinweis:**

*Für den Fall, dass bei einer als vollständig, wirksam und angemessen umgesetzt eingestuften Anforderung durch die Begutachtung zusätzliche Verbesserungspotenziale identifiziert wurden, ist die Festlegung von Sicherheitsempfehlungen gemäß Kapitel 5.5.4 zulässig.*

### **5.4.2 Teilweise umgesetzt**

Einige Maßnahmen, die der Anforderung zugeordnet sind, sind umgesetzt, andere noch nicht oder nur teilweise.

Es ist zu beurteilen, ob dies einen Sicherheitsmangel oder einen schwerwiegenden Sicherheitsmangel für den Prüfgegenstand darstellt. Es ist auch zu dokumentieren, welche der Maßnahmen, die der Anforderung gegenüberstehen, noch umgesetzt werden müssen.

### **5.4.3 Nicht umgesetzt**

Die der Anforderung gegenüberstehenden Maßnahmen sind überwiegend noch nicht umgesetzt. Die umgesetzten Maßnahmen decken die Anforderung nicht ab.

Es ist zu beurteilen, ob dies einen Sicherheitsmangel oder einen schwerwiegenden Sicherheitsmangel für den Prüfgegenstand darstellt.

#### **5.4.4 Nicht anwendbar**

Die Anforderung ist zwar im Steckbrief enthalten, jedoch nicht anwendbar für die konkrete Ausprägung des Prüfgegenstandes (z. B. weil der Prüfgegenstand nur einen Teilprozess des im Steckbrief definierten Gesamtprozesses darstellt). Es ist jedoch weiterhin zu beachten, dass grundsätzlich alle Anforderungen eines Steckbriefes verpflichtend sind. Die Zuordnung einer Anforderung zum Produkt / Anbieter ist dabei stets maßgeblich, nicht der Adressat in der Anforderung. Wird eine Anforderung seitens des Gutachters mit der Bewertung "Nicht anwendbar" eingestuft, so ist eine nachvollziehbare Begründung im Gutachten anzugeben. Im Falle einer Einstufung als "Nicht anwendbar" ist eine detaillierte Darstellung erforderlich, die aufzeigt, welche Instanz statt des Prüfgegenstandes / Herstellers / Anbieters / Betreibers die Verantwortung für die Einhaltung der Anforderung trägt. Im Zweifelsfall ist Rücksprache mit der gematik zu halten, ob einzelne Anforderungen für den gewählten Prüfgegenstand entfallen können.

### **5.5 Sicherheitsbewertung**

Die Bewertung der Umsetzung einer Anforderung durch Maßnahmen erfolgt unter Berücksichtigung potenzieller Sicherheitsmängel. Identifizierte Sicherheitsmängel sind hinsichtlich ihrer Kritikalität für die Aufrechterhaltung und Gewährleistung der Informationssicherheit und/oder des Datenschutzes zu bewerten. Die Einordnung ist in dem Gutachten nachvollziehbar zu begründen. Für die Bewertung sind folgende Kategorien zu verwenden:

- kein Sicherheitsmangel (OK)
- Schwerwiegender Sicherheitsmangel (Major Non Conformity / NC-A)
- Sicherheitsmangel (Minor Non Conformity / NC-B)
- Sicherheitsempfehlung (Potential for Improvement / PI)

Die ermittelten Sicherheitsmängel bzw. Sicherheitsempfehlungen sind in dem Gutachten in folgendem Format durchzunummerieren, um eine eindeutige Zuordnung in der nachgelagerten Behandlung zu ermöglichen:

- NC-A-lfdNr. (z. B. NC-A-001)
- NC-B-lfdNr. (z. B. NC-B-001)
- PI-lfdNr. (z. B. PI-001)

#### **5.5.1 Kein Sicherheitsmangel (OK)**

Wird die Kategorie "kein Sicherheitsmangel" gewählt, so werden die definierten Anforderungen durch die vorliegenden Maßnahmen vollumfänglich erfüllt. Das geforderte Datenschutz- und Informationssicherheitsniveau ist somit hinreichend gewährleistet. Dies bedeutet, dass keine Sicherheitslücke bzw. Abweichung gegenüber dem Soll-Zustand vorliegt und die Vorschriften zum Schutz personenbezogener Daten eingehalten werden.

#### **5.5.2 Schwerwiegender Sicherheitsmangel (NC-A)**

Bei der Wahl der Kategorie „schwerwiegender Sicherheitsmangel“ liegt z. B. aufgrund der Nichterfüllung einer Pflichtanforderung eine Abweichung/Sicherheitslücke vor, die unverzüglich geschlossen werden muss, da andernfalls das Erreichen der geforderten

Schutzziele hinsichtlich des geforderten Datenschutz- und Informationssicherheitsniveaus stark gefährdet und ein erheblicher Schaden zu erwarten ist. Der Gutachter hat eine Behebungsfrist zu definieren, innerhalb derer der Mangel durch den Anbieter/Betreiber/Hersteller zu beheben ist.

### **5.5.3 Sicherheitsmangel (NC-B)**

Bei der Wahl der Kategorie „Sicherheitsmangel“ liegt z. B. aufgrund der Nichterfüllung einer Pflichtanforderung eine Abweichung/Sicherheitslücke vor, die mittelfristig geschlossen werden muss. Die Erreichung der definierten Schutzziele hinsichtlich des geforderten Datenschutz- und Informationssicherheitsniveaus ist beeinträchtigt und nicht ausreichend gewährleistet. Der Gutachter hat eine Behebungsfrist zu definieren, innerhalb derer der Mangel durch den Anbieter/Betreiber/Hersteller zu beheben ist.

### **5.5.4 Sicherheitsempfehlung (PI)**

Die Auswahl der Kategorie „Sicherheitsempfehlung“ erfolgt unter der Prämisse, dass die definierten Anforderungen durch die implementierten Maßnahmen grundsätzlich erfüllt werden (der Umsetzungsstatus der Anforderung wird mit „umgesetzt“ bewertet, siehe Kapitel 5.4.1) Hinsichtlich der Informationssicherheit und des Datenschutzes bestehen jedoch weitere Verbesserungspotenziale, deren Realisierung den Reifegrad der Gesamtsicherheit weiter erhöhen könnte. Für die Sicherheitsempfehlung ist seitens des Gutachters eine Prüffrist festzulegen, innerhalb derer die Empfehlung durch den Anbieter/Betreiber/Hersteller zu prüfen und zu bewerten ist.



---

## **6 Prüfmethoden**

---

Der Begriff „Prüfmethoden“ bezeichnet alle Methoden, die zur Feststellung eines Sachverhalts herangezogen werden. Die Auswahl der anzuwendenden Prüfmethoden erfolgt unter Berücksichtigung des jeweiligen Prüfgegenstands bzw. der jeweiligen Anforderung aus dem Steckbrief. Zudem erfordern bestimmte Prüfmethoden spezifische Qualifikationen des Gutachters, sodass einige Prüfmethoden vom Sicherheitsgutachter und andere vom Produktgutachter durchzuführen sind (siehe Kapitel 6.1).

Der Gutachter muss die in den Kapiteln 6.2 bis 6.11 festgelegten Prüfmethoden dem Gutachten zugrunde legen. Die Kombination mehrerer Prüfmethoden zur Prüfung einer Anforderung ist möglich und in vielen Fällen sogar erforderlich. Aus dem Gutachten müssen für jede validierte Anforderung aus den zugehörigen Steckbriefen die seitens der Gutachter gewählten Prüfmethoden ersichtlich sein.

Darüber hinaus steht es im Ermessen des Gutachters, die Anwendung weiterer Prüfmethoden zu bestimmen, um eine zuverlässige, objektive und vollständige Prüfung eines Sachverhalts zu gewährleisten.

### **6.1 Gutachten-Typ-spezifische Festlegungen**

#### **6.1.1 Sicherheitsgutachten**

Bei Sicherheitsgutachten liegt die Wahl der Prüfmethode im Ermessen des Gutachters, wobei nach Möglichkeit eine „Inaugenscheinnahme und Beobachtung“ (siehe Kapitel 6.6) sowie eine „Technische Prüfung ohne eigenen Zugriff auf das System“ (siehe Kapitel 6.8) durchgeführt werden sollte. Als sekundäre Prüfmethoden bieten sich zudem die „Aktenanalyse“ (siehe Kapitel 6.2), die „Datenanalyse“ (siehe Kapitel 6.3) sowie die „Verwendung bestehender Nachweise“ (siehe Kapitel 6.11) an. Eine Ausnahme hiervon ist nur bei geringfügigen Nachbegutachtungen aufgrund von Änderungen am Prüfgegenstand (Delta-Gutachten) möglich. Die Wahl dieser Ausnahme ist im Sicherheitsgutachten nachvollziehbar zu begründen.

Des Weiteren ist durch den Gutachter festzulegen, welche Standorte für die Durchführung einer Vor-Ort-Prüfung ausgewählt wurden. Sofern für einzelne Betriebsstandorte des definierten Prüfgegenstandes keine Vor-Ort-Prüfung durchgeführt wurde, ist dies vom Gutachter nach einem risikobasierten Ansatz nachvollziehbar zu begründen.

#### **6.1.2 Produktgutachten**

Bei Produktgutachten muss der Produktgutachter für jede Anforderung zwingend eine der folgenden Prüfmethoden anwenden:

- Quellcode-Analyse (siehe Kapitel 6.4),
- Technische Prüfung mit Zugriff auf das System (siehe Kapitel 6.9) oder
- Penetrationstest (siehe Kapitel 6.10)

Darüber hinaus können und sollten weitere Prüfmethoden angewendet werden, bspw. die „Aktenanalyse“ (siehe Kapitel 6.2), um ein tieferes Verständnis für den Prüfgegenstand zu erlangen. Abweichungen von diesen Methoden sind durch den Produktgutachter im

Produktgutachten zu begründen. Für die Anwendung der genannten Prüfmethoden ist eine entsprechende Qualifikation des Gutachters erforderlich.

## 6.2 Aktenanalyse (DOK)

Die Aktenanalyse stellt einen zentralen Bestandteil jeder Prüfungstätigkeit dar und umfasst die sorgfältige Sichtung aller für den Prüfungsgegenstand maßgeblichen Unterlagen. Die vom Auftraggeber bereitgestellten Dokumente und Unterlagen, die für den Prüfgegenstand von Relevanz sind, sind durch den Gutachter sowohl auf Aktualität und Vollständigkeit als auch auf Anwendbarkeit auf den gewählten Prüfgegenstand zu überprüfen. Die Aktenanalyse bildet die Grundlage für die weiteren Prüftätigkeiten und ermöglicht dem Gutachter neben einem umfassenden Überblick über den Prüfgegenstand auch die Identifikation potenzieller Problembereiche sowie die Vorbereitung späterer vertiefender Validierungen (z. B. im Rahmen von Interviews, Vor-Ort-Begehungen, Prozessaudits etc.).

## 6.3 Datenanalyse (DA)

Der Auftraggeber, der die Prüfung veranlasst hat, stellt dem Gutachter Daten des Prüfgegenstandes zur Verfügung (z. B. Logfiles, Quellcode, Betriebsdaten, Systemkonfigurationen oder Prüfprotokolle). Im Rahmen der durchzuführenden Soll-Ist-Analyse werden die bereitgestellten Daten mit den vorgegebenen Sollwerten zu vergleichen sein.

## 6.4 Quellcode-Analyse (SCA)

Bei der Prüfmethode „Quellcode-Analyse“ ist die softwaretechnische Umsetzung einer oder mehrerer Anforderungen durch die Bewertung der entsprechenden Quellcode-Abschnitte zu validieren. Der Gutachter muss sich in geeigneter Weise vergewissern, dass der vom Auftraggeber zur Verfügung gestellte Quellcode und die darauf basierende Software mit dem vom Gutachter zu prüfenden System (Prüfgegenstand) übereinstimmen.

Die Quellcode-Analyse kann sowohl manuell als auch Tool-gestützt erfolgen. Der Gutachter muss das gewählte Vorgehen bei der Quellcode-Analyse, die durchgeführten Prüfschritte (unter Angabe der verwendeten Tools) und deren Ergebnisse - insbesondere die gefundenen Schwachstellen - im Gutachten nachvollziehbar dokumentieren. Für den Nachweis des Umsetzungsstandes (siehe Kapitel 5.4) der durch die Quellcode-Analyse geprüften Anforderungen ist eine kurze Erläuterung mit Verweis auf die entsprechenden Stellen in der Gesamtdokumentation der Quellcode-Analyse ausreichend.

## 6.5 Befragung (BE)

Befragungen dienen der systematischen und standardisierten Erhebung von Informationen. Eine sorgfältige Vorbereitung ist daher unerlässlich, um aussagekräftige Ergebnisse zu erhalten. Dies umfasst die Identifikation der relevanten Gesprächspartner, die Erstellung eines strukturierten Fragenkatalogs und die Definition klarer Prüfziele. Befragungen können sowohl in mündlicher als auch in schriftlicher Form durchgeführt werden.

### **6.5.1 Mündliche Befragungen**

Für die Erhebung von aussagekräftigen Ergebnissen ist eine sorgfältige Vorbereitung unerlässlich, die insbesondere die Ermittlung der relevanten Gesprächspartner, die Erstellung eines strukturierten Fragenkatalogs sowie die Festlegung klarer Prüfziele umfasst. Die mündliche Befragung sollte verschiedene Themenbereiche abdecken, wie z. B. Kenntnis der Sicherheitsrichtlinien, Risikobewusstsein und Umgang mit Sicherheitsvorfällen. Eine sorgfältige Dokumentation der Antworten und Beobachtungen ist unerlässlich und bildet die Grundlage für die spätere Analyse. Die Verifizierung der gewonnenen Informationen erfolgt durch den Abgleich mit den bestehenden Richtlinien und durch die Gegenüberstellung der Aussagen verschiedener Befragter.

Die mündliche Befragung ermöglicht es dem Gutachter, über eine reine Dokumentenprüfung hinauszugehen und ein tieferes Verständnis für die tatsächliche Umsetzung (Soll-Ist-Vergleich) sowie das Bewusstsein für die tatsächliche Informationssicherheit in der geprüften Organisation zu erlangen. Die mündliche Befragung stellt daher ein wertvolles Instrument zur Beurteilung der Wirksamkeit von Sicherheitsmaßnahmen und des Reifegrades der Sicherheitskultur dar.

### **6.5.2 Schriftliche Befragungen**

Die schriftliche Befragung stellt eine wesentliche Prüfmethode dar, da sie eine strukturierte Erfassung von Informationen über Sicherheitspraktiken und -prozesse ermöglicht. Idealerweise sollte eine Kombination aus geschlossenen Fragen für quantifizierbare Daten und offenen Fragen für detailliertere Informationen verwendet werden. Der Fragebogen sollte präzise formuliert sein, um Missverständnisse zu vermeiden, und eine logische Struktur aufweisen, die von allgemeinen zu spezifischen Themen führt. Die Formulierung neutraler Fragen ist dabei von besonderer Relevanz, um Verzerrungen zu minimieren. In der Auswertungsphase sind die gesammelten Daten systematisch zu analysieren, wobei sowohl quantitative als auch qualitative Methoden zum Einsatz kommen können. Bei umfangreichen Befragungen können statistische Auswertungen helfen, Trends und Muster zu erkennen, während die Inhaltsanalyse offener Antworten tiefere Einblicke in spezifische Problembereiche liefert. Die Ergebnisse sind mit den bestehenden Richtlinien, Best Practices und früheren Auditergebnissen zu vergleichen, um Abweichungen und Verbesserungspotenziale aufzudecken.

Die schriftliche Befragung zeichnet sich durch ihre Fähigkeit aus, eine breite Datenbasis zu schaffen. Sie eignet sich besonders gut, um das allgemeine Sicherheitsbewusstsein, die Kenntnis von Richtlinien und die Wahrnehmung von Sicherheitsrisiken innerhalb der Organisation zu erfassen. Allerdings empfiehlt es sich, diese Methode mit anderen Prüfungsmethoden, wie etwa Interviews oder Vor-Ort-Prüfungen, zu kombinieren, um ein umfassendes Bild der Informationssicherheitslage zu erhalten.

## **6.6 Inaugenscheinnahme und Beobachtung (IB)**

Bei Vor-Ort-Prüfungen finden zwei wesentliche Prüfmethoden Anwendung: die Inaugenscheinnahme und die Beobachtung. Beide Methoden dienen der Validierung der Eigenschaften des Prüfgegenstandes, unterscheiden sich jedoch in ihrem Fokus und ihrer Durchführung.

Sowohl die Inaugenscheinnahme als auch die Beobachtung beinhalten eine visuelle Begutachtung von Sachverhalten, Vorgängen und Ereignissen und stellen gleichzeitig eine kritische und genaue Überprüfung der umgesetzten Konzepte und Richtlinien dar. Das Ziel besteht in der Validierung der korrekten und vollständigen Anwendung der

definierten Anforderungen an technische Systeme, Objekte, Räumlichkeiten und Prozesse.

### **6.6.1 Inaugenscheinnahme**

Die Inaugenscheinnahme dient der gezielten Überprüfung spezifischer Kriterien, z. B. der Zutrittskontrollen zu einem Serverraum. Hauptmerkmal der Inaugenscheinnahme ist ein systematisches und strukturiertes Vorgehen, welches in seiner Art wiederholbar und objektiv ist. Der Fokus liegt dabei in der Regel auf bestimmte Aspekte oder Eigenschaften des Prüfgegenstandes.

### **6.6.2 Beobachtung**

Die Beobachtung dient der Gewinnung eines Gesamteindrucks, z. B. des allgemeinen Verhaltens von Mitarbeitern im Umgang mit sensiblen Daten. Hauptmerkmal der Beobachtung ist ein weniger strukturiertes als vielmehr exploratives Vorgehen. Insbesondere ermöglicht die Beobachtung eine flexible Identifikation möglicher Prüfungsschwerpunkte.

## **6.7 Prüfung physischer Schutzmaßnahmen (INF)**

Im Rahmen der Begutachtung von Produkten im Gesundheitswesen ist neben der digitalen Sicherheit auch der physische Schutz von signifikanter Relevanz. Unter physische Schutzmaßnahmen werden alle Vorkehrungen subsumiert, die das Produkt vor unbefugten Zutritts-, Zugangs-, Zugriffs- oder Manipulationsversuchen schützen. Hierzu zählen beispielsweise:

- Spezielle Zutrittskontrollsysteme
- Automatische Erkennungssysteme für Eindringversuche
- Sensoren, die das unbefugte Öffnen des Gehäuses melden

Bei der Prüfung physischer Schutzmaßnahmen soll der Gutachter validieren, dass die getroffenen physischen Schutzmaßnahmen nicht nur in der Theorie, sondern insbesondere auch in der Praxis wirksam sind. Dies trägt wesentlich zur Gesamtsicherheit des Produkts bei und hilft, potenzielle Schwachstellen frühzeitig zu erkennen und zu beheben. Eine reine Prüfung der Maßnahme auf Dokumentenebene ist daher nicht ausreichend. Prüfungen, die zur Beschädigung oder gar Zerstörung des Prüfgegenstandes führen, sind zu unterlassen. In solchen Fällen ist aber zumindest eine Sichtprüfung durchzuführen.

## **6.8 Technische Prüfung ohne eigenen Systemzugriff (TP)**

Die Prüfmethode „Technische Prüfung ohne eigenen Systemzugriff“ erfordert eine sorgfältige Planung, bei der ein detaillierter Prüfplan erstellt und mit dem Auftraggeber abgestimmt wird. Die technische Prüfung wird vom Gutachter durchgeführt, ohne dass dieser selbst administrativen Zugriff auf das System hat. Die konkrete Durchführung der technischen Schritte erfolgt durch die entsprechenden Verantwortlichen des Auftraggebers, wobei der Gutachter die Durchführung begleitet und beobachtet, um die Authentizität der Ergebnisse nachvollziehen zu können. Der Gutachter muss daher in der Lage sein, komplexe technische Zusammenhänge schnell zu erfassen und mögliche

Schwachstellen zu erkennen, ohne selbst in die Systeme einzugreifen. Die aus den Beobachtungen resultierenden Schlussfolgerungen sind fundiert und nachvollziehbar im Gutachten zu formulieren, wobei die möglichen Restriktionen des geprüften Unternehmens zu berücksichtigen sind.

### 6.9 Technische Prüfung mit Systemzugriff (TP+)

Bei der Prüfmethode „Technische Prüfung mit Systemzugriff“ ist eine sorgfältige Planung und Abstimmung mit dem Auftraggeber unerlässlich, um den Umfang und die Grenzen der Prüfung festzulegen. Der Gutachter erhält vollen administrativen Zugriff auf die zu prüfenden Systeme, was ein hohes Maß an Verantwortung und ein tiefes Verständnis der möglichen Auswirkungen seines Handelns erfordert.

Im Unterschied zu Penetrationstests wird bei der Prüfmethode „Technische Prüfung mit Systemzugriff“ die Annahme eines Angreifers mit Insiderwissen und vollen Zugriffsrechten als Szenario festgelegt. Das Ziel ist nicht das Eindringen von außen, sondern die Identifizierung von Schwachstellen, die ein privilegierter Nutzer ausnutzen könnte. Dazu gehören beispielsweise Aktivitäten wie das Extrahieren sensibler Daten, das Umgehen von Sicherheitsmechanismen oder das Manipulieren von Systemkonfigurationen. Eine besondere Aufmerksamkeit gilt der Überprüfung von Zugriffskontrollen, Verschlüsselungsmechanismen, Protokollierungssystemen und der Trennung von Privilegien.

Der Gutachter muss stets darauf achten, keine unbeabsichtigten Schäden oder Betriebsunterbrechungen zu verursachen und alle Aktivitäten sorgfältig zu dokumentieren. Die Ergebnisse der Prüfung, einschließlich identifizierter Schwachstellen und potenzieller Risiken, sind im Gutachten detailliert und nachvollziehbar festzuhalten. Dabei ist es wichtig, nicht nur die technischen Details zu beschreiben, sondern auch die möglichen Auswirkungen auf die Geschäftsprozesse und die Vertraulichkeit der Daten zu erläutern. Abschließend sollte der Gutachter konkrete Empfehlungen zur Behebung der gefundenen Schwachstellen geben und mögliche Maßnahmen zur Verbesserung der internen Sicherheitskontrollen vorschlagen.

### 6.10 Penetrationstest (PEN)

Im Rahmen der Durchführung von Penetrationstests wird der Fokus auf die Identifikation und insbesondere die Validierung von Schwachstellen gelegt, die potenziell von einem Angreifer ausgenutzt werden könnten. Penetrationstests sollen sowohl zur Prüfung einzelner Anforderungen als auch zur Bewertung der Gesamtsicherheit des geprüften Systems durchgeführt werden.

Der Auftraggeber ist im Vorfeld über den Umfang der Tests, insbesondere die betroffenen Teilsysteme und die zeitliche Planung, zu informieren, da solche Tests potenziell zu einem Ausfall von Systemen und Komponenten führen können. Die Verantwortung für die Bereitstellung eines funktionsfähigen und geeigneten Testsystems liegt grundsätzlich beim Auftraggeber. Das System soll möglichst produktions- und betriebsnah sein, muss jedoch nicht zwingend dem Produktivsystem entsprechen, wenn dadurch Einschränkungen der Testbarkeit zu erwarten sind und/oder die Abweichungen keinen wesentlichen Einfluss auf die Bewertung der geprüften Anforderungen oder der Gesamtsicherheit haben. Die Auswahl der Methoden und Werkzeuge sowie die konkrete Vorgehensweise obliegen der Verantwortung der Gutachter.

Für die Bewertung der Gesamtsicherheit des Prüfgegenstandes müssen Umfang und Tiefe des Penetrationstests angemessen gewählt werden, um eine belastbare Sicherheitsaussage zu erhalten. Ein ausreichender Prüfumfang umfasst insbesondere:

- die Prüfung aller Außenschnittstellen des Systems (inklusive Schnittstellen zur TI und weiteren Hintergrundsystemen),
- die Prüfung von wichtigen Teilen der Geschäftslogik,
- falls vorhanden: die Prüfung der vertrauenswürdigen Ausführungsumgebung (VAU) und des Verbindungsaufbaus mit der VAU

Um eine ausreichende Prüftiefe zu erreichen, muss die Prüfung dynamisch erfolgen. Insbesondere bei mobilen Anwendungen sind rein statische Analysen allein nicht geeignet, eine ausreichende Prüftiefe zu gewährleisten. Gleiches gilt für eine alleinige Durchführung von Schwachstellen-Scans. Ist eine ausreichende Prüftiefe mit den verfügbaren Standardwerkzeugen nicht zu erreichen, kann auch die Entwicklung produktspezifischer Testwerkzeuge erforderlich sein. Bereits vorhandene Entwicklungen von Testwerkzeugen des Auftraggebers können verwendet werden, wenn der Gutachter sie für geeignet hält. Die Prüftiefe ist auf der Grundlage einer Risikoanalyse festzulegen. Die Risikoanalyse sollte insbesondere realistische Angriffsszenarien, die im System verarbeiteten Datentypen, die Zugänglichkeit der zu prüfenden Systemteile sowie das Vorhandensein ergänzender Sicherheitsmaßnahmen berücksichtigen.

Obwohl ein Penetrationstest individuell auf das zu prüfende Objekt und die zu prüfenden Anforderungen auszurichten ist, ist der Gutachter grundsätzlich einem standardisierten Vorgehen verpflichtet, wie es beispielsweise im Leitfaden für Penetrationstests des BSI [BSI\_LF\_PT] beschrieben ist. Ferner sind in der sicherheitstechnischen Bewertung geläufige Schwachstellentypen (bspw. gemäß QWASP Best Practices) sowie weitere typische produktspezifische Schwachstellen zu berücksichtigen.

Die Dokumentation muss nachvollziehbar danach ausgerichtet werden. Als Ausgangspunkt kann ein vorgelagerter, nicht-invasiver Schwachstellenscan dienen. Bei Software-Eigenentwicklungen sind jedoch individuelle, auf das Produkt zugeschnittene Tests notwendig, um potentielle Schwachstellen zu identifizieren. Das im Rahmen des Penetrationstests gewählte risikobasierte Vorgehen hinsichtlich der durchgeführten Prüfschritte und der verwendeten Werkzeuge sowie die Beschreibung der Ergebnisse sind im Gutachten nachvollziehbar zu dokumentieren.

### 6.11 Verwendung bestehender Nachweise (ZER)

Bei der Erstellung eines Gutachtens für einen komplexen Prüfgegenstand, das sich aus mehreren Teilbereichen zusammensetzt, können die Gutachter auf bereits vorliegende Prüfergebnisse für einzelne Teilbereiche zurückgreifen. Dies wird als „Verwendung bestehender Nachweise“ bezeichnet. Diese Vorgehensweise ermöglicht eine effiziente Nutzung vorhandener Informationen, ohne die Verantwortung und Unabhängigkeit des Gutachters zu beeinträchtigen. Sie trägt dazu bei, Doppelarbeit zu vermeiden und gleichzeitig die Qualität und Zuverlässigkeit des Gesamtgutachtens sicherzustellen. Die folgenden Informationen können beispielhaft als Nachweise verwendet werden:

- Zertifizierungen (z. B. nach ISO 27001)
- Prüfberichte aus früheren Untersuchungen
- Gutachten anderer Experten, die sicherheitsrelevante Aspekte behandeln

Es ist jedoch zu beachten, dass der Gutachter auch bei der Verwendung bestehender Nachweise die volle Verantwortung für das Gesamtgutachten behält. Der Gutachter muss sicherstellen, dass:

- eine eigenständige Planung und Durchführung der Prüfung erfolgt ist,
- eine eigene Bewertung vorgenommen wird, ob die Sicherheits- und Datenschutzanforderungen der Telematikinfrastruktur erfüllt sind und
- ein unabhängiges Prüfungsurteil (Votum) abgegeben wird.

Darüber hinaus sind seitens des Gutachters bei der Verwendung bestehender Nachweise folgende Voraussetzungen sorgfältig abzuwägen:

- Welchen Einfluss haben diese Nachweise auf das Gesamturteil?
- Wie bedeutsam ist der vom Gutachter selbst geprüfte Teil im Verhältnis zum Gesamtobjekt?
- Wie verlässlich sind die bestehenden Nachweise?
- Wie aktuell sind die Nachweise
- Welche Anforderungen werden durch die bestehenden Nachweise tatsächlich abgedeckt?

Um die Qualität der bestehenden Nachweise beurteilen zu können, muss sich der Gutachter kritisch mit deren Prüfergebnissen auseinandersetzen. Des Weiteren sind im Gutachten folgende Punkte transparent darzustellen:

- Welche bestehenden Nachweise wurden für die Prüfung herangezogen?
- Welche Maßnahmen wurden ergriffen, um sich von der Qualität der Nachweise zu überzeugen?
- Für welche Teilbereiche des Prüfgegenstandes sind die verwendeten bestehenden Nachweise anwendbar und relevant?

Bei einer periodischen Neu-Begutachtung nach drei Jahren (Stichwort: Folgegutachten) sind vorhergehende Vollgutachten nicht als bestehender Nachweis anzusehen. Es ist daher eine vollständige Prüfung durchzuführen. Aufbauend auf das vorherige Gutachten können andere Stichproben gewählt werden, jedoch reduziert sich der Prüfungsumfang reduziert nicht durch die Erkenntnisse und Bewertungen aus älteren Sicherheits- oder Produktgutachten.



---

## **7 Prüfplan**

---

Die Prüfhandlungen bei Sicherheits- oder Produktgutachten dienen im Wesentlichen dazu, durch einen Soll-Ist-Vergleich festzustellen, ob das Sicherheitsniveau des Prüfgegenstandes ausreichend ist. Dabei ist insbesondere zu prüfen, ob und inwieweit die Anforderungen des Steckbriefs erfüllt sind oder nicht. Um zu verlässlichen, nachvollziehbaren und vergleichbaren Schlussfolgerungen und Ergebnissen zu gelangen, ist daher eine strukturierte Dokumentation der Sachverhalte und Prüfhandlungen erforderlich.

Der Prüfplan als Leitfaden für die Prüfhandlungen beschreibt den gesamten Ablauf der sicherheitstechnischen Eignungsprüfung. Der Prüfplan muss mindestens folgende Inhalte umfassen:

- Ableitung von Aktivitäten, die sich aus dem Anforderungskatalog und den Prüfmethoden ergeben,
- Dokumentation weiterer als notwendig erachteter Prüfmethoden für einzelne Anforderungen,
- Auflistung der Ansprechpartner des Auftraggebers mit ihren spezifischen Verantwortungsbereichen,
- Zuordnung der Ressourcen sowohl des Gutachters als auch des Auftraggebers zu den einzelnen Aktivitäten,
- Termine für die einzelnen Aktivitäten - bei kritischen Terminen auch Ausweichtermine,
- Termine für die Aggregation der Ergebnisse zur Bewertung des Prüfgegenstandes auf Anforderungsebene,
- Termine für Abstimmungsgespräche mit dem Auftraggeber über den Projektfortschritt,
- Termine für die Übergabe von Statusberichten an den Auftraggeber,
- Termin für die Übergabe des Gutachtens an den Auftraggeber.

### **7.1 Festlegung anzuwendender Prüfmethoden**

Die Prüfmethoden sind vom Gutachter für die jeweiligen Anforderungen festzulegen, wobei die Vorgaben gemäß Kapitel 6 zu beachten sind.



---

## 8 Gutachten

---

Der Erstgutachter ist für die Erstellung und den Inhalt des Gutachtens verantwortlich. Das Gutachten muss eine umfassende, korrekte und eindeutige Darstellung sowie eine nachvollziehbare Bewertung des Prüfgegenstandes hinsichtlich seiner sicherheitstechnischen Eignung enthalten. Führt der Auftraggeber aufgrund des Gutachtens Maßnahmen zur Erfüllung bestimmter Anforderungen durch, so ist der Abschluss und die Wirksamkeit der Korrekturmaßnahmen zu überprüfen, bevor das Gutachten entsprechend geändert wird.

Der Erstgutachter erstellt für jedes Prüfverfahren ein Gutachten, welches alle Prüfergebnisse enthält. Die Mindestinhalte sowie die damit verbundene Kapitelstruktur für das jeweilige Gutachten sind den Vorgaben gemäß dem Anhang A (A5 - Muster Gutachten Kapitelstruktur) zu entnehmen und entsprechend zu berücksichtigen.

Zusätzlich zum Gutachten ist obligatorisch eine tabellarische Auflistung aller Steckbrief-relevanten Anforderung im xlsx-/ods-Format mitzuliefern. Die Inhalte der Tabelle stellen dabei ein Duplikat der Sachstände aus dem Gutachten dar. Der Aufbau der Tabelle sollte sich an dem nachfolgenden Beispiel orientieren:

Afo-ID	Afo-Titel	Prüfmethoden	Sachverhalt	Sicherheitsmangel	Umsetzungsstatus
<..>	<..>	<..>	<..>	<..>	<..>

### 8.1 Gutachten-Beurteilung & Nachforderungen

Die Prüfbegleitung der Zulassungsstelle prüft das eingereichte Gutachten unter Berücksichtigung des jeweiligen Zulassungsgegenstandes auf die nachfolgenden Kriterien:

#### **Vollständig**

- Es wird bewertet, ob alle in der [gemRL\_PruefSichEig\_DS] festgelegten Anforderungen und Kriterien durch das vorgelegte Gutachten erfüllt werden. Darüber hinaus wird bewertet, ob alle Anforderungen des Steckbriefs geprüft wurden und ob die Vorgehensweise und die entsprechenden Prüfergebnisse im Gutachten dokumentiert sind.

#### **Sorgfältig**

- Es wird bewertet, ob das Gutachten auf eine gründlich durchgeführte Prüfung schließen lässt, in welcher der Stand der Technik und relevanten Best Practices berücksichtigt wurden.

#### **Objektiv**

- Es wird bewertet, ob das Gutachten eine objektive, unparteiische, unvoreingenommene, unabhängige und interessenfreie Prüfung erkennen lässt.

#### **Nachvollziehbar**

- Es wird bewertet, ob ein sachverständiger Dritter auf der Grundlage des Gutachtens zu einer vergleichbaren Schlussfolgerung gelangen würde.

Die Prüfbegleitung ist befugt, bei Bedarf Nachforderungen an den Erstgutachter oder den geprüften Lieferanten/Betreiber/Hersteller zu stellen. Diese können potenziell zu einer inhaltlichen Nachbesserung im Gutachten führen. Im Falle von Nachforderungen seitens der Prüfbegleitung (etwa bei unvollständigen, fehlenden oder unklaren Angaben im Gutachten) sind diese vom Erstgutachter innerhalb der in der Stellungnahme genannten Frist zu erledigen. Ist absehbar, dass die genannte Frist nicht eingehalten werden kann, so hat der Erstgutachter unverzüglich mit der Prüfbegleitung Kontakt aufzunehmen und eine begründete Fristverlängerung zu beantragen.

Die Prüfbegleitung entscheidet in Zusammenarbeit mit der Zulassungsstelle, ob und in welcher Frist die im Gutachten festgestellten Abweichungen zu beheben sind.

## **8.2 Bestätigung durch die Zulassungsstelle**

Sobald der Prüfbericht der Prüfbegleitung zum eingereichten Gutachten vollständig bei der Zulassungsstelle der gematik vorliegt, prüft diese den Prüfbericht auf die Einhaltung aller formalen Vorgaben des jeweils gültigen Zulassungsschemas. Diese Prüfung erfolgt mit dem Ziel, ein einheitliches Niveau aller Zulassungs- und Bestätigungsverfahren und die Vergleichbarkeit der einzelnen Zulassungsaussagen zu gewährleisten.

---

## **9 Gutachter-Kompetenz**

---

Für die Erstellung von Gutachten im Rahmen der Überprüfung der Sicherheitseignung müssen die Gutachter bestimmte Qualifikationen nachweisen. Diese werden im Folgenden in Abhängigkeit von der Art der Begutachtung definiert. Grundsätzlich ist eine ständige Fort- und Weiterbildung der Gutachter eine der Grundvoraussetzungen für ihre Tätigkeit. Da je nach Prüfgegenstand auch spezielle Fachkenntnisse erforderlich sein können, die nicht bei jedem Gutachter als Basiswissen vorausgesetzt werden können, ist das Hinzuziehen weiterer Fachexperten nicht nur zulässig, sondern ausdrücklich erwünscht (siehe auch 9.3).

### **9.1 Sicherheitsgutachter**

Der Sicherheitsgutachter muss über ein breites und fundiertes Wissen auf den Gebieten des Datenschutzes und der Informationssicherheit sowie über die zur Durchführung von Audits erforderlichen Kenntnisse und Erfahrungen verfügen. Darüber hinaus muss der Sicherheitsgutachter Grundkenntnisse der Telematikinfrastruktur nachweisen können. Die Akkreditierung zum Sicherheitsgutachter setzt sowohl eine bestätigte Basisqualifikation als auch eine Zusatzqualifikation zum Sicherheitsgutachter Telematikinfrastruktur voraus.

#### **9.1.1 Basisqualifikation**

Der Sicherheitsgutachter muss im Rahmen seiner Akkreditierung gegenüber der gematik den aktuell gültigen Nachweis zur fachlichen Basisqualifikation durch Vorlage der entsprechenden Zertifikate / Bestätigungen (Kopien) erbringen. Folgende Nachweise werden für eine Basisqualifikation akzeptiert:

##### **ISO-27001-Auditor auf Basis von IT-Grundschutz**

Zertifikat zur Bestätigung als ISO-27001-Auditor durch das BSI (ISO-27001 auf der Basis von IT-Grundschutz) oder alternativ Angabe der Zertifikat-Nummer gemäß der offiziellen Liste der zertifizierten Auditteamleiter des BSI.

##### **ISO/IEC-27001-Lead-Auditor bei einer akkreditierten Zertifizierungsstelle**

Bestätigung einer aktuell gültigen Lead Auditor-Berufung für den Security Standard ISO/IEC-27001 bei einer akkreditierten Zertifizierungsstelle. Diese Zertifizierungsstelle muss bei einer international anerkannten Akkreditierungsstelle geführt werden. Die Liste der gültigen Akkreditierungsstellen ist der Übersicht des [IAF] zu entnehmen.

##### **Kombination aus CISA und CISSP**

Zertifikat einer gültigen Qualifikation als Certified Information Systems Auditor (CISA) und Certified Information Systems Security Professional (CISSP) nach ISO/IEC 17024.

##### **Kombination aus CISA und T.I.S.P.**

Zertifikat einer gültigen Qualifikation als Certified Information Systems Auditor (CISA) und TeleTrust Information Security Professional (T.I.S.P.).

##### **Common Criteria Evaluator**

Nachweis zur BSI-seitig erfolgten Kompetenzfeststellung als Common Criteria Evaluator sowie eine Bestätigung der Common Criteria Prüfstelle zur gültigen Berufung als Common Criteria Evaluator.

### **9.1.2 Zusatzqualifikation „Sicherheitsgutachter TI“**

Neben der Basisqualifikation gemäß Kapitel 9.1.1 ist für die initiale Akkreditierung zum „Sicherheitsgutachter TI“ ein Nachweis der fachlichen Zusatzqualifikation „Sicherheitsgutachter TI“ zwingend erforderlich.

Im Rahmen einer kompakten Schulung werden die spezifischen Themen der Telematikinfrastruktur vermittelt. Neben den damit begründeten Anforderungen an die Informationssicherheits- und Datenschutzaspekten sowie den technologischen Grundlagen einschließlich der Sicherheitsarchitektur der Telematikinfrastruktur werden in der Schulung auch die Aufgaben- und Verantwortungsbereiche der Sicherheitsgutachter erläutert. Die Schulung schließt mit einer fachlichen Prüfung ab. Erst mit Bestehen dieser Prüfung (Zertifikat) ist die Zusatzqualifikation „Sicherheitsgutachter TI“ erfolgreich abgeschlossen. Die Gültigkeit der Akkreditierung ist auf jeweils drei Jahre befristet. Die Bedingungen für die Aufrechterhaltung der Akkreditierung sind im nachfolgenden Kapitel 9.1.3 aufgeführt.

### **9.1.3 Aufrechterhaltung der Sicherheitsgutachter-Akkreditierung**

Die technischen und organisatorischen Anforderungen zur Gewährleistung der Informationssicherheit und des Datenschutzes nach dem Stand der Technik unterliegen ebenso wie die Rahmenbedingungen für Anbieter/Betreiber/Hersteller innerhalb der Telematikinfrastruktur einer ständigen Weiterentwicklung. Daher ist eine kontinuierliche Fortbildung und Erweiterung der Auditerfahrung in den Bereichen Informationssicherheit und Datenschutz eine wesentliche Voraussetzung für eine kompetente und qualifizierte Beurteilung der Prüfgegenstände durch die Gutachter.

Die Akkreditierung erstreckt sich über einen Zeitraum von drei Jahren und kann anschließend jeweils um eine weitere Laufzeit von drei Jahren verlängert werden. Die aktive Mitwirkung an Gutachtenverfahren in der Rolle des Erst- und/oder Zweitgutachters ist obligatorisch. Innerhalb der Laufzeit einer aktiven Akkreditierung muss der Gutachter mindestens vier Erfahrungspunkte (4 EP) erreichen, um eine aktive Mitwirkung an Gutachtenverfahren nachzuweisen. Die Vergabe der Erfahrungspunkte (EP) gliedert sich wie folgt:

- Rolle Erstgutachter je Gutachtenverfahren: zwei Erfahrungspunkte (2 EP)
- Rolle Zweitgutachter je Gutachtenverfahren: ein Erfahrungspunkt (1 EP)

Die Erreichung der Mindest-EP wäre z. B. mit zwei Gutachtenverfahren als Erstgutachter oder mit vier Gutachtenverfahren als Zweitgutachter erreicht. Werden die Mindest-EP innerhalb der Akkreditierungsgültigkeit nicht erreicht, ist seitens des Gutachters eine erneute Teilnahme an der Schulung „Zusatzqualifikation Sicherheitsgutachter TI“ erforderlich.

Neben einer aktiven Mitwirkung an Gutachtenverfahren ist seitens des Gutachters zur Aufrechterhaltung der Akkreditierung eine weiterhin bestätigte Gültigkeit der Basisqualifikation erforderlich. Aktualisierte Nachweise einer gültigen Basisqualifikation (z. B. Verlängerung der Berufung durch eine Zertifizierungsstelle) sind durch den Gutachter proaktiv bei der gematik einzureichen. Die Verlängerung einer Akkreditierung wird dem Gutachter seitens der gematik durch eine signierte Urkunde bestätigt.

## **9.2 Produktgutachter**

### **9.2.1 Basisqualifikation**

Ein Produktgutachter benötigt je nach konkreter Ausprägung des Prüfgegenstandes Spezialwissen auf den nachfolgend exemplarisch aufgeführten Fachgebieten:

- Implementierung/Prüfung von Virtualisierungs- und Containerlösungen
- Durchführung von Penetrationstests und Sicherheitsaudits,
- Analyse von Quellcode in Hinblick auf Sicherheitsaspekte,
- fundierte Kenntnisse in Softwareentwicklung und Programmiersprachen,
- Verständnis von Netzwerktechnologien und -protokollen und
- Kenntnisse in Kryptographie und Sicherheitsalgorithmen.

Als Nachweis für die Qualifikation auf dem jeweiligen Gebiet wird eine Berufserfahrung von je mindestens zwei Jahren oder die Vorlage entsprechender Personen-Zertifizierungen vorausgesetzt. Folgende unabhängige Qualifikationsbestätigungen bieten sich exemplarisch als Nachweise an (ohne Anspruch auf Vollständigkeit):

#### **Domäne Quellcode-Analyse / SSDLC**

- ISC2 Certified Secure Software Lifecycle Professional (CSSLP)
- Offensive Security Certified Professional (OSCP)
- BSI Common Criteria Evaluator
- ISTQB Certified Tester Advanced Level Test Analyst (CTAL-TA)
- iSAQB Certified Professional for Software Architecture-Advanced Level (CPSA-A)
- Quality Assurance Management Professional (QAMP)

#### **Domäne Penetrationstest**

- Certified Ethical Hacker (CEH)
- Offensive Security Certified Professional (OSCP)
- BSI IS-Penetrationstester
- GIAC Penetration Tester Certification (GPEN)
- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
- GIAC Web Application Penetration Tester (GWAPT)
- CompTIA PenTest+

Die Nachweise sind im Produktgutachten geeignet festzuhalten und per Unterschrift vom Produktgutachter und vom Sicherheitsgutachter zu bestätigen. Tritt der Sicherheitsgutachter selbst als Produktgutachter auf, sind die Nachweise ebenso erforderlich und per Unterschrift von Erst- und Zweitgutachter zu bestätigen.

### **9.2.2 Zusatzqualifikation „Sicherheitsgutachter TI“**

Die Zusatzqualifikation „Sicherheitsgutachter TI“ gemäß Kapitel 9.1.2 ist für die Rolle des Produktgutachters nicht notwendig.

### **9.2.3 Begutachtung von Frontends des Versicherten**

Für die Begutachtung von Frontends des Versicherten (FdV, Apps für Versicherte) müssen seitens des Produktgutachters zudem Kenntnisse im Bereich App-Testing nachgewiesen werden, wobei auch eine Berufserfahrung von mindestens zwei Jahren vorausgesetzt wird. Zudem müssen Produktgutachter, die ein FdV begutachten, durch das BSI

- als IS-Penetrationstester,
- als TR-Prüfern BSI TR-03161
- oder als CC-Evaluator

anerkannt sein. Die Anerkennungsnachweise des BSI sowie die Benennungsnachweise durch die jeweilige Prüfstelle sind dem Gutachten beizufügen. Ferner sind die Nachweise zur Erfahrung im Bereich App-Testing im Produktgutachten geeignet festzuhalten und per Unterschrift vom Produktgutachter und vom Sicherheitsgutachter zu bestätigen.

## **9.3 Fachexperten**

Für die Prüfung von Anforderungen aus speziellen Fachgebieten, die nicht notwendigerweise im Kompetenzbereich der Gutachter liegen, ist es zulässig und ausdrücklich erwünscht, entsprechende Fachexperten hinzuzuziehen. Bei Sicherheitsgutachten können dies z. B. Datenschutzexperten sein (da dieses Thema nicht zwingend durch die Grundqualifikation abgedeckt ist). Bei Produktgutachten kann es bspw. sinnvoll sein, weitere Experten für die Durchführung von Penetrationstests und Quellcode-Analysen hinzuzuziehen.

Im Gutachten muss die Qualifikation der Fachexperten nachgewiesen werden. Es ist auch anzugeben, welche Prüfungen und Bewertungen von diesen Fachexperten durchgeführt wurden.

## **9.4 Vier-Augen-Prinzip**

Zur Förderung der Unabhängigkeit und Objektivität müssen stets (mindestens) zwei Gutachter an der Erstellung eines Gutachtens beteiligt sein („Vier-Augen-Prinzip“). Es ist jedoch nicht zwingend notwendig, jeden Prüfschritt zu zweit durchzuführen, solange im Nachgang eine ausreichende Kenntnis zum Prüfverfahren vorliegt, um eine fachliche und inhaltliche Qualitätssicherung im Vier-Augen-Prinzip durchführen zu können.

Der Sicherheitsgutachter (gemäß Kapitel 9.1) tritt sowohl bei einem Sicherheitsgutachten als auch bei einem Produktgutachten als Erstgutachter auf. Der Zweitgutachter wird vom Sicherheitsgutachter hinzugezogen.

### **9.4.1 Allgemeines**

Die Zugehörigkeit des Zweitgutachters zu einer anderen Firma ist nicht erforderlich.

Weitere Fachexperten können gemäß Abschnitt 9.3 hinzugezogen werden, tragen aber nicht zum hier geforderten Vier-Augen-Prinzip bei, sofern sie nicht über die in Kapitel 9.1.1 genannten Basisqualifikationen verfügen.

Lediglich bei geringfügigen Nachbegutachtungen aufgrund von Änderungen am Prüfgegenstand (Delta-Gutachten) kann vom Vier-Augen-Prinzip abgewichen werden, wobei dies im Gutachten explizit und nachvollziehbar zu begründen ist.

### **9.4.2 Sicherheitsgutachten**

Im Falle eines Sicherheitsgutachtens muss der Zweitgutachter mindestens über die Basisqualifikation entsprechend der Regelungen in Kapitel 9.1.1 verfügen, deren Nachweis in Kopie dem Gutachten beizufügen ist.

Bei einem Sicherheitsgutachten ist der überwiegende Teil der Prüfungen von dem Erstgutachter durchzuführen.

### **9.4.3 Produktgutachten**

Im Falle eines Produktgutachtens muss der Zweitgutachter ein Produktgutachter gemäß den Regelungen in Kapitel 9.2 sein. Der Sicherheitsgutachter (als hauptverantwortliche Instanz für die Vorbereitung, Durchführung und Dokumentation der Prüftätigkeiten) muss als Erstgutachter anhand der Eigenschaften des Prüfgegenstandes beurteilen, welche Qualifikation der Produktgutachter im konkreten Fall aufweisen muss. Die Qualifikation des Zweitgutachters ist im Produktgutachten durch Berufungsurkunden, Zeugnisse oder die Darstellung der einschlägigen Berufserfahrung in kurzer, tabellarischer Form nachzuweisen und von beiden Gutachtern durch Unterschrift zu bestätigen.

Für den Fall, dass der Sicherheitsgutachter bei der Erstellung eines Produktgutachtens auch die Rolle des Produktgutachters übernimmt, ist von ihm ein Zweitgutachter mit einer Basisqualifikation gemäß den Regelungen in Kapitel 9.2.1 hinzuzuziehen.

Der Hauptteil der Prüfungen muss bei einem Produktgutachten immer vom Produktgutachter durchgeführt werden, auch wenn dieser nicht als Erstgutachter tätig wird.

## **9.5 Unabhängigkeit und Objektivität**

Die Gutachter haben im Rahmen der Zulassung gegenüber der gematik durch eine schriftliche Selbsterklärung zu bestätigen, dass sie unabhängig und objektiv prüfen und in den letzten 24 Monaten vor der Prüfung eines Prüfgegenstandes nicht beratend oder ausführend an der Konzeption, Erstellung oder Konfiguration des Prüfgegenstandes beteiligt waren. Diese Erklärung ist im Gutachten zu dokumentieren.

---

## **10 Anhang A - Verzeichnisse**

---

### **10.1 A1 - Abkürzungen**

<b>Kürzel</b>	<b>Erläuterung</b>
BSI	Bundesamt für Sicherheit in der Informationstechnik
CEH	Certified Ethical Hacker
CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional
CPSA-A	Certified Professional for Software Architecture-Advanced Level
CSSLP	Certified Secure Software Lifecycle Professional
CTAL-TA	Certified Tester Advanced Level Test Analyst
GPEN	GIAC Penetration Tester Certification
GWAPT	GIAC Web Application Penetration Tester
GXPEN	GIAC Exploit Researcher and Advanced Penetration Tester
OSCP	Offensive Security Certified Professional
QAMP	Quality Assurance Management Professional
T.I.S.P.	TeleTrust Information Security Professional
TR-03161	technische Richtlinie des BSI zu Anforderungen an Anwendungen im Gesundheitswesen

### **10.2 A2 - Referenzierte Dokumente**

<b>[Quelle]</b>	<b>Herausgeber (Erscheinungsdatum): Titel</b>
[BSIInfRev]	BSI: Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz.
[BSI_LF_PT]	BSI: Ein Praxis-Leitfaden für IS-Penetrationstests.



[gematik Fachportal]	gematik: Fachportal ( <a href="https://fachportal.gematik.de/informationen-fuer/sicherheitsgutachter">https://fachportal.gematik.de/informationen-fuer/sicherheitsgutachter</a> )
[gemRL_PruefSichEig_DS]	gematik: Richtlinie zur Prüfung der Sicherheitseignung
[gemSpecPages]	gematik: Online-Reader gemSpecPages ( <a href="https://gemspec.gematik.de/">https://gemspec.gematik.de/</a> )
[IAF]	International Accreditation Forum: Listing of Accreditation Bodies ( <a href="https://iaf.nu/en/accreditation-bodies/">https://iaf.nu/en/accreditation-bodies/</a> )
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels, S. Bradner.

### 10.3 A3 - Muster Gutachten Kapitelstruktur

Das Gutachten muss mindestens die folgenden Punkte enthalten und die folgende Struktur aufweisen. Die genannten Inhalte inkl. des Anhangs müssen alle in einem einzigen Dokument zusammengeführt werden.

#### 10.3.1 Deckblatt

- Sicherheits- oder Produktgutachten?
- Voll- oder Deltagutachten?
- Verfahrensnummer des Gutachtens
- Benennung des Prüfgegenstandes
- Benennung des Auftraggebers
- Name der Gutachter
- Dokumenteninformationen (Version, Stand, Klassifizierung, usw.)

#### 10.3.2 Dokumentenhistorie

Die Version des Gutachtens wird durch den Gutachter fortgeschrieben. Jede Änderung muss in der Versionshistorie dokumentiert werden.

Datum	Version	Verfasser	Bemerkungen
<..>	<..>	<..>	<..>

#### **Hinweis:**

*In die Felder für das Datum wird entweder ein konkretes Datum (TT.MM.JJJJ) oder ein Zeitraum (TT.MM.JJJJ – TT.MM.JJJJ) eingetragen. Die Version sollte fortlaufend fortgeschrieben werden, beginnend mit der 0.1 für die initiale Erstellung, 0.2 für die weitere Bearbeitung. Im Feld für die Bemerkungen werden die wichtigsten Änderungen erfasst, z. B. initiale Erstellung, Anpassungen nach Nachbesserungen oder Anpassungen*

*nach Kommentierung durch die gematik. Die Tabelle für die Versionshistorie muss mit jeder Änderung oder Ergänzung fortgeschrieben werden.*

### **10.3.3 Kontaktdaten des Antragstellers**

Kontaktinformationen des Antragstellers (auditierte Institution):

<b>Antragsteller</b>	<..>
<b>Straße / Hausnummer</b>	<..>
<b>PLZ / Ort</b>	<..>
<b>E-Mail</b>	<..>

Ansprechpartner für die Zulassung beim Antragsteller:

<b>Name</b>	<..>
<b>Funktion</b>	<..>
<b>Telefon</b>	<..>
<b>E-Mail</b>	<..>
<b>Optional: Abweichende Anschrift</b>	<..>

**Hinweis:**

*Der Ansprechpartner für die Zulassung wird in allen Prozessschritten in Zusammenhang mit dem Verfahren eingebunden. Die Informationen für die auditierte Institution müssen vollständig erfasst werden. Das Feld für die abweichende Anschrift muss nur ausgefüllt werden, wenn der Ansprechpartner unter einer abweichenden postalisch erreichbar ist.*

### **10.3.4 Kontaktdaten der Gutachter / Fachexperten**

Die Gutachtenleitung erfolgte durch den folgenden Erstgutachter:

<b>Name</b>	<..>
<b>Unternehmen</b>	<..>
<b>Straße / Hausnummer</b>	<..>
<b>PLZ / Ort</b>	<..>
<b>Telefon</b>	<..>
<b>E-Mail</b>	<..>

Folgende Gutachter / Fachexperten haben an der Auditierung mitgewirkt:

<b>Name</b>	<..>
<b>Unternehmen</b>	<..>
<b>Straße / Hausnummer</b>	<..>
<b>PLZ / Ort</b>	<..>
<b>Telefon</b>	<..>
<b>E-Mail</b>	<..>

**Hinweis:**

*Für jedes Zulassungsverfahren ist ein leitender Gutachter (Erstgutachter) zu benennen. Das Gutachterteam ist durch weitere Gutachter und Fachexperten zu ergänzen, um insbesondere das Vier-Augen-Prinzip zu gewährleisten. Die Wahl der Teamzusammensetzung ist unter Berücksichtigung des Prüfgegenstandes und der damit verbundenen erforderlichen Sach- und Fachkenntnisse zu treffen. Alle Felder sind auszufüllen. Im Feld „Telefon“ kann sowohl eine Büro- als auch eine Mobiltelefonnummer eingetragen werden. Hier sollte sichergestellt sein, dass der Erstgutachter während der Gutachten-Beurteilung für Rückfragen der gematik-Prüfbegleitung zu den üblichen Bürozeiten erreichbar ist. Sind mehrere Personen an der Auditierung beteiligt, ist die Tabelle der Gutachter / Fachexperten für jede weitere Person zu kopieren und auszufüllen.*

### **10.3.5 Management Summary**

- Aufgabenstellung
- Zusammenfassung der wesentlichen Feststellungen
- tabellarische Zusammenfassung der Prüfergebnisse je Steckbriefanforderung
- Gesamtvotum

**Hinweis:**

*In dem Gesamtvotum stellt der Erstgutachter in kurzer Form seine Gesamteinschätzung dar, die auf den Ergebnissen der für das Auditverfahren beschriebenen Prüfschritte basiert. Umstände oder Ergebnisse, die eine Umsetzung der Steckbriefanforderungen besonders positiv oder negativ beeinflussen, können an dieser Stelle herausgestellt werden. So bei der Validierung der sicherheitstechnischen Anforderungen etwaige Mängel ermittelt wurden, sind deren potentielle Auswirkungen in dem Gesamtvotum des Erstgutachters entsprechend zu berücksichtigen.*

*Das Gutachten ist nach der Finalisierung durch den Erst- und Zweitgutachter digital zu signieren und der Zulassungsstelle der gematik sowie dem Ansprechpartner des geprüften Auftraggebers zu übermitteln.*

### **10.3.6 Grundlagen der Prüfung**

- Bezeichnung des Prüfobjektes
- Zielsetzung und Umfang der Prüfung

- eindeutige Benennung Produkttyp-, Anbietertyp- bzw. Anwendungssteckbriefversion und Referenz auf den herangezogenen Steckbrief

### **10.3.7 detaillierte Beschreibung der Prüfung**

#### **10.3.7.1 Beschreibung des Prüfgegenstandes**

- grundlegende Tätigkeiten, Abläufe, Prozesse
- Aufbau, angrenzende Systeme
- Verantwortlichkeiten und ggf. Angaben zu Prozessen/Komponenten wofür der Auftraggeber gerade nicht verantwortlich ist

#### **10.3.7.2 Standorte des Prüfgegenstandes**

In der nachfolgenden Tabelle sind die Standorte aufgeführt, die in Summe für den Betrieb des Prüfgegenstandes zum Einsatz kommen und notwendig sind.

<b>Betreiber</b>	<b>Adresse</b>	<b>Standort-Funktion</b>
<..>	<..>	<..>

**Hinweis:**

*Standorte aller vom Gutachten umfassten und für die Erfüllung der Steckbriefanforderungen relevanten Standorte.*

#### **10.3.7.3 Liste der Dienstleister**

In der Liste der Dienstleister werden alle externen Dienstleister erfasst, die Einfluss auf den Prüfgegenstand nehmen können bzw. für dessen Betrieb erforderlich sind.

<b>Dienstleister</b>	<b>Funktion / Aufgabe</b>
<..>	<..>

**Hinweis:**

*Die Liste der externen Dienstleister umfasst alle Dienstleister, die auf ein Zielobjekt aus dem Prüfgegenstand Zugriff haben können. Hierbei sind sowohl die vollständigen Angaben zu den externen Dienstleistern als auch deren Funktionen / Aufgaben gegenüber den Zielobjekten aufzuführen.*

#### **10.3.7.4 Beschreibung des Prüfplans**

In diesem Kapitel wird der zeitliche Ablauf der Auditierung in tabellarischer Form aufgeführt. Der Plan enthält eine Übersicht der erfolgten Aktivitäten, der Zeiträume und der benötigten Audittage (alle Angaben ohne Reisezeiten).

<b>Aktivität</b>	<b>Datum / Zeitraum</b>	<b>Aufwand (in PT)</b>
<..>	<..>	<..>

**Hinweis:**

Die Angaben für die einzelnen Aktivitäten werden in Personentagen (PT) angegeben. Ein Personentag umfasst normalerweise acht Stunden pro Person.

In die Spalte Datum / Zeitraum werden in folgendem Format die Angaben eingetragen: Datum entspricht einer Aktivität, die an einem Tag bzw. Werktag durchgeführt wurde, z. B. das Format: TT.MM.JJJJ. Als Zeitraum wird die Aktivität an mehreren Tagen durchgeführt. Der Zeitraum umfasst dann zwei Daten, ein Start- und ein Enddatum, z. B. TT.MM.JJJJ bis TT.MM.JJJJ. Die Angaben für den Zeitraum müssen nicht mit der Anzahl der Personentage übereinstimmen, da freie Tage in dem Zeitraum liegen können.

In die Spalte Aufwand (in PT) werden die Netto-Arbeitszeiten aller Beteiligten für jede Aktivität als Summe eingetragen.

## 10.3.7.5 Absprachen

Zwischen der gematik und dem Gutachterteam wurden die folgenden Absprachen getroffen:

Absprache zu	Angabe von Datum, Beteiligten, Art, usw.	Nachweis
<..>	<..>	<..>

### Hinweis:

Alle zwischen der gematik und dem Gutachterteam getroffenen Absprachen müssen hier dokumentiert werden. Eine Absprache ist nur gültig, wenn sie schriftlich dokumentiert und seitens der gematik freigegeben / mitgezeichnet wurde. Zur Art der Absprache sollte der zugehörige Nachweis (bspw. E-Mail, Protokollnotiz, etc.) referenziert werden. Für jede Absprache muss eine eigene Zeile ausgefüllt werden. Eine Verwendung der Phrase „wie mit der gematik besprochen“ ohne weitere Angaben auf die konkreten Nachweise ist nicht ausreichend.

Sollte es keine Absprachen zwischen der gematik und dem Gutachterteam geben, kann in den drei Feldern ein „n.a.“ eingetragen werden.

## 10.3.7.6 Beschreibung bei Vor-Ort-Prüfungen

Betreiber	Adresse	Vor-Ort-Prüfung	Bemerkungen
<..>	<..>	<Ja / Nein>	<..>

### Hinweis:

Die für den Prüfgegenstand relevanten Standorte gemäß der Übersicht in Kapitel "Standorte des Prüfgegenstandes" sind in dieser Tabelle aufzuführen. Sollte eine Vor-Ort-Prüfung nicht erfolgt sein, so ist diese Entscheidung in dem Feld "Begründung" nachvollziehbar zu dokumentieren.

### 10.3.8 Dokumentation der Prüfergebnisse

<b>Afo-ID</b>	<..>
<b>Afo-Beschreibung</b>	<..>
<b>Prüfmethoden</b>	<DOK / DA / SCA / BE / IB / INF / TP / TP+ / PEN / ZER>
<b>Sachverhalt</b>	<..>
<b>Nachweise</b>	<..>
<b>Sicherheitsbewertung</b>	<OK / NC-A / NC-B / PI> <Beschreibung der Folgemaßnahmen/Auflagen> + <NC-A- / NC-B- / PI-lfdNr>
<b>Frist</b>	<TT.MM.JJJJ>
<b>Umsetzungsstatus</b>	<Umgesetzt / Teilweise umgesetzt / Nicht umgesetzt / Nicht anwendbar>

**Hinweis:**

Die Felder sind für die Dokumentation der Prüfergebnisse für jede einzelne Steckbriefanforderung wie folgt zu befüllen:

- **Afo-ID:** Kennziffer der geprüften Steckbriefanforderung (z. B.: A\_19147)
- **Afo-Beschreibung:** Anforderungstext (z. B.: Der Hersteller eines Produktes MUSS einen Testplan für Sicherheitstests erstellen und auf Verlangen der gematik zur Verfügung stellen.
- **Prüfmethoden:** Gutachter-seitig angewendete Prüfmethoden (Auswahl siehe Kapitel 6). Eine Mehrfachauswahl ist zulässig.
- **Sachverhalt:** Bewertung der Steckbriefanforderung in Bezug auf den Umsetzungsstand sowie eine nachvollziehbare Erläuterung, wie die Erfüllung der Anforderung konkret gewährleistet wird. Zu jeder geprüften Anforderung ist im Sachverhalt inhaltlich auf alle etwaig enthaltenen Teilanforderungen einzugehen. Besteht eine Anforderung z. B. aus fünf Teilaspekten, so ist im Sachverhalt zu jedem dieser Aspekte inhaltlich konkret Stellung zu nehmen. Eine alleinige, generische Aussage (z. B. "Die vorliegende Anforderung ist erfüllt.") ist für eine Bewertung nicht ausreichend.
- **Nachweise:** sofern anwendbar, Auflistung der jener Informationen/Dokumente/Screenshots/Exports etc., die zur Umsetzungsbewertung ergänzend hinzugezogen wurden.
- **Sicherheitsbewertung:** Auswahl gemäß den Vorgaben aus Kapitel 5.5 und Festlegung notwendiger Folgemaßnahmen/ Auflagen zur Erfüllung der Anforderungen, sofern der Umsetzungsstatus „umgesetzt“ nicht erreicht worden ist.
- **Frist:** sofern anwendbar, Bewertung durch den Gutachter auf Basis der gewonnenen Prüferkenntnisse, bis wann die Behandlung des ermittelten Sicherheitsmangel erfolgen sollte. Für jeden Sicherheitsmangel der Kategorien NC-A und NC-B wird eine Nachbesserungsfrist festgelegt, in welcher der Sicherheitsmangel beseitigt werden

*muss. Für jeden Sicherheitsmangel der Kategorie PI wird eine Überprüfungsfrist festgelegt, in der die Sicherheitsempfehlung geprüft und bewertet werden muss.*

- **Umsetzungstatus:** Auswahl gemäß den Vorgaben aus Kapitel 5.4

### 10.3.9 Eigenerklärung der Gutachter / Fachexperten

Ich erkläre, dass ich

- unabhängig und objektiv prüfe und
- in den letzten 24 Monate vor der Prüfung des Prüfgegenstandes nicht beratend oder ausführend an der Konzeption, Erstellung oder Konfiguration des untersuchten Prüfgegenstandes beteiligt war.

Ort, Datum, Name, Unterschrift

#### **Hinweis:**

*Die Eigenerklärung ist seitens jeder Person, die Teil des Gutachterteams und somit Teil der Prüfung war, abzugeben und in dem Gutachten durch eine digitale Unterschrift zu bestätigen.*

### 10.3.10 Anhang

- Abkürzungsverzeichnis
- Abbildungs- und Tabellenverzeichnis
- Referenzdokumente
- Nachweise (bspw. Kopien der Zertifikate) der Gutachter/Fachexperten zu Basis- und Fachqualifikationen (siehe Kapitel 9.1, 9.2 und 9.3)

#### **Hinweis:**

*Das Beifügen einer bestehenden Urkunde „Sicherheitsgutachter TI“ ist nicht erforderlich, da die Gültigkeitsstatus der Akkreditierungen der gematik bereits vorliegen.*