Elektronische Gesundheitskarte und Telematikinfrastruktur

Richtlinie zur Prüfung der Sicherheitseignung

Version:	2.2.0
Stand:	28.02.2023
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

Inhaltsverzeichnis

1 Einordnung des Dokumentes

1.1 Zielsetzung

Im Rahmen der Zulassungs- und Bestätigungsverfahren (im Folgenden wird nur noch von Zulassung gesprochen, wobei dies die Bestätigung inkludiert) der gematik für zentrale Dienste, Fachdienste, Dienste sicherer Übermittlungsverfahren, die Anbieter dieser Dienste der Telematikinfrastruktur (TI) sowie für weitere Anwendungen, die die TI beeinträchtigen können, ist die Bewertung der Sicherheitseignung erforderlich. Dazu werden vom Zulassungsnehmer Prüfaufträge an geeignete Sicherheitsgutachter vergeben. Diese bewerten in von ihnen erstellten Sicherheits- oder Produktgutachten (im Folgenden wird zusammenfassend von „Gutachten" gesprochen) die Sicherheitseigenschaften des Prüfobjekts. Auf Basis dieser Gutachten beurteilt die gematik daraufhin die Zulassungseignung.

Anhand des vorliegenden Handlungsleitfadens für Gutachten in der TI und anhand der spezifischen Produkttyp-, Anbietertyp- und Anwendungssteckbriefe (im Folgenden wird zusammenfassend von „Steckbriefen" gesprochen) des jeweiligen Prüfobjektes werden die notwendigen Eigenschaften bezüglich des Datenschutzes und bezüglich der Informationssicherheit geprüft.

Zur sprachlichen Vereinfachung wird im Fortgang des Dokumentes der Begriff „Sicherheit" benutzt – dies meint zum einen „Informationssicherheit" und schließt zum anderen „Datenschutz" implizit mit ein.

Die Prüfmethodik orientiert sich zum einen am BSI-Leitfaden für die Informationssicherheitsrevision [BSIInfRev]. Elemente des dort beschriebenen Verfahrens für die Durchführung einer Informationssicherheitsrevision wurden auf die Prüfung der Sicherheitseignung adaptiert. Neben den Unterschieden in den Prüfobjekten gibt es allerdings auch Unterschiede in der Zielsetzung, da hier insbesondere auf die Bewertbarkeit und Vergleichbarkeit der Gutachten Wert gelegt werden muss.

Eine weitere Grundlage für die Prüfmethodik ist [IDWPS330], der Prüfungsstandard „Abschlussprüfung beim Einsatz von Informationstechnologie" des Instituts der Wirtschaftsprüfer, dem insbesondere Elemente in der Durchführung der Prüfung entliehen sind. Da vielfach bei der Prüfung auf die Ergebnisse vorangegangener Prüfungen aufgesetzt werden muss, ist [IDWPS320] „Verwendung der Arbeit eines anderen Prüfers" ebenfalls relevant.

1.2 Zielgruppe

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

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und

deren Anwendung in Zulassungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Das Dokument ist für die Erstellung und Prüfung von Gutachten verbindlich, die im Rahmen der Zulassung von Anbietern und Produkten der Telematikinfrastruktur und von weiteren Anwendungen vorgelegt werden müssen.

1.4 Abgrenzung des Dokumentes

Das Dokument definiert keine neuen Anforderungen an die Prüfobjekte. Festgelegt werden lediglich Anforderungen an den Prüfprozess und an das Gutachten.

Der Nachweis der sicherheitstechnischen Eignung der dezentralen Produkte der TI wird nicht durch ein Gutachten im Sinne des vorliegenden Dokuments erbracht. Aus diesem Grund hat das im vorliegenden Dokument beschriebene Verfahren derzeit keine Relevanz für die Zulassung von dezentralen Produkten der TI. (Eine indirekte Relevanz kann sich durch ein notweniges Sicherheitsgutachten für Gerätekartenherausgabeprozesse ergeben, sofern dieses Voraussetzung für die Zulassung einer dezentralen Komponente ist.)

1.5 Methodik

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

2 Gutachten-Typen

Für den Nachweis der Sicherheitseignung von zentralen Diensten, Fachdiensten, Diensten sicherer Übermittlungsverfahren und Anbietern dieser Dienste sowie von weiteren Anwendungen gibt es zwei Typen von Gutachten: Das Sicherheitsgutachten und das Produktgutachten. Im weiteren Verlauf des Dokuments sind häufig beide Typen gemeint, weshalb zusammenfassend von „Gutachten" gesprochen wird. An den relevanten Stellen wird jedoch explizit auf Besonderheiten des jeweiligen Gutachtentyps 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 eine Gültigkeit von 3 Jahren und müssen dann entsprechend wiederholt werden, um die Aussage zur Sicherheitseignung aufrecht zu erhalten.

2.1 Sicherheitsgutachten

Das Sicherheitsgutachten umfasst auch technische Prüfungen von Hardware und Software, hat aber im Großteil der Anforderungen einen Fokus auf dem sicheren Rechenzentrumsbetrieb sowie auf den Prozessen die zur Einhaltung der Sicherheit dienen.

2.2 Produktgutachten

Das Produktgutachten umfasst auch die Prüfung von Sicherheits-Prozessen, hat seinen Schwerpunkt aber in der tiefen technischen Prüfung einer konkreten IT-Lösung, die auch die Analyse von Quellcode sowie Penetrationstest umfasst.

Pro Jahr ist vom Hersteller pro Produkt **ein (1)** Voll- bzw. Delta-Produktgutachten einzureichen.

- Beim ersten Produktrelease ist ein Vollproduktgutachten notwendig, dass vor der Verwendung des Produkts in der PU erstellt worden sein muss. Ein neues Vollproduktgutachten ist nach drei Jahren zu erstellen.
- In **jedem Zwischenjahr** (d.h. 1 Jahr nach Vollgutachten und 2 Jahre nach Vollgutachten) ist **ein (1)** Delta-Produktgutachten zu erstellen, sofern an dem Produkt wesentliche sicherheits- bzw. datenschutzrelevante Änderungen vorgenommen wurden, die in der letzten Begutachtung noch nicht geprüft wurden. Die Auswirkungen von am Produkt vorgenommenen Änderungen auf Sicherheit und Datenschutz werden vom Hersteller unter Einbeziehung des Gutachters dokumentiert und bewertet. Das Delta-Produktgutachten kann entfallen, falls seit der letzten Begutachtung keine Änderungen vorgenommen wurden, die als relevant hinsichtlich Sicherheit und Datenschutz bewertet wurden.

2.3 Delta-Gutachten

Kommt es an einem Produkt, welches durch ein Sicherheits- oder Produktgutachten geprüft wurde, zu wesentlichen Änderungen, muss vom Anbieter bzw. Hersteller stets der Sicherheitsgutachter mit einbezogen werden, sofern nicht produkttypspezifische Regelungen bereits definieren, wann eine erneute Begutachtung notwendig wird. Ist letzteres nicht der Fall, entscheidet der Sicherheitsgutachter (im Falle von Produktgutachten ggf. zusammen mit dem Produktgutachter), ob die Änderungen hinsichtlich Datenschutz und Informationssicherheit so relevant sind, dass die Änderungen vor Inbetriebnahme erneut begutachtet werden müssen und ob das Sicherheits- bzw. Produktgutachten anzupassen ist. Wird das Gutachten angepasst, muss lediglich der die Änderung umfassende Teil im Gutachten neu beschrieben und bewertet werden. Die restlichen Inhalte können unverändert bleiben, sofern die durchgeführten Änderungen keinen Einfluss auf weitere Teile des Produkts (oder im Extremfall das gesamte Produkt) haben. Die neue Version des Gutachtens ist dann ein sogenanntes „Delta-Gutachten". Hierbei ist zu beachten, dass die zeitliche Gültigkeit des ursprünglichen (vollen) Sicherheits- bzw. Produktgutachtens bestehen bleibt, also durch ein Delta-Gutachten nicht verlängert wird.

Das Delta-Gutachten ist somit kein eigener Gutachten-Typ, sondern ein Spezialfall des Sicherheits- bzw. Produktgutachtens im Falle von wesentlichen Änderungen die nur einen kleineren Teil des Produkts betreffen und somit nicht eine vollständige Neubegutachtung erfordern.

Die Beschreibungen und Bewertungen im Rahmen der Delta-Begutachtung müssen immer im ursprünglichen Vollgutachten festgehalten werden, wobei die Änderungen kenntlich gemacht werden (bspw. farblich markiert). Dadurch hat der Leser stets den Gesamtüberblick über den Begutachtungsgegenstand und gleichzeitig den Fokus auf die Änderungen zum ursprünglichen Vollgutachten.

3 Prüfauftrag

Der Prüfauftrag ist Bestandteil der Vereinbarung zwischen dem Auftraggeber (Zulassungsnehmer) und dem Sicherheitsgutachter. Der Prüfauftrag soll eindeutig auf die Anforderungen der gematik Bezug nehmen.

Der Gutachter muss im Rahmen der Erstellung eines Gutachtens die ihm benannten Prüfobjekte explizit anhand der in diesem Dokument [gemRL_PruefSichEig_DS] normierten Vorgehensweisen sowie anhand der Vorgaben der gematik (Steckbrief) prüfen und bewerten.

Der Gutachter muss im Rahmen der Erstellung eines Gutachtens das aktuelle Sicherheitsniveau der Prüfobjekte sowie die Einhaltung der Vorschriften zum Schutz der personenbezogenen Daten feststellen und anhand der Vorgaben der gematik bewerten.

Der Gutachter muss im Rahmen der Erstellung eines Gutachtens Sicherheitslücken und Mängel, die das Erreichen des von der gematik geforderten Datenschutz- und Sicherheitsniveaus oder die Einhaltung der Vorschriften zum Schutz der personenbezogenen Daten verhindern, dokumentieren.

4 Prüfumfang und -grundlage

Als Prüfgrundlage muss der Gutachter die aktuelle, von der gematik veröffentlichte, zulassungsfähige Produkttyp-, Anbietertyp- bzw. Anwendungsversion und den dazugehörigen Steckbrief heranziehen (Festlegung zulassungsfähiger Versionen im Fachportal der gematik). Bei Wiederholungsgutachten – insbesondere bei neuen Vollgutachten nach 3 Jahren (siehe Kapitel 2) – wird somit in der Regel eine neuere Version des Steckbriefs verwendet als dies bei der eigentlichen Zulassung des Produkts, Anbieters oder der Anwendung der Fall war. Bei Abweichungen davon – bspw. bei Delta-Gutachten – ist frühzeitig eine Abstimmung mit der gematik herbeizuführen um zu klären, ob das Vorgehen zulässig ist.

Der Gutachter muss die Übereinstimmung des Prüfobjektes mit den Anforderungen aus dem herangezogenen Steckbrief prüfen und bewerten. Relevant sind dabei die Anforderungen, die im Steckbrief bei der Aufzählung der Anforderungen zur sicherheitstechnischen Eignung in den Unterabschnitten „Sicherheitsgutachten" bzw. „Produktgutachten" aufgelistet sind.

Es kann notwendig sein und es ist entsprechend gestattet, aus Anforderungen des Steckbriefes weitere detailliertere Anforderungen abzuleiten, um die Erfüllung der ursprünglichen Anforderung zu prüfen (z. B. konkrete Umgebungsanforderungen eines Prüfobjekts oder Anforderungen an die Sicherheit von Managementnetzen und Virtualisierungslösungen).

Werden von einem Gutachter mehrere Produkte, Anbieter oder Anwendungen begutachtet, ist es gestattet, dass diese in einem einzigen Gutachten zusammengefasst werden, wobei sich das Votum ausdrücklich auf alle begutachteten Prüfobjekte beziehen muss oder jeweils ein Votum pro Prüfobjekt verfasst werden muss.

Das vorliegende Dokument definiert keine weiteren fachlichen Anforderungen an Produkte, Anbieter und Anwendungen, die über den jeweiligen Steckbrief hinausgehen.

Für Produktgutachten gilt:

- Abgesehen von konkreten Hardware-Maßnahmen zum physischen Schutz, wird Hardware vom Produktgutachter nicht geprüft.
- Der Produktgutachter kann von der Prüfung am Markt verfügbarer Produkte von Drittanbietern, die geeignet sind, die Sicherheitsziele des Produkttyps umzusetzen und deren Sicherheit von vertrauenswürdigen Quellen bereits beurteilt wurde (idealer Weise in Form von Zertifizierungen), absehen (Beispiele: Betriebssysteme, Betriebssystemerweiterungen des Betriebssystemherstellers, Laufzeitumgebungen). Der Produktgutachter muss in diesen Fällen seine Entscheidung für eine Nichtprüfung im Produktgutachten begründen.

5 Prüfkriterien und Bewertungsschema

Die Prüftätigkeit zielt darauf ab, das Datenschutz- und Sicherheitsniveau zu bewerten.

Das Gutachten zeigt dem Auftraggeber in strukturierter Form den Umsetzungsstatus und das Sicherheitsniveau und ggf. den Handlungsbedarf aufgrund bestehender Sicherheitsdefizite auf, die durch fehlende oder nur unzureichend umgesetzte Anforderungen verursacht werden. Das Gutachten dient damit auch als Hilfsmittel für den weiteren Optimierungsprozess.

Der Gutachter muss dem Gutachten die in diesem Kapitel dokumentierten Bewertungsschemata zu Grunde legen.

5.1 Aktualität

Es ist zu prüfen, dass die implementierten Sicherheitsmaßnahmen sich am aktuellen Stand der Technik und Wissenschaft orientieren.

5.2 Angemessenheit

Die Prüfung der Angemessenheit der Umsetzung von Anforderungen durch Maßnahmen beinhaltet die Beurteilung im Hinblick auf deren Wirksamkeit, auch in Relation zum Aufwand.

Um die Angemessenheit einer Maßnahme zu bewerten, sollen die Antworten auf folgende Fragen (vergleiche [BSI], Kapitel 8) ausgewertet werden:

- Welches Risiko soll durch die Realisierung der Maßnahme verringert werden?
- Welches Restrisiko verbleibt? Ist dieses Restrisiko lt. Aktenlage tragbar?
- Ist die Maßnahme geeignet und in der Praxis umsetzbar?
- Ist die Maßnahme anwendbar, leicht verständlich und wenig fehleranfällig?
- Sind die getroffenen Maßnahmen der jeweils angestrebten Risikomitigierung angemessen?
- Stehen die Kosten und der Aufwand für die Umsetzung in einem sachgerechten Verhältnis zum Schutzbedarf des betroffenen Assets?

Bei der Prüfung der Angemessenheit werden dadurch folgende Aspekte berücksichtigt:

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

5.3 Sicherheitsmängel

Die Umsetzung einer Anforderung durch Maßnahmen muss jeweils hinsichtlich vorhandener Sicherheitsmängel bewertet werden. Bei einem „Sicherheitsmangel" liegt z. B. eine Sicherheitslücke vor, die entsprechend ihrer Kritikalität bewertet wird. Bei der Bewertung sind folgende Kategorien zu verwenden:

- kein Sicherheitsmangel
- Sicherheitsmangel
- schwerwiegender Sicherheitsmangel
- Sicherheitsempfehlung

5.3.1 Kein Sicherheitsmangel

Den in der Kategorie „kein Sicherheitsmangel" eingeordneten Anforderungen sind Maßnahmen gegenübergestellt, die das geforderte Datenschutz- und Sicherheitsniveau ausreichend sicherstellen – es liegt u. A. keine Sicherheitslücke vor und die Vorschriften zum Schutz der personenbezogenen Daten werden eingehalten.

5.3.2 Sicherheitsmangel

Bei einem „Sicherheitsmangel" liegt z. B. eine Sicherheitslücke vor, die mittelfristig behoben werden muss. Das Erreichen der geforderten Schutzziele eines Assets ist beeinträchtigt.

5.3.3 Schwerwiegender Sicherheitsmangel

Ein „schwerwiegender Sicherheitsmangel" ist z. B. eine Sicherheitslücke, die umgehend geschlossen werden muss, da das Erreichen der geforderten Schutzziele eines Assets stark gefährdet ist und erheblicher Schaden zu erwarten ist.

Wird ein Sicherheitsmangel als schwerwiegend bewertet, muss diese Einordnung im Gutachten begründet werden.

5.3.4 Sicherheitsempfehlung

Zusätzlich können zu den geprüften Maßnahmen noch „Sicherheitsempfehlungen" gegeben werden. Diese beziehen sich auf Verbesserungsvorschläge für die Umsetzung von Anforderungen.

5.4 Vollständigkeit der Maßnahmen

Hinsichtlich der Vollständigkeit der den Anforderungen gegenübergestellten Maßnahmen muss geprüft werden, ob durch diese Maßnahmen alle Aspekte der Anforderung abgedeckt werden.

5.5 Umsetzung der Anforderungen

Es muss geprüft werden, ob die Anforderungen aus dem Steckbrief mit wirkungsvollen Maßnahmen umgesetzt sind.

Als Ergebnis muss ein Katalog vorliegen, in dem für jede Anforderung der

Umsetzungsstatus „umgesetzt", „teilweise umgesetzt", „nicht umgesetzt" oder „nicht relevant" erfasst und begründet ist.

5.5.1 Umgesetzt

Alle der Anforderung gegenübergestellten Maßnahmen sind vollständig, wirksam und angemessen umgesetzt. Die umgesetzten Maßnahmen mitigieren das Risiko in ausreichendem Maße.

5.5.2 Teilweise umgesetzt

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

Es muss beurteilt werden, ob dadurch ein Sicherheitsmangel oder ein schwerwiegender Sicherheitsmangel für das Prüfobjekt vorliegt.

Es soll dokumentiert werden, welche der Anforderung gegenübergestellte Maßnahmen noch umgesetzt werden müssen.

5.5.3 Nicht umgesetzt

Die der Anforderung gegenübergestellten Maßnahmen sind größtenteils noch nicht umgesetzt. Die umgesetzten Maßnahmen decken die Anforderung nicht ab.

Es muss beurteilt werden, ob dadurch ein Sicherheitsmangel oder ein schwerwiegender Sicherheitsmangel für das Prüfobjekt vorliegt.

5.5.4 Nicht relevant

Die Anforderung ist zwar im Steckbrief vorhanden, jedoch für die konkrete Ausprägung des Prüfobjekts nicht relevant (bspw. weil das Prüfobjekt nur einen Teilprozess des durch den Steckbrief definierten Gesamtprozesses darstellt).

6 Prüfmethoden

Unter Prüfmethoden werden alle für die Ermittlung eines Sachverhaltes verwendeten Methoden verstanden.

Welche Prüfmethoden angewendet werden, ist abhängig vom jeweiligen Prüfobjekt bzw. von der jeweiligen Anforderung aus dem Steckbrief. Ebenso sind für bestimmte Prüfmethoden besondere Qualifikationen des Gutachters notwendig, weshalb einige Prüfmethoden vom Sicherheitsgutachter und einige vom Produktgutachter durchzuführen sind (siehe 6.1).

Der Gutachter muss dem Gutachten die im Folgenden festgelegten Prüfmethoden zu Grunde legen.

Der Gutachter muss entscheiden, ob und welche Prüfmethoden darüber hinaus einzusetzen sind, um eine zuverlässige, objektive und vollständige Prüfung eines Sachverhaltes zu ermöglichen.

Die Kombination mehrerer Prüfmethoden zur Prüfung einer Anforderung ist möglich bzw. in vielen Fällen sogar notwendig.

6.1 Gutachten-Typ-spezifische Festlegungen

6.1.1 Sicherheitsgutachten

Für Sicherheitsgutachten liegt die Wahl der Prüfmethode im Ermessen des Sicherheitsgutachters, wobei – wann immer möglich – eine Inaugenscheinnahme und Beobachtung (6.3) sowie Technische Prüfung ohne eigenen Zugriff auf das System (6.4) durchgeführt werden soll. In jedem Fall muss der Sicherheitsgutachter für ein Sicherheitsgutachten eine Vor-Ort-Prüfung vornehmen. Eine Ausnahme hiervon ist lediglich bei kleineren Nachbegutachtungen auf Grund von Änderungen am Prüfobjekt (Delta-Gutachten) möglich und muss nachvollziehbar im Sicherheitsgutachten begründet werden. Für die Prüfmethoden der Absätze 6.2 bis 6.7 sind vorrangig die Qualifikationen im Bereich Audit notwendig, weshalb sie vom Sicherheitsgutachter durchgeführt werden sollen.

6.1.2 Produktgutachten

Bei Produktgutachten muss der Produktgutachter für jede Anforderung zwingend eine der Prüfmethoden Penetrationstest (6.8), Technische Prüfung mit Zugriff auf das System (6.9) oder Quellcode-Analyse (6.10) anwenden. Eine Abweichung hiervon muss für die jeweilige Anforderung vom Produktgutachter im Produktgutachten nachvollziehbar begründet werden. Für die genannten Prüfmethoden (6.8, 6.9, 6.10) sind entsprechende Qualifikationen des Gutachters notwendig, sodass sie zwingend vom Produktgutachter durchgeführt werden müssen.

6.2 Aktenanalyse

Durch den Auftraggeber muss die vollständige Dokumentation des Prüfobjektes bereitgestellt werden. Gegebenenfalls sind weitere Dokumente durch den Gutachter nachzufordern. Dokumente können in Papier oder elektronischer Form angefordert bzw. bereitgestellt werden. Zunächst werden die Dokumente auf Aktualität und

Vollständigkeit geprüft. Hinsichtlich der Vollständigkeit ist inhaltlich zu prüfen, ob alle wesentlichen Aspekte des Prüfobjektes bezogen auf den Prüfgegenstand erfasst wurden. Der Gutachter muss die Version der Dokumente (Dokumentenname, Version, Datum der Publikation) dokumentieren, auf deren Basis die Aktenanalyse erfolgt.

6.3 Inaugenscheinnahme und Beobachtung

Die Inaugenscheinnahme vor Ort ist eine auf ein bestimmtes Kriterium gerichtete Prüfoperation; die Beobachtung hingegen dient dem Zweck, einen Gesamteindruck zu bekommen und mögliche Ansätze für einen Prüfungsschwerpunkt zu finden. Im Gegensatz zur Beobachtung ist die Inaugenscheinnahme systematisch und damit wiederholbar.

Im Rahmen einer Vor-Ort-Prüfung müssen die spezifizierten Eigenschaften des Prüfobjektes durch Inaugenscheinnahme und Beobachtung validiert werden. Hierbei muss ein objektives, genaues und kritisches Prüfen von Sachverhalten, Vorgängen und Ereignissen durch visuelles Begutachten der realisierten Konzepte und Richtlinien erfolgen. Die Inaugenscheinnahme und Beobachtung werden insbesondere bei technischen Systemen und Gegenständen, aber auch bei Räumlichkeiten und Orten (z. B. Zutrittsregelung) angewendet.

Die Inaugenscheinnahme kann eine Demonstration durch den Auftraggeber umfassen. Der Gutachter greift dabei nie selbst in das System ein.

Bei komplexen Systemen und Verfahren ist eine direkte Auswertung vor Ort nicht immer möglich. Zu Dokumentationszwecken können jedoch technische Hilfsmittel benutzt werden, z. B. Videos, Fotos, Screenshots sowie Skizzen und Protokolle. Die Verwendung dieser Dokumentationsmittel ist im Voraus mit dem Koordinator des Auftraggebers abzustimmen. Darüber hinaus muss im Vorhinein ein Terminplan der In-Augenscheinnahmen bzw. Beobachtungen erstellt und mit dem Auftraggeber abgestimmt werden.

6.4 Technische Prüfung ohne eigenen Zugriff auf das System

Im Rahmen einer Vor-Ort-Prüfung müssen die spezifizierten Eigenschaften durch eine dem Prüfobjekt entsprechende technische Prüfung bewertet werden. Hierbei muss eine Prüfung der Umsetzung der Konzepte und Richtlinien erfolgen. Die technische Prüfung wird durch den Gutachter vorgenommen, jedoch ohne dass dieser selbst administrativen Zugriff auf das System hat. Die konkrete Durchführung technischer Schritte wird durch den entsprechenden Verantwortlichen des Auftraggebers geleistet, wobei der Gutachter die Durchführung begleitet und beobachtet, um die Echtheit der Ergebnisse nachvollziehen zu können (bspw. kann sich der Gutachter die Konfiguration eines HSMs oder der eingesetzten TLS-Bibliothek direkt im System zeigen lassen). Zu Dokumentationszwecken können technische Hilfsmittel benutzt werden, z. B. Videos, Fotos, Screenshots sowie Skizzen und Protokolle. Die Verwendung dieser Dokumentationsmittel ist im Voraus mit dem Auftraggeber abzustimmen.

Darüber hinaus muss im Vorhinein ein Terminplan der technischen Prüfung erstellt und mit dem Auftraggeber abgestimmt werden.

6.5 Datenanalyse

Durch den Auftraggeber, der die Prüfung veranlasst hat, werden Daten des Prüfobjektes

bereitgestellt. Unter Daten werden u. a. Logfiles, Quellcode, Betriebsdaten, Systemkonfigurationen und Prüfprotokolle verstanden. Es muss eine Soll-Ist-Analyse durchgeführt werden, in der die bereitgestellten Daten den spezifizierten Vorgabewerten gegenübergestellt werden.

6.6 Verwendung bestehender Nachweise

In einem Gutachten einer Gesamteinheit (in Teileinheiten unterteiltes Prüfobjekt) werden Prüfungsaussagen zu einer oder mehreren Teileinheiten verwendet. Die Verwendung dieser Prüfungsaussage für eine Teileinheit berührt die Verantwortlichkeit des Gutachters für die Gesamteinheit nicht. Der Gutachter muss in eigener Verantwortung die Prüfung planen und durchführen sowie anschließend eine Prüfungsbewertung in Bezug auf die Einhaltung der sicherheitstechnischen und datenschutzrelevanten Vorgaben der Telematikinfrastruktur treffen und das Prüfungsurteil (Votum) fällen.

Diese Vorgehensweise schließt die Verwendung bestehender Nachweise zur Sicherheitseignung (bspw. eine Zertifizierung nach ISO 27001 oder Prüfberichte oder Gutachten von anderen Prüfungen, die Sicherheitsaspekte beinhalten) nicht aus. Jedoch muss der Gutachter hierbei beurteilen, welchen Einfluss diese bestehenden Nachweise auf die Gesamtaussage haben werden und welche relative Bedeutung der von ihm selbst geprüfte Teil noch an der Gesamteinheit hat. Der Gutachter muss stets seiner Verantwortung für ein eigenverantwortliches Prüfungsurteil nachkommen.

In welchem Ausmaß und mit welcher Gewichtung ein bestehender Nachweis verwendet werden kann, hängt neben der Bedeutung dieser Teileinheit für das Gesamturteil des Gutachters von der Qualität des bestehenden Nachweises ab. Die Qualität der bestehenden Nachweise muss der Gutachter durch geeignete Prüfungshandlungen ausreichend und angemessen sicherstellen. Zu diesen Prüfungshandlungen zählen u. a. die kritische Würdigung der Prüfungsfeststellungen des Nachweises sowie der Prüfungsplanung, -durchführung und der Arbeitspapiere. Der Gutachter muss im Gutachten die Verwendung und Einschätzung von bestehenden Nachweisen und die durchgeführten Qualitätssicherungsmaßnahmen darstellen. Der Gutachter muss im Gutachten die Verwendung von bestehenden Nachweisen dokumentieren, insbesondere die betroffenen Teileinheiten und deren Bedeutung für die zu prüfende Gesamteinheit.

6.7 Befragung

Die Befragung dient der systematischen, standardisierten und strukturierten Informationsgewinnung. Bei der Vollstandardisierung sind die Reihenfolge, der Wortlaut und mögliche Antworten von Fragen vorgegeben. Der Befragung liegt ein vorgegebener Fragenkatalog zugrunde, der kategoriale, geschlossene (Ja/Nein) oder skalierte (Zuordnung der Antwort zu Werten auf einer Skala) Antworten verlangt. Weiterhin kann der Fragenkatalog aus offenen Fragen, Eingruppierungsfragen sowie Summen- und Rangfragen bestehen. Die Befragung kann mündlich (Interview) oder schriftlich durchgeführt werden.

In jedem Fall sind geeignete Ansprechpartner zu identifizieren.

6.7.1 Mündliche Befragung

Bei Interviews mit Mitarbeitern des Auftraggebers, der die Prüfung veranlasst hat, muss im Vorhinein ein Terminplan erstellt und abgestimmt werden.

Interviews sollen von Gutachterteams à 2 Personen geführt werden. Dabei notiert und protokolliert eine Person die Ergebnisse, gefundene Mängel und Anmerkungen, die andere stellt die notwendigen Fragen und interagiert mit dem Interviewpartner.

Die Protokolle müssen vom Befragten auf ihre sachliche Richtigkeit geprüft werden, bevor sie Eingang in den Prüfprozess finden.

6.7.2 Schriftliche Befragung

Bei der schriftlichen Befragung muss dem Befragten die Gelegenheit gegeben werden, Verständnisfragen im Vorhinein klären zu können.

6.8 Penetrationstest

Beim „Penetrationstest" liegt der Fokus auf dem Auffinden von Schwachstellen, die durch einen Außentäter ausgenutzt werden können.

Bei Penetrationstests ist der Auftraggeber stets im Vorfeld über den Umfang, insbesondere die betroffenen Teilsysteme und die zeitliche Planung zu informieren, da solche Tests ggf. zum Ausfall von Systemen führen können. Die Wahl der Methoden und Tools sowie des konkreten Vorgehens liegt beim Gutachter.

Der Penetrationstest muss zwar individuell auf das Prüfobjekt und die zu prüfenden Anforderungen ausgerichtet sein, jedoch muss der Gutachter grundsätzlich einem standardisierten Vorgehen – wie es bspw. im Leitfaden für Penetrationstests des BSI [BSI_LF_PT] beschrieben ist – folgen und seine Dokumentation danach ausrichten.

Ausgangspunkt kann ein *nicht invasiver Schwachstellenscan* (vgl. [BSI_LF_PT]) sein. Insbesondere bei Software-Eigenentwicklungen sind aber individuelle auf das Produkt zugeschnittene Tests notwendig, um Schwachstellen zu identifizieren. Da die Prüfung an Systemen mit Testdaten durchgeführt wird, ist auch eine darüber hinaus gehende Nutzung von Exploits – bspw. zum Beweis der Ausnutzbarkeit gefundener Schwachstellen – möglich.

Die Dokumentation des Penetrationstests, die das gewählte Vorgehen, die durchgeführten Prüfschritte (unter Angabe der verwendeten Tools) und deren Ergebnisse nachvollziehbar beschreibt, muss in einem eigenen Absatz im Gutachten übergreifend festgehalten werden. Für die Begründung des Umsetzungsstatus (siehe 5.5) der durch den Penetrationstest geprüften Anforderungen ist dann eine kürzere Erklärung mit Verweis auf die entsprechenden Stellen in der übergreifenden Dokumentation des Penetrationstests ausreichend.

6.9 Technische Prüfung mit Zugriff auf das System

Bei der „technischen Prüfung mit Zugriff auf das System" liegt der Fokus auf dem Auffinden von Schwachstellen, die durch einen Innentäter ausgenutzt werden können („Administrator-Angriff").

Im Gegensatz zur technischen Prüfung ohne eigenen Zugriff auf das System führt der Gutachter bei dieser Methode die Prüfungen selbstständig am System durch und hat dabei administrativen Zugriff. Technische Prüfungen mit Zugriff auf das System sind mit dem Auftraggeber stets im Vorfeld abzustimmen. Die Wahl der Methoden und Tools sowie des konkreten Vorgehens liegt beim Gutachter.

Im Gegensatz zum Penetrationstest wird bei der technischen Prüfung mit Zugriff auf das

System ein Angreifer angenommen, der Zugriff zum System inklusive administrativer Rechte besitzt (Innen-Täter). Ziel ist es, für Fälle, in denen auch der Auftraggeber (in der Rolle des Betreibers) selbst nicht auf verarbeitete Daten zugreifen darf, zu prüfen, dass dies auch „von innen her" nicht möglich ist (bspw. durch Ziehen eines Dumps oder maliziöse Rekonfiguration des Systems). Der Gutachter muss das Vorgehen bei der technischen Prüfung mit Zugriff auf das System, die durchgeführten Prüfschritte (unter Angabe der verwendeten Tools) und deren Ergebnisse – insbesondere gefundene Schwachstelle – in einem eigenen Absatz übergreifend im Gutachten nachvollziehbar dokumentieren. Für die Begründung des Umsetzungsstatus (siehe 5.5) der durch die technische Prüfung mit Zugriff auf das System geprüften Anforderungen ist dann eine kürzere Erklärung mit Verweis auf die entsprechenden Stellen in der übergreifenden Dokumentation ausreichend.

6.10 Quellcode-Analyse

Ziel der Quellcode-Analyse ist es, die Umsetzung einer oder mehrerer Anforderungen mit der höchst möglichen Sicherheit zu bestimmen. Daher muss sich der Gutachter in geeigneter Art und Weise davon überzeugen, dass der gesichtete, vom Auftraggeber bereitgestellte Quellcode und die darauf beruhende Software im vom Gutachter geprüften System (Prüfobjekt) übereinstimmen. Dies ist besonders relevant, wenn Zugriffe durch den Auftraggeber (in der Rolle des Betreibers) selbst technisch ausgeschlossen werden müssen.

Die Quellcode-Analyse kann manuell sowie Tool-unterstützt stattfinden. Der Gutachter muss das Vorgehen bei der Quellcode-Analyse, die durchgeführten Prüfschritte (unter Angabe der verwendeten Tools) und deren Ergebnisse – insbesondere gefundene Schwachstelle – in einem eigenen Absatz übergreifend im Gutachten nachvollziehbar dokumentieren. Für die Begründung des Umsetzungsstatus (siehe 5.5) der durch die Quellcode-Analyse geprüften Anforderungen ist dann eine kürzere Erklärung mit Verweis auf die entsprechenden Stellen in der übergreifenden Dokumentation der Quellcode-Analyse ausreichend.

6.11 Prüfung physischer Schutzmaßnahmen

Werden zur Erreichung der Gesamtsicherheit des zu prüfenden Produkts Maßnahmen zum physischen Schutz umgesetzt (bspw. dedizierter Zutrittsschutz für das Produkt oder aktives Erkennen und automatische Reaktion auf Zutrittsversuche oder Gehäuseöffnungsversuche), sind diese Maßnahmen vom Gutachter zu prüfen. Dabei muss sich der Gutachter von der korrekten Funktion der Maßnahme am tatsächlichen Produkt überzeugen. Eine reine Prüfung der Maßnahme auf Dokumentenebene ist nicht ausreichend. Prüfungen, die zur Beschädigung oder gar Zerstörung des Produkts führen, sind zu unterlassen. In solchen Fällen ist aber zumindest eine Sichtprüfung durchzuführen. Die durchgeführten Prüfungen und ggf. gefundene Schwachstellen sind nachvollziehbar im Gutachten zu beschreiben (siehe 5.5).

7 Prüfplan

Der Prüfplan beschreibt den gesamten Ablauf der Prüfung der Sicherheitseignung.

Im Kern soll bei dieser Prüfung anhand eines Soll-Ist-Vergleiches herausgefunden werden, ob das Sicherheitsniveau des Prüfobjektes ausreichend ist, also die Anforderungen des Steckbriefs erfüllt sind oder nicht. Um zu zuverlässigen, nachvollziehbaren und vergleichbaren Schlussfolgerungen und Ergebnissen zu kommen, ist eine strukturierte Dokumentation der Sachverhalte und Prüfungshandlungen notwendig.

7.1 Erweiterung der zu prüfenden Anforderungen

Abgeleitete Anforderungen (siehe Kapitel 4) müssen neben den Anforderungen aus dem Steckbrief vom Gutachter in den Anforderungskatalog aufgenommen und entsprechende Prüfkriterien dokumentiert werden.

7.2 Festlegung anzuwendender Prüfmethoden

Die Prüfmethoden (siehe Kapitel 6) für die Anforderungen sind vom Gutachter festzulegen, wobei die Vorgaben in 6.1 zu beachten sind.

7.3 Inhalte des Prüfplans

Der Prüfplan soll mindestens folgende Inhalte haben:

- Ableitung von Aktivitäten, die sich aus dem Anforderungskatalog und Prüfmethoden ergeben,
- Dokumentation von weiteren, als notwendig erachteten Prüfmethoden für einzelne Anforderungen,
- Auflistung der Ansprechpartner des Auftraggebers mit ihren spezifischen Verantwortungsbereichen,
- Zuordnung von Ressourcen sowohl des Gutachters als auch des Auftraggebers zu den einzelnen Aktivitäten,
- Termine der einzelnen Aktivitäten – für kritische Termine auch Ausweichtermine,
- Darstellen von Abhängigkeiten zwischen den Aktivitäten,
- Termine zur Aggregation der Befunde zum Bewerten des Prüfobjektes auf Anforderungsebene,
- Termine von Abstimmungsgesprächen mit dem Auftraggeber zum Projektfortschritt,
- Termine für die Übergabe von Statusberichten an den Auftraggeber,
- Termin der Übergabe des Gutachtens an den Auftraggeber.

8 Gutachten

Der Sicherheitsgutachter ist verantwortlich für die Erstellung und den Inhalt des Gutachtens.

Das Gutachten muss eine umfassende, genaue und eindeutige Darstellung sowie nachvollziehbare Bewertung des Prüfobjekts hinsichtlich seiner Sicherheitseignung geben.

Dem Auftraggeber kann eine Frist eingeräumt werden, innerhalb derer er Hinweise, Rückfragen, Kommentare oder Unstimmigkeiten zu einzelnen Punkten des vorläufigen Gutachtens vorbringen kann. Diese werden vom Gutachter entsprechend nachgeprüft und der dann aktuelle Umsetzungsstatus im Gutachten dokumentiert.

Wenn der Auftraggeber auf Grund des Gutachtens Maßnahmen umsetzt, um bestimmte Anforderungen zu erfüllen, müssen der Abschluss und die Wirksamkeit der Korrekturmaßnahmen geprüft werden, bevor das Gutachten entsprechend geändert wird.

Das Gutachten muss mindestens die folgenden Punkte enthalten und soll die folgende Struktur haben:

- Deckblatt
  - Name der Gutachter
  - Nummer des Gutachtens
  - Benennung des Prüfobjektes
  - Benennung des Auftraggebers
  - Dokumenteninformationen (Version, Stand, Klassifizierung usw.)
- Dokumentenhistorie
- Kontaktdaten der Gutachter (insbesondere Telefon, E-Mail)
- Inhaltsverzeichnis, Verzeichnis der Anhänge
- Management Summary
  - Aufgabenstellung
  - Zusammenfassung der wesentlichen Feststellungen
  - Zusammenfassung der Prüfergebnisse (inkl. Votum)
- Grundlagen der Prüfung
  - Prüfauftrag
  - Bezeichnung des Prüfobjektes
  - Zielsetzung und Umfang der Prüfung
  - Zeitraum der Prüfung
- detaillierte Beschreibung der Prüfung
  - Beschreibung des Prüfobjektes (grundlegende Tätigkeiten, Abläufe, Prozesse; Aufbau, angrenzende Systeme; Verantwortlichkeiten und ggf. wofür der Auftraggeber gerade nicht verantwortlich ist; eindeutige Benennung Produkttyp-, Anbietertyp- bzw. Anwendungssteckbriefversion und Referenz auf den herangezogenen Steckbrief; postalische Adresse aller vom Gutachten umfassten Standorte des Prüfobjekts)
  - Beschreibung des Prüfplans

  - Beschreibung der angewendeten Prüfmethoden (bzw. Erläuterung, warum eine Prüfmethode nicht verwendet wurde) und der durchgeführten Prüfaktivitäten
  - Beschreibung der verwendeten Prüfhilfsmittel und -tools
  - Beschreibung bei Vor-Ort-Prüfungen
    - Prüfzeitpunkt
    - Prüfstandort
    - Prüfumgebungseinflüsse
  - Verzeichnis der Teilnehmer an den einzelnen Prüfungen differenziert nach
    - Auftraggeber
    - Gutachter
    - Funktion/Rolle
    - Thema
  - Dokumentation der herangezogenen Dokumente und der Prüfergebnisse, tabellarisch erfasst:
    - gematik-Afo-ID | Anforderung (min. Titel) | Prüfmethode (siehe 6) | Umsetzungsstatus (siehe 5.5) | Sicherheitsmängel (siehe 5.3) | Begründung/Bemerkung/Empfehlung/Risiken
  - notwendige Folgemaßnahmen und Auflagen zur Erfüllung der Anforderungen, sofern der Umsetzungsstatus „umgesetzt" nicht erreicht worden ist

- Zusammenfassung der Prüfergebnisse inkl. Mängel/Auflagen und Begründung, warum diese die Sicherheitseignung nicht schmälern
- von beiden Gutachtern (siehe 9.2) unterschriebenes Prüfungsurteil in Form eines Votums in Bezug auf die Einhaltung der sicherheitstechnischen und datenschutzrelevanten Vorgaben der Telematikinfrastruktur
- Anhang
  - Abkürzungsverzeichnis
  - Glossar
  - Abbildungs- und Tabellenverzeichnis
  - Referenzdokumente
  - Arbeitsdokumente (Protokolle, etc.)
  - Prüfplan
  - Eigenerklärung der Gutachter zu Unabhängigkeit und Objektivität
  - Nachweise (bspw. Kopien der Zertifikate) der Gutachter zu Basisqualifikation und Zusatzqualifikation (siehe Absatz 9.1)

Die hier genannten Inhalte inkl. des Anhangs müssen alle in einem einzigen Dokument zusammengeführt werden.

9 Gutachter

9.1 Fachliche Kompetenz

Für die Erstellung von Gutachten im Rahmen der Prüfung der Sicherheitseignung müssen die Gutachter bestimmte Qualifikationen nachweisen, welche im Folgenden entsprechend der Gutachtentypen definiert werden. Grundsätzlich ist eine permanente Weiter- und Fortbildung der Gutachter eine Grundvoraussetzung für ihre Arbeit. Da je nach Prüfobjekt ggf. auch Spezial-Fachwissen notwendig ist, welches nicht von jedem Gutachter als Basis-Wissen vorausgesetzt werden kann, ist das Hinzuziehen von weiteren Fachexperten nicht nur gestattet, sondern ausdrücklich erwünscht (siehe auch 9.1.3).

9.1.1 Sicherheitsgutachter

Der Sicherheitsgutachter benötigt sowohl breites als auch tiefes Wissen auf den Gebieten Datenschutz und Informationssicherheit sowie die notwendigen Kenntnisse zur Durchführung von Audits. Zusätzlich muss der Sicherheitsgutachter grundlegende Kenntnisse zur Telematikinfrastruktur vorweisen können.

9.1.1.1 Basisqualifikation

Der Sicherheitsgutachter muss im Rahmen der Zulassung gegenüber der gematik den aktuell gültigen Nachweis seiner Basisqualifikation durch Vorlage der entsprechenden Zertifikate (Kopien) gemäß 9.1.1.1.1 oder 9.1.1.1.2 oder 9.1.1.1.3 erbringen.

9.1.1.1.1 ISO-27001-Auditor auf Basis von IT-Grundschutz

Zertifikat der Lizenzierung als ISO-27001-Auditor durch das BSI (ISO-27001 auf der Basis von IT-Grundschutz).

9.1.1.1.2 ISO/IEC-27001-Lead-Auditor einer bei der DAkkS gelisteten Zertifizierungsstelle

Zertifikat (ISO/IEC 27001 Lead Auditor) und Auditor-Berufung bei der akkreditierten Zertifizierungsstelle für akkreditierte ISO/IEC-27001-Auditoren, die von einer bei der DAkkS (Deutsche Akkreditierungsstelle) gelisteten Zertifizierungsstelle geführt werden.

9.1.1.1.3 Kombination aus CISA und CISSP

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

9.1.1.2 Zusatzqualifikation „Sicherheitsgutachter Telematikinfrastruktur"

Die gematik bietet eine Zusatzqualifikation zu spezifischen Themen der Telematikinfrastruktur an. Hierbei handelt es sich um eine kompakte Schulung – insbesondere zur Gesetzeslage, den speziellen Datenschutzaspekten sowie den technologischen Grundlagen inkl. Sicherheitsarchitektur der Telematikinfrastruktur. Die Schulung schließt mit einer Prüfung ab. Erst mit Bestehen dieser Prüfung (Zertifikat) ist die Zusatzqualifikation erfolgreich absolviert. Die Gültigkeit ist auf 3 Jahre beschränkt und deren Aufrechterhaltung an weitere Bedingungen geknüpft.

Die konkreten Details insbesondere zur Gültigkeit sind unter

https://fachportal.gematik.de/service/sicherheitsgutachter/ veröffentlicht.

Der Sicherheitsgutachter muss gegenüber der gematik zusätzlich zur geforderten Basisqualifikation das erfolgreiche Absolvieren und die Gültigkeit der Zusatzqualifikation „Sicherheitsgutachter TI" nachweisen.

Abbildung 1 fasst die notwendigen Qualifikationen für Sicherheitsgutachter zusammen:

Abbildung 1: Anforderungen an die Qualifikation von Sicherheitsgutachtern

9.1.2 Produktgutachter

9.1.2.1 Basisqualifikation

9.1.2.1.1 Allgemein

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

- Implementierung/Prüfung von Virtualisierungs- und Containerlösungen
- Durchführung von Penetrationstests, und
- Analyse von Quellcode in Hinblick auf Sicherheitsaspekte.

Als Nachweis für die Qualifikation auf dem jeweiligen Gebiet wird eine Berufserfahrung von je mindestens 2 Jahren oder die Vorlage entsprechender Personen-Zertifizierungen vorausgesetzt.

Die Nachweise sind im Produktgutachten geeignet festzuhalten und per Unterschrift vom Produktgutachter und vom Sicherheitsgutachter (siehe 9.2) zu bestätigen. Tritt der Sicherheitsgutachter selbst als Produktgutachter auf, sind die Nachweise ebenso erforderlich und per Unterschrift von Erst- und Zweitgutachter zu bestätigen (siehe 9.2).

9.1.2.1.2 Begutachtung von Frontends des Versicherten

Für die Begutachtung von Frontends des Versicherten (FdV, Apps für Versicherte) müssen zudem Kenntnisse im Bereich App-Testing nachgewiesen werden, wobei auch eine Berufserfahrung von mindestens 2 Jahren vorausgesetzt wird. Zudem müssen Produktgutachter, die ein FdV begutachten vom Bundesamt für Sicherheit in der Informationstechnik (BSI)

- entweder als IS-Penetrationstester
- oder als CC-Evaluator

anerkannt sein.

Die Anerkennungsnachweise des BSI sind dem Gutachten beizufügen und die Nachweise zur Erfahrung im Bereich App-Testing sind im Produktgutachten geeignet festzuhalten und per Unterschrift vom Produktgutachter und vom Sicherheitsgutachter (siehe 9.2) zu bestätigen. Tritt der Sicherheitsgutachter selbst als Produktgutachter auf, sind die Nachweise ebenso erforderlich und per Unterschrift von Erst- und Zweitgutachter zu bestätigen (siehe 9.2).

9.1.2.2 Zusatzqualifikation „Sicherheitsgutachter Telematikinfrastruktur"

Die Zusatzqualifikation „Sicherheitsgutachter TI" ist für den Produktgutachter nicht notwendig.

9.1.3 Hinzugezogene Fachexperten

Für die Prüfung von Anforderungen aus speziellen Fachgebieten, die nicht notwendigerweise im Kompetenzbereich der Gutachter liegen ist es gestattet und auch erwünscht entsprechende Fachexperten hinzuzuziehen. Bei Sicherheitsgutachten können dies bspw. Experten zum Datenschutz sein (da dieses Thema nicht zwingend durch die Basisqualifikation abgedeckt ist). Bei Produktgutachten kann es sinnvoll sein für Penetrationstests und Quellcode-Prüfung weitere Experten hinzuzuziehen.

Für diese Fachexperten ist kein Nachweis einer Qualifikation im Gutachten notwendig, jedoch muss kenntlich gemacht werden, welche Prüfungen durch diese Experten durchgeführt wurden. Insgesamt soll der Teil der Prüfung, die durch hinzugezogene Experten durchgeführt wurden, nicht den Teil der Prüfungen überschreiten, die durch die verantwortlichen Gutachter durchgeführt wurden, da diese eine eigenverantwortliche Bewertung des Prüfobjekts vornehmen müssen.

9.2 Vier-Augen-Prinzip

Zur Förderung der Unabhängigkeit und Objektivität müssen stets (mindestens) zwei Gutachter an der Erstellung eines Gutachtens beteiligt sein („Vier-Augen-Prinzip").

Der Sicherheitsgutachter – gemäß Abschnitt 9.1.1 – tritt sowohl bei einem Sicherheitsgutachten als auch bei einem Produktgutachten als Erstgutachter auf.

Der Zweitgutachter wird vom Sicherheitsgutachter hinzugezogen.

9.2.1 Sicherheitsgutachten

Im Falle eines Sicherheitsgutachtens muss der Zweitgutachter mindestens die Basisqualifikation entsprechend Abschnitt 9.1.1.1 aufweisen, deren Nachweis in Kopie

dem Gutachten beizulegen ist.

Der Hauptanteil der Prüfungen ist bei einem Sicherheitsgutachten vom Erstgutachter durchzuführen.

9.2.2 Produktgutachten

Im Falle eines Produktgutachtens muss der Zweitgutachter ein Produktgutachter entsprechend Abschnitt 9.1.2 sein (eine Basisqualifikation entsprechend Abschnitt 9.1.1.1 ist dann für den Produktgutachter nicht notwendig). Der Sicherheitsgutachter muss als Erstgutachter anhand der Eigenschaften des Prüfgegenstandes beurteilen, welche Qualifikationen der Produktgutachter im konkreten Fall aufweisen muss (siehe Abschnitt 9.1.2.1). Die Qualifikation des Produktgutachters ist im Produktgutachten durch Zertifikate oder Darstellung der relevanten Berufserfahrungen in kurzer, tabellarischer Form festzuhalten und von beiden Gutachtern mittels 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 entsprechend Abschnitt 9.1.1.1 hinzuzuziehen.

Der Hauptanteil der Prüfungen ist bei einem Produktgutachten immer vom Produktgutachter durchzuführen – auch wenn dieser nicht als Erstgutachter auftritt.

9.2.3 Allgemeines

Die Zugehörigkeit des zweiten Gutachters zu einem anderen Unternehmen wird nicht vorausgesetzt.

Weitere Experten können entsprechend Abschnitt 9.1.3 hinzugezogen werden, tragen aber nicht zum hier geforderten Vier-Augen-Prinzip bei, sofern sie nicht die genannten Qualifikationen vorweisen können.

Lediglich im Fall von kleineren Nachbegutachtungen auf Grund von Änderungen am Prüfobjekt (Delta-Gutachten) kann vom Vier-Augen-Prinzip abgewichen werden, wobei dies im Gutachten nachvollziehbar zu begründen ist.

9.3 Unabhängigkeit und Objektivität

Die Gutachter müssen im Rahmen der Zulassung gegenüber der gematik schriftlich durch Eigenerklärung bestätigen, dass sie unabhängig und objektiv prüfen und im Zeitraum von 24 Monaten vor der Prüfung eines Prüfobjektes nicht beratend oder ausführend an der Konzeption, Erstellung oder Konfiguration des Prüfobjektes beteiligt waren. Diese Erklärung muss im Gutachten dokumentiert werden.

10 Beurteilung des Gutachtens durch die gematik

Die gematik beurteilt das Gutachten im Rahmen des Zulassungsverfahrens der entsprechenden Zulassungsobjekte. Dabei werden die in den nachfolgenden Kapiteln (Abschnitt 10.1 bis 10.4) aufgeführten Kriterien bewertet.

10.1 Vollständig

Beurteilt wird, ob alle in diesem Dokument vorgegebenen Anforderungen und Kriterien an ein Gutachten erfüllt sind, ob alle Anforderungen des Steckbriefes geprüft wurden und ob das Vorgehen und die entsprechenden Prüfergebnisse im Gutachten dokumentiert sind.

10.2 Sorgfältig

Geprüft wird, ob das Gutachten auf eine gründlich durchgeführte Prüfung schließen lässt, in dem der Stand der Technik und Best Practices berücksichtigt wurden.

10.3 Objektiv

Geprüft wird, ob das Gutachten auf eine Prüfung schließen lässt, die sachlich, wertfrei, unvoreingenommen, unabhängig und frei von spezifischen Interessen sind.

10.4 Nachvollziehbar

Geprüft wird, ob ein sachverständiger Dritter anhand der Dokumentation der Prüfung zu einer vergleichbaren Schlussfolgerung kommen würde.

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CISA	Certified Information Systems Auditor (Zertifizierung der Information Systems Audit and Control Association (ISACA))
CISSP	Certified Information Systems Security Professional (Zertifizierung vom International Information Systems Security Certification Consortium (auch: (ISC)²)
DAkkS	Deutsche Akkreditierungsstelle

A2 – Glossar

Das Glossar wird als eigenständiges Dokument auf der Website der gematik (Fachportal) zur Verfügung gestellt.

A3 – Abbildungsverzeichnis

A4 – Referenzierte Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI]	BSI: BSI-Standard 200-2, IT-Grundschutz-Methodik.
[BSIInfRev]	BSI: Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz.
[BSI_LF_PT]	BSI: Ein Praxis-Leitfaden für IS-Penetrationstests.
[IDWPS320]	IDW (2004): Prüfungsstandard 320: Verwendung der Arbeit eines anderen externen Prüfers.
[IDWPS330]	IDW (2002): Prüfungsstandard 330: Abschlussprüfung bei Einsatz von Informationstechnologie.
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels, S. Bradner.