Zum Produktgutachten E-Rezept-Frontend des Versicherten (E-Rezept-App)

Berlin, Juli 2021 – Für die gematik sind externe Sicherheitsgutachten ein essentieller Nachweis der Erfüllung der Sicherheitsanforderungen in allen von ihr spezifizierten Produkttypen. Diese Sicherheitsgutachten werden durch von der gematik akkreditierte Gutachter erstellt. Bei technisch komplexeren Produkttypen fordert die gematik zusätzlich ein Produktgutachten. Die Gutachter hier müssen zusätzlich vom Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannt sein.

Im Fall des E-Rezept-Frontend des Versicherten (eRp-FdV), auch E-Rezept-App genannt, hat die gematik beide Gutachten eingefordert. Hier besteht für die gematik die gesetzliche Pflicht, nach § 360 Abs. 10 ein Gutachten zu erstellen und dieses durch das BSI bestätigen zu lassen.

Eine Veröffentlichung ist nicht verpflichtend vorgesehen. Die gematik hat sich in Abstimmung mit ihren Gesellschaftern freiwillig dazu entschieden, das Produktgutachten (im Folgenden kurz als Gutachten bezeichnet) zur Vertrauensbildung und Transparenz zu veröffentlichen. Zusätzlich veröffentlicht sie – siehe weitere Anlagen – die Zusammenfassung aus den Produktgutachten des Fachdienstes und des Identity Providers (IDP) sowie die Ergebnisse des Penetrationstests für das gesamte System. Der Penetrationstest wurde ebenfalls durch externe Prüfer durchgeführt, die von der gematik beauftragt wurden. Darüber hinaus hat die gematik sichergestellt, dass der vollständige Quellcode für die Apps (in den Versionen für iOS und Android), den Fachdienst sowie den IDP veröffentlicht wird. Auch dies geschieht im Geiste einer größtmöglichen Offenheit.

Das Gutachten betrachtet sowohl die Anforderungen der gematik als auch jene des BSI an die Sicherheit der E-Rezept-App. Grundsätzlich veröffentlicht die gematik Anforderungen an alle Produkttypen auf ihrem Fachportal (https://fachportal.gematik.de/). Das BSI hat seine Anforderungen speziell für das E-Rezept in einer Prüfrichtlinie beschrieben, deren Inhalt im Gutachten

wiedergegeben wird. Die Prüfrichtlinie entspricht im Wesentlichen der Technischen Richtlinie „Sicherheitsanforderungen an digitale Gesundheitsanwendungen" (BSI TR 03161).

Die Gutachter besagen in ihrem Votum hinsichtlich der Anforderungen der gematik: „Die Produktgutachter sind der Auffassung, dass das eRp-FdV (…) den sicherheitstechnischen sowie datenschutzrechtlichen Anforderungen der gematik entsprechen und somit geeignet sind, Teil der TI (…) zu werden. Einer kontrollierten Inbetriebnahme in den Produktionsbetrieb steht aus Sicht der Gutachter nichts im Wege." (vgl. Gutachten, Abschnitt 1.3)

Bezüglich der Erfüllung der Prüfvorschrift des BSI schreiben die Gutachter: „Bei der Prüfung der Sicherheit der Anwendung haben wir technisch implementierte Anforderungen hinsichtlich ihrer Wirksamkeit analysiert und deren Effektivität bewertet. Dabei konnten wir kein Versagen feststellen." (vgl. Gutachten, Abschnitt 3.9)

In Bezug auf die gematik-Anforderungen wurden keine Sicherheitslücken festgestellt (vgl. Gutachten, Abschnitt 3.8.2). Es wurden lediglich acht Empfehlungen ausgesprochen, die derzeit durch die gematik umgesetzt werden. Bei den Anforderungen aus der BSI-Prüfvorschrift stellen die Gutachter fest, dass 23 Anforderungen nicht erfüllt werden. Die Gutachter haben für jede dieser Abweichungen eine Risikoanalyse durchgeführt und sind zu dem Urteil gelangt, dass das hieraus entstehende Risiko akzeptabel ist. Das BSI erklärt in seinem Bestätigungsschreiben hierzu: „Diese Restrisiken sind in einem begrenzten Test- oder Probebetrieb hinnehmbar unter der Voraussetzung, dass alle Teilnehmer an der Testphase darüber informiert werden, dass das FdV noch nicht in seiner endgültigen Fassung vorliegt und deshalb vom BSI Sicherheitsrisiken niedrigen Umfangs festgestellt wurden, die bis zum Produktivbetrieb zu beheben sind." Die gematik sieht eine entsprechende Begleitinformation für Nutzer der E-Rezept-App vor. Diese Information wird in den jeweiligen App-Stores veröffentlicht.

Für zehn dieser Abweichungen hat das BSI die Auflage erteilt, dass entsprechende Maßnahmen zur Behebung bis 31.12.2021 umgesetzt werden sollen beziehungsweise müssen. Die gematik plant die Umsetzung der

Maßnahmen und wird die Umsetzung wiederum durch externe Gutachter prüfen lassen. Darüber hinaus empfiehlt das BSI bei drei Abweichung, dass eine Klärung mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) durch die gematik angestrebt werden sollte. Hierbei handelt es sich um den Einsatz von Google SafetyNet unter anderem zur Feststellung der Integrität und Authentizität der App selbst. Grundsätzlich hat das BSI selbst aus Sicht der IT-Sicherheit keine Bedenken gegen Google SafetyNet. Laut BSI ist der Einsatz des Service bei Apps Im Bankensektor üblich.

Die Ergebnisse des BSI zu den Abweichungen können dem BSI-Prüfbericht über das Frontend-des-Versicherten E-Rezept der gematik entnommen werden, der mit diesem Gutachten veröffentlicht wird.

Kontakt: Pressestelle gematik GmbH – Tel. +49 (0) 30 40041-441 – presse@gematik.de

Inhalt

Produktgutachten

eRezept-Frontend des Versicherten

gematik GmbH

Dokumentenart: Gutachten

Autor: XXXXXXXXXXXXXXX

Version: 1.2

Status: Freigegeben

Inhaltsverzeichnis

Abkürzungsverzeichnis

eRp	Elektronisches Rezept
FdV	Frontend des Versicherten
GdV	Gerät des Versicherten
gematik	Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
ISMS	Informationssicherheitsmanagementsystem
PwC	PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft
TI	Telematikinfrastruktur

Glossar

Für fachlich relevante Beschreibungen wird auf das von der gematik erstellte Glossar in Version 5.0.0 [gemGlossar_V5.0.0] verwiesen. Es wurden im Rahmen des Produkt- und Sicherheitsgutachtens darüber hinaus keine Begrifflichkeiten verwendet, die eine Erläuterung in einem Glossar erforderlich machen.

Abbildungsverzeichnis

Tabellenverzeichnis

Dokumentenhistorie

Version	Datum	Änderung	Autor
0.1	28.05.2021	Initiale Erstellung	XXXXXXXXXXXXXXX
1.0	31.05.2021	Freigabe	XXXXXXXXXXXXXXX
1.1	09.06.2021	Hinzufügen Anhang 4.6 und kleinere redaktionelle Anpassungen	XXXXXXXXXXXXXXX
1.2	23.06.2021	Überarbeitung Anhang 4.7 (ehemals 4.6) und Ergänzung der Risikomanagementmethodik unter 4.6	XXXXXXXXXXXXXXX

1 Management Summary

1.1 Aufgabenstellung

Die gematik GmbH (im Folgenden „gematik“ genannt) beauftragte die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft (im Folgenden „PwC“ genannt) mit der Erstellung eines Produktgutachtens für das elektronische Rezept - Frontend des Versicherten (im Folgenden „eRp-FdV“ genannt), das von der gematik erstellt und vertrieben wird. Das Produktgutachten umfasst dabei ausschließlich die genannten Anforderungen gemäß

- Prüfvorschrift “**E-Rezept-Frontend des Versicherten**” in der Produkttypversion 1.2.0-0, Version 1.0.0 vom 19. Februar 2021 [gemProdT_eRp_FdV_PTV_1.2.0-0]

sowie im Rahmen der Prüfung des Identity Provider Authentisierungsmoduls, das Teil des eRp-FdVs ist, die Anforderungen gemäß

- Prüfvorschrift “**Identity Provider - Authentisierungsmodul**” in der Produkttypversion 1.0.0-0, Version 1.0.0 vom 18. Mai 2021 [gemProdT_IDP-AuthModul_PTV_1.0.0-0],

wobei in Bezug auf [gemProdT_IDP-AuthModul_PTV_1.0.0-0] für Android nur die ersten fünfzehn (15) sowie letzten beiden (2) Anforderungen relevant sind, für iOS hingegen die gesamte Liste der Anforderungen für das Produktgutachten.

Die E-Rezept App ist die Frontend-Schnittstelle für den Versicherten. Sie nutzt die Backendsysteme Identitätsprovider, Fachdienst und Apothekenverzeichnis. Leistungserbringer haben eigene Schnittstellen zu den Backendsystemen und bringen über diese Schnittstellen Daten in das Gesamtsystem ein.

Beispiel für einen konkreten Prozessablauf des Gesamtsystems E-Rezept: Ein Arzt stellt einem Versicherten ein Rezept ein. Das Rezept wird im Fachdienst abgelegt. Der Versicherte greift auf das Rezept mit der E-Rezept App zu. Der Versicherte weist einem Apotheker das Rezept über Anzeige eines DataMatrix-Codes zu, die der Apotheker scannt. Der Apotheker greift mit Hilfe des DataMatrix-Codes auf das Rezept im Fachdienst zu und dispensiert das Medikament.

Ausführungsumgebung des FdV ist ein Gerät des Versicherten (GdV), bspw. ein stationäres Gerät oder ein mobiles Endgerät. Es steht unter alleiniger Kontrolle des Versicherten. Dem Versicherten obliegt es, durch geeignete Maßnahmen die Sicherheit der Daten zu stärken.

Das eRp-FdV kann zusätzliche Funktionalitäten anbieten, die nicht der Fachanwendung eRp zugeordnet werden und somit nicht der Regelungshoheit der gematik unterliegen.

Für die Durchführung des Auftrags und unsere Verantwortlichkeit sind, auch im Verhältnis zu Dritten, die diesem Bericht in den Anlagen beigefügten Allgemeinen Auftragsbedingungen vom 1. Januar 2017 vereinbart.

1.2 Wesentliche Feststellungen

Es konnte kein Sicherheitsmangel in Bezug auf die von der gematik definierten Anforderungen festgestellt werden. PwC spricht acht (8) Empfehlungen aus, welche die Implementierung des FdV betreffen, aber keinen Sicherheitsmangel darstellen.

Ein übergreifendes Informationssicherheitsmanagementsystem (im Folgenden „ISMS“ genannt) wird betrieben. Die notwendigen Aktivitäten eines ISMS, wie beispielsweise

- Durchführung von internen Audits,
- Durchführung von Risikoanalysen,
- Behandlung von Sicherheitsvorfällen,
- Unterstützung der Bereiche der gematik in sicherheitstechnischen Fragestellungen und

- Berichterstattung an den Vorstand

sind in angemessener Form, insbesondere in Bezug auf das Prüfobjekt, etabliert.

Insbesondere lässt sich feststellen, dass die Entwicklung und Anpassung des eRp-FdV in das vorhandene ISMS integriert ist.

1.3 Prüfergebnis (inkl. Votum)

Die Produktgutachter sind der Auffassung, dass das eRp-FdV und die normativen Festlegungen, beziehungsweise Anforderungen zur Telematikinfrastruktur (im Folgenden “TI“ genannt) des deutschen Gesundheitswesens für den Online-Produktivbetrieb, nach reiflicher Begutachtung und Bewertung den sicherheitstechnischen sowie datenschutzrechtlichen Anforderungen der gematik entsprechen und somit geeignet sind, Teil der TI des Produkttyp **eRp-FdV** einschließlich der durch ihn bereitgestellten Schnittstellen zu werden. Einer kontrollierten Inbetriebnahme in den Produktionsbetrieb steht aus Sicht der Gutachter nichts im Wege.

2 Grundlagen der Prüfung

Sämtliche Änderungen an Prozessen und Komponenten, die eine Auswirkung auf die sicherheitstechnische und datenschutzrechtliche Eignung des eRp-FdV haben können, sind proaktiv durch den Antragsteller an die Produkt- und Sicherheitsgutachter zu melden und anschließend im Rahmen einer Deltabegutachtung neu zu bewerten.

Im Produktgutachten werden ausschließlich die zum Zeitpunkt der Prüfung von der gematik freigegebenen Anforderungen berücksichtigt. Werden im Zuge weiterer Entwicklungen der TI ergänzende Anforderungen an den Antragsteller gestellt, welche das FdV betreffen, ist auch dies an den Gutachter zu melden und die ergänzenden Anforderungen im Rahmen einer Deltabegutachtung zu bewerten.

Im Folgenden sind die Grundlagen der Prüfung beschrieben.

2.1 Prüfauftrag

Am 24. März 2021 beauftragte der Antragsteller einen Produktgutachter mit der Erstellung eines Produktgutachtens (Vollgutachten) für das eRp-FdV zur Bestätigung der sicherheitstechnischen und datenschutzrechtlichen Eignung gemäß den Anforderungen der gematik auf Basis der Begutachtung eRp-FdV in der Version 1.0.0 vom 19.02.2021 [gemProdT_ePA_FdV_PTV_1.2.0-0].

Der Antragsteller ist die **gematik GmbH**. Primärer Ansprechpartner ist:

Name	Rolle	Kontaktdaten
Birgit Wilhalm	Hauptansprechpartnerin, Prüfung und Audit	gematik GmbH Friedrichstraße 136 10117 Berlin E-Mail: birgit.wilhalm@gematik.de Telefon: +49 30 40041-366

Der Prüfauftrag wurde PwC erteilt. Als Produktgutachter wurden die folgenden, durch die gematik bestätigten Gutachter, eingesetzt:

Name	Rolle	Kontaktdaten
XXXXXXXXXXXXXXX	Erstgutachter, Sicherheitsgutachter	PwC GmbH Wirtschaftsprüfungsgesellschaft XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX
XXXXXXXXXXXXXXX	Zweitgutachter, Produktgutachter	PwC Cyber Security Services GmbH XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX

2.2 Bezeichnung des Prüfobjektes

Das Prüfobjekt umfasst die Sicherheit für den Produkttyp eRp-FdV. Explizit **nicht** im Begutachtungsrahmen enthalten sind der Identitätsproviderdienst, der Fachdienst und das Apothekenverzeichnis. Der Produkttyp besteht aus den folgenden Komponenten:

- E-Rezept Frontend des Versicherten,
- Authenticator Modul

Eine detaillierte Beschreibung des Prüfobjekts ist in Abschnitt 3.1 enthalten.

2.3 Zielsetzung und Umfang der Prüfung

Das Ziel der Prüfung ist es, zu bewerten, ob und inwieweit der Antragsteller für das Prüfobjekt die von der gematik definierten Anforderungen an die Sicherheit für den Produkttyp "**eRp-Frontend des Versicherten"** einschließlich der durch ihn bereitgestellten Schnittstellen umgesetzt hat.

Die Prüfung umfasst dabei alle Anforderungen (Vollgutachten) gemäß:

- Prüfvorschrift "**E-Rezept-Frontend des Versicherten**" in der Produkttypversion 1.2.0-0, Version 1.0.0 vom 19. Februar 2021 [gemProdT_eRp_FdV_PTV_1.2.0-0]

sowie im Rahmen der Prüfung des Identity Provider Authentisierungsmoduls die Anforderungen gemäß

- Prüfvorschrift "**Identity Provider - Authentisierungsmodul**" in der Produkttypversion 1.0.0-0, Version 1.0.0 vom 18. Mai 2021 [gemProdT_IDP-AuthModul_PTV_1.0.0-0],

wobei in Bezug auf [gemProdT_IDP-AuthModul_PTV_1.0.0-0] für Android nur die ersten fünfzehn (15) sowie letzten beiden (2) Anforderungen relevant sind, für iOS hingegen die gesamte Liste der Anforderungen für das Produktgutachten.

2.4 Zeitraum der Prüfung

Die Begutachtung und Bewertung der Sicherheit für den Produkttyp **eRp-FdV** erfolgte im Zeitraum vom 25.03.2021 bis 27.05.2021 durch die von der gematik zugelassenen Sicherheitsgutachter für zentrale Produkte der Telematikinfrastruktur.

3 Detaillierte Beschreibung der Prüfung

3.1 Beschreibung des Prüfobjektes

Die E-Rezept App ist die Frontend-Schnittstelle für den Versicherten. Sie nutzt die Backendsysteme Identitätsprovider, Fachdienst und Apothekenverzeichnis. Leistungserbringer haben eigene Schnittstellen zu den Backendsystemen und bringen über diese Schnittstellen Daten in das Gesamtsystem ein.

Beispiel für einen konkreten Prozessablauf des Gesamtsystems E-Rezept: Ein Arzt stellt einem Versicherten ein Rezept ein. Das Rezept wird im Fachdienst abgelegt. Der Versicherte greift auf das Rezept mit der E-Rezept App zu. Der Versicherte weist einem Apotheker das Rezept über Anzeige eines DataMatrix-Codes zu, die der Apotheker scannt. Der Apotheker greift mit Hilfe des DataMatrix-Codes auf das Rezept im Fachdienst zu und dispensiert das Medikament.

Inkremente des Produktes

Das Produkt besteht aus zwei Inkrementen: einer iOS Applikation und einer Android Applikation. Die Inkremente werden über über den Apple AppStore und den Google Play Store bereitgestellt. Ferner wird die Android Version auch in die Huawei App Gallery ausgespielt.

Die Applikationen sind kompatibel zu den Mindestversionen iOS 14 und Android API Level 23.

Funktionen des Produktes

Rezepte fotografieren

Der Versicherte kann von seinem Arzt papierbehaftete Rezepte erhalten. Diese verfügen über einen DataMatrix-Code. Dieser Code kann mit der E-Rezept App fotografiert werden. In der App kann der Code gespeichert und angezeigt werden. Der Nutzer kann in einer Apotheke diesen Code auf dem Telefon anzeigen, und somit sein Medikament beziehen.

Rezepte vom Fachdienst abholen

Auf dem Fachdienst eingestellte Rezepte kann der Nutzer in die App laden und auf dem Telefon laden. Hierzu muss er sich am Identitätsprovider autorisieren und mit dieser Autorisierung die Rezepte vom Fachdienst abrufen.

Rezepte an Apotheke zuweisen

Vom Fachdienst geholte Rezepte können an Apotheken unter Nutzung des Fachdienstes übermittelt werden. Der Nutzer kann somit verbindliche Reservierungen oder Bestellungen via Versand beauftragen.

Rezeptverwaltung

Rezepte können gelöscht werden. Vom Fachdienst können auch Protokolldaten zu Rezepten geladen und angezeigt werden.

Convenience Funktionen

Die App bietet übliche Nutzungsfunktionen wie das Absichern des Starts mit Biometrie, Fehlermeldungen usw.

Technischer Überblick

Gesamtüberblick

Das Schaubild zeigt das Gesamtsystem E-Rezept. Das in diesem Dokument fokussierte Produkt ist das in der Personal Zone befindliche Frontend des Versicherten.

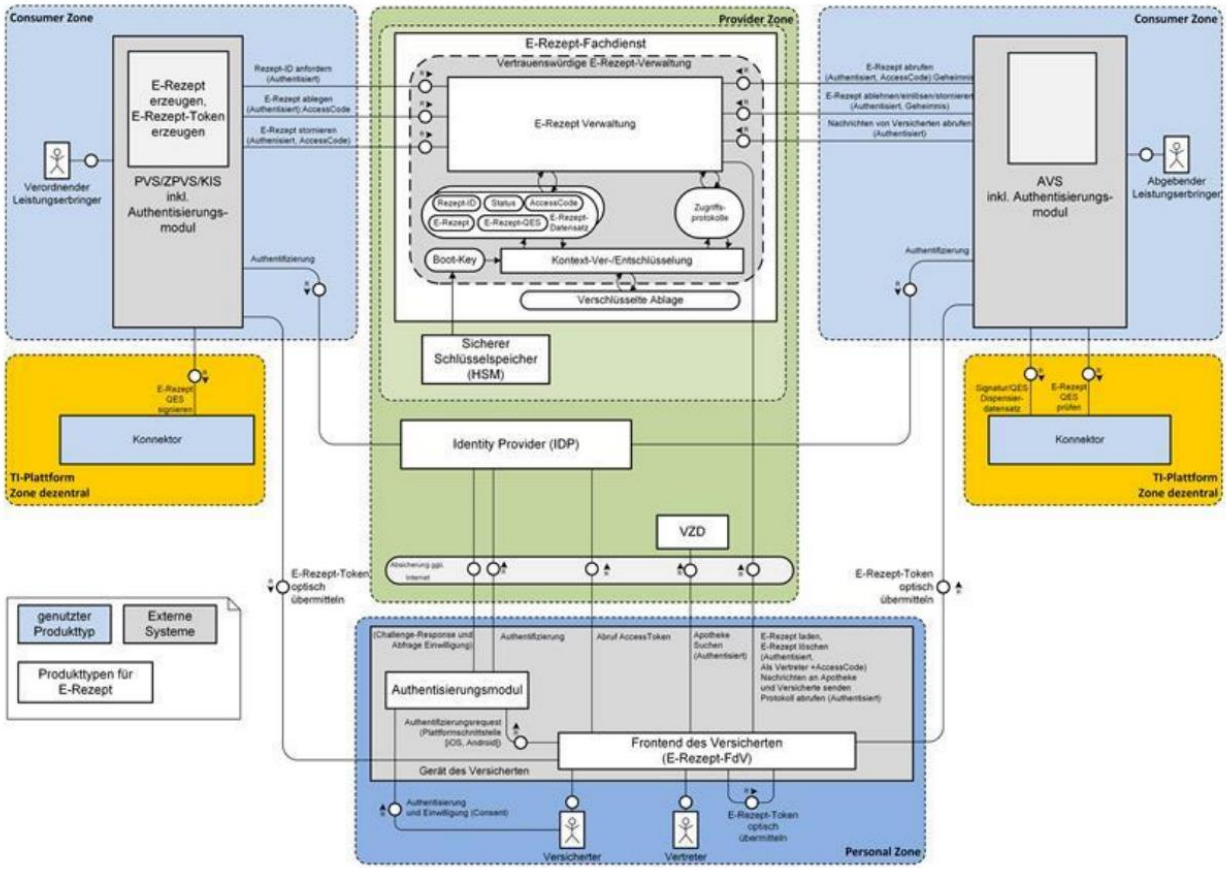

Abbildung 1: Gesamtsystem E-Rezept

Technischer Überblick FdV

In dem Gesamtschaubild werden in der Personal Zone auf dem Gerät des Versicherten zwei Komponenten visualisiert: das E-Rezept FdV und das Authentisierungsmodul. Dieses sind technisch nicht getrennt; beide architektonischen Komponenten sind integriert in der „E-Rezept App“ und somit dem „FdV“.

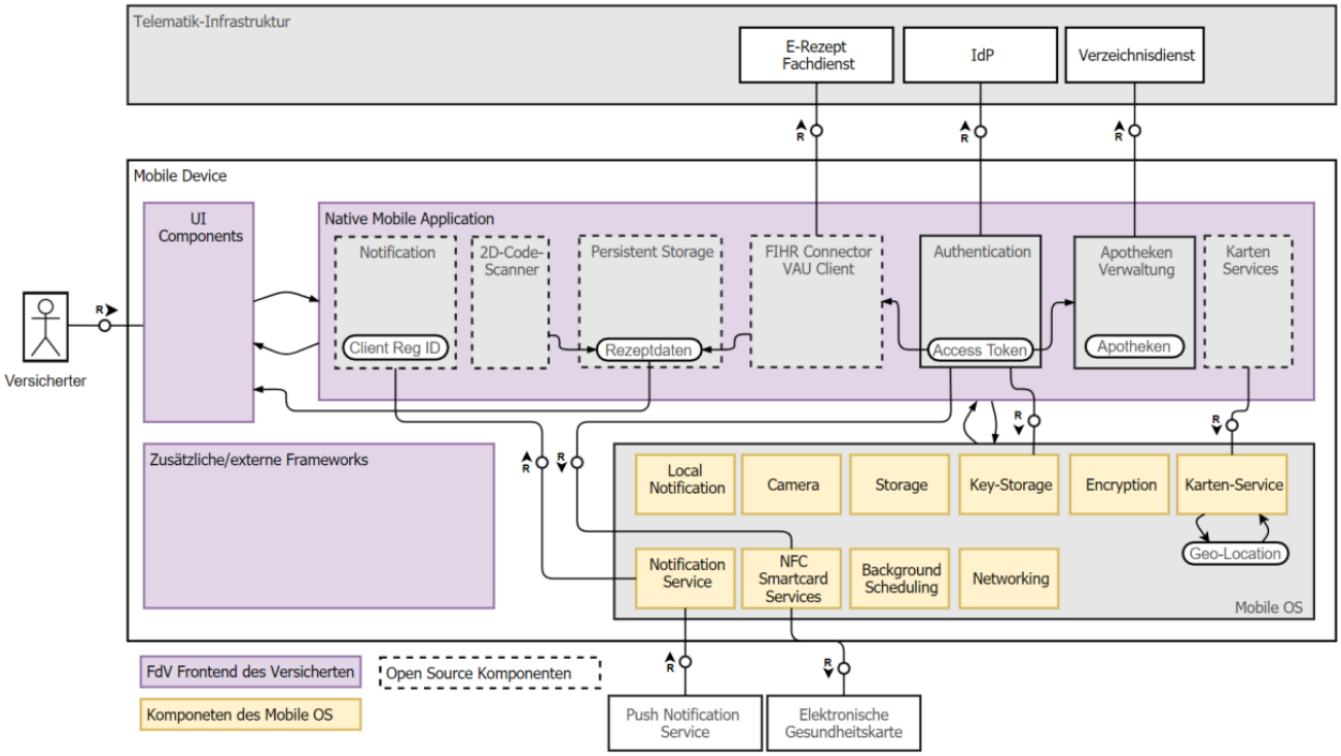

Abbildung 2: Gesamtschaubild FdV

Die dargestellte Funktionsblock-Übersicht stellt einen geplanten Zielzustand dar. Nicht den zum 01. Juli 2021 in Produktion gehenden. So sind Notification und Kartenservices nicht Bestandteil der Version 1.0.

3.2 Beschreibung des Prüfplans

Im Folgenden ist der Prüfplan für die Begutachtung beschrieben.

Tabelle 1: Prüfplan

#	Datum	Thema	Anforderungen	Verantwortlich
1	25.03.2021	Kick-Off Termin	keine Anforderungen	XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX
2	08.04.2021 – 27.05.2021	Evidenzenprüfung/Penetrationstest/ Dokumentenprüfung	alle Anforderungen	XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX
3	19.04.2021	Evidenzenprüfung/Dokumentenprüfung	A_19086	XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX
4	20.04.2021	Evidenzenprüfung/Dokumentenprüfung	A_19087	XXXXXXXXXXXXXXX
5	04.05.2021	Evidenzenprüfung/Dokumentenprüfung	A_19088	XXXXXXXXXXXXXXX
6	04.05.2021	Evidenzenprüfung/Dokumentenprüfung	A_19089	XXXXXXXXXXXXXXX
7	03.05.2021	Penetrationstest/Dokumentenprüfung	A_19090	XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX
8	04.05.2021	Penetrationstest/Dokumentenprüfung	A_19091	XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX
9	26.04.2021	Penetrationstest/Dokumentenprüfung	A_19092	XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX
10	26.04.2021	Penetrationstest/Dokumentenprüfung	A_19093	XXXXXXXXXXXXXXX
11	04.05.2021	Penetrationstest/Dokumentenprüfung	A_19094	XXXXXXXXXXXXXXX
12	05.05.2021	Penetrationstest/Dokumentenprüfung	A_19095	XXXXXXXXXXXXXXX
13	04.05.2021	Penetrationstest/Dokumentenprüfung	A_19096	XXXXXXXXXXXXXXX
14	26.04.2021	Penetrationstest/Dokumentenprüfung	A_19097	XXXXXXXXXXXXXXX
15	19.04.2021	Penetrationstest/Dokumentenprüfung	A_19177	XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX
16	13.05.2020	Penetrationstest/Dokumentenprüfung	A_19178	XXXXXXXXXXXXXXX
17	03.05.2021	Penetrationstest/Dokumentenprüfung	A_19179	XXXXXXXXXXXXXXX
18	20.05.2021	Penetrationstest/Dokumentenprüfung	A_19181	XXXXXXXXXXXXXXX
19	12.05.2021	Evidenzenprüfung/Dokumentenprüfung	A_19182	XXXXXXXXXXXXXXX
20	10.05.2021	Penetrationstest/Dokumentenprüfung	A_19183	XXXXXXXXXXXXXXX
21	26.04.2021	Penetrationstest/Dokumentenprüfung	A_19184	XXXXXXXXXXXXXXX
22	06.05.2021	Penetrationstest/Dokumentenprüfung	A_19185	XXXXXXXXXXXXXXX

#	Datum	Thema	Anforderungen	Verantwortlich
23	19.04.2021	Penetrationstest/Dokumentenprüfung	A_19186	XXXXXXXXXXXXXXX
24	17.05.2021	Penetrationstest/Dokumentenprüfung	A_19187	XXXXXXXXXXXXXXX
25	15.04.2021	Penetrationstest/Dokumentenprüfung	A_19188	XXXXXXXXXXXXXXX
26	23.04.2021	Penetrationstest/Dokumentenprüfung	A_19215	XXXXXXXXXXXXXXX
27	30.04.2021	Penetrationstest/Dokumentenprüfung	A_19229	XXXXXXXXXXXXXXX
28	14.04.2021	Penetrationstest/Dokumentenprüfung	A_19480	XXXXXXXXXXXXXXX
29	12.05.2021	Penetrationstest/Dokumentenprüfung	A_19739	XXXXXXXXXXXXXXX
30	16.04.2021	Penetrationstest/Dokumentenprüfung	A_19979	XXXXXXXXXXXXXXX
31	26.04.2021	Penetrationstest/Dokumentenprüfung	A_19980	XXXXXXXXXXXXXXX
32	26.04.2021	Penetrationstest/Dokumentenprüfung	A_19981	XXXXXXXXXXXXXXX
33	17.05.2021	Penetrationstest/Dokumentenprüfung	A_19982	XXXXXXXXXXXXXXX
34	22.04.2021	Penetrationstest/Dokumentenprüfung	A_19983	XXXXXXXXXXXXXXX
35	05.05.2021	Penetrationstest/Dokumentenprüfung	A_19984	XXXXXXXXXXXXXXX
36	11.05.2021	Penetrationstest/Dokumentenprüfung	A_20033	XXXXXXXXXXXXXXX
37	06.05.2021	Penetrationstest/Dokumentenprüfung	A_20167	XXXXXXXXXXXXXXX
38	13.05.2021	Penetrationstest/Dokumentenprüfung	A_20172	XXXXXXXXXXXXXXX
39	14.04.2021	Evidenzenprüfung/Dokumentenprüfung	A_20181	XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX
40	20.04.2021	Penetrationstest/Dokumentenprüfung	A_20182	XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX
41	23.04.2021	Penetrationstest/Dokumentenprüfung	A_20183	XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX
42	08.04.2021	Penetrationstest/Dokumentenprüfung	A_20184	XXXXXXXXXXXXXXX
43	17.05.2021	Penetrationstest/Dokumentenprüfung	A_20186	XXXXXXXXXXXXXXX
44	26.04.2021	Penetrationstest/Dokumentenprüfung	A_20187	XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX
45	20.04.2021	Penetrationstest/Dokumentenprüfung	A_20193	XXXXXXXXXXXXXXX
46	20.04.2021	Penetrationstest/Dokumentenprüfung	A_20194	XXXXXXXXXXXXXXX
47	20.04.2021	Penetrationstest/Dokumentenprüfung	A_20206	XXXXXXXXXXXXXXX
48	11.05.2021	Penetrationstest/Dokumentenprüfung	A_20208	XXXXXXXXXXXXXXX
49	10.05.2021	Penetrationstest/Dokumentenprüfung	A_20285	XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX
50	10.05.2021	Penetrationstest/Dokumentenprüfung	A_17124	XXXXXXXXXXXXXXX
51	26.04.2021	Penetrationstest/Dokumentenprüfung	A_17205	XXXXXXXXXXXXXXX
52	29.04.2021	Evidenzenprüfung/Dokumentenprüfung	A_17207	XXXXXXXXXXXXXXX

#	Datum	Thema	Anforderungen	Verantwortlich
53	22.04.2021	Penetrationstest/Dokumentenprüfung	A_17322	XXXXXXXXXXXXXXX
54	10.05.2021	Penetrationstest/Dokumentenprüfung	A_17359	XXXXXXXXXXXXXXX
55	04.05.2021	Penetrationstest/Dokumentenprüfung	A_17775	XXXXXXXXXXXXXXX
56	19.04.2021	Penetrationstest/Dokumentenprüfung	A_18464	XXXXXXXXXXXXXXX
57	23.04.2021	Penetrationstest/Dokumentenprüfung	A_18467	XXXXXXXXXXXXXXX
58	22.04.2021	Penetrationstest/Dokumentenprüfung	A_20309	XXXXXXXXXXXXXXX
59	26.04.2021	Penetrationstest/Dokumentenprüfung	A_20483	XXXXXXXXXXXXXXX
60	17.05.2021	Penetrationstest/Dokumentenprüfung	A_20512	XXXXXXXXXXXXXXX
61	28.04.2021	Penetrationstest/Dokumentenprüfung	A_20529	XXXXXXXXXXXXXXX
62	26.04.2021	Penetrationstest/Dokumentenprüfung	A_20602	XXXXXXXXXXXXXXX
63	17.05.2021	Penetrationstest/Dokumentenprüfung	A_20603	XXXXXXXXXXXXXXX
64	28.04.2021	Penetrationstest/Dokumentenprüfung	A_20605	XXXXXXXXXXXXXXX
65	19.04.2021	Penetrationstest/Dokumentenprüfung	A_20606	XXXXXXXXXXXXXXX
66	23.04.2021	Penetrationstest/Dokumentenprüfung	A_20608	XXXXXXXXXXXXXXX
67	27.04.2021	Penetrationstest/Dokumentenprüfung	A_20623	XXXXXXXXXXXXXXX
68	29.04.2021	Penetrationstest/Dokumentenprüfung	A_20624	XXXXXXXXXXXXXXX
69	17.05.2021	Evidenzenprüfung/Dokumentenprüfung	A_20625	XXXXXXXXXXXXXXX
70	11.05.2021	Penetrationstest/Dokumentenprüfung	A_20740	XXXXXXXXXXXXXXX
71	26.04.2021	Penetrationstest/Dokumentenprüfung	A_20741	XXXXXXXXXXXXXXX
72	27.04.2021	Evidenzenprüfung/Dokumentenprüfung	A_21218	XXXXXXXXXXXXXXX
73	11.05.2021	Evidenzenprüfung/Dokumentenprüfung	A_21222	XXXXXXXXXXXXXXX
74	20.04.2021	Penetrationstest/Dokumentenprüfung	A_21275-01	XXXXXXXXXXXXXXX
75	20.04.2021	Penetrationstest/Dokumentenprüfung	A_21332	XXXXXXXXXXXXXXX
76	06.05.2021	Evidenzenprüfung/Dokumentenprüfung	GS-A_4357	XXXXXXXXXXXXXXX
77	11.05.2021	Penetrationstest/Dokumentenprüfung	GS-A_4361	XXXXXXXXXXXXXXX
78	17.05.2021	Evidenzenprüfung/Dokumentenprüfung	GS-A_4367	XXXXXXXXXXXXXXX
79	30.04.2021	Penetrationstest/Dokumentenprüfung	GS-A_4368	XXXXXXXXXXXXXXX
80	19.04.2021	Penetrationstest/Dokumentenprüfung	GS-A_4385	XXXXXXXXXXXXXXX
81	19.04.2021	Penetrationstest/Dokumentenprüfung	GS-A_4387	XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX
82	19.04.2021	Penetrationstest/Dokumentenprüfung	GS-A_5035	XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX
83	07.05.2021	Penetrationstest/Dokumentenprüfung	GS-A_5322	XXXXXXXXXXXXXXX
84	20.04.2021	Evidenzenprüfung/Dokumentenprüfung	GS-A_5339	XXXXXXXXXXXXXXX

#	Datum	Thema	Anforderungen	Verantwortlich
85	30.04.2021	Penetrationstest/Dokumentenprüfung	GS-A_5526	XXXXXXXXXXXXXXX
86	30.04.2021	Penetrationstest/Dokumentenprüfung	GS-A_5542	XXXXXXXXXXXXXXX
87	20.04.2021	Penetrationstest/Dokumentenprüfung	A_19937	XXXXXXXXXXXXXXX
88	29.04.2021	Penetrationstest/Dokumentenprüfung	A_19938	XXXXXXXXXXXXXXX
89	12.05.2021	Penetrationstest/Dokumentenprüfung	A_20032-01	XXXXXXXXXXXXXXX
90	26.04.2021	Penetrationstest/Dokumentenprüfung	A_20079	XXXXXXXXXXXXXXX
91	14.05.2021	Penetrationstest/Dokumentenprüfung	A_20085	XXXXXXXXXXXXXXX
92	14.05.2021	Penetrationstest/Dokumentenprüfung	A_20161-01	XXXXXXXXXXXXXXX
93	10.05.2021	Penetrationstest/Dokumentenprüfung	A_20174	XXXXXXXXXXXXXXX
94	14.05.2021	Penetrationstest/Dokumentenprüfung	A_20175	XXXXXXXXXXXXXXX
95	14.05.2021	Penetrationstest/Dokumentenprüfung	A_20283	XXXXXXXXXXXXXXX
96	17.05.2021	Evidenzenprüfung/Dokumentenprüfung	A_20526-01	XXXXXXXXXXXXXXX
97	16.05.2021	Evidenzenprüfung/Dokumentenprüfung	A_20614	XXXXXXXXXXXXXXX
98	15.05.2021	Penetrationstest/Dokumentenprüfung	A_21322	XXXXXXXXXXXXXXX
99	18.05.2021	Penetrationstest/Dokumentenprüfung	A_19908-01	XXXXXXXXXXXXXXX
100	17.05.2021	Evidenzenprüfung/Dokumentenprüfung	A_20068-01	XXXXXXXXXXXXXXX
101	17.05.2021	Evidenzenprüfung/Dokumentenprüfung	A_20499	XXXXXXXXXXXXXXX
102	18.05.2021	Penetrationstest/Dokumentenprüfung	A_20525	XXXXXXXXXXXXXXX
103	18.05.2021	Penetrationstest/Dokumentenprüfung	A_20527	XXXXXXXXXXXXXXX
104	18.05.2021	Penetrationstest/Dokumentenprüfung	A_20600	XXXXXXXXXXXXXXX
105	17.05.2021	Penetrationstest/Dokumentenprüfung	A_20601	XXXXXXXXXXXXXXX
106	15.05.2021	Penetrationstest/Dokumentenprüfung	A_20607	XXXXXXXXXXXXXXX
107	17.05.2021	Penetrationstest/Dokumentenprüfung	A_20609	XXXXXXXXXXXXXXX
108	15.05.2021	Penetrationstest/Dokumentenprüfung	A_20617-01	XXXXXXXXXXXXXXX
109	17.05.2021	Evidenzenprüfung/Dokumentenprüfung	A_20618	XXXXXXXXXXXXXXX
110	18.05.2021	Penetrationstest/Dokumentenprüfung	A_20700-07	XXXXXXXXXXXXXXX
111	25.05.2021	Penetrationstest/Dokumentenprüfung	A_21414	XXXXXXXXXXXXXXX
112	19.05.2021	Penetrationstest/Dokumentenprüfung	A_21416	XXXXXXXXXXXXXXX
113	20.05.2021	Penetrationstest/Dokumentenprüfung	A_21431	XXXXXXXXXXXXXXX
114	20.05.2021	Penetrationstest/Dokumentenprüfung	A_21443	XXXXXXXXXXXXXXX
115	26.05.2021	Penetrationstest/Dokumentenprüfung	A_21574	XXXXXXXXXXXXXXX
116	26.05.2021	Penetrationstest/Dokumentenprüfung	A_21576	XXXXXXXXXXXXXXX
117	20.05.2021	Penetrationstest/Dokumentenprüfung	A_21578	XXXXXXXXXXXXXXX

#	Datum	Thema	Anforderungen	Verantwortlich
118	20.05.2021	Penetrationstest/Dokumentenprüfung	A_21579	XXXXXXXXXXXXXXX
119	20.05.2021	Penetrationstest/Dokumentenprüfung	A_21580	XXXXXXXXXXXXXXX
120	20.05.2921	Penetrationstest/Dokumentenprüfung	A_21581	XXXXXXXXXXXXXXX
121	20.05.2021	Penetrationstest/Dokumentenprüfung	A_21582	XXXXXXXXXXXXXXX
122	20.05.2021	Penetrationstest/Dokumentenprüfung	A_21583	XXXXXXXXXXXXXXX
123	20.05.2021	Penetrationstest/Dokumentenprüfung	A_21584	XXXXXXXXXXXXXXX
124	26.05.2021	Penetrationstest/Dokumentenprüfung	A_21585	XXXXXXXXXXXXXXX
125	25.05.2021	Penetrationstest/Dokumentenprüfung	A_21586	XXXXXXXXXXXXXXX
126	20.05.2021	Evidenzenprüfung/Dokumentenprüfung	A_21587	XXXXXXXXXXXXXXX
127	26.05.2021	Penetrationstest/Dokumentenprüfung	A_21588	XXXXXXXXXXXXXXX
128	19.05.2021	Evidenzenprüfung/Dokumentenprüfung	A_21589	XXXXXXXXXXXXXXX
129	19.05.2021	Evidenzenprüfung/Dokumentenprüfung	A_21590	XXXXXXXXXXXXXXX
130	19.05.2021	Evidenzenprüfung/Dokumentenprüfung	A_21591	XXXXXXXXXXXXXXX
131	19.05.2021	Penetrationstest/Dokumentenprüfung	A_21595	XXXXXXXXXXXXXXX
132	25.05.2021	Penetrationstest/Dokumentenprüfung	A_21598	XXXXXXXXXXXXXXX
133	25.05.2021	Penetrationstest/Dokumentenprüfung	A_21600	XXXXXXXXXXXXXXX
134	18.05.2021	Evidenzenprüfung/Dokumentenprüfung	A_21603	XXXXXXXXXXXXXXX
135	18.05.2021	Penetrationstest/Dokumentenprüfung	A_21275-01	XXXXXXXXXXXXXXX
136	18.05.2021	Penetrationstest/Dokumentenprüfung	GS-A_4385	XXXXXXXXXXXXXXX

3.3 Beschreibung der angewendeten Prüfmethoden

Im Rahmen der Begutachtung wurden die folgenden, von der gematik vorgegebenen, Prüfmethoden angewandt:

- Penetrationstest
  - Methodisch durchgeführt gemäß den Grundsätzen der Standards „BSI Leitfaden Penetrationstest“[1] und „Open Source Security Methodology Manual“[2].
  - Methodisch ergänzt durch die Anleitungen des OWASP Mobile Security Testing Guide[3]
- Quellcodeanalyse
  - Methodisch durchgeführt gemäß den Grundsätzen der Standards „OWASP Mobile Security Testing Guide“, „OWASP Mobile Application Security Verification Standard“[4] in der Version 1.2 und “Technische Richtlinie BSI TR-03161”[5]
- Nachstellung und Ausführung vereinzelter Funktionalitäten,

[1] Vgl. BSI (2016), Website des Bundesamtes für Sicherheits in der Informationstechnik, Stand 21.10.2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.html
[2] Vgl. ISECOM (2010), Website der ISECOM, Stand 21.10.2020, https://www.isecom.org/OSSTMM.3.pdf
[3] Vgl. OWASP (2019), Website der OWASP, Stand 21.10.2020, https://owasp.org/www-project-mobile-security-testing-guide/
[4] Vgl. OWASP (2020), Github-Repository der OWASP, Stand 21.10.2020, https://github.com/OWASP/owasp-masvs/releases
[5] Vgl. BSI (2020), Website des Bundesamtes für Sicherheits in der Informationstechnik, Stand 21.10.2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03161/BSI-TR-03161.html

- Befragung,
- Inaugenscheinnahme und Beobachtung (im Folgenden „Inaugenscheinnahme“ genannt)
    - durchgeführt mittels Begutachtung per Video,
    - visuelle Zugriff über Werkzeuge zum Teilen des Desktops und
- Verwendung bestehender Gutachten.

Eine Beschreibung der Prüfmethoden ist der Richtlinie zur Prüfung der Sicherheitseignung zu entnehmen.

3.4 Beschreibung der verwendeten Prüfhilfsmittel

Im Rahmen der Begutachtung wurden die folgenden gesonderten Prüfhilfsmittel eingesetzt:

- iOS Testgeräte (iPhone 6 Plus, iPhone 8) mit iOS 14 (mit “checkra1n” Jailbreak),
- Android Testgeräte (Samsung Galaxy A51 und A5) mit Android 10 (mit Root),
- Android Debug Bridge ADB (https://developer.android.com/studio/command-line/adb),
- Android Studio inkl. virtualisierter Devices (https://developer.android.com/studio),
- Burp Suite (https://portswigger.net/burp),
- dnsmasq (https://wiki.debian.org/dnsmasq),
- Frida (https://github.com/frida/frida-python),
- Fridump3 (https://github.com/rootbsd/fridump3),
- Mitmproxy (https://mitmproxy.org/),
- Sideloadly (https://iosgods.com/topic/130167-windowsmacos-introducing-sideloadly-working-cydia-impactor-alternative/),
- SSL Labs SSL Server Test (https://www.ssllabs.com/ssltest/),
- Wireshark (https://www.wireshark.org/),
- Xcode (Apple AppStore),
- diverse Linux Standardtools.

3.5 Beschreibung der Prüfungen vor Ort

Auf eine Begutachtung vor Ort wurde Aufgrund der besonderen Lage verzichtet. Stattdessen wurde in der Zeit vom 25.03.2021 bis 27.05.2021 eine Begutachtung mittels Einsatzes von Informations- und Kommunikationswerkzeugen (IKT), hier Videotelefonie, durchgeführt.

Betriebsstätten:

Hauptprojektstandort in Deutschland:

- gematik GmbH
  Friedrichstraße 136
  10117 Berlin

3.6 Teilnehmerverzeichnis

Im Folgenden sind die an der Begutachtung beteiligten Mitarbeiter der gematik GmbH und Softwareentwickler aufgeführt.

Tabelle 2: Teilnehmer Antragsteller

#	Name	Rolle	Thema
1	**Birgit Wilhalm**	Hauptansprechpartnerin	E-Rezept-App
2	**Marcel Basquitt**	Product Owner	E-Rezept App
3	**Michael Henke**	Stellv. Ansprechpartner	E-Rezept App
4	**Alexey Tschudnowsky**	Stellv. Ansprechpartner	E-Rezept App
5	**Stefan Wagner**	Stellv. Ansprechpartner	E-Rezept App
6	**Wolfgang Schwab**	Stellv. Ansprechpartner	E-Rezept App
7	**Paul Laufer**	Leiter Prüfung und Audit	E-Rezept App
8	**Martin Fiebig**	iOS Head Developer	E-Rezept App
9	**Joachim Gärtner**	Android Head Developer	E-Rezept App
10	**Gerald Bartz**	iOS Developer	E-Rezept App

Im Folgenden sind die an der Begutachtung beteiligten Verantwortlichen von PwC aufgeführt.

Tabelle 3: Teilnehmer Produktgutachter

#	Name	Rolle	Verantwortlichkeit
1	**XXXXXXXXXXXXXX**	Erstgutachter, Sicherheitsgutachter	Prüfung der Anforderungen
2	**XXXXXXXXXXXXXX**	Zweitgutachter, Produktgutachter	Prüfung der Anforderungen
3	**XXXXXXXXXXXXXX**	Auditassistenz Produktgutachten	Prüfung der Anforderungen
4	**XXXXXXXXXXXXXX**	Auditassistenz Produktgutachten	Prüfung der Anforderungen
5	**XXXXXXXXXXXXXX**	Auditassistenz Produktgutachten	Prüfung der Anforderungen
6	**XXXXXXXXXXXXXX**	Auditassistenz Produktgutachten	PMO

3.7 Prüfergebnisse

Im Folgenden sind die Prüfergebnisse dargestellt. Die konkreten Feststellungen zu den einzelnen Anforderungen sind der in Anlage 1 des Produktgutachtens zu entnehmen (vergleiche Abschnitt 4.2).

Tabelle 4: Prüfergebnisse Herausgabe- und Nutzungsprozesse des eRp

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
1	A_19086	E-Rezept-FdV: Verbot von Werbe-Tracking	☐Penetrationstest ☒Quellcodeanalyse ☒Befragung ☐Inaugenscheinnahme ☒Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
2	A_19087	E-Rezept-FdV: Erlaubnis von Usability-Tracking sowie Crash-Reporting	☐Penetrationstest ☒Quellcodeanalyse ☒Befragung ☐Inaugenscheinnahme ☒Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
3	A_19088	E-Rezept-FdV: Informierte Einwilligung	☐Penetrationstest ☒Quellcodeanalyse ☒Befragung ☐Inaugenscheinnahme ☒Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
4	A_19089	E-Rezept-FdV: Informationen zur Einwilligung	☐Penetrationstest ☒Quellcodeanalyse	☒AFO umgesetzt ☐AFO teilweise umgesetzt	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
			☒Befragung ☒Inaugenscheinnahme ☒Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO nicht umgesetzt ☐AFO entbehrlich	
5	A_19090	E-Rezept-FdV: Aktivierung erst nach Lesebestätigung der Einwilligungsinformationen	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
6	A_19091	E-Rezept-FdV: Verbot von mehrmaligen Einwilligungsabfragen	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
7	A_19092	E-Rezept-FdV: Kopplungsverbot	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
8	A_19093	E-Rezept-FdV: Keine direkt identifizierenden personenbezogenen Daten	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
9	A_19094	E-Rezept-FdV: Keine Weitergabe von Sicherheitsmerkmalen	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
			☐Verwendung bestehender Gutachten		
10	A_19095	E-Rezept-FdV: Generierung von Nutzersession-basierten Merkmalen	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
11	A_19096	E-Rezept-FdV: Neue Generierung der Pseudonyme	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☒AFO entbehrlich	kein Sicherheitsmangel
12	A_19097	E-Rezept-FdV: Deaktivierung zu jeder Zeit	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
13	A_19177	E-Rezept-FdV – Anzeige von Protokolldaten	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
14	A_19178	E-Rezept-FdV – Schutzmaßnahmen gegen die OWASP-Mobile-Top-10-Risiken	☒Penetrationstest ☒Quellcodeanalyse ☒Befragung ☒Inaugenscheinnahme ☒Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	Sicherheitsempfehlung

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
15	A_19179	E-Rezept-FdV – Qualität verwendeter Schlüssel	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
16	A_19181	E-Rezept-FdV – Privacy bei default	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
17	A_19182	E-Rezept-FdV – Sicherheitsrisiken von Software-Bibliotheken minimieren	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
18	A_19183	E-Rezept-FdV – Zustimmung zur Weiterleitung von Daten	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
19	A_19184	E-Rezept-FdV – Information über weitergeleitete Daten	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
20	A_19185	E-Rezept-FdV – Nachvollziehbarkeit der Weiterleitung von Daten	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung	☒AFO umgesetzt ☐AFO teilweise umgesetzt	Sicherheitsempfehlung

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
			☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO nicht umgesetzt ☐AFO entbehrlich	
21	A_19186	E-Rezept-FdV – Sichere Speicherung lokaler Daten	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
22	A_19187	E-Rezept-FdV – Authentisierung vor Zugang zum Dienst	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
23	A_19188	E-Rezept-FdV - Sichere Deinstallation	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
24	A_19215	E-Rezept-FdV: Kommunikation über TLS-Verbindung	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
25	A_19229	E-Rezept-FdV: E-Rezepte lokal löschen - Löschen	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
26	A_19480	E-Rezept-FdV – Schutz der Session-Daten	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
27	A_19739	E-Rezept FdV: verpflichtende Zertifikatsprüfung	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
28	A_19979	E-Rezept-FdV – Kein Zugriff von Diensten Dritter auf personenbezogene medizinische Daten	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
29	A_19980	E-Rezept-FdV – Information über Datenweitergabe an Dienste Dritter	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☒AFO entbehrlich	kein Sicherheitsmangel
30	A_19981	E-Rezept-FdV – Zustimmung über Datenweitergabe an Dienste Dritter	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☒AFO entbehrlich	kein Sicherheitsmangel
31	A_19982	E-Rezept-FdV – Rücknahme der Zustimmung über Datenweitergabe an Dienste Dritter	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung	☐AFO umgesetzt ☐AFO teilweise umgesetzt	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
			☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO nicht umgesetzt ☒AFO entbehrlich	
32	A_19983	E-Rezept-FdV – Keine Nutzung von Diensten Dritter mit bekannten Schwachstellen	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
33	A_19984	E-Rezept-FdV – Validierung eingehender Daten von Diensten Dritter	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
34	A_20033	E-Rezept-FdV: Prüfung Internet-Zertifikate	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	Sicherheitsempfehlung
35	A_20167	E-Rezept-FdV: Authentisierung - Rolle Authenticator-Modul und Anwendungsfrontend	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
36	A_20172	E-Rezept-FdV: Zugriffsschutz - Online-Authentisierung	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
37	A_20181	E-Rezept-FdV: 2D-Code anzeigen - personenbezogene Daten	☐Penetrationstest ☒Quellcodeanalyse ☐Befragung ☒Inaugenscheinnahme ☒Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
38	A_20182	E-Rezept-FdV - Makelverbot	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
39	A_20183	E-Rezept-FdV: Apotheke suchen: neutrale Darstellung Suchergebnisse	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
40	A_20184	E-Rezept-FdV - Speicherung der Session-Daten	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
41	A_20186	E-Rezept-FdV - Session-Daten löschen	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
42	A_20187	E-Rezept-FdV: Einwilligung Tracking widerrufen	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung	☒AFO umgesetzt ☐AFO teilweise umgesetzt	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
			☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO nicht umgesetzt ☐AFO entbehrlich	
43	A_20193	E-Rezept-FdV: Anwendungsspezifische Nutzung Gerätefunktionalitäten	☒Penetrationstest ☒Quellcodeanalyse ☒Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
44	A_20194	E-Rezept-FdV: Information zur Verwendung von Gerätefunktionalitäten	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
45	A_20206	E-Rezept-FdV: Kommunikation über TLS-Verbindung mit Diensten Dritter	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
46	A_20208	E-Rezept-FdV: Apotheke suchen - Nutzung Verzeichnisdienst	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
47	A_20285	E-Rezept-FdV: Wettbewerbsneutralität für Darstellung Apotheken	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
48	A_17124	TLS-Verbindungen (ECC-Migration)	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
49	A_17205	Signatur der TSL: Signieren und Prüfen (ECC-Migration)	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☒AFO entbehrlich	kein Sicherheitsmangel
50	A_17207	Signaturen binärer Daten (ECC-Migration)	☐Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
51	A_17322	TLS-Verbindungen nur zulässige Ciphersuitenund TLS-Versionen (ECC-Migration)	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
52	A_17359	Signaturen binärer Daten (Dokumente) (ECC-Migration)	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☒AFO entbehrlich	kein Sicherheitsmangel
53	A_17775	TLS-Verbindungen Reihenfolge Ciphersuiten (ECC-Migration)	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung	☐AFO umgesetzt ☐AFO teilweise umgesetzt	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
			☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO nicht umgesetzt ☒AFO entbehrlich	
54	A_18464	TLS-Verbindungen, nicht Version 1.1	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
55	A_18467	TLS-Verbindungen, Version 1.3	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
56	A_20309	Bildung von "CODE_VERIFIER" und"CODE_CHALLENGE"	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
57	A_20483	Formulierung und Inhalte der Anfrage zum "AUTHORIZATION_CODE" für einen "ACCESS_TOKEN"	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
58	A_20512	Regelmäßiges Einlesen des Discovery Document	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
59	A_20529	Senden von "AUTHORIZATION_CODE" und "code_verifier" an den Token-Endpunkt	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
60	A_20602	Einreichen des "ACCESS_TOKEN" beim Fachdienst	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☒AFO entbehrlich	kein Sicherheitsmangel
61	A_20603	Organisatorische Registrierung des Anwendungsfrontends	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
62	A_20605	Fehlermeldung des Token-Endpunktes Formatierung	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
63	A_20606	Anwendungsfrontend: Kommunikation über TLS-Verbindung	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
64	A_20608	Anwendungsfrontend: Unzulässige TLS-Verbindungen ablehnen	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung	☒AFO umgesetzt ☐AFO teilweise umgesetzt	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
			☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO nicht umgesetzt ☐AFO entbehrlich	
65	A_20623	Anwendungsfrontend: Prüfung der Signatur des Discovery Document	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
66	A_20624	Anwendungsfrontend: Prüfung der Signatur des AUTHORIZATION_CODE	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☒AFO entbehrlich	kein Sicherheitsmangel
67	A_20625	Anwendungsfrontend: Prüfung der Signatur des ID_TOKEN	☐Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
68	A_20740	Bekanntgabe der Redirect-URI des Anwendungsfrontend	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
69	A_20741	Speicherung des Downloadpunktes des Discovery Document im Anwendungsfrontend	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
70	A_21218	E-Rezept-Client, Zertifikatsprüfung auf Basis derX.509-Root	☐Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
71	A_21222	E-Rezept-Client, allgemein Zertifikatsprüfung	☐Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
72	A_21275−01	TLS-Verbindungen, zulässige Hashfunktionenbei Signaturen im TLS-Handshake	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
73	A_21332	E-Rezept: TLS-Vorgaben	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
74	GS-A_4357	X.509-Identitäten für die Erstellung und Prüfungdigitaler nicht-qualifizierter elektronischer Signaturen	☐Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
75	GS-A_4361	X.509-Identitäten für die Erstellung und Prüfungdigitaler Signaturen	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung	☒AFO umgesetzt ☐AFO teilweise umgesetzt	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
			☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO nicht umgesetzt ☐AFO entbehrlich	
76	GS-A_4367	Zufallszahlengenerator	☐Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
77	GS-A_4368	Schlüsselerzeugung	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
78	GS-A_4385	TLS-Verbindungen, Version 1.2	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
79	GS-A_4387	TLS-Verbindungen, nicht Version 1.0	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
80	GS-A_5035	Nichtverwendung des SSL-Protokolls	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
81	GS-A_5322	Weitere Vorgaben für TLS-Verbindungen	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
82	GS-A_5339	TLS-Verbindungen, erweiterte Webbrowserinteroperabilität	☐Penetrationstest ☒Quellcodeanalyse ☒Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
83	GS-A_5526	TLS-Renegotiation-Indication-Extension	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
84	GS-A_5542	TLS-Verbindungen (fatal Alert bei Abbrüchen)	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
85	A_19937	Fehlermeldungen des Token-Endpunktes Anzeige	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
86	A_19938	Annahme des ID_TOKEN	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung	☒AFO umgesetzt ☐AFO teilweise umgesetzt	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
			☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO nicht umgesetzt ☐AFO entbehrlich	
87	A_20032−01	E-Rezept-FdV: Prüfung TI-Zertifikate	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☒AFO entbehrlich	kein Sicherheitsmangel
88	A_20079	Ausfall der Fehlermeldung des Token-Endpunktes	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	Sicherheitsempfehlung
89	A_20085	Fehlermeldungen des Anwendungsfrontends	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	Sicherheitsempfehlung
90	A_20161−01	E-Rezept-Client, Request-Erstellung	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
91	A_20174	E-Rezept-Client, Response-Auswertung	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
92	A_20175	E-Rezept-Client, Speicherung Nutzerpseudonym	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
93	A_20283	Annahme des "ACCESS_TOKEN"	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
94	A_20526-01	Authenticator-Modul: Response auf das CHALLENGE_TOKEN des Authorization-Endpunkts	☐Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
95	A_20614	"Authenticator-Modul: Prüfung der Signatur des Discovery Document"	☐Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
96	A_21322	Sichere Speicherung des "SSO-TOKEN"	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
97	A_19908-01	Authenticator-Modul: Prüfung der Signatur des "CHALLENGE_TOKEN"	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung	☒AFO umgesetzt ☐AFO teilweise umgesetzt	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
			☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO nicht umgesetzt ☐AFO entbehrlich	
98	A_20068-01	Authenticator-Modul: Prüfung Internet-Zertifikate	☐Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	Sicherheitsempfehlung
99	A_20499	Authenticator-Modul: Temporäre Speicherung von "SSO_TOKEN"	☐Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
100	A_20525	Authenticator-Modul: Anzeige des "user_consent" und PIN-Abfrage	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	Sicherheitsempfehlung
101	A_20527	Authenticator-Modul: Übertragung des "AUTHORIZATION_CODE" an das Anwendungsfrontend	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☒AFO entbehrlich	kein Sicherheitsmangel
102	A_20600	Authenticator-Modul: Annahme des "user_consent" und des "CHALLENGE_TOKEN"	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
103	A_20601	Authenticator-Modul: Übergabe des Authorization-Requests an den Authorization-Endpunkt	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
104	A_20607	Authenticator-Modul: Kommunikation über TLS-Verbindung	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
105	A_20609	Authenticator-Modul: Unzulässige TLS-Verbindungen ablehnen	☒Penetrationstest ☒Quellcodeanalyse ☒Befragung ☒Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
106	A_20617-01	Authenticator-Modul: Verpflichtende Zertifikatsprüfung	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
107	A_20618	Authenticator-Modul: Unzulässige TLS-Verbindungen ablehnen	☐Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
108	A_20700-07	Authenticator-Modul: Signatur der "CHALLENGE"	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung	☒AFO umgesetzt ☐AFO teilweise umgesetzt	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
			☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO nicht umgesetzt ☐AFO entbehrlich	
109	A_21414	Authenticator-Modul: Umschlüsselung des ACCESS_TOKEN für Pairing-Endpunkt	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
110	A_21416	Authenticator-Modul: Einleiten der Registrierung	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
111	A_21431	Authenticator-Modul: Übermittelung von Authentifizierungsdaten zur Verwendung von alternativen Authentisierungsmitteln	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
112	A_21443	Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Verschlüsselung des ACCESS_TOKEN	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
113	A_21574	Warnhinweise an den Nutzer	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
114	A_21576	Löschung bestehender alternativer Authentisierungsmittel	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO umgesetzt ☒AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
115	A_21578	Sicherstellung des Vorliegens einer geeigneten Umgebung zur Speicherung von biometrischen Referenzmerkmalen	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
116	A_21579	Sicherstellung des Vorliegens einer geeigneten Umgebung für Schlüsselerzeugung, Anwendung und Speicherung	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
117	A_21580	Ausschluss von Eigenimplementierungen zur Schlüsselverwaltung	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
118	A_21581	Verfügbarkeit von kryptographischen Algorithmen	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
119	A_21582	Lokale Authentisierung des Nutzers vor Anwendung des PrK_SE_AUT zur Authentisierung	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung	☒AFO umgesetzt ☐AFO teilweise umgesetzt	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
			☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO nicht umgesetzt ☐AFO entbehrlich	
120	A_21583	Qualitative Anforderungen an lokale Authentisierungsmittel	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
121	A_21584	Verwendung von Geräte-eigenen Mechanismen zur Authentisierung des Nutzers	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
122	A_21585	Beschränkung der Nutzung des PrK_SE_AUT auf das Authenticator-Modul	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
123	A_21586	Löschung des PrK_SE_AUT als Reaktion auf Systemereignisse	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
124	A_21587	Beschränkung des PrK_SE_AUT auf Signaturbildung	☐Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
125	A_21588	Erzeugung eines Key-Identifiers für das Schlüsselpaar PrK_SE_AUT/PuK_SE_AUT gegenüber dem IdP-Dienst	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
126	A_21589	Erzeugung des Schlüsselpaars PrK_SE_AUT/PuK_SE_AUT	☐Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
127	A_21590	Beschränkung der Nutzung des PrK_SE_AUT auf Authentisierung gegenüber dem IdP-Dienst	☐Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
128	A_21591	Erhebung von Geräteinformationen	☐Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
129	A_21595	Lokale Speicherung des C.CH.AUT	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
130	A_21598	Löschung von lokalen Daten bei Fehlschlag	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung	☒AFO umgesetzt ☐AFO teilweise umgesetzt	kein Sicherheitsmangel

#	AFO-ID	Afo-Bezeichnung	Prüfmethode	Umsetzungsstatus	Sicherheitsmängel
			☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☐AFO nicht umgesetzt ☐AFO entbehrlich	
131	A_21600	Einholen von aktuellen Geräteinformationen	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
132	A_21603	Ermöglichung der Löschung von alternativen Authentisierungsmitteln und lokal gespeicherten Daten	☐Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
133	A_21275−01	TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel
134	GS−A_4385	TLS-Verbindungen, Version 1.2	☒Penetrationstest ☒Quellcodeanalyse ☐Befragung ☐Inaugenscheinnahme ☐Technische Prüfung ☐Verwendung bestehender Gutachten	☒AFO umgesetzt ☐AFO teilweise umgesetzt ☐AFO nicht umgesetzt ☐AFO entbehrlich	kein Sicherheitsmangel

3.8 Auflagen, Folgemaßnahmen und Empfehlungen

In den folgenden Abschnitten werden die relevanten Auflagen, Folgemaßnahmen und Empfehlungen beschrieben.

3.8.1 Auflagen und Folgemaßnahmen

Im Folgenden sind die Auflagen und die dazugehörigen Folgemaßnahmen beschrieben.

Tabelle 5: Auflagen und Folgemaßnahmen

#	AFO-ID	Auflage/Folgemaßnahme	Termin
-	-	-	-

3.8.2 Empfehlungen

Im Folgenden sind die Empfehlungen beschrieben.

Tabelle 6: Empfehlungen

#	AFO-ID	Empfehlung
1	A_19178	Wir empfehlen, alle etwaigen Testfiles vor Veröffentlichung aus dem Repository zu entfernen und diese nicht mehr in Builds einzubeziehen (mit Blick auf M10).
2	A_19185	Wir empfehlen, nicht nur die Daten aus dem eRp-FD zu protokollieren (vgl A_19183), sondern alle Daten, die im Kontext des eRp-FdV entstehen - also auch zum Beispiel Suchanfragen ans Apothekenverzeichnis. Da diese Informationen keine so hohe Sensitivität haben, wie Daten des eRp-FdV, sprechen wir an dieser Stelle lediglich eine Sicherheitsempfehlung aus.
3	A_20033	Es ist die Umstellung von LetsEncrypt auf die neue ISRG Root CA zu beachten da die Lebenszeit der aktuellen IdenTrust CA demnächst abläuft. Es entstehen keine Sicherheitsbedenken, da die neue Zertifizierungsstelle auch den Anforderungen entspricht.
4	A_20512	Zwar erneuert das eRp-FdV das Discovery Document nach 24h, da das Expiration Date hier stets serverseitig als 24h kommuniziert wird und die Anwendung so programmatisch immer nach 24h das Dokument erneut lädt. Im Falle eines kompromittierten Servers wäre es allerdings möglich, dass dieser eine längere Dauer für das Expiration Date kommuniziert. Wir empfehlen somit, zusätzlich zum Expiration Date des Discovery Documents auch lokal das Datum der letzten Aktualisierung zu pflegen. Das Aktualisieren des Discovery Documents sollte sich dann nach dem eher abgelaufenen Datum dieser beiden richten (kürzere Dauer), wobei im Normalfall von 24h ausgegangen werden kann.
5	A_20085	Wir empfehlen, auch solche Fehlermeldungen, die normale Nutzer der programmatischen Logik folgend nicht erhalten, klar zu formulieren und die Platzhalter zu nutzen.
6	A_20068-01	Es ist die Umstellung von LetsEncrypt auf die neue ISRG Root CA zu beachten da die Lebenszeit der aktuellen IdenTrust CA demnächst abläuft. Es entstehen keine Sicherheitsbedenken, da die neue Zertifizierungsstelle auch den Anforderungen entspricht.
7	A_20525	In beiden Fällen handelt es sich um eine automatische Willenserklärung ohne Hinweise für

#	AFO-ID	Empfehlung
		den Nutzer. Es ist zu empfehlen, dass der Nutzer noch einmal über einen Dialog/Text auf die Willenserklärung hingewiesen wird.
8	A_21576	Das Fehlen der Funktion zur Deregistrierung sollte dennoch, mit den entsprechenden Dialogen und Warnhinweisen, in eine künftige Version der Anwendung einfließen. Da ansonsten eine Deaktivierung der biometrischen Authentifizierung für den Nutzer nur über einen Logout realisiert werden.

3.9 Zusammenfassung der Prüfergebnisse

Es konnte kein Sicherheitsmangel in Bezug auf die von der gematik definierten Anforderungen festgestellt werden. PwC spricht acht (8) Empfehlungen aus, welche die Implementierung des eRp-FdV betreffen, aber keinen Sicherheitsmängel darstellen.

Ein übergreifendes Informationssicherheitsmanagementsystem (im Folgenden „ISMS“ genannt) wird betrieben. Die notwendigen Aktivitäten eines ISMS, wie beispielsweise:

- Durchführung von internen Audits,
- Durchführung von Risikoanalysen,
- Behandlung von Sicherheitsvorfällen,
- Unterstützung der Bereiche der gematik in sicherheitstechnischen Fragestellungen und
- Berichterstattung an den Vorstand

sind in angemessener Form, insbesondere in Bezug auf das Prüfobjekt, etabliert.

Bei der Prüfung der Sicherheit der Anwendung haben wir technisch implementierte Anforderungen hinsichtlich ihrer Wirksamkeit analysiert und deren Effektivität bewertet. Dabei konnten wir kein Versagen feststellen.

3.10 Prüfungsurteil

Die Produktgutachter wurden im Rahmen des Begutachtungsprozesses ohne Einschränkungen durch die gematik unterstützt.

Als Ergebnis unserer Prüfungshandlungen wurden keine Sicherheitsmängel identifiziert, die den gesetzten Anforderungen gemäß Prüfgrundlage widersprechen. Die erforderlichen Prozesse sind grundsätzlich angemessen etabliert. Verbleibende geringfügige Abweichungen ohne Sicherheitsmangel sind aus Sicht der Gutachter nicht zulassungsverhindernd und sollten im Rahmen der regelmäßigen Begutachtungen erneut geprüft werden. Es wurden acht (8) Empfehlungen ausgesprochen, die jedoch keinen wesentlichen Sicherheitsmangel des Prüfobjektes adressieren.

Die Produktgutachter sind somit der Auffassung, dass das **eRp-Frontend des Versicherten (FdV)** nach reiflicher Begutachtung und Bewertung den sicherheitstechnischen und datenschutzrechtlichen Anforderungen der gematik entsprechen und somit geeignet sind, Teil der Telematikinfrastruktur der elektronischen Gesundheitskarte zu werden. Einer kontrollierten Inbetriebnahme in den Produktionsbetrieb steht aus Sicht der Gutachter nichts im Wege.

XXXXXX, den 31. Mai 2021

Ort, Datum	**Unterschrift (Erstgutachter)**

XXXXXX, den 31. Mai 2021

Ort, Datum	**Unterschrift (Produktgutachter)**

.

4 Anhang

4.1 Referenzdokumente

Tabelle 7: Referenzdokumente

#	Referenz	Dokument	Version	Stand
1	Siehe Dokumente zur Prüfvorschrift “E-Rezept-Frontend des Versicherten“	Dokumente zur Prüfvorschrift “E-Rezept-Frontend des Versicherten“	1.0.0	19.02.2021
2	Siehe Dokumente zur Prüfvorschrift “Identity Provider - Authentisierungsmodul”	Dokumente zur Prüfvorschrift “Identity Provider - Authentisierungsmodul”	1.0.0	18.05.2021

4.2 Arbeitsdokumente

Dem Gutachten ist die Anlage „Produktgutachten – Anlage 1“ beigefügt, in der im Rahmen der Begutachtung:

- die referenzierten Dokumente,
- die konkreten Feststellungen,
- die angewandte Prüfmethode,
- der bewertete Umsetzungsstatus,
- die Bewertung (Spalte „Sicherheitsmängel“),
- die Anmerkungen, die Risiken oder die Empfehlungen,
- die Folgemaßnahmen und Auflagen sowie
- die Termine dokumentiert sind.

4.3 Prüfplan

Der komplette Prüfplan für das Produktgutachten ergibt sich aus den Informationen in Kapitel 2.

4.4 Eigenerklärung zur Unabhängigkeit und Objektivität

Hiermit bestätigen wir, XXXXXXXXXXXXXXX und XXXXXXXXXXXXXXX, dass wir keine Verbindungen, weder geschäftlich noch privat, zu dem zu prüfenden Unternehmen, seinen Mitarbeitern oder dem Antragsteller verbundene Unternehmen und deren Mitarbeitern unterhalten, die unsere Unparteilichkeit gefährden können. Insbesondere haben wir das zu prüfende Unternehmen in den letzten zwei Jahren nicht bei Planung, Aufbau, Implementierung, Betrieb oder Verbesserung des ISMS oder der Umsetzung der Anforderungen von der gematik beratend unterstützt.

- Das zu prüfende Unternehmen ist die gematik GmbH.

- Der Prüfungsgegenstand umfasst die eRp-FdV.
- Es bestehen keine relevanten Verbindungen zu dem zu prüfenden Unternehmen.
- Unsere Unparteilichkeit ist nicht gefährdet, weil keine relevanten Verbindungen zwischen uns und dem geprüften Unternehmen bestehen.

Diese Erklärung gilt für das zu prüfende Unternehmen sowie für alle verbundenen Unternehmen. Sollte sich im Verlauf der projektbezogenen Tätigkeit die Beziehung zu dem geprüften Unternehmen sowie den verbundenen Unternehmen ändern, verpflichten wir uns, die gematik hierüber unverzüglich in Kenntnis zu setzen.

XXXXXX, den 31. Mai 2021 XXXXXX, den 31. Mai 2021

Erstgutachter **Produktgutachter**

4.5 Zertifikat für die Basis- und Zusatzqualifikation

Folgende Zertifikate der Produktgutachter für die erforderlichen Basis- und Zusatzqualifikationen sind dem Gutachten beigefügt:

Tabelle 8: Qualifikationsnachweise

#	Sicherheits- und Produktgutachter	Qualifikation	Nachweis
1	XXXXXXXXXXXXXXX	Basisqualifikation	XXXXXXXXXXXXXXX
2	XXXXXXXXXXXXXXX	Zusatzqualifikation	XXXXXXXXXXXXXXX
3	XXXXXXXXXXXXXXX	Basisqualifikation	XXXXXXXXXXXXXXX
4	XXXXXXXXXXXXXXX	Zusatzqualifikation	XXXXXXXXXXXXXXX
5	XXXXXXXXXXXXXXX	Basisqualifikation	XXXXXXXXXXXXXXX
6	XXXXXXXXXXXXXXX	Zusatzqualifikation	XXXXXXXXXXXXXXX

4.6 Risikomanagementverfahren und allgemeine Hinweise zur Bewertung vorliegender Risiken

Im Rahmen der Prüfung von e-Rp-FdVs sowie von ePA-FdVs ist eine weitere, prüfungsrelevante Vorschrift in dem BSI Dokument „Prüfvorschrift für den Produktgutachter des „ePA-Frontend des Versicherten“ und des „E-Rezept Frontend des Versicherten““ (im Folgenden „BSI Prüfvorschrift“ genannt) vorliegend. In dieser wird die Bewertung potentieller Risiken, die aus der nicht-Umsetzung oder lediglich teilweiser Umsetzung einzelner Prüfaspekte entstehen, gefordert. Im vorliegenden Kapitel wird die dem Verfahren zugrundeliegende Methodik beschrieben.

Die in Anhang 4.7 begründeten Restrisikobewertungen basieren auf einer Risikomanagementmethodik nach ISO/IEC 27005, welche auf das „**E-Rezept FdV**“ abgestimmt ist. Ziel unseres Prozesses zur Risikobewertung ist es,

- eine Identifikation von Risiken durchzuführen,
- je Risiko eine Einschätzung von Eintrittswahrscheinlichkeit und Auswirkung auf den Risikoträger zu erhalten,
- eine Gesamteinschätzung je Risiko abzugeben, ob und wie dieses im Hinblick auf Eintrittswahrscheinlichkeit und Auswirkung tragbar bzw. akzeptabel ist, und
- eine übergreifende Einschätzung hinsichtlich der Gesamtheit an Risiken zu erhalten, welche über die Eignung des zu bewertenden Objekts in Bezug auf ihre Aufnahme in den Gesamtkontext der Telematikinfrastruktur richten soll.

Eine Übersicht über unser Vorgehen (Figure 1 aus [ISO/IEC 27005]) gibt die folgende Grafik:

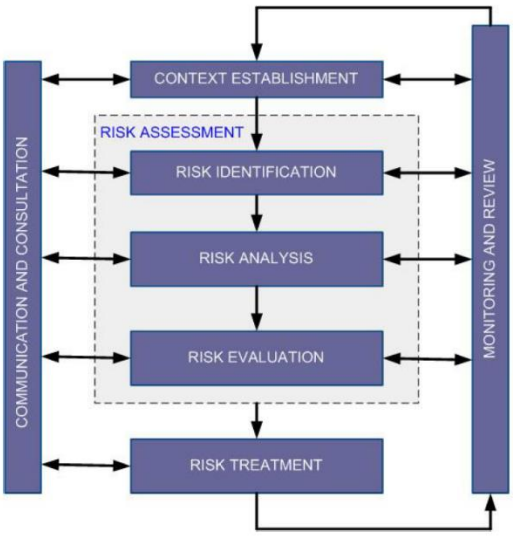

Abbildung 2: Risikomanagementprozess nach ISO/IEC 27005

In den nachfolgenden Kapiteln wird unser Vorgehen in der Bewertung der Restrisiken schrittweise, unter Referenzierung der Phasen der obigen Grafik, beschrieben. Der Raum „Risk Assessment“ ist hierbei maßgeblich für unsere Vorgehensweise, wobei die umliegenden Prozesse in Teilen auch in unsere Bewertung einfließen. Nach unserer initialen Bewertung der Risiken empfehlen wir dringend, diese weiterzuverfolgen und inakzeptable Risiken (Schwellwert: ≥ 3) zu behandeln. Darüber hinaus sollten diese in die eigenen Überwachungs- und Reviewprozesse aufgenommen werden. Eine Behandlung von Risiken mit einem niedrigeren Risikoniveau ist durch den Hersteller darüber hinaus auch möglich.

Risikokontext (Context Establishment)

Informationen und Werte stehen immer in einem organisatorisch-technischen Kontext. Daraus können für die Werte und Informationen unterschiedliche Risiken entstehen. Die Bewertung von Risiken steht also immer in einem Zusammenhang mit den organisatorisch-technischen Gegebenheiten

In unserer Betrachtung von eRp-FdVs und ePA-FdVs begutachten wir primär mobile Anwendungen, typischerweise auf der Android- und iOS-Plattform. Der Kontext von portablen Geräten als Hauptzugang zu den Informationen in einer Anwendung birgt viele Herausforderungen für die Sicherheit, da die verwendeten Endgeräte sich einer anderen Menge an der Bedrohungen ausgesetzt sehen als beispielsweise eine Infrastrukturkomponente, die nur in einem abschließbaren Büro steht und somit einem geringeren, physischen Risiko ausgesetzt ist als Smartphones, welche viele Nutzer ständig mit sich führen. Darüber hinaus ist auch der Kontext von medizinischen Daten, wie sie durch eRp- und ePA-FdVs verarbeitet werden, relevant, da hier ein besonderer Schutzbedarf für diese sensiblen und schutzbedürftigen Daten anzusetzen ist.

Aber auch jenseits der verwendeten Plattformen fließen besondere Anforderungen in die Risikobewertungen von eRp- und ePA-FdVs ein:

So eröffnet die BSI Prüfvorschrift in Anhang B weitere Begutachtungsperspektiven und nennt diverse Begutachtungsthemen, welche für die Prüfung relevant sind und den Gesamtkontext der Prüfung mit ihren Hintergründen besser darstellen sollen.

Risikoidentifizierung (Risk Identification)

Im Wesentlichen orientiert sich die Identifizierung von Risiken an den „Bedrohungen, Annahmen und organisatorischen Sicherheitspolitiken“ der Anwendung (Kapitel 4.1 der BSI Prüfvorschrift). Ziel dieser Phase ist die Aufarbeitung des Sicherheitsproblems und die Feststellung des Schutzbedarfs der verarbeiteten sensiblen Daten.

Die Aufarbeitung des Sicherheitsproblems sieht vor, dass auf Basis der „Bedrohungen, Annahmen und organisatorischen Sicherheitspolitiken“ (Kapitel 4.1 der BSI Prüfvorschrift) ein Verständnis über die sensiblen Daten gewonnen wird.

In der anschließenden Schutzbedarfsfeststellung wird ermittelt, welche Auswirkungen eine Verletzung der Schutzziele für Dateninhaber mit Blick auf die sensiblen Daten mit sich bringt.

Darüber hinaus findet die Identifizierung von Risiken anhand der Prüfaspekte der BSI Prüfvorschrift statt. Der in einem Prüfaspekt geforderte Mindestumfang der Prüfung hilft dem Prüfer bei der Identifizierung von Risiken. Eine Abweichung in einem Prüfaspekt vom SOLL bzw. MUSS Zustand ist ein zusätzlicher Indikator für das Vorliegen eines Risikos.

Die Gesamtheit aus sensiblen Daten, der Schutzbedarfe und der identifizierten Risiken geht im Anschluss in die Risikoanalyse ein.

Risikoanalyse (Risk Analysis)

Alle Risiken bewerten wir besonders vor dem Hintergrund der Begutachtungsperspektive, die die BSI Prüfvorschrift einführt.

Zu Beginn ist es notwendig, festzustellen, mit welchen Auswirkungen durch die Kombinationen von Bedrohungen und Schwachstellen für die einzelnen Werte auszugehen ist.

Geringe Auswirkung	0	Ein Verlust von Vertraulichkeit, Verfügbarkeit oder Integrität beeinträchtigt weder den Zahlungsfluss noch die rechtlichen oder vertraglichen Verpflichtungen oder das Ansehen der Organisation.
Mittlere Auswirkung	1	Ein Verlust von Vertraulichkeit, Verfügbarkeit oder Integrität verursacht zusätzliche Kosten und hat geringe oder mäßige Auswirkung auf rechtliche oder vertragliche Verpflichtungen oder das Ansehen der Organisation.
Hohe Auswirkung	2	Ein Verlust von Vertraulichkeit, Verfügbarkeit oder Integrität hat beträchtliche und/oder unmittelbare Auswirkung auf den Zahlungsfluss, den Betrieb, rechtliche oder vertragliche Verpflichtungen oder das Ansehen der Organisation.

Nach Einschätzung der Auswirkungen ist es notwendig, die Komplexität eines solchen Risikos festzustellen, z.B. die Wahrscheinlichkeit, dass eine Bedrohung die Schwachstelle des betreffenden Wertes ausnutzen könnte. mit Bezug darauf, wie komplex ein Angriff durchführbar ist.

Hohe Komplexität	0	Der durchzuführende Angriff ist entweder sehr komplex oder nur unter stark beschränkten (Labor-)Bedingungen durchführbar, oder aber ein sehr hoher Zeitaufwand wäre vonnöten.
Mittlere Komplexität	1	Der durchzuführende Angriff ist entweder komplex oder nur unter außergewöhnlichen Bedingungen durchführbar, oder aber ein hoher Zeitaufwand wäre vonnöten.
Niedrige Komplexität	2	Der durchzuführende Angriff ist entweder mit vertretbarem Aufwand ungeachtet anderer Bedingungen durchführbar, oder aber ein mittlerer oder geringer Zeitaufwand wäre vonnöten.

Diese Einschätzungen gehen dann wiederum in die Risikoeinschätzung über.

Risikoeinschätzung (Risk Evaluation)

Nach dem Erfassen der Werte für Auswirkung und Komplexität im Verzeichnis zur Risikoeinschätzung wird das Risikoniveau durch das Addieren der zwei Werte berechnet. Bereits vorhandene Maßnahmen, die ein Risiko abseits des begutachteten Prüfaspekts beeinflussen können, werden hierbei berücksichtigt. In Anlehnung an die Prüfvorschrift für den Produktgutachter des „ePA-Frontend des Versicherten“ und des „E-Rezept-Frontend des Versicherten“ blicken wir hier auf zeitbasierte und reaktive Maßnahmen. Bspw. kann ein Brute-Force Angriff auf ein bestimmtes Zertifikat ein Risiko darstellen, das in seiner Auswirkung dramatische Folgen hat, jedoch ist hier – hinreichende Zufallszahlengeneratoren und Kryptoroutinen vorausgesetzt – die benötigte Zeit für den Angriff derart limitierend, dass eine Eintrittswahrscheinlichkeit dahingehend sehr niedrig und eine Angriffskomplexität sehr hoch wäre.

Die Werte 0, 1 und 2 sind akzeptable Risiken („*akzeptabel*“), die Werte 3 und 4 nehmen wir als inakzeptable Risiken („*inakzeptabel*“) auf. Aus der Summierung der Werte für Auswirkung und Komplexität und dem genannten Risikoakzeptanzkriterium leiten wir folgende Matrix ab:

Auswirkung \ Komplexität	0	1	2
2	2	3	4
1	1	2	3
0	0	1	2

Innerhalb der 3x3-Kernmatrix stellt eine grüne Färbung Akzeptanz dar, wobei eine rote Färbung für ein inakzeptables Risiko steht. Die Werte entstehen wie oben beschrieben aus der Addition der Werte von Auswirkung und Komplexität.

Dieses Risikoakzeptanzkriterium wird dann genutzt, um die ermittelten Risiken zu bewerten und eine Abschätzung hinsichtlich der Risikoakzeptanz abzugeben, hier im Sinne einer Bewertung als akzeptabel bzw. inakzeptabel.

Wir empfehlen, die identifizierten Risiken im weiteren Lebenszyklus der Anwendungen zu berücksichtigen und geeignete Maßnahmen im Rahmen der Risikobehandlung für nicht akzeptable Risiken zu wählen.

4.7 Ergänzende Prüfung nach der „BSI Prüfvorschrift für den Produktgutachter des „ePA-Frontend des Versicherten“ und des „E-Rezept Frontend des Versicherten““ in der Entwurfsversion 1.2.6 vom 30.03.2021

Ergänzend zu den Anforderungen der gematik wurde auch nach den Prüfaspekten der BSI Prüfvorschrift geprüft. Es wurden alle 145 Prüfaspekte geprüft, davon wurden

- 85 Prüfaspekte mit „Pass“ bewertet,
- 23 Prüfaspekte mit „Fail“ bewertet,
- 35 Prüfaspekte als „Not Applicable“ bewertet und
- zwei Prüfaspekte konnten nicht abschließend bewertet werden („Inconclusive“).

Der entsprechende, vollständige Prüfplan kann Anlage 2 entnommen werden.

Risikobewertung der Prüfaspekte und Betrachtungsperspektiven mit Einschätzungen „Fail“ und „Inconclusive“ durch den Prüfer

Die Prüfaspekte die nicht erfüllt („Fail“ und „Inconclusive“) wurden, wurden anschließend einer Restrisikobewertung unterzogen. Dabei haben wir unter Bezugnahme auf die Annahmen, und Bedrohungen aus dem Kapitel „4.1 Security Problem Definition“ der BSI Prüfvorschrift das Restrisiko abgeschätzt. Wir sind zur Einschätzung gekommen, dass das Restrisiko, welches durch Nichterfüllung einzelner Prüfaspekte verbleibt, akzeptabel ist. Eine detaillierte Beschreibung unserer Restrisikobewertung und der zugrundeliegenden Risikomanagementmethodik findet sich in Anhang 4.6.

Die Ergebnisse der Restrisikobewertung und unsere Begründungen hinsichtlich einzelner Prüfaspekte können der folgenden Tabelle entnommen werden.

ID Prüfaspekt	Prüfaspekt	Begründung des Prüfungsergebnisses	Aus-wirkung	Komplexität	Risikoniveau	Einschätzung durch Prüfer	Einschätzung des Prüfers
O.Auth_7	Dem Nutzer SOLL eine Möglichkeit gegeben werden, sich über ungewöhnliche Anmeldevorgänge informieren zu lassen.	Dies ist nicht in der Anwendung vorgesehen.	2	0	2	akzeptabel	Die 'Anmeldung' über die elektronische Gesundheitskarte, die online stattfindet, wird lokal nicht protokolliert. Eine Protokollierung der Anmeldeversuche an den Zugriffschutz der App läge ein Bedrohungsszenario zugrunde in dem der Angreifer das Benutzerendgerät stiehlt, versucht sich anzumelden, und das Gerät zurückgibt. Wir schätzen dieses Szenario als unwahrscheinlich ein und bewerten das Restrisiko als gering und somit akzeptabel ein.
O.Tokn_6	Die Anwendung MUSS dem Nutzer bestehende Authentifizierungstoken, auf Anfrage, zur Verfügung stellen.	Diese Funktion ist nicht vorhanden.	2	0	2	akzeptabel	Aufgrund der Architektur kennt die Applikation keine anderen gültigen Token. Zur Generierung eines neuen Token ist entweder der Besitz der eGK, die Umgehung der biometrischen Anmeldung an einem iOS Gerät oder das Auslesen der Secure Enclave unter iOS notwendig. Die erzeugten Token haben eine kurze Lebensdauer. Die Anzeige der bestehenden Authentifizungstoken würde dem Benutzer erlauben illegitime Sitzungen zu erkennen. Da zum Aufbau einer neuen Sitzung die eGK oder die Umgehung der iOS Sicherheitsmaßnahmen erforderlich ist und eine illegitime Sitzung eine kurze Lebensdauer hätte, schätzen wir das Risiko durch die nicht-anzeige der Sitzungen als gering ein.
O.Tokn_7	Die Anwendung MUSS es dem Nutzer ermöglichen ein oder alle zuvor ausgestellten Authentifizierungstoken ungültig zu machen.	Diese Funktion ist nicht vorhanden.	2	0	2	akzeptabel	Vergleiche O.Tokn_6. Die App sieht nur den eigenen Token. Da die Token begrenzte Lebensdauer haben und Token über das Abmelden an der invalidiert werden können schätzen wir das Risiko als gering und somit als akzeptabel ein.
O.Resi_2	Die Anwendung MUSS gerootete oder gejailbreakte Geräte entsprechend dem aktuellen Stand der Technik erkennen und angemessen darauf reagieren. Die Applikation MUSS dem Nutzer darstellen, welche Risiken für die Daten des Nutzers bei einer Fortsetzung der App bestehen (z. B. dass diese offengelegt werden könnten) oder die Fortsetzung unterbinden.	Diese Prüfung findet nicht statt.	1	1	2	akzeptabel	Durch den Einsatz von gerooteten/gejailbreakten Geräten geht der Benutzer der App erhebliche Risiken ein. Eine Unterbindung der Funktion würde aber zu einem Wettrüsten mit dem Benutzer führen, da ein gerootetes Gerät der App immer vortäuschen kann nicht gerootet zu sein. Eine Warnung an den Benutzer über die Risiken die durch das rooten eingegangen werden sollte aus unserer Sicht in der App nachgerüstet werden. Zur Einschätzung des Risikos berufen wir uns auf die Annahme A.Device, dass der Nutzer das Gerät selbst schützt und betreibt, und nicht gerootet hat. Unter Einbeziehung dieser Annahme sehen wir das Risiko als akzeptabel.
O.Plat_1	Für die Nutzung der Anwendung SOLL das Endgerät über einen aktivierten Geräteschutz (Passwort, Mustersperre, o. ä.) verfügen. Im Fall eines nicht aktivierten Geräteschutzes MUSS der Hersteller den Nutzer über die damit verbundenen Risiken aufklären.	Weder in praktischen Tests noch innerhalb des Quellcodes konnte eine solche Funktionalität ausgewiesen werden. Auch die Ausführungen des Herstellers verneinen das Vorhandensein einer solchen Funktion.	1	1	2	akzeptabel	Die Anwendung selbst verfügt über einen Zugriffschutz. Dieser kann vom Benutzer optional deaktiviert werden. Bei der Deaktivierung des Geräteschutz wird der Benutzer auf das Risiko hingewiesen. Wir schätzen das Risiko des illegitimen Datenzugriffs bei fehlendem Geräteschutz und fehlendem Zugriffschutz als sehr hoch ein. Da dies aber nicht die Standardeinstellung der App ist, und der Benutzer entsprechend gewarnt wird, ist es ein akzeptables Risiko.

O.Plat_14	Die Applikation SOLL nach Beenden alle nutzerspezifischen Daten im Arbeitsspeicher sicher überschrieben haben.	Die Applikation überschreibt nicht explizit den Arbeitsspeicher.	1	0	1	akzeptabel	Um auf die Arbeitspeicherdaten der App nach dem Beenden zuzugreifen sind hohe Betriebsystemsberechtigungen notwendig. Diese wurden wahrscheinlich auch den Zugriff während des App Betriebs ermöglichen. Es ist denkbar dass eine Betriebsystemssicherheitslücke den Zugriff auf den freigegebenen Arbeitsspeicher der App, für eine andere nicht privilegierte App ermöglichen könnte. Dem Prüfer ist aus der jüngeren Vergangenheit keine derartige Schwachstelle bekannt und die Betriebsystemsherstelle waren in jüngster Vergangenheit schnell bei der Behebung derartiger Sicherheitslücken. Da Annahme A.Device davon ausgeht, dass der Benutzer sein Gerät aktuell hält, schätzen wir diese Bedrohung als akzeptabel ein.
O.Data_7	Die Speicherung und Verarbeitung von sensiblen Daten SOLL im Backend erfolgen.	Die Speicherung von sensiblen Daten ist eine Kernfunktion der eRezept App. Die Daten werden verschlüsselt und vor Zugriff geschützt gespeichert.	1	0	1	akzeptabel	Die Kernfunktion der App ist die Speicherung von Rezepten. Diese müssen dem Benutzer auch Offline zur Verfügung stehen um die gewünschte Funktionalität der App zu erreichen. Da die App über ausreichende Schutzmaßnahmen zum Schutz dieser Offline gespeicherten Informationen hat (u.a. Zugriffschutz, verschlüsselte Speicherung) schätzen wir die Speicherung als akzeptabel ein.
O.Data_11	Bei der Eingabe sensibler Daten SOLL der Export in die Zwischenablage unterbunden werden. Die Anwendung KANN alternativ eine eigene Zwischenablage implementieren, welche vor dem Zugriff durch andere Apps geschützt ist.	Die Anwendung umfasst die Eingabe der jeweiligen PIN und CAN Nummern der elektronsichen Gesundheitskarte des Anwenders. Diese können bei der Eingabe markiert und in die Zwischenablage des Gerätes kopiert werden. Da hiermit sensible Zugangs-Credentials, also ein Faktor einer zwei Faktor Authentifizierung, einem potentiellen Abfluss ausgesetzt sein kann, wird die Anforderung mit Fail bewertet.	1	0	1	akzeptabel	Der Datenabfluss über die Zwischenablage setzt ein zumindest teilkompromittiertes Gerät voraus. In iOS ist es in der aktuellen Version nur noch möglich, dass Apps im Vordergrund die Zwischenablage auslesen. Da der Workflow der App den Benutzer nicht dazu verleitet, sensible Daten in die Zwischenablage zu kopieren, sehen wir es in der Verantwortung des Benutzers sensible Daten nur zu kopieren, wenn dies notwendig ist. Eine Einschränkung der Zwischenablage würde dabei die Benutzbarkeit der App einschränken. Mit Blick auf A.Device, nach welcher der Benutzer dafür verantwortlich ist, sein System zu aktualisieren und vor Schwachstellen zu schützen, und Abwägung zwischen dem Nutzen der Zwischenablage und dem Risiko des Datenabflusses, sehen wir das Risiko als gering und somit akzeptabel an.
O.Arch_7	Die Anwendung MUSS einen Authentizitäts- und Integritätsschutz für die Applikation und ihre Konfiguration gewährleisten. Die Applikation SOLL dabei regelmäßig eine eigene Authentizitäts- und Integritätsprüfung des Applikations-Binaries, basierend auf einer digitalen Signatur mit Zertifikat, durchführen.	Nicht vorhanden. Die Nutzung dieser Funktion auf mobilen Geräten hätte den Einsatz von DeviceCheck resp. SaftyNet erfordert. Dieser Einsatz ist aufgrund von Datenschutzbedenken des BfDI nicht eingesetzt worden.	1	0	1	akzeptabel	Vergleiche Annahme A.Device. Die Überprüfung der App Integrität findet durch das Android und iOS Betriebssystem statt. Diese Prüfungen schätzen wir als ausreichend ein, wodurch wir ein geringes und somit akzeptables Risiko sehen.
O.Resi_4	Die Anwendung MUSS ihren Start abbrechen, falls sie unter ungewöhnlichen Benutzerrechten gestartet wird (z. B. root oder nobody).	Diese Prüfung findet nicht statt.	1	1	2	akzeptabel	vergleiche O.Resi_2.
O.Resi_5	Die Anwendung MUSS die Integrität des Endgeräts überprüfen, bevor sensible Daten verarbeitet werden.	Diese Prüfung findet nicht statt.	1	1	2	akzeptabel	vergleiche O.Resi_2.
O.Resi_7	Die Applikation SOLL Härtungsmaßnahmen, wie etwa eine Integritätsprüfung vor jeder Verarbeitung sensibler Daten innerhalb des Programmablaufs, realisieren.	Diese Prüfung findet nicht statt.	1	1	2	akzeptabel	vergleiche O.Resi_2.
O.Auth_13	Wurde die Anwendung unterbrochen (in den Hintergrundbetrieb versetzt) MUSS eine erneute Authentisierung durchgeführt werden.	Wenn der Benutzer wählt die App nicht gegen unbefugten Zugriff zu sichern ist nach Unterbrechung der Anwendung keine Authentifizierung notwendig. Der Benutzer kann aber den Zugriffschutz aktivieren, was diese Anforderung umsetzen würde.	1	1	2	akzeptabel	In den Standardeinstellungen der App ist dies der Fall. Die App gibt die Möglichkeit diesen Zugriffschutz zu deaktivieren weswegen diese Anforderungen auf "fail" steht. Da der Nutzer klar auf das Risiko hingewiesen wird und dies selbst eingeht, bewerten wir das Risiko als akzeptabel.
O.Arch_11	Die Applikation SOLL beim Start auf verfügbare sicherheitsrelevante Updates prüfen. Wenn ein sicherheitsrelevantes Update verfügbar ist, DARF die Applikation	Updates werden über den jeweiligen AppStore insofern es der Nutzer eingestellt hat automatisch ausgerollt, es wird beim App-Start keine	2	0	2	akzeptabel	Die Ausführungen des Herstellers, speziell im Bezug auf der Backendvalidierung und die Eingesetzten Validierungsmaßnahmen der Anwendung werden im Hinblick auf den Prüfaspekt als akzeptabel bewertet.

	ohne dieses Update einzuspielen sensible Daten NICHT mehr verarbeiten.	Überprüfung vorgenommen. Die Kommunikation von veraltete App-Versionen werden, nach Aussage der Gematik, von dem Backend über API-Keys verhindert. Ein Nutzer kann weiterhin die aktuellen Rezepte anschauen/bearbeiten und sich einen ACCESS_TOKEN beim IDP holen. Dies wiederspricht sich mit dem Grundsatz, dass die App die Verarbeitung von sensiblen Daten nicht mehr zulassen darf. Außerdem wird innerhalb des Backends nur auf Existenz des Header Felds geprüft und nicht auch auf tatsächliche Versionsnummer.					
O.Arch_8	Nutzt die Anwendung Frameworks oder Bibliotheken von Dritten (etwa für Objektserialisierung), MUSS der Hersteller dem Nutzer Informationen über den Nutzungsumfang und die eingesetzten Sicherheitsmechanismen klar darstellen. Die Anwendung MUSS sicherstellen, dass diese Funktionen in sicherer Weise genutzt werden. Die Anwendung MUSS darüber hinaus sicherstellen, dass ungenutzte Funktionen durch Dritte nicht aktiviert werden können.	Die Anwendung nutzt verschiedene Frameworks/Bibiliotheken von Dritten, hierzu findet eine Aufliustung innerhalb der Datei "3rd party libs in der App.pdf" statt. Über den Nutzungsumfang bzw. die Nutzung derer wird der Nutzer aktuell nicht informiert. Im Rahmen der Gematik Prüfung wurde bereits der sichere Einsatz dieser getestet.	0	0	0	akzeptabel	Die Umsetzung der Einsichtnahme in Frameworks oder Bibliotheken von Dritten wurde für die erste Release Fassung der Anwendung durch den Hersteller zugesagt. Die Umsetzung dieses Prüfaspekts wird in diesem Hinblick als akzeptabel bewertet.
O.Auth_6	Für die Bewertung eines Authentifizierungsvorgangs SOLLEN zusätzliche Informationen (z. B. das verwendete Endgerät, der verwendete WiFi-Zugangsknoten oder die Zeit des Zugriffs) mit einbezogen werden. Bei einer Abweichung von gewohnten Parametern MUSS eine zusätzliche Authentifizierungsmaßnahme (Step-Up- Authentisierung) erfolgen.	Es werden keine zusätzlichen Informationen zur Authentifizierung benutzt. Da die Authentifizierung über die eGK und PIN ein hohes Sicherheitsniveau besitzt und die Authentifizierung gegenüber dem Zugriffsschutz gerätespezifisch ist, erreicht die Applikation unserer Auffassung auch ohne diese Anforderung ein sehr hohes Sicherheitsniveau.	2	0	2	akzeptabel	Da die Authentifizierung über die eGK und PIN ein hohes Sicherheitsniveau besitzt und die Authentifizierung gegenüber dem Zugriffsschutz gerätespezifisch ist, erreicht die Applikation unserer Auffassung auch ohne diese Anforderung ein sehr hohes Sicherheitsniveau. Somit bewerten wir die Umsetzung des Prüfaspekts mit akzeptabel und sehen ein verbleibendes Risiko als gering an.
O.Sess_5	Die Anwendung MUSS die Anwendungssitzung nach einem angemessenen Session-Timeout aktiv beenden.	Innerhalb der Anwendungen ist kein solches Timeout vorhanden.	1	0	1	akzeptabel	In den Standardeinstellungen moderner Smartphones ist eine Bildschirmsperre aktiviert die nach wenigen Minuten das Nutzergerät sperrt. Deaktiviert ein Nutzer diese, oder deaktiviert den Geräteschutz könnte ein Angreifer der sich das Gerät verschaffen kann, Zugriff auf die sensiblen Gesundheitsdaten des Anwenders bekommen, wenn die E-Rezept-App zuletzt geöffnet war (Ansonsten Zugriffsschutz). Da der Benutzer hier stark von den Standardeinstellungen abweicht, selbst das Risiko eingeht, und diese Schwachstelle von einem Angreifer nur mit physischem Zugriff und etwas Glück ausnutzbar ist, bewerten wir sie als akzeptabel.
O.Auth_4	Der Nutzer MUSS mittels zweitem Faktor authentifiziert werden, bevor sensible Daten in der Anwendung verarbeitet werden (Step-Up-Authentisierung).	Die 2F-Authentifizierung an der E-Rezept App ist nicht zwingend, da es sich um ein single user personal device handelt, dass im Regelfall mit Wissen oder biometrischen Merkmalen vor Fremdzugriff geschützt ist. Eine darüber hinausgehende Abfrage biometrischer Merkmale zum Start der App ist umgesetzt. Um (neue) sensible Daten zu erlangen, ist Wissen und Besitz notwendig (eGK und PIN, zusätzlich	1	0	1	akzeptabel	Die Verarbeitung ist im Falle des Einscannens von auf Papier ausgegebenen Rezepten im Rahmen der App Nutzung möglich. Der Hersteller hat zugesagt für die Release Fassung der Anwendung einen Warndialog vor die mögliche Verarbeitung sensibler Daten einzuarbeiten. Hierdurch wird der Nutzer über die Risiken der Anwendungsnutzung im Modus ohne Sicherung aufgeklärt. Daher wird die Umsetzung dieses Aspektes hinsichtlich ihres Risikos als sehr gering und somit akzeptabel bewertet.

		zu dem Besitz des Gerätes und dessen Entsperrung).					
O.Biom_1	Die Verwendung biometrischer Sensoren SOLL nicht als alleiniger Authentifizierungsmechanismus eingesetzt werden. Sie ist lediglich als Teil einer Zwei-Faktor-Authentifizierung zulässig.	Biometrische Sensoren können für den Zugriffschutz verwendet werden. Für den Zugriff auf die TI ist jedoch die TI-Authentisierung notwendig	1	1	2	akzeptabel	Der Einsatz einer alleinigen biometrischen Authentifizierung geschieht für die Anmeldung an den Diensten der TI lediglich innerhalb der iOS Anwendung. Die Android Anwendung bietet für die Authentifizierung der Anwendungssession die alleinige Nutzung der biometrisch hinterlegten Merkmale. Da letztere dem Schutz von manuell eingescannten Rezepten dient und eine Anbindung an die TI durch eine Authentifizierung mittels mehreren Faktoren unterbindet, wird der Einsatz als aktzeptabel gewertet.
O.Tokn_3	Ein Authentifizierungstoken MUSS den voll qualifizierten Namen des Backends umfassen. Die Anwendung MUSS den voll qualifizierten Namen prüfen.	Es werden standardisierte JWT Token verwendet. Diese enthalten nicht den voll qualifizierten Namen.	1	0	1	akzeptabel	Die Nutzung von JWT Tokens wird in Anbetracht der verschiedenen Sicherungsmaßnahmen des Kommunikationsprotokolles als akzeptabel gewertet. Ein Auszug der Prüfung der eingesetzten Tokens: A_20625 A_19938 A_20079 A_20161−01
O.Biom_2	Der Hersteller MUSS definieren, welche Qualität und Eigenschaften ein biometrischer Sensor mindestens aufweisen muss, um von der Anwendung verwendet werden zu dürfen.	Eine derartige Spezifikation wurde nicht von der Gematik definiert. Für offizielle Android Gerät existiert der Standard https://source.android.com/security/biometric/measure#strong-weak-unlocks	1	0	1	akzeptabel	Die Umsetzung innerhalb der iOS-Anwendung, die alleinig für die Biometrische Authentifizierung gegenüber der TI eingesetzt werden kann, und der Einsatz einer Block bzw. Allow Liste auf Seiten der Authentifizierungsdienste wird durch die Prüfer als akzeptabel bewertet.
O.Biom_5	Die Applikation MUSS feststellen, wann die biometrischen Referenzmerkmale verändert wurden und die Anmeldung ablehnen, falls biometrische Referenzmerkmale nachträglich (das heißt seit der Aktivierung des Authentifizierungskontrollmechanismus in der Applikation) verändert worden sind.	Innerhalb von Android haben praktische Tests aufzeigen können, das die Anmeldung auch mit einem erneut hinterlegten Referenzmerkmal möglich war und auch entsprechend zu einer Anmeldung geführt hatte. Tests unter iOS konnten zeigen, dass das für die Authentisierung verwendete Schlüsselmaterial aufgrund des Setzens der entsprechenden Konfiguration nicht mithilfe neu registrierter Referenzmerkmale möglich ist. Dies ist auch Bestandteil der im Pruefplan der Gematikanforderungen unter A_21586 behandelten Anforderung.	2	0	2	akzeptabel	Die Android Anwendung bietet für die Authentifizierung der Anwendungssession die Nutzung von biometrischen Merkmalen. Auch nachträglich hinzugefügte Merkmale können so eine Anwendungssession authentifizieren. Ein Datenaustausch mit der TI ist hierbei nicht möglich. Auch wird der Anwender auf die mit dem Authentifizierungsverfahren zusammenhängenden Risiken hingewiesen und muss diesen explizit zustimmen.
O.Data_19	Die Anwendung MUSS dem Nutzer die Möglichkeit geben, dass bei ihrer Deinstallation alle sensiblen Daten und anwendungsspezifischen Anmeldeinformationen auch im Backend vollständig gelöscht werden. Entscheidet sich der Nutzer, die Daten im Backend nicht zu löschen, MUSS eine für den Zweck angemessene maximale Verweildauer definiert sein. Der Nutzer MUSS über die Verweildauer informiert werden. Nach Ablauf der maximalen Verweildauer MÜSSEN alle sensiblen Daten und anwendungsspezifischen Anmeldeinformationen vollständig gelöscht werden. Dem Nutzer MUSS die Möglichkeit gegeben werden alle Daten auch vor Ablauf der Verweildauer vollständig zu löschen.	Die Rezepte bleiben im Backend gespeichert, unabhängig vom Status der Applikation auf dem Endgerät des Benutzers.	2	0	2	akzeptabel	In Abstimmung mit der gematik wurden die aktualisierten Datenschutzbestimmungen bereitgestellt. Diese beinhalten die maximalen Speicherdauern für die Anwendung, welche sich zum Zeitpunkt der Prüfung jedoch noch in Abstimmung befanden. Die durch die Prüfer eingesehene Arbeitsfassung definierte Verweildauern für die Daten der verschiedenen Dienste und Anwendungen.

Die Prüfungsergebnisse und unsere Begründungen für die als „Inconclusive“ gewerteten Prüfaspekte sind in der folgenden Tabelle aufgelistet.

ID Prüfaspekt	Prüfaspekt	Begründung der Prüfung	Auswirkung	Wahrscheinlichkeit /Komplexität	Risikoniveau	Einschätzung durch Prüfer	Begründung des Prüfers
O.Arch_10	Der Hersteller MUSS dem Nutzer eine barrierearme Möglichkeit bereitstellen, um Sicherheitsprobleme zu melden. Die Kommunikation SOLL über einen verschlüsselten Kanal stattfinden.	Sicherheitsprobleme lassen sich Barrierearm über einen Anruf beim Service-Desk oder mittels einer E-Mail melden. Bei einer E-Mail werden die Standardtlsverschlüsselung der Mailserver verwendet. Der Nutzer sollte jedoch explizit darauf hingewiesen werden, dass er Sicherheitsprobleme dort, und an der offiziellen Seiter der Gematik (https://www.gematik.de/telematikinfrastruktur/datenschutz/), melden kann. Außerdem ist nicht gewährleistet, dass bei einem Anruf die Verbindung gesichert ist.	1	1	2	akzeptabel	Die Möglichkeit einer barrierefreien Meldung von Sicherheitsproblemen wird dem Anwender generell bereitgestellt. Hierbei wird dem Nutzer ein geordneter und dokumentierter Prozess für die Meldung von Sicherheitsvorfällen bzw. -bedenken bereitgestellt. Im Hinblick auf die dem Nutzer bereitgestellten Möglichkeiten und die Ausführungen des Herstellers zu diesem Prozess, wird der Prüfaspekt als akzeptabel bewertet.
O.Data_10	Bei der Eingabe sensibler Daten über die Tastatur SOLL die Anwendung unterbinden, dass Aufzeichnungen für Dritte erkennbar werden. Dies schließt insbesondere Caches, Autokorrektur- und Autovervollständigungsverfahren, Eingabegeräte von Drittanbietern und jegliche für Dritte auswertbare Speicherung, aus.	Der Nutzer kann Tastaturen von Dritten installieren, weder iOS noch Android ermöglichen es das zu erkennen oder zu verhindern. Die Felder sind jeweils als Password Feld gesetzt womit verhindert wird, dass diese in den normalen Tastaturen in Caches oder Autokorrektur gespeichert werden. Der Nutzer sollte klarer auf die Gefahren von Betriebssystem fremden Tastaturen hingewiesen werden oder eine eigene Eingabetastatur sollte erstellt werden um das Problem zu beheben. Somit gilt diese Anforderung als "Inconclusive" da das Benutzen von Tastaturen dritter eine Entscheidung des Nutzers ist und die Hersteller der App das Verhalten nicht beeinflussen können.	2	0	2	akzeptabel	Der Datenabfluss über eine Tastatur eines Drittherstellers setzt ein zumindest Teil-kompromittiertes Gerät voraus. Über die Tastatur könnte der Angreifer in Besitz der CAN, also eines Teil der Authentifizierungsfaktoren kommen. Da der Angreifer auch noch in Besitz der eGK kommen muss und wir uns auf Annahme A.Device beziehen, nach dem der Benutzer dafür Verantwortlich ist sein System zu aktualisieren und vor Schwachstellen zu schützen sehen wir das Risiko als akzeptabel an.

Risikobewertung von implementierungsspezifischen Risiken

Die gematik ist bei der Implementierung der App nach modernen Entwicklungsmethoden und Industriestandards vorgegangen. Aus unserer Sicht ergeben sich daraus keine implementierungsspezifischen Risiken.

Risikobewertung Integration in die geplante Betriebsumgebung

Die Integration in die geplante Betriebsumgebung konnte in diesem Gutachten nicht geprüft werden, da diese seitens des Herstellers zum Prüfzeitpunkt noch nicht durchgeführt wurde. Vor Betriebsstart soll ein externer Penetrationstest durchgeführt werden. Dieser sollte die Konfiguration der aus dem Internet erreichbaren Backend-Schnittstellen überprüfen.

Bewertung des Monitorings und der vorgesehenen Reaktionsmöglichkeiten des Betreibers

Die gematik hat während der Prüfung schnell auf Fragen zu Prüfaspekte reagiert und mehrere gescheiterte Prüfaspekte wurden während der Prüfung ausgebessert und sind jetzt als „Pass“ bewertet. Aus diesem Grund bewerten wir die Reaktionsmöglichkeiten des Betreibers als sehr gut und glauben, dass Sicherheitsprobleme, die in der Produktion auftreten, schnell gelöst werden können.

Das Monitoring des Betreibers wird anhand des Sicherheitskonzepts für das E-Rezept und den definierten Anforderungen an das Sicherheitsmonitoring der entsprechenden Betreiber als geeignet betrachtet. Eine Einsicht in etablierte Prozesse der entsprechenden Fachdienste war aufgrund der zum Prüfzeitpunkt nicht final vorliegenden Anwendungsversionen nicht möglich.

Feststellung des Schutzbedarfs der sensiblen Daten in der Anwendung

Die folgende Einschätzung der Schutzbedarfe der verschiedenen Schutzziele liegt unserer Risikobewertung zugrunde:

	Schutzziele			
Information	**Vertraulichkeit**	**Integrität**	**Authentizität**	**Verfügbarkeit**
Anwendungsdaten	Hoch	Hoch	Hoch	Hoch
Eingabedaten (von extern, Dritter Partei, eine externe Bibliothek, über Tastatur oder von Gerätesensoren)	Sehr hoch	Sehr hoch	Sehr hoch	Hoch
Zugangs-Credentials	Sehr hoch	Sehr hoch	Sehr hoch	Hoch
Kryptographische Schlüssel der App	Sehr hoch	Sehr hoch	Sehr hoch	Hoch
Aggregierte Anwendungsdaten z.B. Therapiebericht als PDF	Sehr hoch	Sehr hoch	Sehr hoch	Hoch
Biometrische Daten	Sehr hoch	Sehr hoch	Sehr hoch	Hoch
Öffentliche Zertifikate sowie Information für das Certificate-Pining	Normal	Hoch	Hoch	Normal

Die Schutzbedarfsfeststellung erfolgte im Rahmen unserer Risikomanagementmethodik. Anhang B der BSI Prüfvorschrift wird hier als Grundlage von verschiedenen Gruppen an Informationen genutzt. Die Auswirkungen auf die Schutzziele beziehen sich auf den Schaden für Dateninhaber.

Anlagen

Anlage 1: Prüfplan – Produktgutachten

Datum: 31. Mai 2021
Stand: Final

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
A_19086	E-Rezept-FdV: Verbot von Werbe-Tracking	gemSpec_eRp_FdV	Das E-Rezept-FdV DARF ein Werbe-Tracking NICHT verwenden.	Quellcodeanalyse Befragung Technische Prüfung	Es wird lediglich ein Usability Tracking verwendet. Das verwendete Tracking wird nicht zu Werbezwecken und geht nur an die gematik selbst..	AFO umgesetzt	kein Sicherheitsmangel			
A_19087	E-Rezept-FdV: Erlaubnis von Usability-Tracking sowie Crash-Reporting	gemSpec_eRp_FdV	Das E-Rezept-FdV KANN ein Usability-Tracking sowie Crash-Reporting verwenden.	Quellcodeanalyse Befragung Technische Prüfung	Das eRp-FdV verwendet unter beiden Betriebssystemen sowohl ein Usability-Tracking als auch ein Crash-Reporting.	AFO umgesetzt	kein Sicherheitsmangel			
A_19088	E-Rezept-FdV: Informierte Einwilligung	gemSpec_eRp_FdV	Das E-Rezept-FdV DARF ein Usability-Tracking sowie Crash-Reporting NICHT verwenden, ohne dass der Nutzer vorher über die Funktionen informiert wurde und über ein Opt-in-Verfahren eingewilligt hat.	Quellcodeanalyse Befragung Technische Prüfung	Zum erstmaligen Start in beiden Version (Android und iOS) wird der Nutzer über das Usability-Tracking sowie Crash-Reporting informiert und muss diesem explizit zustimmen. Ohne ein Opt-In werden die entsprechenden Funktionalitäten nicht genutzt. Dies konnten wir im Rahmen einer technischen Prüfung durch eine Überwachung des Traffics nachvollziehen.	AFO umgesetzt	kein Sicherheitsmangel			
A_19089	E-Rezept-FdV: Informationen zur Einwilligung	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS den Versicherten vor der Einwilligung in die Aktivierung Usability-Tracking sowie Crash-Reporting in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache folgende Einwilligungsinformationen anzeigen: * welche Daten durch die Tracking-Funktionen erhoben werden, * zu welchen Zwecken die Daten erhoben werden, * welche Informationen durch die Auswertung der erhobenen Daten gewonnen werden und ob Rückschlüsse auf den Gesundheitszustand des Nutzers möglich wären, * wer die Empfänger der Daten sind, * wie lange die Daten gespeichert werden, * wie die Tracking-Funktionen deaktiviert werden können.	Quellcodeanalyse Befragung Inaugenscheinnahme Technische Prüfung	Vor der Einwilligung in das Usability-Tracking und das Crash-Reporting bekommt der Nutzer eine ausführliche Information hinsichtlich des Umgangs mit seinen Daten. Dies ist programmatisch vor einer Einwilligung vorgeschaltet, wodurch der Nutzer diese Information erst zur Kenntnis nehmen muss. Die Formulierungen sind leicht verständlich und gehen auf die in der Anforderung genannten Punkte ein. So wird präzise beschrieben, welche Daten erhoben werden und wofür sie genutzt werden. Es wird darauf eingegangen, welche Informationen durch die Auswertung entstehen und dass daraus kein Rückschluss auf die Gesundheit des einzelnen möglich ist. Die Datenempfänger und Speicherdauer werden spezifiziert. Ein Hinweis darauf, dass die Einstellungen bei Bedarf in den Einstellungen	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
					gefunden werden können, ist ebenso enthalten. Die Umsetzung ist dabei für beide Betriebssysteme gleich.					
A_19090	E-Rezept-FdV: Aktivierung erst nach Lesebestätigung der Einwilligungsinformationen	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS sicherstellen, dass die Einwilligung des Nutzers in die Aktivierung von Usability-Tracking sowie Crash-Reporting erst erfolgt, wenn der Nutzer bestätigt, die angezeigten Einwilligungsinformationen gelesen zu haben.	Penetrationstest Quellcodeanalyse	In beiden Versionen wird dem Nutzer zuerst in einem Screen dargestellt, was alles im Rahmen des Usability-Tracking sowie Crash-Reporting gemäß A_19089 erklärt werden muss. Auf dem letzten dieser Screens erklärt der Nutzer sein Verständnis der angezeigten Einwilligungsinformationen. Erst dann erscheint ein Betriebssystemdialog, der abfragt, ob das Nutzerverhalten anonym analysiert werden darf.	AFO umgesetzt	kein Sicherheitsmangel			
A_19091	E-Rezept-FdV: Verbot von mehrmaligen Einwilligungsabfragen	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS technisch sicherstellen, dass der Benutzer der App maximal einmal eine Abfrage zur Einwilligung in das Usability-Tracking sowie Crash-Reporting angezeigt bekommt.	Penetrationstest Quellcodeanalyse	Die Abfrage zur Einwilligung erfolgt im Rahmen des einmaligen, nur beim ersten Appstart nach der Installation ausgeführten "Onboarding". Im Onboarding Prozess wird der Nutzer darum gebeten, dem Usability-Tracking sowie Crash-Reporting zuzustimmen oder es abzulehnen. Der Onboarding Prozess wird nur in diesem Rahmen einmalig durchgeführt, was war in einem praktischen Test sowie mittels Quellcodeprüfung verifizieren konnten. Anschließend kann der Nutzer nur noch in den Einstellungen eine weitere Zustimmung oder Ablehnung einstellen. Hierzu wird er aber nicht gedrängt; dies ist ein normales Toggle-Setting in den Konfigurationsmenüs der iOS/Android App. Eine mehrmalige Einwilligungsabfrage ist programmatisch ausgeschlossen.	AFO umgesetzt	kein Sicherheitsmangel			
A_19092	E-Rezept-FdV: Kopplungsverbot	gemSpec_eRp_FdV	Das E-Rezept-FdV DARF die Nutzung E-Rezept-FdV NICHT an die Aktivierung des Usability-Tracking sowie Crash-Reporting koppeln.	Penetrationstest Quellcodeanalyse	Unter beiden Betriebssystemen ist die Nutzung des Usability-Tracking bzw. Crash-Reporting als optional gekennzeichnet. Über die Kennzeichnung heraus konnten wir feststellen: Die App lässt sich in vollem Umfang auch ohne diese	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
					Funktionalitäten nutzen. Auch wenn man einmal zugestimmt hatte, kann man in den Einstellung jederzeit den Opt-Out durchführen und die App wieder ohne Einschränkungen nutzen. Dies konnten wir in praktischen Tests der App prüfen und das Verhalten auch im Quellcode nachvollziehen, da keiner der Anwendungsfälle an einen Opt-In gebunden ist.					
A_19093	E-Rezept-FdV: Keine direkt identifizierenden personenbezogenen Daten	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS sicherstellen, dass die Informationen zu Usability-Tracking sowie Crash-Reporting keine Daten enthalten, die natürliche Personen direkt identifizieren.	Penetrationstest Quellcodeanalyse	Durch eine Quellcodeanalyse konnte bestätigt werden, dass die durch Piwik Pro erhobenen Daten, das für beide Betriebssysteme zum Einsatz kommt, keine Informationen erhebt, die zur Identifikation einer natürlichen Person geeignet wären. Im Rahmen des Usability-Trackings werden nur aufgerufene Activities, geklickte Buttons etc. getrackt. Hierbei wird nie über den tatsächlichen Inhalt der aktuellen Ansicht berichtet, nur darüber, dass ein bestimmter Button getappt wurde. Zum Beispiel: Klick auf "Rezept einlösen". Dies wird zusammen mit einer anonymen Nutzer-ID, die der Nutzer zurücksetzen kann, übermittelt. Aus diesen Informationen ist Identifizierung des Nutzers nicht möglich. Es lassen sich nur etwaige Nutzungsschemata erkennen, aus denen zB hervorgeht, dass ein Nutzer erst ein E-Rezept einscannt, es dann in der App ansieht und irgendwann einlöst. Inhalt des Rezepts oder andere sensible Informationen sind hier nicht enthalten. Das Crash-Reporting sieht lediglich die Erhebung und der Versand des Stack Trace vor. Dieser enthält keine identifizierenden Informationen. Insbesondere enthält der Crash-Report keinen Memory Dump o.ä., der unter gewissen Umständen kritische	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
					Informationen enthalten könnte.					
A_19094	E-Rezept-FdV: Keine Weitergabe von Sicherheitsmerkmalen	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS sicherstellen, dass in den übermittelten Informationen zu Usability-Tracking sowie Crash-Reporting keine Sicherheitsmerkmale enthalten sind.	Penetrationstest Quellcodeanalyse	In den übermittelten Daten sind zu keiner Zeit Sicherheitsmerkmale enthalten. Insb. beim Crash-Reporting wurde darauf geachtet, dass kein partieller Memory Dump mit dem Log geschickt wird, sondern nur unmittelbar den Crash betreffende Informationen (Zeitpunkt, aufgerufene Funktion). Die eingeschränkte Menge an zu verschickenden Informationen im Rahmen der Nutzung von Piwik Pro ist also frei von Sicherheitsmerkmalen.	AFO umgesetzt	kein Sicherheitsmangel			
A_19095	E-Rezept-FdV: Generierung von Nutzersession-basierten Merkmalen	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS beim Start einer Nutzersession die Nutzersession-ID zufällig neu generieren.	Penetrationstest Quellcodeanalyse	Das eRp-FdV generiert mit dem Start einer Nutzersession automatisch einen neuen Identifier auf Zufallsbasis. Dies konnten wir in einer Quellcodeanalyse innerhalb beider App-Versionen erkennen. Somit ist insbesondere ein sessionübergreifendes Tracking nicht möglich.	AFO umgesetzt	kein Sicherheitsmangel			
A_19096	E-Rezept-FdV: Neue Generierung der Pseudonyme	gemSpec_eRp_FdV	Falls das E-Rezept-FdV ein Session-übergreifendes Tracking umsetzt, MUSS das E-Rezept-FdV technisch sicherstellen, dass pseudonyme Identifier neu generiert werden können.	Penetrationstest Quellcodeanalyse	Das eRp-FdV nutzt auskunftsgemäß kein Session-übergreifendes Tracking. Ein solches Tracking konnten wir weder im Quellcode noch in praktischen Tests identifizieren. Die im Rahmen des Usability-Tracking und Crash-Reporting gesammelten und gesendeten Informationen beziehen sich auf genau eine Session. Mittels zufallsbasierter Identifier, die zum Start einer Nutzersession sowie auf Wunsch zusätzlich manuell in den Einstellungen neu generiert werden, eine Verknüpfung mehrer Sessions ausgeschlossen ist.	AFO entbehrlich	kein Sicherheitsmangel			
A_19097	E-Rezept-FdV: Deaktivierung zu jeder Zeit	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS technisch sicherstellen, dass aktiviertes Usability-Tracking sowie Crash-Reporting jederzeit durch den Nutzer des FdVs deaktiviert werden können.	Penetrationstest Quellcodeanalyse	In den Einstellungen beider App-Versionen ist eine klar erkennbare Opt-Out Möglichkeit eingebaut. Auf Basis dieses Settings werden alle Tracking-Funktionalitäten (Usability-Tracking sowie	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
					Crash-Reporting) zentral gesteuern und ein- bzw. ausgeschaltet. Nicht nur in einem praktischen Test konnten wir das nachvollziehen, sondern auch via Quellcodeanalyse: die entsprechende boolsche Variable wird durch dieses Toggle-Element gesteuert. Ist die flag nicht genau true, werden keine Tracking-Funktionalitäten genutzt.					
A_19177	E-Rezept-FdV – Anzeige von Protokolldaten	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS es den Versicherten ermöglichen, die für die Fachanwendung für ihn erzeugten Protokolleinträge anzeigen zu können.	Penetrationstest Quellcodeanalyse	Die Umsetzung ist bei beiden Apps gleichartig gelöst. Dies konnten wir im Quellcode einsehen, zusätzlich auch in einem Penetrationstest der Apps bestätigen: Unterhalb der Rezepte kann der Nutzer die mit der Fachanwendung kommunizierten Informationen (IDs, Rezepte) in Form von Protokolleinträgen einsehen.	AFO umgesetzt	kein Sicherheitsmangel			
A_19178	E-Rezept-FdV – Schutzmaßnahmen gegen die OWASP-Mobile-Top-10-Risiken	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS Maßnahmen zum Schutz vor den in der jeweils aktuellen Version genannten OWASP-Mobile-Top-10-Risiken [OWASPMobileTop10] umsetzen.	Penetrationstest Quellcodeanalyse Befragung Inaugenscheinnahme Technische Prüfung	Beide App-Versionen nutzen insgesamt gleichartige Maßnahmen, um den OWASP-Mobile-Top-10-Risiken vorzubeugen. Folgendes konnten wir in einem Penetrationstest der App sowie in Quellcodeanalyse und Sichtung der Buildpipelines feststellen: Allgemein - Alle Nightly Builds durchlaufen einen OWASP-Check Speziell in Bezug auf die OWASP-Mobile-Top-10-Risiken konnten wir folgende Aspekte und Maßnahmen in Quellcodeanalysen bzw Penetrationstests vorfinden: M1 Improper Platform Usage - Als Local Storage werden die sicheren Bereiche der Betriebssysteme genutzt (zB Keychain) -> Nutzung sicherer APIs - Starke Authentifizierung (vgl. Auth-Anforderungen) M2 Insecure Data Storage	AFO umgesetzt	Sicherheitsempfehlung	Wir empfehlen, alle etwaigen Testfiles vor Veröffentlichung aus dem Repo zu entfernen und diese nicht mehr in Builds einzubeziehen (mit Blick auf M10).		

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
					- Als Local Storage werden die sicheren Bereiche der Betriebssysteme genutzt (zB Keychain) -> sicherer Storage - Es werden nur die nötigsten Daten lokal gespeichert bzw gecached - Über Authentiisierungsmerkmale und e-Rezepte hinaus keine gespeicherten Merkmale cookie-ähnlicher Natur M3 Insecure Communication - Umsetzung via TLS Anforderungen geklärt, starke Zufallszahlen und aktuelle TLS Versionen - Certificate Pinning gegen MitM M4 Insecure Authentication - Authentifizierung im Sinne der geltenden Best Practices - Nur authentifizierte API Calls des Backends/von APIs - Sichere Authentifizierung via eGK M5 Insufficient Cryptography - Nutzung von Betriebssytemnativa - -> iSv TR-03116-1: starke, symmetrischen (AES) und asymmetrischen (ECC) Schlüssel M6 Insecure Authorization - Eingeschränkte API Calls lassen nur Zugriffe auf eigene Daten zu (backendseitig), da E2E verschlüsselt und nur entschlüsselbar für eGK Nutzer M7 Client Code Quality - Wir konnten keine Pufferüberläufe identifizieren - Secure Coding Rules, Schulungen für Entwickler und SSDLC als organisatorische Ansätze um Code Quality des eRp hoch zu halten M8. Code Tampering - (organisatorisch) Berücksichtigung des MASVS während der Entwicklungsphase - Einhaltung der Guidelines erkennbar an sauberem					

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
					Coding-Style und klar strukturiertem Source Code M9 Reverse Engineering - Wir konnten keine besonderen Maßnahmen (Command Flow oder String Obfuscation) zum Erschweren eines Reverse Engineering vorfinden - Dies bewerten wir als vernachlässigbaren Sachverhalt, da die App als Open Source veröffentlicht wird M10 Extraneous Functionality - Genutzte Endpunkte wurden SSL/TLS Scans unterzogen und erwarten die TLS Versionen, die für die App im Sinne anderer Anforderungen erlaubt sind - Keine auffälligen Flags (zB debug==true) in Config-Files Aufgrund der o.g. Maßnahmen bewerten wir das Risiko von OWASP-Mobile-Top-10-Risiken im Kontext des eRp-FdV als hinreichend mitigiert und gering.					
A_19179	E-Rezept-FdV – Qualität verwendeter Schlüssel	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS sicherstellen, dass die von ihm erzeugten Schlüssel eine ausreichende Qualität besitzen.	Penetrationstest Quellcodeanalyse	Analog zu der Begründung hinsichtlich der Umsetzungsstatus von GS-A_4367 und GS-A_4368, gilt für A_19179 ebenfalls die gleiche Betrachtung der verwendeten Zufallszahlen der OS-Libraries. Die, wie bereits in GS-A_4368 beschrieben, erzeugten Schlüssel verfügen demnach über eine ausreichende Qualität mit Blick auf TR-03116-1#3.8 sowie #3.9.	AFO umgesetzt	kein Sicherheitsmangel			
A_19181	E-Rezept-FdV – Privacy bei default	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS bei Konfigurationsmöglichkeiten die sicherste, datenschutzfreundlichste Option vorauswählen.	Penetrationstest Quellcodeanalyse	XXX: Die Anwendungen bieten keine Konfigurationsmöglichkeit für den Datenschutz, lediglich eine einfache Zustimmung.	AFO umgesetzt	kein Sicherheitsmangel			
A_19182	E-Rezept-FdV – Sicherheitsrisiken von Software-Bibliotheken minimieren	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS Maßnahmen umsetzen, um die Auswirkung von unentdeckten Schwachstellen in	Penetrationstest Quellcodeanalyse	Auf Quellcodeebene setzt die gematik auf Maßnahmen, um unentdeckte Schwachstellen in Software-Bibliotheken in ihrer	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			benutzten Software-Bibliotheken zu minimieren.		Auswirkung abzumildern: - Weitergabe von Dateien an Bibliotheken nur in erforderlichem Maße - Daten in präzisen Formaten wie von Bibliotheken benötigt, keine allg. Weitergabe Außerdem gibt es im SSDLC und den Coding Rules mehrere organisatorische Absicherungen: - Secure Coding Guidelines zum Umgang mit Software-Bibliotheken - Einsatz von Sourcecode und Bibliotheken Dritter löst immer eine Security Story aus Zusätzlich wird für jeden nightly build beider App-Versionen ein automatisierter OWASP Check durchgeführt. MicroFocus "Fortify" kommt als Security Testsoftware zum Einsatz im Build Prozess. Hierdurch werden alle möglichen Inputfelder, Einstellungen und Parameter angesteuert und es wird versucht, Schwachstellen, die durch den Menschen unentdeckt blieben, aufzudecken. Die Summe an Maßnahmen erscheint uns als genügend, um sowohl bekannte als auch unbekannte Schwachstellen auszubremsen und zu eliminieren. Ein verbleibendes Risiko hinsichtlich Schwachstellen, die trotz der oben genannten Maßnahmen übrig bleiben, schätzen wir als sehr gering ein..					
A_19183	E-Rezept-FdV – Zustimmung zur Weiterleitung von Daten	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS sicherstellen, dass Daten, die vom E-Rezept-Fachdienst in das E-Rezept-FdV geladen werden, nur mit Zustimmung des Versicherten unter Nutzung von expliziten Opt-in-Lösungen weitergeleitet werden können, wobei sich das Opt-In nur genau auf die Weiterleitung beziehen und nicht mit anderen Zustimmungen kombiniert werden darf.	Penetrationstest Quellcodeanalyse	Es werden in mehreren Situationen Daten weitergeleitet: Bei der Einlösung in der Apotheke wird mittels DataMatrix Code ein Rezept an diese weitergeleitet. Hierbei sieht der Versicherte alle Details zu dem Rezept und muss explizit auf "Rezept einlösen" tappen.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
					Analog zum Einlösen eines Rezepts in der Apotheke verhält sich die Funktion zur Reservierung bzw. Bestellung eines Rezepts anhand einer Apotheke. Auch hier muss der Versicherte explizit die Reservierung/Bestellung veranlassen und konnte zuvor alle Details hinsichtlich weitergeleiteter Informationen einsehen. Bei der Nutzung der Apothekensuche erhält der Versicherte eine Informationsansicht vor der Nutzung, mittels derer er bestätigen muss, sich über die Daten und Empfänger im Klaren zu sein. In allen Fällen kommen explizite Opt-In Lösungen zum Einsatz und der Versicherte zuvor stets die Details der Weiterleitung einsehen kann.					
A_19184	E-Rezept-FdV – Information über weitergeleitete Daten	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS sicherstellen, dass der Versicherte vor der Zustimmung zur Weiterleitung von Daten aus dem E-Rezept-FdV in verständlicher Weise darüber informiert wird, welche Daten weitergeleitet werden.	Penetrationstest Quellcodeanalyse	Vor der Zustimmung zur Weiterleitung sehen beide Apps eine Ansicht für die Datenschutz sowie Nutzungsbestimmungen vor. Innerhalb der Datenschutzbestimmung wird der Nutzer genau aufgeklärt, welche Daten wie weitergeleitet werden, insb. im Rahmen der Nutzung von Tracking-Funktionalitäten oder anderen Diensten Dritter. Eine Information über die Weiterleitungen findet sich dort in verständlicher Sprache.	AFO umgesetzt	kein Sicherheitsmangel			
A_19185	E-Rezept-FdV – Nachvollziehbarkeit der Weiterleitung von Daten	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS sicherstellen, dass der Versicherte eine Weiterleitung der Daten im Nachhinein nachvollziehen kann (z.B. durch Protokollierung).	Penetrationstest Quellcodeanalyse	In einer Quellcodeanalyse sowie in einem Penetrationstest konnten wir In beiden App-Versionen unter den e-Rezepten in Protokollform nachvollziehen, wie diese weitergeleitet wurden. Dies reicht vom Einscannen hin zum Einlösen und bildet somit den Lebenszyklus der e-Rezepte in der App ab. Die Protokollierung innerhalb der e-Rezepte ist somit eine Abbildung der	AFO umgesetzt	Sicherheitsempfehlung	Wir empfehlen, nicht nur die Daten aus dem eRp-FD zu protokollieren (vgl A_19183), sondern **alle** Daten, die im Kontext des eRp-FdV entstehen - also auch zum Beispiel Suchanfragen ans Apothekenverzeichnis. Da diese Informationen keine so hohe Sensitivität haben, wie Daten des eRp-FdV, sprechen wir an dieser		

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
					Kommunikation mit dem e-Rezept Fachdienst und bezieht sich auf Daten, die vom eRp-FD in das eRp-FdV geladen werden (iSv A_19183).			Stelle lediglich eine Sicherheitsempfehlung aus.		
A_19186	E-Rezept-FdV – Sichere Speicherung lokaler Daten	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS Daten lokal sicher speichern, so dass keine andere App auf demselben Gerät unbefugt Zugriff auf die Daten hat. Insbesondere MUSS das E-Rezept-FdV Zugriffsschlüssel verschlüsselt ablegen. Außerdem MUSS das E-Rezept-FdV sicherstellen, dass vertrauliche Daten nicht vom Betriebssystem an anderen Ablageorten zwischengespeichert werden.	Penetrationstest Quellcodeanalyse	Android Die Anwendung nutzt für die Verschlüsselung der Informationen des E-Rezepts verschlüsselte SharedPreferences die vom Hersteller des Betriebssystems bereitgestellt werden. Die entsprechenden Schlüsselmaterialien werden verschlüsselt abgelegt und der Kontext, für den Zugriff auf die Informationen wurde auf den Kontext der Anwendung beschränkt. Hiermit wird auch sichergestellt das Dateien nicht an anderen Ablageorten abgelegt werden können. Damit kann die Anforderung als erfüllt angesehen werden. iOS Die gespeicherten Informationen werden innerhalb verschlüsselter Datenbanken abgelegt. Die Verschlüsselung erfolgt mit den Mitteln, die vom Hersteller bereitgestellt wurden. Mit diesen ist ein Zugriff anderer Anwendungen auf die Daten des E-Rezeptes nicht möglich. Hiermit wird auch sichergestellt das Dateien nicht an anderen Ablageorten abgelegt werden können. Ein Zugriff ist nur bei einem entsperrten Gerät möglich.	AFO umgesetzt	kein Sicherheitsmangel			
A_19187	E-Rezept-FdV – Authentisierung vor Zugang zum Dienst	gemSpec_eRp_FdV	Das E-Rezept-FdV DARF NICHT eine Verbindung zum E-Rezept-Fachdienst aufbauen, wenn es keinen ACCESS_TOKEN vom IDP erhalten hat.	Penetrationstest Quellcodeanalyse	Wir prüfen die Anforderung mittels Quellcodeanalyse. Die Umsetzung erfolgt in dem VAU Code (VAUInterceptor) bzw in dem IdpUseCase. Das VAU Bearer Token muss gesetzt sein, damit ein Request ausgeführt werden kann. Andernfalls ist ein Verbindungsaufbau zum eRp-FD nicht möglich..	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
A_19188	E-Rezept-FdV - Sichere Deinstallation	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS die von ihm verarbeiteten Daten so speichern, dass die Daten bei einer Deinstallation des E-Rezept-FdV mit gelöscht werden.	Penetrationstest Quellcodeanalyse	Android Innerhalb der Android Anwendung werden Informationen lediglich in Speicherbereichen gehalten, die durch eine Deinstallation auch gelöscht werden. Hierbei handelt es sich zum einen um Shared Preferences und zum anderen um Datenbanken die im Appspeicher gehalten werden. iOS Innerhalb der iOS Implementierung werden die intergrierten Speichermodule genutzt. Diese befinden sich in der vom Betriebssystem bereitgestellten Sandbox und werden bei einer Deinstallation der Anwendung vollständig entfernt. Darüber hinaus wird über den Programmcode sichergestellt das die Dateien keine Sicherung innerhalb des iCloud-Accounts des Nutzers erfährt.	AFO umgesetzt	kein Sicherheitsmangel			
A_19215	E-Rezept-FdV: Kommunikation über TLS-Verbindung	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS mit den Diensten der TI ausschließlich über TLS kommunizieren.	Penetrationstest Quellcodeanalyse	Als einziger Kommunikationsweg konnte für das eRp-FdV sowohl unter Android als auch unter iOS TLS identifiziert werden. In den entsprechenden Netzwerkmodulen im Quellcode lässt sich einzig TLS vorfinden. Wir haben die Apps weiterhin eines Penetrationstests unterzogen und mittels Wireshark ermittelt, welcher Traffic von den Anwendungen erzeugt wird. Hierbei konnten wir nur TLS Verbindungen finden. Dies bestätigt die Erkenntnisse aus der Quellcodeanalyse..	AFO umgesetzt	kein Sicherheitsmangel			
A_19229	E-Rezept-FdV: E-Rezepte lokal löschen - Löschen	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS alle Daten, d.h. die E-Rezept Daten als auch alle damit verknüpften Daten, zu den lokal zu löschenden E-Rezepten im E-Rezept-FdV löschen.	Penetrationstest Quellcodeanalyse	Die Anwendungen löschen alle mit den jeweiligen lokalen Rezepten verbundenen Daten aus der internen Datenhaltung. Dies konnte über praktische Tests, als auch über eine Einsicht in den entsprechenden Sourcecode bestätigt werden.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
A_19480	E-Rezept-FdV – Schutz der Session-Daten	gemSpec_eRp_FdV	Das E-Rezept-FdV DARF Session-Daten (bspw. ACCESS_TOKEN und ID_TOKEN) NICHT an Dritte, außer im Rahmen der in den Anwendungsfällen spezifizierten Kommunikation, weitergeben.	Penetrationstest Quellcodeanalyse	Session- Daten werden von der App zu keinem Zeitpunkt an Dritte übermittelt. Jegliche Kommunikation der Anwendungen erfolgt über die Domains der Gematik.	AFO umgesetzt	kein Sicherheitsmangel			
A_19739	E-Rezept FdV: verpflichtende Zertifikatsprüfung	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS alle Zertifikate, die es aktiv verwendet (bspw. TLS-Verbindungsaufbau), auf Integrität und Authentizität prüfen. Falls die Prüfung kein positives Ergebnis ("gültig") liefert, so MUSS es die von dem Zertifikat und den darin enthaltenen Attributen (bspw. öffentliche Schlüssel) abhängenden Arbeitsabläufe ablehnen. Das E-Rezept-FdV MUSS alle öffentlichen Schlüssel, die es verwenden will, auf eine positiv verlaufene Zertifikatsprüfung zurückführen können.	Penetrationstest Quellcodeanalyse	Die Prüfung der genutzten Zertifikate konnte anhand der Quellcodes validiert werden. Hierbei wird unter beiden Betriebssystemen ein eigener Truststore eingesetzt, der die entsprechenden Funktionalitäten und Zertifikate bereitstellt und über den diese geprüft werden.	AFO umgesetzt	kein Sicherheitsmangel			
A_19979	E-Rezept-FdV – Kein Zugriff von Diensten Dritter auf personenbezogene medizinische Daten	gemSpec_eRp_FdV	Das E-Rezept-FdV DARF Diensten Dritter NICHT Zugriff auf personenbezogene medizinische Daten geben.	Penetrationstest Quellcodeanalyse	Die einzige Nutzung von Diensten Dritter erfolgt durch die in anderen Anforderungen behandelte Nutzung von PiwikPro im Rahmen des Usability Tracking und Crash Reportings. Es konnte bei den Apps festgestellt werden, dass diese den PiwikProTracker einbindet. Es konnte nicht festgestellt werden, dass der Tracker Events mitschneidet. Diese getrackten Events werden an einen externen Dienstleister (piwik.pro) gesendet. Da aber keine personenbezogene Daten mitgeschnitten werden und auch keine Memory Dumps, die theoretisch personenbezogene Daten enthalten könnten, belaufen sich diese Daten nur auf eine zufallsbasierte, nicht-identifizierbare ID und Informationen über die genutzte Funktion (zB Button Taps) oder einen Stacktrace im Falle des Crashs. Es sind keine personenbezogenen Daten (und insb. keine medizinischen Daten) darin enthalten.	AFO umgesetzt	kein Sicherheitsmangel			
A_19980	E-Rezept-FdV – Information über	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS den Versicherten darauf hinweisen, dass durch die Nutzung von Diensten Dritter Daten an	Penetrationstest Quellcodeanalyse	Das eRp-FdV weist den Versicherten im Rahmen des Onboardings darauf hin.	AFO entbehrlich	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
	Datenweitergabe an Dienste Dritter		diese abfließen und welche Daten dies sind.		Innerhalb der Datenschutzbestimmung wird dem Versicherten erklärt, welche Daten im Rahmen der Nutzung an wen abfließen. Dies konnten wir für beide App-Versionen nachvollziehen. Außerdem wird direkt vor der Nutzung einer Funktion, mittels derer Daten abfließen werden, ein Hinweisbildschirm angezeigt. Dieser präzisiert die abfließenden Daten und die Empfänder dieser.					
A_19981	E-Rezept-FdV – Zustimmung über Datenweitergabe an Dienste Dritter	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS vor einer Weitergabe von Daten an Dienste von Dritten einmalig das Einverständnis des Versicherten einholen (OPT-IN).	Penetrationstest Quellcodeanalyse	Vor entsprechenden Funktionen wird das Einverständnis des Nutzers eingeholt. Am Beispiel der Apothekensuche (die mittels Apotheken-Verzeichnis umgesetzt wird) wird dem Nutzer vor der Nutzung ein Hinweisbildschirm gezeigt, der erklärt, welche Daten hierfür genutzt werden, wohin diese fließen, und ob der Versicherte damit einverstanden ist (Opt-In).	AFO entbehrlich	kein Sicherheitsmangel			
A_19982	E-Rezept-FdV – Rücknahme der Zustimmung über Datenweitergabe an Dienste Dritter	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS es dem Versicherten ermöglichen das Einverständnis zur Weitergabe von Daten an Dienste von Dritten zu widerrufen und ihn dabei über eventuelle Einschränkungen in der Funktionalität informieren.	Penetrationstest Quellcodeanalyse	Konnte nicht in der App vorgefunden werden. Laut Daten "2021-05-05_Arbeitsstand pwc.xlsx" noch in Entwicklung.	AFO entbehrlich	kein Sicherheitsmangel			
A_19983	E-Rezept-FdV – Keine Nutzung von Diensten Dritter mit bekannten Schwachstellen	gemSpec_eRp_FdV	Das E-Rezept-FdV DARF NICHT Dienste von Dritten nutzen, wenn diese bekannte Schwachstellen besitzen.	Penetrationstest Quellcodeanalyse	Für den genutzten Dienst Dritter, Piwik Pro, konnten keine bekannten Schwachstellen, bspw. unter cvedetails.com und in ähnlichen Quellen, gefunden werden. Die jüngsten bekannten Schwachstellen von Piwik stammen aus 2015 und sind in den verwendeten Versionen bereits behoben. Andere genutzte Dienste sind lediglich mit Google Maps zu finden. Für diesen konnten wir nach umfassender Suche auch keine bekannten Schwachstellen identifizieren.	AFO umgesetzt	kein Sicherheitsmangel			
A_19984	E-Rezept-FdV – Validierung	gemSpec_eRp_FdV	Das E-Rezept-FdV SOLL eingehende Daten von Diensten Dritter validieren.	Penetrationstest Quellcodeanalyse	Mittels Quellcodeanalyse konnten wir für beide Versionen	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
	eingehender Daten von Diensten Dritter				folgendes feststellen: Alle eingehenden Daten, somit ebenfalls inkludiert etwaige Daten Dritter, werden einer Validierung hinsichtlich erwarteter Form unterzogen. Eingehende Daten sind stets im JSON Format (zB als JWT) erwartet und werden entsprechend validiert. Sind innerhalb eines JSON Objekts einzelne Elemente von komplexerem Aufbau enthalten, werden diese ebenfalls validiert (bspw. anhand einer vorgegebenen Struktur wie "xxx yyy 123", wobei Leerzeichen als Split-Parameter gelten, und nur Objekte von genau dieser Form angenommen werden). Der Body von HTTPS Requests wird bspw. nur verarbeitet, wenn er einem von fünf erlaubten Content Types entspricht (text/html, application/json, application/xml, application/fhir+json, application/fhir+xml)..					
A_20033	E-Rezept-FdV: Prüfung Internet-Zertifikate	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS für die Prüfung des internetseitigen Zertifikats von Diensten der TI das Zertifikat auf ein CA-Zertifikat einer CA, die die "CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (https://cabforum.org/baseline-requirements-documents/ <https://cabforum.org/baseline-requirements-documents/>) erfüllt, kryptographisch (Signaturprüfung) zurückführen können. Ansonsten MUSS es das Zertifikat als "ungültig" bewerten. Das E-Rezept-FdV MUSS die zeitliche Gültigkeit des Zertifikats prüfen. Falls diese Prüfung negativ ausfällt, muss es das Zertifikat als "ungültig" bewerten.	Penetrationstest Quellcodeanalyse	Das Zertifikat welches die TI (web.gematik.solutions) verwendet, stammt von LetsEncrypt. LetsEncrypt selbst erklärt sich konform mit den Browser Forum Baseline Requirements. Die Root CA, in diesem Fall DST Root CA X3 von IdenTrust, ist auch konform zu der Baseline. Somit wird diese Anforderung als erfüllt gesehen. Die zeitliche Prüfung erfolgt automatisch über die Betriebsysteme.	AFO umgesetzt	Sicherheitsempfehlung	Es ist die Umstellung von LetsEncrypt auf die neue ISRG Root CA zu beachten da die Lebenszeit der aktuellen IdenTrust CA demnächst abläuft. Es entstehen keine Sicherheitsbedenken, da die neue Zertifizierungsstelle auch den Anforderungen entspricht.		
A_20167	E-Rezept-FdV: Authentisierung - Rolle Authenticator-Modul und Anwendungsfrontend	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS für den Zugriff auf Dienste der TI, wenn kein gültiger ACCESS_TOKEN vorliegt, sich gegenüber einem Identity Provider der TI in den Rollen Authenticator-Modul und Anwendungsfrontend Applikation authentisieren.	Penetrationstest Quellcodeanalyse	In dem Fall eines fehlenden oder ungültigen ACCESS_TOKENS wird eine NoAuthTokenException geworfen die über MainScreenFragmentDirections .actionMainScreenFragmentTo CardWallFragment() eine Reauthentification erzwingt.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
					Unter iOS wird ein Authentication Error erzeugt der die Reauthentification erzwingt. .					
A_20172	E-Rezept-FdV: Zugriffsschutz - Online-Authentisierung	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS für die Umsetzung der Online-Authentisierung für den Zugriffsschutz des E-Rezept-FdV eine Authentisierung gegenüber einen Identity Provider der TI durchführen.	Penetrationstest Quellcodeanalyse	Das eRp-FdV nutzt per Quellcode eine Authentifizierung gegen den IDP der TI. Der IDP EndPoint ist in einer Subdomain von ti-dienste.de angesiedelt und wird entsprechend anderer Anforderungen zur Authentifizierung genutzt..	AFO umgesetzt	kein Sicherheitsmangel			
A_20181	E-Rezept-FdV: 2D-Code anzeigen - personenbezogene Daten	gemSpec_eRp_FdV	Das E-Rezept-FdV DARF NICHT personenbezogene Daten zusammen mit der Anzeige des 2D-Codes anzeigen.	Quellcodeanalyse Inaugenscheinnahme Technische Prüfung	Sowohl die Android- als auch die iOS-Version des eRp-FdV zeigen lediglich einen Titel, eine kurze Beschreibung und den 2D-Code an. Weder im Titel noch in der Beschreibung sind personenbezogene Daten enthalten.	AFO umgesetzt	kein Sicherheitsmangel			
A_20182	E-Rezept-FdV - Makelverbot	gemSpec_eRp_FdV	Das E-Rezept-FdV DARF NICHT zusätzliche Funktionalitäten enthalten, die die berufs- oder gewerbsmäßige Zuweisung und das Makeln von E-Rezepten unterstützen oder den Nutzer in seiner Entscheidung beeinflussen, welche elektronischen Verordnungen in welcher Apotheke eingelöst werden.	Penetrationstest Quellcodeanalyse	Nach Untersuchung des Quellcodes der App konnten wir keine Funktionen identifizieren, die ein unkonformes Verhalten zur Anforderung darstellen. Weiterhin konnte in einer Befragung festgestellt werden, dass keine solcher Funktion implementiert sind und diese auch nicht für die Zukunft geplant sind. Dies wird durch ein Gremium der gematik, welches diesen Aspekt regelmäßig untersucht, gewährleistet. Weiterhin ist diese Anforderung expliziter Bestandteil der Definition of Done (iSv Scrum), wodurch zusätzlich vermieden wird, dass derartige Funktionen implementiert werden. Die Prozesse der gematik lassen hier keine solche Funktion zu und nach reiflicher technischer Untersuchung konnten keine derartigen Funktionen identifizieren konnten.	AFO umgesetzt	kein Sicherheitsmangel			
A_20183	E-Rezept-FdV: Apotheke suchen: neutrale Darstellung Suchergebnisse	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS ein Suchergebniss so darstellen, dass einzelne Apotheken nicht hervorgehoben oder bevorzugt werden.	Penetrationstest Quellcodeanalyse	Die Suchergebnisse werden in einer neutralen Liste angezeigt. Diese können durch den Nutzer nochmals mittels einer Suche	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
					gefiltert werden.					
A_20184	E-Rezept-FdV - Speicherung der Session-Daten	gemSpec_eRp_FdV	Das E-Rezept-FdV DARF NICHT Session-Daten (bspw. ACCESS_TOKEN und ID_TOKEN) unverschlüsselt auf permanenten Speichermedien ablegen.	Penetrationstest Quellcodeanalyse	Die Android Anwendung nutzt zur Speicherung von Daten zum einen die von Android bereigestellten "SharedPreferences" und eine SQL-lite Datenbank, die verschlüsselt auf dem Gerät abgelegt wird. Der Access Token wird verschlüsselt auf dem Gerätespeicher abgelegt, wohingegen der ID_Tocken nicht persistent gespeichert wird. Somit sind die Anforderungen für die verschlüssselte Speicherung erfüllt. Unter iOS wird die vom Hersteller bereitgestellte Lösung (Core Data / SQLlite) für die persistente Speicherung von Daten genutzt. In dieser werden die Informationen persistent und mit einer Passphrase verschlüsselt im intern geschützten Speicher abgelegt.	AFO umgesetzt	kein Sicherheitsmangel			
A_20186	E-Rezept-FdV - Session-Daten löschen	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS beim Beenden einer Session die Session-Daten (bspw. ACCESS_TOKEN und ID_TOKEN) sicher löschen.	Penetrationstest Quellcodeanalyse	Per Quellcodeanalyse konnten wir folgendes feststellen: Unter iOS: Mit dem Aufruf der Logout Funktion zur Beendigung einer Session werden auch die zuvor genutzten Session Daten allesamt gelöscht. Dies erfolgt durch ein dereferenzieren der Token innerhalb der Keychain (iOS) bzw. der sicheren Storage Datenbank (Android). Diese werden zurückgesetzt und das access_token wird invalidiert. Android: Auch hier gibt es eine Logout-Funktion, die die IDP Konfigurationstabelle in den Shared Preferences bereinigt (nullt) und somit alle Session Daten löscht.	AFO umgesetzt	kein Sicherheitsmangel			
A_20187	E-Rezept-FdV: Einwilligung Tracking widerrufen	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS es dem Versicherten ermöglichen, die Einwilligung in die Aktivierung eines Usability-Tracking sowie Crash-Reporting zu widerrufen und ihn dabei über die Folgen des Widerrufs informieren.	Penetrationstest Quellcodeanalyse	In den Einstellungen beider App-Versionen (Android, iOS) ist jederzeit ein Widerruf der vormals erteilten Einwilligung möglich (Opt-Out). Die entsprechende Flag wird	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
					sodann als False vermerkt und die Tracking-Funktionen sind nicht mehr verfügbar. Hierüber wird der Versicherte informiert.					
A_20193	E-Rezept-FdV: Anwendungsspezifische Nutzung Gerätefunktionalitäten	gemSpec_eRp_FdV	Das E-Rezept-FdV DARF NICHT gerätespezifische Funktionalitäten (z.B. Lagebestimmung, Kamerafunktion, Multi-Touch-Gesten) nutzen, wenn sie nicht für die Anwendung erforderlich sind.	Penetrationstest Quellcodeanalyse Befragung	An gerätespezifischen Funktionen nutzen beide Apps, sowohl Android als auch iOS, die Kamera, biometrische Sensoren und NFC. Die Nutzung von Geolokation ist in einer zukünftigen Version geplant. Folgende Funktionen werden von diesen Sensoren begleitet: Kamera: Abfotografieren des Rezepts (2D-Code). Der Nutzer muss vorab explizit zustimmen und wird davor über diesen Zweck informiert. Biometrische Sensoren: Diese werden zum Absichern der App genutzt. Dies muss zuvor aktiv vom Nutzer eingestellt werden. NFC: Dies wird zum Lesen der eGK benötigt. Der Nutzer wird wie gewohnt über den Betriebssystemdialog darauf hingewiesen. Geolokation: Hiermit können Apotheken gesucht werden (zB die physisch nächsten Apotheken). Auch hierüber wird der Nutzer informiert. Die Verwendung der gerätespezifischen Funktionen erscheint hier sehr sinnvoll und dem Zweck der Umsetzung des e-Rezepts überaus dienlich. Es handelt sich um elementare Funktionen, die für eine sinnvolle Nutzung benötigt werden. Geolokation wird als eine Quality-of-Life Funktion eingebracht, die das Finden der nächsten Apotheke erleichtert. Alle diese Verwendungszwecke dienen dem übergeordneten Sinn der Anwendung und könnten ohne die entsprechenden Sensoren nicht umgesetzt werden. Aufgrund der sinnvollen Nutzung der gerätespezifischen Funktionen, insbesondere keiner unsinnvollen oder nicht erforderlichen Verwendung dieser, bewerten wir diese Anforderung als umgesetzt.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
A_20194	E-Rezept-FdV: Information zur Verwendung von Gerätefunktionalitäten	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS den Nutzer über die Verwendung der gerätespezifischen Funktionalitäten (z.B. Lagebestimmung, Kamerafunktion, Multi-Touch-Gesten) informieren.	Penetrationstest Quellcodeanalyse	Zum Start der jeweiligen Anwendung, sowohl Android als auch iOS, wird der Nutzer über die Verwendung gerätespezifischer Funktionen informiert. Dies ist zum einen im Betriebssystem verankert, wo der Nutzer durch ein Android- bzw. iOS-spezifisches Popup darauf hingewiesen wird. Zum anderen gibt es Hilfetexte in der Anwendung, die bei verschiedenen Funktionen angezeigt werden, welche gerätespezifische Funktionalitäten verwenden.	AFO umgesetzt	kein Sicherheitsmangel			
A_20206	E-Rezept-FdV: Kommunikation über TLS-Verbindung mit Diensten Dritter	gemSpec_eRp_FdV	Das E-Rezept-FdV SOLL mit den Diensten Dritter ausschließlich über TLS kommunizieren.	Penetrationstest Quellcodeanalyse	Im Rahmen der technischen Prüfung der Apps sowie einer Quellcodeanalyse beider Versionen (Android und iOS) konnten wir keine Dienste Dritter identifieren. Es wird einzig eine Kommunikation mit dem Fachdienst sowie dem IDP aufgebaut.	AFO umgesetzt	kein Sicherheitsmangel			
A_20208	E-Rezept-FdV: Apotheke suchen - Nutzung Verzeichnisdienst	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS den Verzeichnisdienst ausschließlich zum Abruf von Apothekeninformationen nutzen und darf den Verzeichnisdienst nicht nach weiteren Einträgen durchsuchen.	Penetrationstest Quellcodeanalyse	Die Anwendungen nutzten den Dienst nur für das Suchen von Apotheken. Eine Nutzung des Verzeichnisdienstes konnte, abseits der Suche von Apotheken nach Namen, nicht gefunden werden. Die in der iOS App genutzten Filterfunktionen werden nicht an den Server übertragen, sondern durch die Anwendung lokal erzielt. Innerhalb der Android Anwendung wird neben der Suche nach Namen auch die Suche nach Standort mithilfe des Verzeichnisdienstes realisiert.	AFO umgesetzt	kein Sicherheitsmangel			
A_20285	E-Rezept-FdV: Wettbewerbsneutralität für Darstellung Apotheken	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS Apotheken wettbewerbsneutral darstellen (bspw. Sortierung nach Alphabet oder Entfernung vom aktuellen Standort des Nutzers).	Penetrationstest Quellcodeanalyse	Die Listenansicht der Apotheken ist neutral gehalten. Hierbei wird keine individuelle Apotheke hervorgehoben oder anderweilig nicht wettbewerbsneutral dargestellt.	AFO umgesetzt	kein Sicherheitsmangel			
A_17124	TLS-Verbindungen (ECC-Migration)	gemSpec_Krypt	Alle Produkttypen, die Übertragungen mittels TLS durchführen, MÜSSEN die folgenden Vorgaben erfüllen: 1. Zur Authentifizierung MUSS eine X.509-Identität gemäß	Penetrationstest Quellcodeanalyse	Die Anforderung konnte über Quellcodeanalysen der Anwendungen bzw. Mitschnitte der Netzwerkpakete validiert werden. Beide Anwendungen prüfen in der vorliegenden	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			[gemSpec_Krypt#GSA_4359] verwendet werden. 2. Als Ciphersuiten MÜSSEN TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xC0,0x2B) und TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC0,0x2C) unterstützt werden. 3. Falls der Produkttyp in der Rolle als TLS-Client agiert, so MUSS er die eben genannten Ciphersuiten gegenüber evtl. ebenfalls von ihm unterstützen RSAbasierte Ciphersuiten (vgl. GS-A_4384) bevorzugen (in der Liste "cipher_suites" beim ClientHello vorne an stellen, vgl. [RFC-5246#7.4.1.2 Client Hello]). 4. Als Basis für den ephemeren ECDH MÜSSEN die Kurven brainpoolP256r1 und brainpoolP384r1 (vgl. [RFC-5639] und [RFC-7027]) unterstützt und verwendet werden.		Version die X.509 Identitäten. Die in der Anforderung genannten Ciphersuites und Kurven werden unterstützt. 3. Die definierten Ciphren werden nicht bevorzugt verwendet. Hier gibt es jedoch lediglich eine Ciphrenkonfiguration die zuvor eingesetzt wird: "TLS_ECDHE_EDSA_WITH_CHACHA20_POLY1305_SHA256" (0xcca9).					
A_17205	Signatur der TSL: Signieren und Prüfen (ECCMigration)	gemSpec_Krypt	Alle Produkttypen, die die TSL(ECC-RSA) signieren oder prüfen, MÜSSEN dafür das Signaturverfahren ECDSA [BSI-TR-03111] auf Basis der Domainparameter brainpoolP256r1 verwenden mit dem XMLDSig-Identifier „http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256“ [XMLDSig]. Als Hashfunktion (Messagedigest) MUSS SHA-256 [FIPS-180-4] verwendet werden.	Penetrationstest Quellcodeanalyse	Da es sich bei dem Frontend nicht um ein Praxisverwaltungssystem (PVS) oder ein Apothekenverwaltungssystem (AVS) handelt, ist die Prüfung der notwendigen Zetifikate über die TSL für das Erezept-FdV nicht notwendig und kann alternativ, nach gematik-krypt 7.2.2, auch anhand der TI-X.509-Root durchgeführt werden. Da die Prüfung anhand der TI-X.509-Root durchgeführt wird, gestaltet sich das Abrufen und somit das Prüfen der TSL als überflüssig und die Anforderung ist als entbehrlich anzusehen.	AFO entbehrlich	kein Sicherheitsmangel			
A_17207	Signaturen binärer Daten (ECC-Migration)	gemSpec_Krypt	Alle Produkttypen, die (nicht-XML-)Signaturen von Daten auf Basis eines ECC-Schlüssels erzeugen oder prüfen, MÜSSEN dafür das Signaturverfahren ECDSA [BSI-TR-03111] auf Basis der Domainparameter brainpoolP256r1 verwenden (vgl. [RFC-5753] und [RFC6090]). Als Hashfunktion (Messagedigest) MÜSSEN sie SHA-256 [FIPS-180-4] verwenden. [<=] Die Anforderung A_17207 gilt für allgemeine (nicht-XML-)Datensignaturen, also auch für	Quellcodeanalyse	Innerhalb des FdV konnte keine Abweichung gefunden werden in der keine XML-Signatur oder BrainpoolP256r1 Signatur verwendet wird.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			Tokensignaturen etc. A_17359 fordert für die Interoperabilität bei der Prüfbarkeit von Dokumentensignaturen die Verwendung des interoperablen Containerformats nach [ETSI-CAdES].							
A_17322	TLS-Verbindungen nur zulässige Ciphersuitenund TLS-Versionen (ECC-Migration)	gemSpec_Krypt	Alle Produkttypen, die Übertragungen mittels TLS durchführen, MÜSSEN sicherstellen, dass sie nur (durch andere Anforderungen) zugelassene TLS-Ciphersuiten bzw. TLSVersionen anbieten bzw. verwenden. Hinweis: Im Rahmen der Zulassungstests und der CC-Evaluierung wurde dies (A_17322) stets so umgesetzt. Mit A_17322 soll dieses Vorgehen explizit auch auf Spezifikationsebene ausgesprochen und transparent gemacht werden.	Penetrationstest Quellcodeanalyse	Die Implementierung unter Android limitiert die nutzbaren Ciphren auf ein Subset der in der technischen Richtlinie des BSI (TR-02102-2) definierten. Diese umfassen alle empfohlenen Varianten für TLS 1.2 und TLS 1.3. Somit ist diese Anforderung durch die Anwendung umgesetzt. Innerhalb von iOS wird die Einhaltung der zugelassenen TLS-Versionen wird zum einen über das manuelle setzen der Mindestversion 1.2 für TLS und zum anderen über den Einsatz von App Transport Security für Netzwerkressourcen realisiert. Die unterstützen Ciphren umfassen die innerhalb der "App Transport Security" integrierten Ciphersuites. Dies stellt die maximalen Sicherheitseinstellungen der vom Betriebssystem bereitgestellten Schnittstellen und Entwicklung dar.	AFO umgesetzt	kein Sicherheitsmangel			
A_17359	Signaturen binärer Daten (Dokumente) (ECCMigration)	gemSpec_Krypt	Alle Produkttypen, die (nicht-XML-)Signaturen von Dokumenten auf Basis eines ECCSchlüssels erzeugen oder prüfen, MÜSSEN dabei die Vorgaben aus A_17207 umsetzen und die Signatur nach [ETSI-CAdES] (interoperables Container-Format) bei der Erzeugung kodieren bzw. bei der Prüfung auswerten. [<=] Hinweis: Signaturen in PDF/A-Dokumenten werden mittels CMS kodiert.	Penetrationstest Quellcodeanalyse	Die Anwendung wurde auf entsprechende Anwendungsfälleuntersucht und es wurde keine von XML abweichende Kommunikation gefunden. Dies bedeutet das keine Dokumente anhand eines ECC Schlüssels erzeugt oder geprüft werden können, da diese in der Anwendung nicht zum tragen kommen.	AFO entbehrlich	kein Sicherheitsmangel			
A_17775	TLS-Verbindungen Reihenfolge Ciphersuiten(ECC-Migration)	gemSpec_Krypt	Alle Produkttypen, die Übertragungen mittels TLS durchführen und in der Rolle TLSServer agieren, SOLLEN die Reihenfolge der Ciphersuiten in der Liste "cipher_suites" aus dem TLS-ClientHello bei der Auswahl der Ciphersuite befolgen. [<=] Unter https://cipherli.st/ findet man Beispielkonfigurationen für unterschiedliche	Penetrationstest Quellcodeanalyse	Das FdV verwendet zwar für die Kommunikation TLS jedoch agiert es nicht in der Rolle als TLSServer.	AFO entbehrlich	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			Software-Pakete. Diese Beispielkonfigurationen entsprechen zwar nicht genau den Vorgaben aus A_17124 und A_17775, bieten aber einen guten Startpunkt für die Konfiguration. Die meisten Software-Pakete oder TLS-zentrierten Hardware-Lösungen (TLS-Terminatoren etc.) unterstützten die (wie oft formuliert) "Honorierung" der Reihenfolge aus der Liste "cipher_suites", aber nicht alle. Deshalb und weil die Honorierung wichtig aber nicht absolut notwendig ist, wurde A_17775 als SOLL-Anforderung formuliert.							
A_18464	TLS-Verbindungen, nicht Version 1.1	gemSpec_Krypt	Alle Produkttypen, die Übertragungen mittels TLS durchführen, DÜRFEN NICHT die TLSVersion 1.1 [RFC-4346] unterstützen.[<=]	Penetrationstest Quellcodeanalyse	Die Standard-HTTP-Schnittstelle setzt unter beiden Betriebssystemversionen als Mindestversion von TLS auf Version 1.2. Dies konnten wir in einer Quellcodeanalyse bestätigen. Ein SSL-Scan der entsprechenden Empfängerseiten zeigte, dass diese ebenfalls kein TLS 1.1 zulassen..	AFO umgesetzt	kein Sicherheitsmangel			
A_18467	TLS-Verbindungen, Version 1.3	gemSpec_Krypt	Alle Produkttypen, die Übertragungen mittels TLS durchführen, KÖNNEN die TLS-Version 1.3 [RFC-8446] unterstützen, falls sie 1. dabei nur nach [BSI-TR-02102-2] empfohlene Verbindungskonfigurationen (Handshake-Modi, (EC)DH-Gruppen, Signaturverfahren, Ciphersuiten etc.) verwenden, und 2. mindestens die Ciphersuite "TSL_AES_128_GCM_SHA256" dabei unterstützen.	Penetrationstest Quellcodeanalyse	Android Die Implementierung forciert die Nutzung von TLS.1.2 und TLS.1.3. Hierbei werden lediglich die vom BSI empfohlenen Ciphren verwendet. Somit wird die Anfoderung als erfüllt angesehen. iOS Für die Sicherstellung der Netzwerk und Transportsicherheit wird in der iOS Anwendung App Transport Security (ATS) eingesetzt. Hierbei werden die Herstellerangaben für die sichere Konfiguration eingehalten und die TLS Kommunikation auf ein Mindestmaß von TLS.1.2 festgelegt.	AFO umgesetzt	kein Sicherheitsmangel			
A_20309	Bildung von "CODE_VERIFIER" und"CODE_CHALLENGE"	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS zur Laufzeit einen "CODE_VERIFIER" (Zufallswert) gemäß [RFC7636 # section-4.1] bilden. Der "CODE_VERIFIER" MUSS eine Entropie von mindestens 43 und maximal 128 Zeichen enthalten. Das	Penetrationstest Quellcodeanalyse	In den jeweiligen App-Versionen sind die Funktionen nach RFC7636 innerhalb des Kontexts der Identiy Provider enthalten und werden zur Laufzeit aufgerufen.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			Anwendungsfrontend MUSS über den "CODE_VERIFIER" einen HASH-Wert, die sogenannte "CODE_CHALLENGE", gemäß [RFC7636 # section-4.2] bilden.[<=]							
A_20483	Formulierung und Inhalte der Anfrage zum"AUTHORIZATION_CODE" für einen"ACCESS_TOKEN"	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS über das Authenticator-Modul den Antrag zum"AUTHORIZATION_CODE" für einen "ACCESS_TOKEN" via Private-Use URI Scheme Redirection [RFC8252 # section-7.1] beim Authorization-Endpunkt in Form eines HTTP/1.1 GET-Request stellen und dabei die folgenden Attribute anführen: • "response_type" • "scope" • "client_id" • "redirect_uri" • "code_challenge" (Hashwert des "code_verifier") [RFC7636 # section-4.2] • "code_challenge_method" HASH-Algorithmus (S256) [RFC7636 # section-4.3] [<=] Hinweis: Der folgende Aufruf skizziert einen beispielhaften HTTP-GET-Request an den IdP-Dienst, welcher vom Betriebssystem gemäß [RFC8252] an das Authenticator-Modul umgeleitet und dort schließlich ausgeführt wird: GET /auth?response_type=code&scope=openid%20erezept&state=af0ifjsldkj&client_id=ZXJlemVwdC1hcHA&redirect_uri=https%3A%2F%2Fapp.erezept.com%2Fauthnres&code_challenge_method=S256&code_challenge=S41HgHxhXL1CIpfGvivWYpbO9b_QKzva-9ImuZbt0Is HTTP/1.1 Host: idp.com X-Anwendungsfrontend-App: 1.0 Accept: application/json User-Agent: Anwendungsfrontend-App/1.0	Penetrationstest Quellcodeanalyse	Die Anwendungen setzen beide die entsprechenden Felder für den Request an den Authorization-Endpunkt. Dies konnte zum einen über ein Sourcecode Audit und eine Prüfung der Abfragen zur Laufzeit bestimmt werden.	AFO umgesetzt	kein Sicherheitsmangel			
A_20512	Regelmäßiges Einlesen des Discovery Document	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS das Discovery Document [RFC8414] löschen, wenn dieses 24 Stunden alt oder älter ist. Das Anwendungsfrontend MUSS das Discovery Document neu herunterladen, einlesen und auswerten und danach die darin aufgeführten URI zu den benötigten öffentlichen Schlüsseln (PUKs) und Diensten verwenden, wenn kein aktuelles Discovery Document vorliegt. [<=] Hinweis: Der IdP-Dienst übergibt den Downloadpunkt während der organisatorischen Registrierung des	Penetrationstest Quellcodeanalyse	"Per Quellcodeanalyse konnten wir folgendes feststellen: Die Implementierung unter Android nimmt das Verfallsdatum aus dem Discovery Document als gegeben an. Da der Server hier stets ein 24-stündiges Zeitlimit kommuniziert, erfüllt dies die Anforderung. Die Validierung des Discovery Documents wird auch innerhalb von iOS auf Basis des übertragenen Verfallsdatums	AFO umgesetzt	kein Sicherheitsmangel	Zwar erneuert das eRp-FdV das Discovery Document nach 24h, da das Expiration Date hier stets serverseitig als 24h kommuniziert wird und die Anwendung so programmatisch immer nach 24h das Dokument erneut lädt. Im Falle eines kompromittierten Servers wäre es allerdings möglich, dass		

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			Anwendungsfrontends bzw. des Primärsystems beim IdP-Dienst.		ausgewertet. Es wird keine maximale Höchstdauer für die Verwendung eines Discovery Documents programmatisch erzwungen. Beide Versionen laden das Dokument dann neu herunter und werten die Informationen anforderungsgemäß aus. Somit ist die Anforderung umgesetzt, wir sprechen aber eine Empfehlung hinsichtlich des Zeitlimits aus."			dieser eine längere Dauer für das Expiration Date kommuniziert. Wir empfehlen somit, zusätzlich zum Expiration Date des Discovery Documents auch lokal das Datum der letzten Aktualisierung zu pflegen. Das Aktualisieren des Discovery Documents sollte sich dann nach dem eher abgelaufenen Datum dieser beiden richten (kürzere Dauer), wobei im Normalfall von 24h ausgegangen werden kann.		
A_20529	Senden von "AUTHORIZATION_CODE" und"code_verifier" an den Token-Endpunkt	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS "AUTHORIZATION_CODE" und "code_verifier" TLS gesichert als HTTP/1.1 POST Request an den Token-Endpunkt senden und dort gegen das "ID_TOKEN" und "ACCESS_TOKEN" eintauschen.[<=] Hinweis: Der folgende Aufruf skizziert beispielhaft den HTTP-POST-Request des Anwendungsfrontends an den Token-Endpunkt. Der mitgegebene "AUTHORIZATION_CODE" wird dabei nur angedeutet: POST /token HTTP/1.1 Host: idp.com Content-Type: application/x-www-form-urlencoded User-Agent: Anwendungsfrontend-App/1.0 grant_type=authorization_code &code=eyJhbGciOiJkaXIiLCJlbmMiOiJBMjU2R0NNIiwiZXhwIjoxNTkx..... &redirect_uri=https%3A%2F%2Fapp.e-rezept.com%2Fauthnres &code_verifier=MApN61C4itdm4-58dCjMkoucuu00jipPlNibsAxjyJk	Penetrationstest Quellcodeanalyse	Beide Implementierunegn implementieren die entsprechenden Aufrufe zum IDP hin. Hierbei werden die geforderten Felder für "AUTHORIZATION_CODE" und "code_verifier" gesetzt und ordnungsgemäß an die API gesendet. Die entsprechende Antwort des Dienstes wird dann entgegengenommen. Hierbei werden "ID_TOKEN" und "ACCESS_TOKEN" entsprechend für die weitere verabrietung gespeichert.	AFO umgesetzt	kein Sicherheitsmangel			
A_20602	Einreichen des "ACCESS_TOKEN" beimFachdienst	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS das "ACCESS_TOKEN" im Rahmen des entsprechenden fachlichen Aufrufs beim Fachdienst einreichen, um Zugang zu den angeforderten Daten zu erhalten.[<=]	Penetrationstest Quellcodeanalyse	Die Umsetzung in beiden Anwendungen erfolgt über die Nutzug von Interceptoren. Hierdurch wird der Access Token innerhalb der Anfragen an den Fachdienst im Header der Anfrage integriert.	AFO umgesetzt	kein Sicherheitsmangel			
A_20603	Organisatorische Registrierung	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS sich über einen organisatorischen Prozess am IdP-Dienst registrieren und die vom IdP-Dienst	Penetrationstest Quellcodeanalyse	Die Anwendungen setzen bei der Kommunikation mit dem IDP Dienst das die client_id	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
	desAnwendungsfrontends		dabei vergebene "client_id" im Anwendungsfrontend speichern. Diese MUSS vom Anwendungsfrontend bei Nutzung des IdP-Dienstes übertragen werden.[<=]		entsprechend dieser Anforderung. Dies geschieht in während der Anfrage und Lösung der Challange. Diese wird jedoch nicht beim Abrufen des Discovery Documents aus dem IDP-Dienst durch die Anwendungen übertragen. Da bei diesem Auruf jedoch die API Dokumentation der Gematik keine Übetragung in diesem Schritt vorschreibt, ist hier lediglich eine Bemerkung vermerkt.					
A_20605	Fehlermeldung des Token-Endpunktes Formatierung	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS den Inhalt der Fehlermeldungen sowie mögliche Hinweise zur Fehlervermeidung vom Token-Endpunkt übernehmen.[<=] Hinweis: Es ist insbesondere der Inhalt der Fehlermeldung gemeint. Die Formatierung darf den Gegebenheiten des Endgerätes entsprechend angepasst werden.	Penetrationstest Quellcodeanalyse	Die durch die API übergebenen Fehlermeldungen werden dargestellt. Dieses Verhalten konnten wir mittels Quellcodeanalyse bestätigen. Die Darstellung erfolgt an die jeweiligen Systeme geeignet angepasst.	AFO umgesetzt	kein Sicherheitsmangel			
A_20606	Anwendungsfrontend: Kommunikation überTLS-Verbindung	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS mit dem IdP-Dienst über TLS kommunizieren.[<=]	Penetrationstest Quellcodeanalyse	Als Kommunikation mit dem IdP-Dienst wird sowohl unter Android als auch unter iOS ausschließlich eine Verbindung mittels TLS zugelassen. Andere Kommunikationswege sind nicht definiert und können nicht genutzt werden..	AFO umgesetzt	kein Sicherheitsmangel			
A_20608	Anwendungsfrontend: Unzulässige TLSVerbindungen ablehnen	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS bei jedem Verbindungsaufbau den IdP-Dienst anhand seines TLS-Zertifikats authentifizieren und MUSS die Verbindung ablehnen, falls die Authentifizierung fehlschlägt.[<=]	Penetrationstest Quellcodeanalyse	Die Umsetzung dieser Anforderung wurde innerhalb des Quellcodes beider Anwendungen validiert. Die Umsetzung wird unter Android über das Setzen der network_security_config.xml und deren Applicationsweiten Einstellungen getätigt. Darüber hinaus werden, auch für ältere SDK Versionen, die einzusetzenden Ciphren und Protokolle codeseitig festgelegt. Die Umsetzung innerhalb von iOS wird mittels ATS realisiert und über die gesamte Anwendung hinweg festgelegt. Hierbei ist jeweils keine Kommunikation im Klartext erlaubt.	AFO umgesetzt	kein Sicherheitsmangel			
A_20623	Anwendungsfrontend: Prüfung der Signatur	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS die Signatur des Discovery Document mathematisch prüfen und auf ein zeitlich	Penetrationstest Quellcodeanalyse	Die Implementierung unter Android prüft das Discovery Document entsprechend der	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
	des Discovery Document		gültiges C.FD.SIG-Zertifikat mit der Rollen-OID "oid_idpd" zurückführen können, welches rückführbar ist auf ein CA-Zertifikat aus einer authentischen, integren und zeitlich gültigen TSL.[<=]		Anforderung richtig. Auch die Unterbrechung der weiteren Verarbeitung wird eingehalten. Auch das Zurückführen der Zertifikatskette auf den Root wird hierbei durchgeführt. Für iOS wurde festgehalten, dass das Discovery Document entgegen der vorhandenen Zertifikate in der Anwendung geprüft wird. Dies geschieht, durch die Implementierung des Truststores und der Validierungsfunktion auf Basis zeitlich gültiger Zertifikate. Somit ist die Anforderung umgesetzt.					
A_20624	Anwendungsfrontend: Prüfung der Signatur des AUTHORIZATION_CODE	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS die Signatur des AUTHORIZATION_CODE mathematisch prüfen und auf ein zeitlich gültiges C.FD.SIG-Zertifikat mit der Rollen-OID oid_idpd zurückführen können, welches rückführbar ist auf ein CA-Zertifikat aus einer authentischen, integren und zeitlich gültigen TSL.[<=]	Penetrationstest Quellcodeanalyse	Auskunftsgemäß (Michael Henke, Gematik) fällt diese Anforderung im Rahmen der Anpassung von gemF_Tokenverschluesselung weg.	AFO entbehrlich	kein Sicherheitsmangel			
A_20625	Anwendungsfrontend: Prüfung der Signatur des ID_TOKEN	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS die Signatur des "ID_TOKEN" mathematisch prüfen und auf ein zeitlich gültiges C.FD.SIG-Zertifikat mit der Rollen-OID oid_idpd zurückführen können, welches rückführbar ist auf ein CA-Zertifikat aus einer authentischen, integren und zeitlich gültigen TSL.[<=]	Quellcodeanalyse	"Wir konnten die Umsetzung mittels Quellcodeanalyse prüfen. Unter beiden Betriebssystemen wird die Signatur des ID_TOKEN geprüft und auf ein gültiges C.FD.SIG-Zertifikat zurückgeführt. Eine fehlgeschlagene Prüfung führt zu einer Fehlermeldung (""invalidSignature ID_TOKEN"") und setzt den Funktionsaufruf zurück. Somit kann nur nach erfolgreicher Prüfung des Zertifikats und Rückführung dieses auf ein CA-Zertifikat anhand einer vertrauenswürdigen Zertifikatskette fortgefahren werden.	AFO umgesetzt	kein Sicherheitsmangel			
A_20740	Bekanntgabe der Redirect-URI desAnwndungsfrontend	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS beim IdP-Dienst bei der Registrierung eine "redirect_uri" hinterlegen. [<=] Hinweis: Der IdP-Dienst nutzt die registrierte "redirect_uri" im späteren Verlauf dazu, eine Redirection auszuführen. Dabei wird der ausgestellte "AUTHORIZATION_CODE" vom	Penetrationstest Quellcodeanalyse	In beiden App-Versionen wird im Quellcode zum IDP Client (iOS RealIDPClient.swift; Android IdpService.kt) die redirect_uri als Teil des Requests hinterlegt.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			Authenticator-Modul an das Anwendungsfrontend weitergeleitet.							
A_20741	Speicherung des Downloadpunktes desDiscovery Document im Anwendungsfrontend	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS den vom IdP-Dienst bei der Registrierung bekanntgegebenen Downloadpunkt des Discovery Document als konfigurierbaren Parameter speichern. [<=] Hinweis: Über das Discovery Document können u. a. die URIs der Endpunkte des IdPDienstes und die Adressen der dazugehörigen öffentlichen Schlüssel bezogen werden.	Penetrationstest Quellcodeanalyse	Der IdP-Endpoint ist sowohl unter Android als auch unter iOS als konfigurierbarer Parameter in den Einstellungen enthalten. Dieser wird persistent gespeichert und bleibt somit nach der Registrierung erhalten.	AFO umgesetzt	kein Sicherheitsmangel			
A_21218	E-Rezept-Client, Zertifikatsprüfung auf Basis derX.509-Root	gemSpec_Krypt	Das E-Rezept-FdV MUSS die RCA3 (das Zertifikat der Version 3 der X.509-Root der TI) als Vertrauensanker im Programm-Code bzw. mit dem Programm-Code fest assoziiert enthalten und als Basis für die Prüfung von TI-Zertifikat verwenden. Das FdV MUSS einen TI-Zertifikate-Truststore enthalten und pflegen, wie folgend definiert. Der Truststore MUSS Prüfschlüssel/Zertifikat aufgeteilt in folgende vier Kategorien enthalten: (A) Root-Schlüssel, (B) CA-Zertifikate, (C) E-Rezept-VAU-Zertifikat, (D) IDPZertifikat(e). Initial kann dieser Truststore nur RCA3 enthalten oder die Zertifikate die mittels Tab_KRYPT_ERP_FD_Zertifikatsliste_erstellen ermittelt werden. Falls im Truststore keine Zertifikate für Kategorie (C) und (D) vorliegen, so MUSS das FdV den Truststore aktualisieren indem es über den FD (URL /CertList) die Zertifikatsliste lädt und diese mittels des Algorithmus Tab_KRYPT_ERP_FdV_Truststore_aktualisieren prüft und ggf. in den Truststore lädt. Das E-Rezept-FdV MUSS über den FD (URL /OCSPList) OCSP-Responses für die Zertifikate (C) und (D) beziehen, wenn aktuell keine OCSP-Responses für diese Zertifikate im FdV vorliegen, die jünger als 12 Stunden sind. Falls in der OCSP-Liste OCSP-Responses enthalten sind die zu keinem der Zertifikate (C) und (D) passen, so MUSS das FdV den Truststore aktualisieren (s. o.). Zertifikate aus (C) und (D) MÜSSEN OCSP-Responses, die jünger als 12 Stunden sind besitzen, damit diese Zertifikate in fachliche Use-Cases im FdV verwendet werden können. Die OCSP-Responder-Zertifikate MÜSSEN per Signaturprüfung auf ein Zertifikat der Kategorie (B) rückführbar sein, ansonsten	Quellcodeanalyse	Folgendes konnten wir in Quellcodeanalysen feststellen: (zB iOS: VAUCertificate, VAUSession, DefaultTrustStoreSession, X509TrustStore, VAUTrustStore; Android: NetworkingModule.kt (X509TrustManager), TrustStoreUseCase, TrustStoreModule) Die generelle Aufteilung der Zertifikate ist der Anforderung entsprechend. Die Root CA ist hinterlegt und dient als Grundlage für die Überprüfung der dann noch nachzuladenden Zertifikate. Truststores sind gemäß der Anforderung enthalten und beherbergen die genannten Kategorieren. Mittels Fachdienst können diese nachgeladen und geprüft werden. Die weitere Prüfung der OCSP-Responder-Zertifikate erfolgt anforderungsgemäß. Hier wird eine Lebensdauer von 12h vorgesehen. Schlägt eine der o.g. Prüfungen fehl, wird dies als FAIL bewertet. Die Umsetzung der Anforderung im Quellcode (insb. aller Unterschritte) erfolgt u.A.n. korrekt. Somit bewerten wir A_21218 als umgesetzt.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			MÜSSEN die entsprechenden OCSP-Responses verworfen werden. Das FdV MUSS bei der Prüfung der TI-Zertifikate in fachlichen Use-Cases im FdV, prüfen ob das Zertifikat im oben beschriebenen Truststore enthalten ist und eine gültige OCSPResponse enthält die jünger als 12 Stunden ist. Falls dies nicht so ist, so ist das Ergebnis der Prüfung des TI-Zertifikats FAIL.							
A_21222	E-Rezept-Client, allgemein Zertifikatsprüfung	gemSpec_Krypt	Ein E-Rezept-Client MUSS bevor er TI-X.509-Zertifikate in fachlichen Abläufen (bspw. VAU-Kanal) verwendet, diese Zertifikate prüfen (vgl. A_21216 und A_21218).[<=]	Quellcodeanalyse	In einer Quellcodeanalyse konnten wir feststellen, dass beide App-Versionen alle X.509 Zertifikate der TI prüfen bevor diese verwendet werden. Insb. mit Blick auf A_21218 sowie GS-A_4357 und GS-A_4361 konnte bestätigt werden, dass sowohl a) eine Prüfung aller Zertifikate stattfindet, und b) diese gemäß den bis 2023 geltenden Anforderungen aus gemSpec_Krypt hinreichend sicher sind.	AFO umgesetzt	kein Sicherheitsmangel			
A_21275-01	TLS-Verbindungen, zulässige Hashfunktionenbei Signaturen im TLS-Handshake	gemSpec_Krypt	Alle Produkttypen, die Übertragungen mittels TLS durchführen, MÜSSEN sicherstellen, dass 1. sie im Rahmen der Erstellung und Prüfung von digitalen Signaturen im Rahmen des TLS-Handshakes ausschließlich folgende kryptographisch geeignete Hashfunktionen verwenden: a. SHA-256, SHA-384, SHA-512 [FIPS-180-4] b. SHA3-256, SHA3-384, SHA3-512 [FIPS-202] 2. sie dabei mindestens SHA-256 unterstützen, (Bitte die Umsetzungshinweise in Bezug auf die "signature_algorithms"-Extension in gemSpec_Krypt#A_21275-* beachten.)[<=] **Umsetzunghinweise** zu A_21275-*: Bei den Anwendungsfällen der TI-Anwendungen sind die Mehrzahl der TLS-Verbindungen einseitig authentisiert. D. h. beim TLS-Handshake signiert nur der TLS-Server dessen (EC)DH-Schlüssel. Bei der Initiierung der TLS-Verbindung sendet der TLS-Client in der "signature_algorithms"-Extension beim ClientHello. In der Extension werden alle vom Client unterstützen Hashfunktionen kodiert. Dort muss also nach A_21275-* mindestens SHA-256 enthalten sein. Bei TLS 1.2 wird von fast allen TLS-Bibliotheken ebenfalls SHA-1 angegeben, dieses Verhalten lässt	Penetrationstest Quellcodeanalyse	Innerhalb der Anwendungen konnten wir per Quellcodeanalyse feststellen: es werden gängige und vom Hersteller (des Betriebssystems) bereitgestellte Mechanismen genutzt, um TLS Verbindungen auf die entsprechenden Parameter bestmöglich einzuschränken. Beide Hersteller bieten keine Möglichkeit an, die für die Validierung der Zertifikate genutzten Hashfunktionen anzupassen, und durch die minimale SDK und iOS Version wird sichergestellt, dass mindestens SHA256 unterstützt wird.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			sich im Normalfall nicht ohne Code-Änderungen in den Bibliotheken verändern -- dieses Verhalten widerspricht zunächst A_21275-*. Das bloße Aufführen von SHA-1 als grundsätzlich unterstützte Hashfunktion soll nicht als fehlerhaftes Verhalten gelten. Wichtig für die Umsetzung von A_21275-* sind die tatsächlich erstellten Signaturen und die Prüfung dieser Signaturen. Informationen zu Algorithmen in der "signature_algorithms"-Extension findet man in [RFC-5246#7.4.1.4.1.] und [RFC-8446-4.2.3.].							
A_21332	E-Rezept: TLS-Vorgaben	gemSpec_Krypt	Ein E-Rezept-FD, ein Apothekenverzeichnis, ein E-Rezept-Client und ein IDP MÜSSEN in Bezug auf die TLS-Verbindung zwischen ihnen 1. folgende Ciphersuiten unterstützen • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x30), • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2F), • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x2C), • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2B). 2. Sie KÖNNEN weitere Cipher-Suiten aus [TR-02102-2, Abschnitt 3.3.1 Tabelle 1] unterstützen. 3. Bei dem ephemeren Elliptic-Curve-Diffie-Hellman-Schlüsselaustausch und bei der Signaturprüfung mittels ECDSA MÜSSEN die Kurven P-256 oder P-384 [FIPS-186-4] unterstützt werden. Daneben SOLLEN die Kurven brainpoolP256r1, brainpoolP384r1 oder brainpoolP512r1 (vgl. [RFC-5639] und [RFC-7027]) unterstützt werden. Andere Kurven SOLLEN NICHT verwendet werden (Hinweis: die Intention des letzten Satzes ist insbesondere, dass die Ordnung des Basispunktes in E(F_p) nicht zu klein werden darf). [<=] Hinweis: GS-A_4384 (TLS_DHE_RSA_WITH_AES_128_CBC_SHA etc.) ist absichtlich nicht den Produkttypen der E-Rezept-Anwendung zugewiesen. Die Interoperabilität zu den Konnektoren ist mindestens über die ersten beiden Ciphersuiten aus A_21332 (1) sichergestellt, ebenfalls über A_17094-*. Ähnlich wie bei der Anwendung ePA endet die TLS-Verbindung am E-Rezept-	Penetrationstest Quellcodeanalyse	"Innerhalb der Android Anwendung werden die entsprechenden Cipher-Suites aus Punkt 1 und 2 unterstützt und beschränkt. Auch die Kurven P-256 und P-384 werden unterstützt. Unter iOS wird aktuell lediglich die Verbindung auf mindestens TLS.1.2 festgelegt. Die Unterstützung für die vorgegebenen Cipher-Suites und Kurven ist vorhanden. Weiter unterstützen die Anwendung für beide Betriebssysteme die Kurve x25519 verwenden, welche jedoch durch die App Entwickler nicht deaktiviert werden kann.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			FD an der Webschnittstelle (Eingangspunkt). Ziel ist es die Code-Komplexität innerhalb der VAU so gering wie möglich zu halten (Trusted Computing Base), um eine ausreichende Sicherheitsanalyse des VAU-Programmcodes überhaupt erst möglich zu machen. Dafür werden die Probleme des TLS-Handlings, der Lastverteilung und des DoS-Schutzes auf Applikationsebene außerhalb der VAU an den Webschnittstellen des Fachdienstes ERezept bearbeitet. So kann sich der Programmcode in der VAU auf seine zentrale Aufgabe des Zugriffsschutzes der über die VAU einstellbaren und abholbaren E-Rezepte fokussieren. Um die Verbindungsstrecke zwischen Webschnittstelle und E-Rezept-VAU in Bezug auf Vertraulichkeit zu schützen, wird eine Verschlüsselung auf Anwendungsebene eingeführt. Bei ePA ist dies das VAU-Protokoll. Beim E-Rezept kann aufgrund der andersartigen Anwendungslogik in der E-Rezept-VAU ein einfacheres Sicherungsverfahren verwendet werden. Dieses ist in Abschnitt 7- Kommunikationsprotokoll zwischen E-Rezept-VAU und E-Rezept-Clients normativ definiert.							
GS-A_4357	X.509-Identitäten für die Erstellung und Prüfungdigitaler nicht-qualifizierter elektronischerSignaturen	gemSpec_Krypt	Alle Produkttypen, die X.509-Identitäten bei der Erstellung oder Prüfung digitaler nichtqualifizierter elektronischer Signaturen verwenden, MÜSSEN die in Tab_KRYPT_002 aufgeführten Algorithmen unterstützen und die Tabellenvorgaben erfüllen. Produkttypen, die Zertifikate (X.509-Identitäten) auf Basis der Schlüsselgeneration „ECDSA“ ausstellen (vgl. Abschnitt 5.1) oder verwenden, MÜSSEN die in Tab_KRYPT_002a aufgeführten Algorithmen und die Tabellenvorgaben erfüllen. [<=]	Quellcodeanalyse	In einer Quellcodeanalyse (mit Blick auf die genutzen Crypt-Routinen) konnten wir verzifizieren, dass beide Apps öffentliche Schlüssel auf RSA Basis verwenden und eine Schlüssellänge von 2048bit nutzen (iSv Tab_KRYPT_002, Zelle [2,1]). Im Weiteren wird stets SHA-256 mit RSA gemäß Tab_KRYPT_002, Zelle [2,2], verwendet, um die genannten Anwendungsfälle abzudecken: - Zertifikate signieren - OCSP-Responses und OCSP-Responder Zertifikate signieren - Eine CRL signieren - Zertifikate auf Basis einer CRL signieren Der zweite Teil der Anforderung hinsichtlich der Ausstellung von Zertifikaten hinfällig, da das eRp-FdV keine Zertifikate selbst ausstellt.	AFO umgesetzt	kein Sicherheitsmangel			
GS-A_4361	X.509-Identitäten für die Erstellung und	gemSpec_Krypt	Alle Produkttypen, die X.509-Identitäten verwenden, die zur Erstellung und Prüfung	Penetrationstest Quellcodeanalyse	Analog zur Betrachung von GS-A_4357 werden die	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
	Prüfungdigitaler Signaturen		digitaler Signaturen in Bezug auf TI-Komponenten (technische X.509-Zertifikate) genutzt werden, MÜSSEN alle in Tab_KRYPT_002 aufgeführten Algorithmen unterstützen und die Tabellenanforderungen erfüllen. Produkttypen die Zertifikate (X.509-Identitäten) auf Basis der Schlüsselgeneration „ECDSA“ ausstellen (vgl. Abschnitt 5.1) oder verwenden, MÜSSEN die in Tab_KRYPT_002a aufgeführten Algorithmen und die Tabellenvorgaben erfüllen. [<=]		Anforderungen und Algorithmen aus Tab_KRYPT_002 umgesetzt bzw. unterstützt. Dies ist insbesondere in Bezug auf TI-Komponenten ebenso der Fall, da die genutzten X.509 Routinen für Identitäten einheitlich für alle X.509 Prüfungen genutzt werden. Zertifikatsausstellungen sind nicht Teil des eRp-FdV.					
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt	Alle Produkttypen, die Zufallszahlen generieren, MÜSSEN die Anforderungen aus [BSITR-03116-1#3.8 Erzeugung von Zufallszahlen] erfüllen.	Quellcodeanalyse	"Wir konnten die Anforderung mittels Quellcodeanalyse prüfen. Die androidseitige Implementierung nutzt für die Generierung von Zufallszahlen einen Seed mit 256 Bit Entropie und einen kryptografisch starken Zufallszahlengenerator. Diese Umsetzung entspricht den Anforderungen der TR-03116-1 (Kapitel 3.8). Der unter iOS eingesetzte PRNG nutzt für die Generierung von Zufallszahlen 128 Bit Entropie oder mehr. Für die Umsetzung wird die vom Hersteller (Apple) bereitgestellte Kryptografie Schnittstelle des Betriebssystems (secureRandom bzw SecRandomCopyBytes) genutzt.	AFO umgesetzt	kein Sicherheitsmangel			
GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt	Alle Produkttypen, die Schlüssel erzeugen, MÜSSEN die Anforderungen aus [BSI-TR03116-1#3.9 Schlüsselerzeugung] erfüllen.[<=] Hinweis: im Rahmen der Sicherheitszertifizierung von Komponenten, wie bspw. des Konnektors, wird dies überprüft.	Penetrationstest Quellcodeanalyse	Unter iOS werden zur Schlüsselerzeugung Zufallszahlen von SecRandomCopyBytes genutzt. Diese Funktion erzeugt Zufallszahlen basierend auf verschiedensten Sensoren wie zB dem Beschleunigungssensor und dem Kompass sowie Gyroskop. Mit Verweis auf die BSI TR-03116-1#3.8, die Anforderungen an physikalische Zufallszahlengeneratoren stellt und mittels BSI AIS-31 (und referenzierter Quellen)	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
					präzisiert, bewerten wir die mit iOS-Bordmitteln erzeugten Zufallszahlen als hinreichend sicher. Eine analoge Betrachtung ergab sich uns bei der Prüfung der Android-nativen Zufallszahlengeneratoren rund um "SecureRandom". Diese sind laut Aussagen und Tests von Google selbst FIPS-140-2 compliant und bieten somit eine ähnliche gute Sicherheit. Die Zufallszahlen beider Betriebssysteme sind also iSv BSI-TR-03116-1#3.8 sicher genug und stellen Class PTG.3 Zufallszahlengeneratoren iSv BSI AIS 31 bzw. KS2011 (Quelle aus AIS 31) dar. Mit Blick auf die Schlüsselerzeugung nach BSI-TR-03116-1#3.9, die auf die Zufallszahlen angewiesen ist, konnten wir auch hier die Implementierungen beider Betriebssysteme prüfen. Die verwendeten Schlüssellängen sind für äquivalente Funktionen identisch. Für symmetrische Schlüssel wird auf AES (GCM) zurückgegriffen, welches lt. BSI-TR-03116-1#3.9.1 keine schwachen oder semi-schwachen Schlüssel nutzt. Asymmetrische Schlüssel setzen im Falle von Verfahren, die auf elliptische Kurven zurückgreifen, auf die Standardkurven der BSI TR-03111 (brainpool). Asymmetrische Schlüssel aller DSA-Varianten setzen auf den Digital Signature Standard (DSS) und nutzen somit nur dessen empfohlene Schlüssellängen.					
GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt	Alle Produkttypen, die Übertragungen mittels TLS durchführen, MÜSSEN die TLS-Version 1.2 [RFC-5246] unterstützen. [<=]	Penetrationstest Quellcodeanalyse	Die Standard-HTTP-Schnittstelle setzt als Mindestversion TLS 1.2 an. Dies geht aus dem Quellcode klar hervor und konnte in praktischen Tests bestätigt werden.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
GS-A_4387	TLS-Verbindungen, nicht Version 1.0	gemSpec_Krypt	Alle Produkttypen, die Übertragungen mittels TLS durchführen, DÜRFEN NICHT die TLSVersion 1.0 unterstützen.[<=]	Penetrationstest Quellcodeanalyse	Die Standard-HTTP-Schnittstelle setzt als Mindestversion TLS 1.2 an. Dies geht aus dem Quellcode klar hervor und konnte in praktischen Tests bestätigt werden.	AFO umgesetzt	kein Sicherheitsmangel			
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt	Alle Produkttypen, die Daten über Datenleitungen übertragen wollen, DÜRFEN NICHT das SSL-Protokoll unterstützen.[<=]	Penetrationstest Quellcodeanalyse	Innerhalb von iOS wird die Anforderung über das Setzen der Minimalen TLS Version auf 1.2 realisiert und somit umgesetzt. Innerhalb der Android Anwendung wird die Anforderung über das Setzen der entsprechenden Ciphersuites und TLS Version eingerichtet.	AFO umgesetzt	kein Sicherheitsmangel			
GS-A_5322	Weitere Vorgaben für TLS-Verbindungen	gemSpec_Krypt	Alle Produkttypen, die Übertragungen mittels TLS durchführen, MÜSSEN u. a. folgende Vorgaben erfüllen: • Falls der Produkttyp als Klient oder als Server im Rahmen von TLS an einer Session-Resumption mittels SessionID (vgl. [RFC-5246, Abschnitt 7.4.1.2]) teilnimmt, MUSS er sicherstellen, dass nach spätestens 24 Stunden das über den Diffie-Hellman-Schlüsselaustausch ausgehandelte Schlüsselmaterial und alles davon abgeleitete Schlüsselmaterial (vgl. [RFC-5246, Abschnitt 8.1 und 6.3]) bei ihm sicher gelöscht wird. • Falls der Produkttyp als Klient im Rahmen von TLS an einer Session-Resumption nach [RFC-5077] teilnimmt, MUSS er sicherstellen, dass nach spätestens 24 Stunden das über den Diffie-Hellman-Schlüsselaustausch ausgehandelte Schlüsselmaterial und alles davon abgeleitete Schlüsselmaterial (vgl. [RFC-5246, Abschnitt 8.1 und 6.3]) bei ihm sicher gelöscht wird. Damit verbundene SessionTickets MUSS er ebenfalls sicher löschen. • Falls der Produkttyp als Server im Rahmen von TLS an einer Session-Resumption nach [RFC-5077] teilnimmt, MUSS er sicherstellen, dass nach spätestens 24 Stunden das über den Diffie-Hellman-Schlüsselaustausch ausgehandelte Schlüsselmaterial und alles davon abgeleitete Schlüsselmaterial (vgl. [RFC-5246, Abschnitt 8.1 und 6.3]) bei ihm sicher gelöscht wird. Damit verbundene SessionTickets MUSS er, falls bei ihm vorhanden, sicher löschen. Das	Penetrationstest Quellcodeanalyse	Für Android gilt, dass Aufgrund der Stanard Implementeirung des javax.net.ssl.SSLSessionContextImpl die SessionTimeout auf 24h gesetzt ist, somit wird das verwendete Schlüselmaterial innerhalb der Session gelöscht. Da Session Tickets verwendet werden gilt, dass nach 24 das ausgehandelte DH-Schlüsselmaterial nach eine Session Resumption auch gelöscht ist. Da Android BoringSSL als Standardbibliothek verwendet, was auf einer OpenSSL Version > 0.9.8m basiert, ist boringSSL compliant mit der RFC-5746. Für iOS gilt, dass die App die internen Bibliotheken (CoreTLS) verwendet. Dort sieht man in der Datei appleSession.c, dass eine Session für 10 Minuten definiert ist. Während der Initalisierung oder Reinitalisierung, wird die Lifetime der Session geprüft und gegebenenfalls die Session gelöscht. (siehe Funktionen SessionCacheLookupEntry() und SessionCacheEntryDelete()). Core TLS verhält sich auf compliant zu RFC-5746 (nachvollziehbar in	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			Schlüsselmaterial, dass bei der Erzeugung des SessionTickets (für die Sicherung von Vertraulichkeit und Authentizität der SessionTickets) verwendet wird, MUSS spätestens alle 48 Stunden gewechselt werden und das alte Material MUSS sicher gelöscht werden. Als kryptographische Verfahren zur Erzeugung/Sicherung der SessionTickets MÜSSEN ausschließlich nach [BSI-TR-03116-1] zulässige Verfahren verwendet werden und das Schlüsselmaterial muss die Entropieanforderungen gemäß [gemSpec_Krypt#GS-A_4368] erfüllen. • Falls ein Produkttyp als Klient oder Server im Rahmen von TLS die Renegotiation unterstützt, so MUSS er dies ausschließlich nach [RFC-5746] tun. Ansonsten MUSS er die Renegotiation-Anfrage des Kommunikationspartners ablehnen.		sslHandshakeHello.c und sslHandshake.h). Da beide FdVs lediglich als Client an der Session teilnehmen ist Unterpunkt drei nicht relevant.					
GS-A_5339	TLS-Verbindungen, erweiterte WebbrowserInteroperabilität	gemSpec_Krypt	Alle Produkttypen, die TLS verwenden und bei denen insbesondere WebbrowserInteroperabilität (Webportale, Download-Punkte o. Ä.) wichtig ist, MÜSSEN zur Absicherung der TLS-Übertragung neben der in [gemSpec_Krypt#GS-A_4384] aufgeführten Vorgaben zusätzlich Folgendes sicherstellen: 1. Der Produkttyp MUSS zusätzlich folgende Ciphersuiten unterstützen: • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC0, 0x14), • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC0, 0x13), • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x30) und • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2F). 2. Der TLS-Server KANN weitere Cipher-Suiten aus [TR-02102-2, Abschnitt 3.3.1 Tabelle 1] unterstützen. 3. Bei dem ephemeren Elliptic-Curve-Diffie-Hellman-Schlüsselaustausch MÜSSEN die Kurven P-256 oder P-384 [FIPS-186-4] unterstützt werden. Daneben KÖNNEN die Kurven brainpoolP256r1, brainpoolP384r1 oder brainpoolP512r1 (vgl. [RFC-5639] und [RFC-7027]) unterstützt werden. Andere Kurven SOLLEN NICHT verwendet werden (Hinweis: die Intention des letzten Satzes ist insbesondere, dass die Ordnung des	Quellcodeanalyse Befragung	"In einer Quellcodeanalyse konnte verifiziert werden, dass iSv (1) alle genannten Ciphersuiten unterstützt werden. Darüber hinaus werden unter TLS 1.2 iSv (2) die folgenden ECDHE Ciphersuites unterstützt, die laut [TR-02102-2, Abschnitt 3.3.1] bis 2027+ verwendet werden können: - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384. Außerdem wird unter TLS 1.2 eine ECDH Ciphersuite genutzt: - TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256. Drei Ciphersuiten unter TLS 1.3 kommen zum Einsatz: - TLS_AES_128_GCM_SHA256, - TLS_AES_256_GCM_SHA384, -	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			Basispunktes in E(F_p) nicht zu klein werden darf).		TLS_CHACHA20_POLY1305_ SHA256. Zu (3) gilt es zu sagen, dass die Kurven P-256 sowie P-384 zum Einsatz kommen. Darüber hinaus werden alle drei genannten (laut Anforderung optionalen) Brainpool Kurven verwendet. Außer diesen fünf Kurven wird keine weitere verwendet.					
GS-A_5526	TLS-Renegotiation-Indication-Extension	gemSpec_Krypt	Alle Produkttypen, die das TLS-Protokoll verwenden, SOLLEN den RFC 5746 (TLSRenegotiation-Indication-Extension [RFC-5746]) unterstützen.	Penetrationstest Quellcodeanalyse	Die eingesetzte Implementierung nutzt die unterliegende SSLEngine von Google. Diese unterstützt seit der API Version 11 eine konforme Art der Neuverhandlung der TLS Verbindung und erfüllt daher de Anforderungen dieser Anforderung. Als Netzwerkinterface wird innerhalb von iOS die Herstellerigene App Transport Security (ATS) eingesetzt, welche eine sichere TLS Renegotiation unterstützt. Damit erfüllt die Anwendung die Anforderung an die Umsetzung des RFC.	AFO umgesetzt	kein Sicherheitsmangel			
GS-A_5542	TLS-Verbindungen (fatal Alert bei Abbrüchen)	gemSpec_Krypt	Alle Produkttypen, die das TLS-Protokoll verwenden, MÜSSEN sicherstellen, dass alle von ihnen durchgeführten Verbindungsabbrüche (egal ob im noch laufenden TLS-Handshake oder in einer schon etablierten TLS-Verbindung) mit einer im TLS-Protokoll aufgeführten Fehlermeldung (fataler Alert) angekündigt werden, außer das TLS-Protokoll untersagt dies explizit. [<=] Sicherheitsziel bei der Verwendung von TLS in der TI ist die Forward Secrecy [BSI-TR02102-1, S. ix], was sich u. a. in den vorgegebenen CipherSuites (vgl. GS-A_4384 und A_17124) widerspiegelt. Um dieses Ziel zu erreichen, muss sichergestellt werden, dass in regelmäßigen Abständen frisches Schlüsselmaterial über einen authentisierten DiffieHellman-Schlüsselaustausch gebildet wird, welches	Penetrationstest Quellcodeanalyse	Basierend auf der Minimum Anforderung von TLS1.2 lässt sich davon ausgehen, dass eine TLS Verbindung damit abgebrochen wird, dass zumindest ein close_notify mit dem Alert Level "warning" gesendet wird. Mittels TLS - Scan ließ sich nachweisen, dass der Server für "Forward Secrecy" ausgelegt ist und somit das FdV diese Funktionalität nutzen kann. Mittels eines Netzwerkmitschnitts konnte festgestellt werden, dass der Austausch des Schlüsselmaterials nach Initialisierung der Verbindung, durch den Server initiiert und in Folge erfolgreich durchgeführt werden konnte.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			das alte Material ersetzt, wobei das alte Material sowohl im Klienten als auch im Server sicher gelöscht wird. Insbesondere bei der Nutzung von TLS-Resumption (vgl. [RFC-5246, S. 36] oder [RFC-5077]) kann die Dauer einer TLS-Session deutlich länger sein als die Lebensdauer der TCP-Verbindung innerhalb welcher der initiale Schlüsselaustausch stattgefunden hat. Aus diesem Grunde werden analog zu den IPsec-Vorgaben (vgl. [gemSpec_Krypt#GS-A_4383]) Vorgaben für die maximale Gültigkeitsdauer dieses Schlüsselmaterials gemacht (vgl. auch [SDH2016]).							
A_19937	Fehlermeldungen des Token-EndpunktesAnzeige	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS in der Lage sein, die vom Token-Endpunkt übertragenenFehlermeldungen anzuzeigen.	Penetrationstest Quellcodeanalyse	In der API, die mit dem Token Endpoint kommuniziert, ist eine Fehlerbehandlung inbegriffen, die die vom Token Endpoint genannte Fehlermeldung genau darstellt. Dieses Verhalten konnten wir mittels Quellcodeanalyse bestätigen.	AFO umgesetzt	kein Sicherheitsmangel			
A_19938	Annahme des ID_TOKEN	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS das vom Token-Endpunkt ausgegebene "ID_TOKEN" als HTTP/1.1 Statusmeldung 200 verarbeiten. Das Anwendungsfrontend MUSS das "ID_TOKEN" ablehnen, wenn dieses außerhalb der mit dem Token-Endpunkt etablierten TLS-Verbindung übertragen wird.[<=] **Hinweis**: Das Anwendungsfrontend nimmt sowohl den "ID_TOKEN", als auch den "ACCESS_TOKEN" aus der Antwort des Token-Endpunktes des IdP-Dienstes. Der TokenEndpunkt antwortet mit den Token auf die erfolgreiche Übergabe und Validierung des "AUTHORIZATION_CODE" durch das Anwendungsfrontend. Nachfolgend wird beispielhaft die Antwort des Token-Endpunktes skizziert. Der "ID_TOKEN" und der "ACCESS_TOKEN" werden dabei nur angedeutet: HTTP/1.1 200 OK Content-Type: application/json Cache-Control: no-store Pragma: no-cache {"token_type": "Bearer", "expires_in": 300, "id_token": "...",	Penetrationstest Quellcodeanalyse	ID_TOKEN werden als HTTP 200er Status entgegengenommen und verarbeitet. Das ID_TOKEN befindet sich in der Response im Feld "id_token". ID_TOKEN außerhalb einer etablierten TLS-Verbindung werden dahingehend abgelehnt, dass das eRp-FdV diese Verbindungen grundsätzlich ablehnt, unabhängig davon, ob was gesendet wird.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			"access_token": "...", ... }							
A_20032−01	E-Rezept-FdV: Prüfung TI-Zertifikate	gemSpec_eRp_FdV	Das E-Rezept-FdV MUSS bei der Prüfung von X.509-Zertifikaten der TI folgende Prüfschritte durchlaufen. * Prüfung der zeitlichen Gültigkeit des Zertifikats auf Basis der aktuellen Systemzeit (orientiert an [gemSpec_PKI#TUC_PKI_002]) * Ist das Zertifikat kryptographisch (Signaturprüfung) rückführbar auf ein CA-Zertifikat aus einer authentischen und integeren und zeitlich gültigen, vertrauenswürdigen Zertifikatskette? (siehe Festlegungen in [gemSpec_Krypt#7.2.2] "Client-seitige Prüfung der E-Rezept-VAU-Identität") * Prüfung auf den für den Anwendungsfall korrekten Zertifikatstyp gemäß TAB_FdVERP_017. Die OID des Zertifikatstyps gemäß [gemSpec_OID] muss in der Extension CertificatePolicies enthalten sein. * Falls das Zertifikat für den Aufbau des sicheren Kanals zur VAU verwendet wird (VAU-Zertifikat innerhalb des VAU-Protokolls, vgl. [gemSpec_Krypt#Kommunikationsprotokoll zwischen VAU und E-Rezept-Clients]), so MUSS die Rolle "oid_erp-vau" gemäß im EE-Zertifikat aufgeführt sein (analog [gemSpec_PKI#TUC_PKI_009]). Falls nein, MUSS das Zertifikat für den Aufbau des sicheren Kanals zur VAU abgelehnt werden. * Falls das Zertifikat ein EE-Zertifikat ist: Ermittlung der OCSP-Statusinformation. Ist das Zertifikat nicht gesperrt (Status "good" [RFC-6960#2.2 Response]) (vgl. A_15869)? Eine OCSP-Antwort KANN lokal maximal 4 Stunden gecacht und als Prüfgrundlage verwendet werden. Die Prüfung ist analog gemSpec_PKI#TUC_PKI_006 mit den Parametern Referenzzeitpunkt=Systemzeit, OCSP-Graceperiod=4 Stunden. * Prüfung der Extensions KeyUsage und ExtendedKeyUsage auf die richtige Belegung gemäß dem Anwendungsfall (orientiert an [gemSpec_PKI#TUC_PKI_018] Schritt 2). Führt einer der Prüfschritte nicht zu einem positiven Prüfergebnis, so MUSS das Zertifikat abgelehnt werden und die weitere Verarbeitung des Zertifikats oder der	Penetrationstest Quellcodeanalyse	Lt. Projektleitung ist diese Anforderung hinfällig, da sie durch andere Anforderungen der gemSpec_krypt abgebildet wird.	AFO entbehrlich	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			Attribute darin abgelehnt werden. Das E-Rezept-FdV muss die referenzierten technischen Use Cases (TUC_PKI_*) aus [gemSpec_PKI] im Rahmen dieser Anforderung nicht normativ umsetzen.							
A_20079	Ausfall der Fehlermeldung des TokenEndpunktes	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS im Falle eines Timeout selbständig eine Fehlermeldung generieren, wenn eine Fehlermeldung durch den Token-Endpunkt ausbleibt.[<=]	Penetrationstest Quellcodeanalyse	Die Anwendung erzeugt eigenständige Fehlermeldungen wenn eine Verbindung zum Dienst nicht möglich ist bzw. das Zeitlimit überschirtten wird. Dies wurde in beiden Anwendungen gleichermaßen nachgewiesen.	AFO umgesetzt	Sicherheitsempfehlung			
A_20085	Fehlermeldungen des Anwendungsfrontends	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS leicht verständliche Fehlermeldungen ausgeben. Eine exakte Form der Fehlermeldung ist nicht vorgegeben [RFC6749 # section-1.7 <https://tools.ietf.org/html/rfc6749#section-1.7>].	Penetrationstest Quellcodeanalyse	In einem Penetrationstest haben wir verschiedene Fehlermeldung mittels konfigurierbarer Parameter oder per Steuerung von Betriebssystemsettings (zB WLAN) provoziert. Die meisten der uns vorliegenden Fehlermeldungen sind verständlich und geben klare Auskunft darüber, was das Problem ist und (wenn nicht serverseitig) wie es zu lösen ist bzw. wo man Hilfe erhält. Hier wählt das eRp-FdV für Fehlermeldungen eine rote Schrift, die gemeinhin mit Fehlermeldungen verbunden wird. Die Formulierungen sind klar. Jedoch gilt das nicht für alle Fehlermeldungen. Zum Beispiel bei einem Fehler beim Parsing des JWT erscheint lediglich der Fehler "JWTError.malformedJWT". Diesen Fehler konnten wir jedoch nicht während der normalen Nutzung der App provozieren, sondern nur dadurch, dass wir in einem Penetrationstest manipulierte JWTs genutzt haben. Per normalem Execution Workflow sollte dieses Fehler nicht auftreten können. Somit bewerten wir die Anforderung als umgesetzt, sprechen aber eine Empfehlung darüber aus, alle Fehlermeldungen - auch solche, die eigentlich nicht in der normalen Nutzung	AFO umgesetzt	Sicherheitsempfehlung	Wir empfehlen, auch solche Fehlermeldungen, die normale Nutzer der programmatischen Logik folgend nicht erhalten, klar zu formulieren und die Platzhalter zu nutzen.		

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
					auftreten können, die aber im Quellcode vorbereitet sind, zu überprüfen und die Platzhalter entsprechend zu nutzen/ersetzen.					
A_20161-01	E-Rezept-Client, Request-Erstellung	gemSpec_Krypt	Ein E-Rezept-Client MUSS, falls ihm noch kein gültiges E-Rezept-VAU-Zertifikat vorliegt, ein solches nach den fachlichen Vorgaben von A_20160 beziehen (/VAUCertificate). Ein E-Rezept-Client MUSS sicherstellen, dass gültige Sperrinformation (OCSP-Response mit Sperrstatus "good") für das Zertifikat vorliegen, die maximal 12 Stunden alt sind. Liegen diese nicht vor so MUSS der Client ein Verbindungsaufbau auf VAU-Protokoll-Ebene ablehnen/unterbinden. Ein E-Rezept-Client MUSS bei der Request-Erstellung folgende Schritte durchführen. 1. Er erzeugt einen HTTP-Request, den er an die VAU senden möchte, als Datenstruktur (vgl. Beispiele nach dieser Anforderung). 2. Er erzeugt zufällig eine 128-Bit lange hexadezimalkodierte Request-ID (also 32 Zeichen, Buchstaben a-f kleingeschrieben). 3. Er erzeugt zufällig einen 128-Bit AES-Schlüssel (im Weiteren auch Antwortschlüssel genannt), den er hexadezimal kodiert (also 32 Zeichen, Buchstaben a-f kleingeschrieben). 4. Er MUSS die Request-ID und den AES-Schlüssel für jeden HTTP-Request an die VAU zufällig neu erzeugen. 5. Er erzeugt die folgende Zeichenkette p mit p="1" + " " + JWT-Authentisierungstoken + " " + Request-ID + " " + AESSchlüssel + " " + Datenstruktur aus Schritt 1. 6. Die Zeichenkette p MUSS mittels des ECIES-Verfahrens [SEC1-2009] und mit folgenden Vorgaben verschlüsselt werden: a. Er MUSS ein ephemeres ECDH-Schlüsselpaar erzeugen und mit diesem und dem VAU-Schlüssel aus A_20160-* ein ECDH gemäß [NIST-800-56-A] durchgeführen. Das somit erzeugte gemeinsame Geheimnis ist Grundlage für die folgende Schlüsselableitung. b. Als Schlüsselableitungsfunktion MUSS er die HKDF nach [RFC-5869] auf Basis von SHA-256 verwenden. c. Dabei MUSS er den Ableitungsvektor "ecies-vau-transport" verwenden, d. h. in der Fomulierung von [RFC-5869] info="ecies-vau-transport" .	Penetrationstest Quellcodeanalyse	Wir konnten die Umsetzung der Anforderung anhand mehrerer Quellcodeanalysen verifizieren (zB in VAUInterceptor und VAUCrypto) Das eRp-FdV geht hier für beide Betriebssysteme in der Umsetzung analog vor. Der Request wird als Datenstruktur (Objekt) erzeugt und erhält eine 32-stellige, zufallsbasierte hexadezimal ID (mit Kleinbuchstaben) für jeden Request an die VAU. Ein one-time-use AES-Schlüssel ebenfalls zufallsbasiert erzeugt (mit Entropie gemäß anderer Anforderungen zur kryptografischen Zufallszahlenerzeugung). Diese Informationen werden wie gefordert in einem String gespeichert. Die Umsetzung des ECIES-Verfahren gemäß SEC1-2009 iSv Punkt 6 erfolgt in VAUCrypt.swift bzw. Crypto.kt statt. Der abschließende HTTPS Request, der aus den obigen Schritten folgt, wird nun erzeugt und erfüllt die Spezifikationen der Anforderungen an Pfad, Content-Type und Method.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			d. Er MUSS mit dieser Schlüsselableitung einen AES-128-Bit Content-EncryptionKey für die Verwendung von AES/GCM ableiten. e. Er MUSS für Verschlüsselung mittels AES/GCM einen 96 Bit langen IV zufällig erzeugen. f. Er MUSS mit dem CEK und dem IV mittels AES/GCM p verschlüsseln, wobei dabei ein 128 Bit langer Authentication-Tag zu verwenden ist. g. Er MUSS das Ergebnis wie folgt kodieren: chr(0x01) || <32 Byte X-Koordinate von öffentlichen Schlüssel aus (a) > || <32 Byte Y-Koordinate> || <12 Byte IV> || <AES-GCM-Chiffrat> || <16 Byte AuthenticationTag> (vgl. auch Tab_KRYPT_ERP und folgende die Beispielverschlüsselung). Die Koordinaten sind (wie üblich) vorne mit chr(0) zu padden solange bis sie eine Kodierungslänge von 32 Byte erreichen. 7. Er erzeugt einen HTTPS-Request an den FD mit der POST-Methode und dem Pfad /VAU/<Nutzerpseudonym>[/optional-beliebiger-weiterer-URL-Pfadteil] mit dem Content-Type 'application/octet-stream' und sendet diesen an die Webschnittstelle des FD. "Nutzerpseudonym" MUSS eine ggf. aus der vorherigen (zeitlich letzten) Antwort des FD dem Nutzer übergebene URL-sichere Zeichenkette sein (bspw. ein 128 Byte langer Hexadezimal-Kode). Falls dem Client kein Nutzerpseudonym vorliegt so MUSS er "0" als Nutzerpseudonym verwenden.							
A_20174	E-Rezept-Client, Response-Auswertung	gemSpec_Krypt	Ein E-Rezept-Client MUSS bei der Response-Auswertung (vgl. vorgehenden ClientRequest aus A_20161) folgende Schritte durchführen. Dabei MUSS der Client bei Fehlschlagens im Folgenden aufgeführten Prüfungen die Analyse der Response abbrechen, und er MUSS die Request-ID und den AES-Antwortschlüssel sicher löschen. 1. Er MUSS prüfen, ob der Content-Type der Response 'application/octet-stream' ist. 2. Wenn im Response-Header die Variable "Userpseudonym" vorhanden ist, so MUSS er den Wert von "Userpseudonym" als NP für den nächsten Request an die VAU verwenden. (Der Client MUSS einen ggf. vorhandenen alten Wert des NP im Client überschrieben.) 3. Er MUSS das Antwort-Chiffrat mit den Vorgaben aus A_20163 (9) und dem AESAntwort entschlüsseln und prüfen ob die Entschlüsselung erfolgreich möglich	Penetrationstest Quellcodeanalyse	Die Umsetzung der Anforderung erfolgt unter iOS zum einen in der VAUCrypto und zum anderen innerhalb der VAUInterceptor. Unter Android wird diese innerhalb der VauBase umgesetzt. Eine Antwort wird mit dem symmetrischen AES Schlüssel entschlüsselt. Bei einem Scheitern wird ein Fehler geworfen, andernfalls kann normal fortgefahren werden. Anschließend nutzt das eRp-FdV eine Split Operation, um die korrekte Struktur des Klartextes und das Vorhandensein der Request-ID zu prüfen. Auch hier wird ggf. ein Fehler geworfen, andernfalls gibt die Funktion das dritte Element aus p für die	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			war. 4. Er MUSS prüfen, ob die Struktur des erhaltenen Klartextes p der Struktur aus A_20163 (8) entspricht. 5. Er MUSS prüfen, ob die Request-ID in p der Request-ID aus dem Client-Request entspricht (Gleichheit prüfen). 6. Er MUSS das dritte Feld-Element in p ("Response-Header-und-Body") als HTTPAntwort der E-Rezept-VAU in fachlich weiter verarbeiten.		weitere Verarbeitung zurück. Dieses kann nun von der aufrufenden Funktion weiterverarbeitet werden.					
A_20175	E-Rezept-Client, Speicherung Nutzerpseudonym	gemSpec_Krypt	Ein E-Rezept-Client MUSS das im Request verwendete Nutzerpseudonym (NP) in Software speichern (kein HSM/TPM/SE) und das NP ausschließlich für seinen Einsatzzweck der E-Rezept-VAU-Kommunikation verwenden. Insbesondere MUSS der Client die Vertraulichkeit des NP wahren (bspw. nicht unnötig in Protokolleinträgen und Fehlermeldungen aufführen).[<=] Der Fachdienst E-Rezept besitzt eine REST-Schnittstelle, d. h. Fehler werden mittels HTTP-Status/Fehler-Codes signalisiert. Die in der folgenden Tabelle (Tab_KRYPT_VAUERR) aufgeführten Fehler kann ein E-Rezept-Client in Bezug auf die in diesem Abschnitt definierte kryptographische Sicherung zwischen Client und VAU treffen.	Penetrationstest Quellcodeanalyse	Das Nutzerpseudonym wird in der Android Anwendung im Rahmen der Kommunikation mit dem Fachdienst entnommen und innerhalb einer privaten Variable der aufrufenden Klasse gehalten. Aus dieser wird diese nicht in andere, unsichere Kontexte übergeben. Daher kann die Anforderung als erfüllt angesehen werden. Die Usersession in iOS wird aus der Response des Fachdienstes entnommen und in der darauffolgenden Kommunikation mit dem Dienst verwendet.	AFO umgesetzt	kein Sicherheitsmangel			
A_20283	Annahme des "ACCESS_TOKEN"	gemSpec_IDP_Frontend	Das Anwendungsfrontend MUSS das vom Token-Endpunkt ausgegebene "ACCESS_TOKEN" in der HTTP/1.1 Statusmeldung 200 verarbeiten. Das Anwendungsfrontend MUSS das "ACCESS_TOKEN" ablehnen, wenn dieses außerhalb der mit dem TokenEndpunkt etablierten TLS-Verbindung übertragen wird.[<=]	Penetrationstest Quellcodeanalyse	In einer Quellcodeanalyse (bspw Networkingmodule.kt und TokenPayload.swift) und einem Penetrationstest (Netzwerkmitschnitt) konnten wir für beide App-Versionen folgendes feststellen: Das in der Antwort an das Frontend übermittelte Token wird im Rahmen der Authentisierung an den IDP Fachdienst anforderungskonform weiterverarbeitet. Die TLS-Verbindung wird über betriebssystemnative Funktionen realisiert. Da das eRp-FdV lediglich TLS-Verbindungen erlaubt, wird das ACCESS_TOKEN in allen anderen Fällen abgelehnt.	AFO umgesetzt	kein Sicherheitsmangel			
A_20526-01	Authenticator-Modul: Response auf das CHALLENGE_TOKEN	gemF_Tokenverschlüsselung	"Das Authenticator-Modul MUSS das eingereichte ""CHALLENGE_TOKEN"" mittels JWS (JSON Web	Quellcodeanalyse	Mittels Quellcodeanalyse konnten wir folgendes feststellen:	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
	des Authorization-Endpunktes		Signature) mit der Smartcard signieren, und das Authentifizierungszertifikat der verwendeten Smartcard als x5c Parameter einbetten, dieses Objekt mittels JWE (JSON Web Encryption) mit dem öffentlichen Schlüssel des Authorization-Endpunktes ""PUK_IDP_ENC"" verschlüsseln und in Form eines HTTP-POST-Requests an den Authorization-Endpunktes senden. Der Aufbau der der Anfrage und des der einzureichenden Objekte entspricht gemSpec_IDPDienst# Kapitel 7.3 [<=] Hinweis: Das Signieren und Verschlüsseln des ""CHALLENGE_TOKEN"" ist durch die Verwendung eines Nested JWT [angelehnt an den folgenden Draft: https://tools.ietf.org/html/draft-yusef-oauth-nestedjwt- 03] zu realisieren. Im cty-Header ist ""NJWT"" zu setzen, um anzuzeigen, dass es sich um einen Nested JWT handelt. Das Signieren wird dabei durch die Verwendung einer JSON Web Signature (JWS) [RFC7515 # section-Compact Serialization] gewährleistet. Die Verschlüsselung des signierten Token wird durch die Nutzung der JSON Web Encryption (JWE) [RFC7516 # section-3] sichergestellt. Als Verschlüsselungsalgorithmus ist ECDH-ES (Elliptic Curve Diffie-Hellman Ephemeral Static key agreement) vorgesehen."		Die Umsetzung erfolgt. (iOS: CardWallReadCardDomain; Android: idpUseCase, SignChallengeExchange, AuthenticationUseCaseProduction) Das CHALLENGE_TOKEN wird mittels JSON Web Signature signiert, bekommt das auth-cert der Smartcard eingebettet, wird gemäß Anforderung verschlüsselt und gemäß den Erwartungen des IdP Dienstes als Objekt übermittelt.					
A_20614	"Authenticator-Modul: Prüfung der Signatur des Discovery Document"	gemSpec_IDP_Frontend	Das Authenticator-Modul MUSS die Signatur des Discovery Document mathematisch prüfen und auf ein zeitlich gültiges C.FD.SIG-Zertifikat mit der Rollen-OID "oid_idpd" zurückführen können, welches von einer ihm bekannten Komponenten-PKI ausgestellt wurde. [<=]	Quellcodeanalyse	Analog zu A_20623 konnten wir in einer Quellcodeanalyse folgendes feststellen: Die Anforderung ist wie in A_20623 beschrieben umgesetzt. Zusätzlich konnten wir die Rückführung auf oid_idpd bestätigen.	AFO umgesetzt	kein Sicherheitsmangel			
A_21322	Sichere Speicherung des "SSO-TOKEN"	gemSpec_IDP_Frontend	Das Authenticator-Modul MUSS empfangene SSO-Token gegen unberechtigten Zugriff schützen. [<=]	Penetrationstest Quellcodeanalyse	In einer Quellcodeanalyse und einem Penetrationstest konnten wir feststellen: Empfangene SSO_Token werden für iOS verschlüsselt in der Keychain gespeichert. Diese wird per Schnittstelle regelmäßig als sicherer Speicherungsort genutzt und wird betriebssystemseitig bereitgestellt	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
					(KeychainStorage). Ein Zugriff darauf ist nur von der App möglich. Androidseitig wird ein "IdpRepository" genutzt, das auf SharedPreferences basiert, einer betriebssystemnativen Implementierung zur Ablage von Einstellungen und Informationen. Hier werden Daten, insb. das SSO-Token, verschlüsselt abgelegt. Da die Ablage des SSO_TOKEN für beide Betriebssysteme vor Unberechtigen geschützt ist.					
A_19908-01	Authenticator-Modul: Prüfung der Signatur des "CHALLENGE_TOKEN"	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS die Signatur des ""CHALLENGE_TOKEN"" gegen den aktuellen öffentlichen Schlüssel des Authorization-Endpunktes ""PUK_AUTH"" prüfen.Liegt dem Authenticator-Modul der öffentliche Schlüssel des Authorization-Endpunktes noch nicht vor, MUSS es diesen vom Authorization Server gemäß den Angaben der Adresse PUK_URI_AUTH im Discovery Document abrufen. [<=]	Penetrationstest Quellcodeanalyse	Die Prüfung des Zertifikats und des CHALLENGE_TOKENS konnte über Quellcodeanalysen für iOS und zusätzliche praktische Tests für die Android Anwendung validiert werden. Hierbei wird der öffentliche Schlüssel auf die in der Anwendung vorhandene ROOT-CA zurückgeführt. Beide Anwendungen nutzen einen Authentisierungsflow, bei dem das Discovery Document und andere für die Authentifizierung notwenidgen Schritte vor der Validierung des Challenge Tokens geschehen. Somit wird sichergestellt, dass der notwendige öffentliche Schlüssel vorliegt. Fehlerbehandlungen sind hier an mehreren Stellen eingebaut und verhindern die erfolgreiche Validierung einer falschen bzw. fehlerhaften Signatur.	AFO umgesetzt	kein Sicherheitsmangel			
A_20068-01	"Authenticator-Modul: Prüfung Internet-Zertifikate"	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS das Internet-seitige Zertifikat des IdP-Dienstes prüfen. Hierfür MUSS das Authenticator-Modul sowohl eine Signaturprüfung als auch eine Prüfung der zeitlichen Gültigkeit durchführen. Falls diese Prüfung negativ ausfällt, MUSS es das Zertifikat als ""ungültig"" bewerten. Das Authenticator-Modul MUSS das Zertifikat anhand der Signaturprüfung auf ein CA-Zertifikat einer CA, die die ""CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates"" (https://cabforum.org/baseline-	Quellcodeanalyse	Die zeitliche Prüfung der Internetzertifikate erfolgt automatisch über die Betriebsysteme, auch die Rückführung auf eine gültige CA wird mit dem TrustStores des jeweiligen Betriebssystems durchgeführt.	AFO umgesetzt	Sicherheitsempfehlung	Es ist die Umtesllung von LetsEncrypt auf die neue ISRG Root CA zu beachten da die Lebenszeit der aktuellen IdenTrust CA demnächst abläuft. Es entstehen keine Sicherheitsbedenken, da die neue Zertifizierungsstelle auch den Anforderungen entspricht.		

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			requirements-documents/) erfüllt, zurückführen können. Ansonsten MUSS es das Zertifikat als ""ungültig"" bewerten. [<=] Hinweis: Eine positiv ausgefallene Signaturprüfung von A_20068-01 ist gleichbedeutend damit, dass das CA-Zertifikat im Zertifikats-Truststore eines aktuellen Webbrowsers vorhanden ist"							
A_20499	**Alte Formulierung:** "Authenticator-Modul: Temporäre Speicherung von ""SSO_TOKEN""" **Neue Formulierung:** Authenticator-Modul: aktives Löschen von "SSO_TOKEN"	gemSpec_IDP_Frontend	**Alte Formulierung:** Das Authenticator-Modul MUSS beim aktiven Beenden der Anwendung vorhandene "SSO_TOKEN" aus dem RAM sowie lokal gespeicherte Kopien desselben sicher löschen. [<=] **Neue Formulierung:** A_20499-01 - Authenticator-Modul: aktives Löschen von "SSO_TOKEN" Das Authenticator-Modul MUSS "SSO_TOKEN" löschen, wenn der Anwender einen aktiven Logout durchführt. Dazu MUSS das Authenticator-Modul dem Anwender eine auslösende Funktionalität anbieten. [<=]	Quellcodeanalyse	Die Auslegung der Anforderung wurde nochmals mit der Gematik abgestimmt. Hierbei ist eine Umformulierung der Anforderung in Aussicht gestellt worden. Da die Änderung der Spezifikationslage jedoch nicht mehr bis zum Abschluss des Gutachtens formell abgewickelt werden konnte, wurde die beide Fassungen hinterlegt, die Anwendung jedoch bereits auf die neue Formulierung getestet. Die Funktion zum Logout wird dem Nutzer durch die Anwendung angeboten und diese löscht u.a. den SSO_Token, wie von der Anforderung gefordert.	AFO umgesetzt	kein Sicherheitsmangel		.	
A_20525	Authenticator-Modul: Anzeige des "user_consent" und PIN-Abfrage	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS im Zusammenhang mit der PIN-Abfrage für die Signatur des ""CHALLENGE_TOKEN"" durch die Smartcard im selben Dialog die Consent-Freigabe des ""user_consent"" durch den Nutzer einfordern, damit dieser durch die PIN-Eingabe seine Willenserklärung abgibt und der Verwendung seiner Daten in diesen Claims zustimmt. [<=]	Penetrationstest Quellcodeanalyse	In Android und in iOS wird für die Willenserklärung zur Signatur des CHALLENGE_TOKEN die PIN für der egK abgefragt.	AFO umgesetzt	Sicherheitsempfehlung	In beiden Fällen handelt es sich um eine automatische Willenserklärung ohne Hinweise für den Nutzer. Es ist zu empfehlen, dass der Nutzer noch einmal über einen Dialog/Text auf die Willenserklärung hingewiesen wird.		
A_20527	Authenticator-Modul: Übertragung des "AUTHORIZATION_CODE" an das Anwendungsfrontend	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS den vom Authorization-Endpunkt empfangenen ""AUTHORIZATION_CODE"" an das Anwendungsfrontend übertragen. [<=]	Penetrationstest Quellcodeanalyse	Beide Anwendungen sind für die Verwaltung von E-Rezepten durch einen Endanwender konzipiert und erstellt worden. In diesem Rahmen wurde das Authentication Modul und das Frontend des Versicherten innerhalb der Anwendung implementiert. Da hierbei keine Trennung der beiden Module stattfindet, steht der empfangene AUTHORIZATION_CODE und SSO_TOKEN nach dem	AFO entbehrlich	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
					Empfangen durch die Anwendung, beiden Modulen über die gemeinsame Datenhaltung zur Verfügung.					
A_20600	Authenticator-Modul: Annahme des "user_consent" und des "CHALLENGE_TOKEN"	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS den ""user_consent"" und den ""CHALLENGE_TOKEN"" vom Authorization-Endpunkt des IdP-Dienstes entgegennehmen. [<=]	Penetrationstest Quellcodeanalyse	Über Quellcodeaudits konnte festgestellt werden, dass beide Anwendungen jeweils den CHALLENGE_TOKEN und den user_consent entgegennehmen. Hierbei werden beide Felder über einen JSON parser in den jeweils für diese Felder vorgesehenen Datenstrukturen gespeichert. .	AFO umgesetzt	kein Sicherheitsmangel			
A_20601	Authenticator-Modul: Übergabe des Authorization-Request an den Authorization-Endpunkt	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS den Authorization-Request, welchen dieses vom Anwendungsfrontend erhalten hat, an den Authorization-Server des IdP-Dienstes schicken. Der Authorization-Request MUSS folgende Parameter enthalten:	Penetrationstest Quellcodeanalyse	Beide Anwendungen setzen den Authorization Request entsprechend zusammen und senden diesen dann an den IDP-Dienst. Dies wurde über den Quellcode beider Anwendung, und einen Mitschnitt der Android Anwendung validiert.	AFO umgesetzt	kein Sicherheitsmangel			
A_20607	Authenticator-Modul: Kommunikation über TLS-Verbindung	gemSpec_IDP_Frontend	Das Authenticator-Modul MUSS mit dem IdP-Dienst der TI über TLS kommunizieren. [<=]	Penetrationstest Quellcodeanalyse	In einer Quellcodeanalyse konnten wir bestätigen, dass die Kommunikation von Authenticator-Modul und IdP-Dienst der TI ausschließlich über TLS stattfindet. Das eRp-FdV kommuniziert nur via TLS mit allen etwaigen Diensten.	AFO umgesetzt	kein Sicherheitsmangel			
A_20609	Authenticator-Modul: Unzulässige TLS-Verbindungen ablehnen	gemSpec_IDP_Frontend	Das Authenticator-Modul MUSS bei jedem Verbindungsaufbau den IdP-Dienst anhand seines TLS Zertifikats authentifizieren und MUSS die Verbindung ablehnen, falls die Authentifizierung fehlschlägt. [<=]	Penetrationstest Quellcodeanalyse Befragung Inaugenscheinnahme	Die Prüfung der Zertifikate geschieht bei beiden Anwendungen zunächst auf Ebene des Betriebssystems. Bei dieser wird das Zertifikat des IDP auf ein gültiges TLS Zertifikat geprüft. Hierbei wird auf beiden Betriebssystemen lediglich dem vom System eingespielten Zertifizierungsstellen vertraut. Lediglich auf Android unter der SDK Version 24 wird zusätzlich Benutzerzertifikaten vertraut. Darüber hinaus wird das IDP Zertifikat über einen Truststore der Anwendung validiert, wodurch lediglich Zertifikate, die auf das Root-Zertifikat der Gematik zurückzuführen sind, zulässig sind und durch die	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
					Anwendung nicht verworfen werden.					
A_20617-01	Authenticator-Modul: Verpflichtende Zertifikatsprüfung	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS aktiv verwendete Zertifikate (bspw. für den TLS-Verbindungsaufbau), welche auf Root-Zertifikaten aus der TSL basieren, gemäß ""TUC_PKI_018"" auf Integrität und Authentizität prüfen. Das Authenticator-Modul MUSS die von dem Zertifikat und den darin enthaltenen Attributen (bspw. öffentliche Schlüssel) abhängenden Arbeitsabläufe ablehnen, wenn die Prüfung kein positives Ergebnis (""gültig"") liefert. Das Authenticator-Modul MUSS alle öffentlichen Schlüssel, die es verwenden will, auf eine positiv verlaufene Zertifikatsprüfung zurückführen können. [<=]	Penetrationstest Quellcodeanalyse	In einer Quellcodeanalyse (ähnlich zu A_19739) konnten wir folgendes feststellen: (zB iOS DefaultIDPSession) Öffentliche Schlüssel werden anhand der Zertifikatskette auf eine positiv verlaufene Prüfung zurückgeführt. Aktiv verwendete Zertifikate werden auf Integrität und Authentizität geprüft. Dies geschieht in der Funktion validate, die als Teil von validateOrNil genutzt wird. Als Zeitdienst fü die Prüfung wird hier Date genutzt. Schlägt die Prüfung fehl, bspw. aufgrund eines abgelaufenen Zertifikats, wird es abgelehnt und alle folgenden Arbeitsabläufe werden nicht durchgeführt (return eines Just(nil), auf Basis dessen die übertragenen Attribute verworfen werden).	AFO umgesetzt	kein Sicherheitsmangel			
A_20618	Authenticator-Modul: Unzulässige TLS-Verbindungen ablehnen	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS bei jedem Verbindungsaufbau den IdP-Dienst anhand seines TLS Zertifikats authentifizieren und MUSS die Verbindungen ablehnen, falls die Authentifizierung fehlschlägt. [<=]	Quellcodeanalyse	Die Prüfung dieser Anforderung wurde mit der Prüfung von A_20609 bereits durchgeführt.	AFO umgesetzt	kein Sicherheitsmangel			
A_20700-07	Authenticator-Modul: Signatur der "CHALLENGE"	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS die vom Authorization-Endpunkt empfangene CHALLENGE_TOKEN mit dem Zertifikat C.CH.AUT aus der Smartcard des Nutzers signieren. Hierbei wird der über die CHALLENGE_TOKEN gebildete HASH-Wert zur Signatur überreicht (siehe Abschnitt 9.3.7.3 Signiervorgang in diesem Dokument). Im Fall der Authentisierung mit einem alternativen Authentisierungsmittel signiert das Authenticator-Modul die folgenden Daten mit Hilfe des PrK_SE_AUT: - das vom Authorization-Endpunkt bezogene Challenge-Token - das auf dem Gerät gespeicherte Authentifizierungszertifikat C.CH.AUT - den Key-Identifier für das Schlüsselpaar PrK_SE_AUT, PuK_SE_AUT - die aktuell erhobenen Geräteinformationen die Art des vom Nutzer verwendeten, lokalen	Penetrationstest Quellcodeanalyse	Mithilfe von Quellcodeanalysen und einer praktischen Analyse unter Android konnte festgehalten werden, dass: Für die Signierung des Challenge Tokens das entsprechende C.CH.AUT Zertifikat der Smartcard genutzt wird. Die hieraus resultierende Signatur und verwendeter Algorithmus den Regelungen der Anforderung entspricht (ECDSA). Da keine alternative Authentisierungsmittels innerhalb der Android-Anwendungen umgesetzt wurde, sind die hiermit verbunden Anforderungen nicht umgesetzt, werden jedoch als	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			Authentisierungsmittels zur Freischaltung der Anwendung des Schlüssels PrK_SE_AUT. Es MUSS hierbei eine Datenstruktur vom Typ ""Signed_Authentication_Data"" produzieren. Der zur Signatur zu verwendende Algorithmus MUSS ECDSA mit SHA-256 sein. Das Feld ""amr"" MUSS hierbei wie folgt in Abhängigkeit der vom Nutzer verwendeten Methode belegt werden: Art Authentication-Method-Reference (""amr"") Biometrisch [""mfa"",""hwk"",""generic-biometric""] PIN [""mfa"",""hwk"",""kba""] Passwort [""mfa"",""hwk"",""kba""] Muster [""mfa"",""hwk"",""kba""] [<=] Hinweis: Der Datentyp ""Signed_Authentication_Data"" ist in Anhang C des Dokuments [gemSpec_IDP_Dienst] beschrieben."		entbehrlich angesehen. Die iOS Anwendung implementiert eine alternative Authentifizierung mit den entsprechenden Anforderungen. Lediglich Das Feld "amr" wird anhand des eingesetzten Authentifizierungsmerkmals gesetzt.					
A_21414	Authenticator-Modul: Umschlüsselung des ACCESS_TOKEN für Pairing-Endpunkt	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS das zur Autorisierung und Authentifizierung des Nutzers verwendete ACCESS_TOKEN mit dem öffentlichen Schlüssel PuK_IDP_Enc aus dem Discovery Document verschlüsseln. Dazu muss es vorher unter Verwendung des TOKEN-Key, der dem Token-Endpunkt übermittelt wurde, entschlüsselt werden."	Penetrationstest Quellcodeanalyse	Die Anwendung verschlüsselt die entsprechenden Daten zur Authentifikation mit dem geforderten Schlüssel aus dem Discovery Document und hält so die Vorgaben dieser Anforderungen ein.	AFO umgesetzt	kein Sicherheitsmangel			
A_21416	Authenticator-Modul: Einleiten der Registrierung	gemF_Biometrie	"Das Authenticator-Modul MUSS Registrierungsdaten in Form eines ""Registration_Data""-Objekts produzieren und diese mit dem PuK_IDP_ENC aus dem Discovery Document verschlüsseln. [<=]"	Penetrationstest Quellcodeanalyse	Die innerhalb der Anforderung geforderte Erstellung der Datensturktur konnte im Quellcode der iOS Anwendung nachvollzogen werden. Auch die Verschlüsselung mit dem öffentlichem Schlüssel entspricht dem Text dieser Anforderung.	AFO umgesetzt	kein Sicherheitsmangel			
A_21431	Authenticator-Modul: Übermittelung von Authentifizierungsdaten zur Verwendung von alternativen Authentisierungsmitteln	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS die produzierte Signed_Authentication_Data-Struktur mit dem PuK_IDP_Enc aus dem Discovery Document verschlüsseln und an den Authorization-Endpunkt als Antwort auf die vom Authorization-Endpunkt empfangene Challenge übermitteln. Der Wert des Header-	Penetrationstest Quellcodeanalyse	Die Anwendung verschlüsselt die entsprechenden Daten zur Authentifikation mit dem geforderten Schlüssel aus dem Discovery Document und hält so die Vorgaben dieser Anforderungen ein. Auch das Feld "exp" wird anforderiungskonform gesetzt. Somit ist die Anfoderung als umgesetzt anzusehen.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			Claims ""exp"" der hierbei produzierten ""Encrypted_Authentication_Data""-Struktur MUSS hierbei identisch mit dem gleichnamigen Claim aus den Body-Claims des empfangenen Challenge-Token belegt werden. [<=]"							
A_21443	Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Verschlüsselung des ACCESS_TOKEN	gemF_Biometrie	"Das zur Authentifizierung des Nutzers und Autorisierung des Authenticator-Moduls verwendete ACCESS_TOKEN MUSS vom Authenticator-Modul mit dem öffentlichen Schlüssel PuK_IDP_Enc aus dem Discovery Document verschlüsselt werden. [<=]"	Penetrationstest Quellcodeanalyse	Über einen Quellcodeaudit konnte für die iOS Anwendung validiert werden das diese über die Deregistrierungsfunktion für Biometrische Anmeldungen verfügt. Hierbei wird das AccessToken übertragen und mit dem öffentlichen Schlüssel des Discovery Documents verschlüsselt.	AFO umgesetzt	kein Sicherheitsmangel			
A_21574	Warnhinweise an den Nutzer	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS dem Nutzer Warnhinweise geben, dass die Sicherheit des Verfahrens bei der Verwendung von Folgendem beeinträchtigt werden kann: - Geräten, bei denen ein sog. ""Rooten"" oder ein ""Jailbreak"" vollzogen wurde. - Installationen, bei denen es sich um Simulationsumgebungen der eigentlichen Zielplattform handelt. - Geräten, die gemeinschaftlich verwendet werden. - Geräten, die einem Mobile-Device-Management unterliegen, z. B. bei Dienstgeräten im Rahmen von COPE (""Corporate Owned, Personally Enabled"")-Lösungen. - Installationen innerhalb von Containerlösungen auf Mobilgeräten zur Abschottung von Unternehmensanwendungen im Rahmen von BYOD (""Bring-Your-Own-Device"")-Lösungen. Der Nutzer MUSS diese Aussage zur Kenntnis nehmen und diesen Umstand über die Benutzeroberfläche bestätigen. Im Fall der Ablehnung durch den Nutzer DARF das Authenticator-Modul die Verwendung von alternativen Authentisierungsmitteln NICHT anbieten. Das Authenticator-Modul MUSS bei einer technischen Detektion von solchen Umständen auf das Anbieten der Verwendung von alternativen Authentisierungsmitteln verzichten. Es MUSS den Nutzer dann über die Gründe des	Penetrationstest Quellcodeanalyse	Die Anforderung wird über einen Systemdialog realisiert, der dem Nutzer die Gefahren bei Aktivierung der Funktionalität näher bringt. Dieser muss durch den Nutzer bestätigt werden und beinhaltet die Gefahren aus dem Anforderungstext.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			Wegfallens der Option zur Verwendung von alternativen Authentisierungsmitteln aufklären. [<=]"							
A_21576	Löschung bestehender alternativer Authentisierungsmittel	gemSpec_IDP_Frontend	"Sofern für das verwendete Gerät und Nutzer bereits ein alternatives Authentisierungsmittel registriert ist, MUSS das Authenticator-Modul den Nutzer zur Deregistrierung der Pairing-Daten auffordern. Der Nutzer MUSS jederzeit die Möglichkeit haben, ein von ihm registriertes alternatives Authentisierungsmittel zu erneuern. [<=]"	Penetrationstest Quellcodeanalyse	Die Umsetzung dieser Anforderung wird als teilweise umgesetzt gewertet. Da die Implementierung der Authentisierungsfunktionen, speziell für die biometrischen Merkmale, durch das Betriebssystem gehandhabt werden und die hierbei hinterlegten Merkmale durch den Nutzer über die entsprechenden Einstellungen des Betriebssystems jederzeit angepasst werden können. Die fehlende Aufforderung zur Deregistrierung der Pairing-Daten wird weiter nicht als Sicherheitsmangel angesehen, da das entsprechenden Schlüsselmaterial innerhalb der SecureEnclave bei einer Änderung des biometrischen Merkmales automatisch invalidiert wird.	AFO teilweise umgesetzt	kein Sicherheitsmangel	Das Fehlen der Funktion zur Deregistrierung sollte dennoch, mit den entsprechenden Dialogen und Warnhinweisen, in eine künftige Version der Anwendung einfließen. Da ansonsten eine Deaktivierung der biometrischen Authentifizierung für den Nutzer nur über einen Logout realisiert werden.		
A_21578	Sicherstellung des Vorliegens einer geeigneten Umgebung zur Speicherung von biometrischen Referenzmerkmalen	gemSpec_IDP_Frontend	"Das Authenticator-Modul SOLLTE prüfen, ob biometrische Referenzmerkmale oder wissensbasierte Faktoren auf dem Gerät in einer gesicherten Umgebung gespeichert werden. Hierzu MÜSSEN über Betriebssystem-APIs bereitgestellte Informationen ausgewertet werden. [<=]"	Penetrationstest Quellcodeanalyse	Die Umsetzung erfolgt über den SecureEnclaveSignatureProvider, der die mittels Betriebssystem-API bereitgestellten Attribute auswertet. Da diese mittels Secure Enclave abgesichert sind, sind sie in einer gesicherten Umgebung im Sinne der Anforderung gespeichert.	AFO umgesetzt	kein Sicherheitsmangel			
A_21579	Sicherstellung des Vorliegens einer geeigneten Umgebung für Schlüsselerzeugung, Anwendung und Speicherung	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS sicherstellen, dass die Erzeugung des Schlüsselpaares PrK_SE_AUT/PuK_SE_AUT, dessen Speicherung, Anwendung und die Löschung des PrK_SE_AUT ausschließlich durch eine gesonderte, vertrauenswürdige Ausführungsumgebung erfolgt, die den Zugriff auf den PrK_SE_AUT als Datenobjekt pauschal allen Anwendungen entzieht (hierbei eingeschlossen sind Geräte-Backups). die die Anwendung des Schlüssels auf Daten zum Zweck der Signaturbildung auf das Authenticator-Modul und denjenigen	Penetrationstest Quellcodeanalyse	Innerhalb der iOS Anwendung wurde eine Secure-Enclave implementiert, die sich die iOS eigenen Funktionalitäten zu eigen macht. Hierbei wird der Schlüssel innerhalb dieser erzeugt und mithilfe der übergebenen Attribute wird der Zugriff auf den erzeugten Schlüssel limitiert.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			am Gerät authentifizierten Nutzer beschränkt, der den Schlüssel PrK_SE_AUT erzeugt hat. Das Authenticator-Modul MUSS bei Verfügbarkeit einer auf Hardware-Ebene realisierten Absonderung der oben genannten Ausführungsumgebung diese zwingend nutzen. Eine reine auf Software-basierte Implementierung DARF NICHT verwendet werden. Hierzu MÜSSEN über Betriebssystem-APIs bereitgestellte Informationen ausgewertet werden. [<=] Hinweis 1: Die Anforderung soll ausschließen, dass Implementierungen des Authenticator-Moduls unter ggf. möglicher Umgehung der Betriebssystem-APIs eigene (z. B. Software-basierte) Lösungen implementieren oder, sofern möglich, andere Hardwareeinheiten als die fest im Gerät verbauten verwenden. Hinweis 2: Im Fall von Android-Geräten muss das Gerät mit einem Trusted Execution Environment ausgestattet sein. Sofern das Gerät eine StrongBox Keymaster-Implementierung besitzt, muss diese verwendet werden. Apple iOS-Geräten muss das Gerät mit einer Secure-Enclave ausgestattet sein."							
A_21580	Ausschluss von Eigenimplementierungen zur Schlüsselverwaltung	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS für die Schlüsselerzeugung des Schlüsselpaars PuK_SE_AUT/PrK_SE_AUT Mechanismen des Geräts verwenden. Es DARF kryptographische Schlüssel NICHT selbst erzeugen, innerhalb des ihm zur Verfügung stehenden Speicherbereichs speichern oder auf Daten anwenden. [<=]"	Penetrationstest Quellcodeanalyse	Kryptographische Schlüssel werden nicht selbst erzeugt, sondern gemäß Quellcodeanalyse über den Secure Enclave (SecureEnclaveSignatureProvider) - einen Hardwaresicherheitsmechanismus des Geräts. Das Vorhandensein dieser Secure Enclave ist programmatisch vorausgesetzt und zudem durch die minimale iOS Version (iOS 14) dadurch forciert, das alle mit iOS 14 betreibbaren Geräte über einen Secure Enclave verfügen.	AFO umgesetzt	kein Sicherheitsmangel			
A_21581	Verfügbarkeit von kryptographischen Algorithmen	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS sicherstellen, dass die in der folgenden Tabelle genannten Algorithmen zur Anwendung des PrK_SE_AUT zur Verfügung stehen: Tabelle 3: Kryptographische Verfahren Schema - Algorithmus - Schlüssel	Penetrationstest Quellcodeanalyse	Es wird eine Elliptic curve für die generierung des Schlüssel mit einer Größe von 256Bits verwendet. Die Signatur erfolgt anschließend mittels eines SHA256.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			Signatur - ECDSA auf Basis der Kurve P-256 und SHA-256 - PrK_SE_AUT [<=]"							
A_21582	Lokale Authentisierung des Nutzers vor Anwendung des PrK_SE_AUT zur Authentisierung	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS dem Nutzer die Wahl einer lokal verfügbaren Authentisierungsmethode überlassen, die zur autorisierten Anwendung des PrK_SE_AUT verwendet wird, das Authenticator-Modul MUSS hierbei auf dem Gerät bereits unter dem Nutzeraccount registrierte Mittel anbieten. Der Nutzer MUSS hierbei eine Auswahl treffen können, MUSS dem Benutzer hierbei mindestens eine pauschale Gruppierung in biometrische oder wissensbasierte Faktoren anbieten. Zugelassen sind die in der folgenden Tabelle genannten Mittel, DARF den Nutzer zur Anlage solcher Mittel auffordern. Das Authenticator-Modul MUSS den Nutzer über spezifische Schwächen seiner Wahl aufklären (z. B. solcher in Verbindung mit der Anwendung von Mustern) und ggf. Hinweise zu einer geeigneten Verwendung geben. Das Authenticator-Modul MUSS in den Parametern, die dem Betriebssystem zur Schlüsselerzeugung gesetzt werden, festlegen, auf Basis welcher der vom Nutzer gewählten Mittel die Anwendung des Schlüssels PrK_SE_AUT auf Daten durch den Nutzer autorisiert wird, dass die Anwendung des Schlüssels PrK_SE_AUT auf den zum Zeitpunkt der Erzeugung verwendeten Nutzeraccount beschränkt ist. Faktor - Zugelassen: Finger - ja Stimme - ja Gesicht - ja Iris - ja PIN - ja Passwort - ja Muster - ja Wischen - nein Kopplung mit einer Uhr - nein Knopfdruck - nein Körpersensoren - nein [<=]"	Penetrationstest Quellcodeanalyse	Es werden auf dem iOS Geräte die Optionen des Finger bzw. Gesichts zur Verfügung gestellt, da ein iOS Gerät nur eines der beiden biometrischen Verfahren zur Verfügung stellt ist eine Auswahl durch den Nutzer nicht notwendig. Beide biometrischen Methoden sind erlaubt und es gibt keine weiteren Verfahren. Ein Nutzer wird auf die Risiken der Verwendung von biometrischen Authentifizierung informiert.	AFO umgesetzt	kein Sicherheitsmangel			
A_21583	Qualitative Anforderungen an lokale Authentisierungsmittel	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS sicherherstellen, dass die von Gerät und Hardware realisierten	Penetrationstest Quellcodeanalyse	Die Mindestbetriebssystemversion ist iOS14, somit besitzen alle Geräte die diese Version Unterstützen eine	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			Mechanismen zur biometrischen Authentisierung bzw. Authentifizierung von ausreichender Qualität sind. [<=] Hinweis: Als qualitativ ausreichend werden biometrische Mittel der Güte Biometric.STRONG im Kontext von Android-Implementierungen angesehen (siehe [androidbiom]). Im Fall von Apple-iOS-Geräten sind die vom Gerät implementierten biometrischen Mittel qualitativ ausreichend, wenn das Gerät mit einer Secure-Enclave ausgestattet ist."		SecureEnclave, welche auch über den Code forciert wird.					
A_21584	Verwendung von Geräte-eigenen Mechanismen zur Authentisierung des Nutzers	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS sich zur Implementierung der Authentifizierungsverfahren zur autorisierten Anwendung des PrK_SE_AUT auf diejenigen Mechanismen beschränken, die durch die Kombination von Betriebssystem und Hardware zur Verfügung gestellt werden. Das Authenticator-Modul DARF hierbei ausschließlich die vom Betriebssystem zur Verfügung gestellte Information über eine erfolgreiche oder nicht-erfolgreiche Authentifizierung und deren Art verarbeiten. [<=]"	Penetrationstest Quellcodeanalyse	IOS erlaubt keine anderen APIs zu Verwendung der biometrischen Sensoren als die Betriebssystemeigenen, für das verwenden des SChlüssel PrK_SE_AUT muss zuvor die Eingabe eines biometrischen Authentifizierungsmerkmales erfolgen.	AFO umgesetzt	kein Sicherheitsmangel			
A_21585	Beschränkung der Nutzung des PrK_SE_AUT auf das Authenticator-Modul	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS die Parameter für die Erzeugung des Schlüsselpaars PrK_SE_AUT/PuK_SE_AUT so setzen, dass sichergestellt ist, dass der Schlüssel PrK_SE_AUT ausschließlich über das Authenticator-Modul auf Daten anwendbar ist. Eine App-übergreifende Nutzung MUSS ausgeschlossen werden. [<=]"	Penetrationstest Quellcodeanalyse	Die Erzeugung des Schlüsselpaars und die Speicherung erfolgt innerhalb der private Access Group der Anwendung und ist somit nicht von anderen Anwendungen aus zugreifbar. Darüber hinaus wird bei der Erzeugung für den privaten Schlüssel eine Nutzung der SecureEnclave vorgeschrieben. Somit schlägt diese fehl, wenn eine Implementierung der Secure Enclave auf der Hardware nicht vorhanden seien sollte. .	AFO umgesetzt	kein Sicherheitsmangel			
A_21586	Löschung des PrK_SE_AUT als Reaktion auf Systemereignisse	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS bei der Übergabe des Kommandos zur Schlüsselerzeugung an das Betriebssystem in den Parametern festlegen, dass bei folgenden Systemereignissen der private Schlüssel PrK_SE_AUT nicht mehr verwendbar ist: - Löschung des lokalen Geräte-Accounts, innerhalb dessen der PrK_SE_AUT erzeugt wurde.	Penetrationstest Quellcodeanalyse	Ein Löschen des lokalen Accounts führt dazu, dass alle Daten die sich auf einem iOS Gerät befinden nicht mehr zugänglich sind, da die kryptographischen Schlüssel entfernt wurden. Das Löschen ist kann nur über einen Reset erfolgen. Das generierte Schlüsselmaterial wird so erzeugt, dass dieses nur lokal	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			- Setzen von schwachen Authentifizierungsmethoden oder entfernen von Authentifizierungsmethoden des Geräte-Accounts. - Reset des Gerätes oder Deinstallation von Betriebssystem-Updates. - Re-Enrolment oder Löschung von biometrischen Referenzmerkmalen. [<=]"		auf dem Gerät gespeichert ist und nicht synchronisiert wird. Außerdem führt ein Ändern der biometrischen Merkmale zu einer invalidierung des Schlüsselmaterials. iOS erlaubt es nicht update rückgängig zu machen und ein Downgrade des Betriebssystems ist gleich wie das Entfernen eines Accounts zu betrachten.					
A_21587	Beschränkung des PrK_SE_AUT auf Signaturbildung	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS die Parameter für die Erzeugung des Schlüsselpaars PrK_SE_AUT/PuK_SE_AUT so setzen, dass sichergestellt ist, dass der Schlüssel PrK_SE_AUT ausschließlich zum Zweck der Signaturbildung auf Daten angewendet werden kann. [<=]"	Quellcodeanalyse	Bei dem Erstellen der Schlüssel in der Apple Secure Enclave werden diese so gespeichert, dass sie nur für Signatur von Daten verwendet werden können.	AFO umgesetzt	kein Sicherheitsmangel			
A_21588	Erzeugung eines Key-Identifiers für das Schlüsselpaar PrK_SE_AUT/PuK_SE_AUT gegenüber dem IdP-Dienst	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS einen Key-Identifier zur Identifikation des Schlüsselpaars PrK_SE_AUT/PuK_SE_AUT gegenüber dem IdP-Dienst erzeugen. Der Key-Identifier MUSS so erzeugt werden, dass die Erzeugung ein und desselben Identifiers über verschiedene Geräte eines Nutzers mit hoher Wahrscheinlichkeit ausgeschlossen ist. Der Key-Identifier MUSS zufällig erzeugt werden. Er DARF NICHT aus Nutzer- oder Gerätedaten abgeleitet werden. Der zum IdP-Dienst übertragene Key-Identifier MUSS eine Länge von 32 Byte besitzen. Der Wert KANN zur Referenzierung des PrK_SE_AUT im lokalen Schlüsselspeicher verwendet werden. Der Key-Identifier selbst oder ein Datenobjekt, aus dem er abgeleitet werden kann, MUSS auf dem Endgerät gespeichert werden. Der Key-Identifier selbst oder das Datenobjekt MUSS gegen Löschung und anwendungsübergreifende Verwendung geschützt sein. [<=] Umsetzungshinweis: Lokale Schlüsselspeicher haben ggf. eigene Anforderungen an die Art eines Identifiers. Es wird empfohlen, einen solchen durch einmaliges Anwenden von SHA-256 auf die geforderte Länge zu bringen."	Penetrationstest Quellcodeanalyse	Der Key Identifier innerhalb der iOS Anwendung wird randomisiert erzeugt. Hierzu werden die vom Betrriebssystem bereitgestellten Funktionalitäten genutzt und eine Länge von 32 Byte verwendet. Dieser wird in der gesicherten Keychain abgelegt und bei Notwendigkeit dieser entnommen.	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
A_21589	Erzeugung des Schlüsselpaars PrK_SE_AUT/PuK_SE_AUT	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS ein Schlüsselpaar PrK_SE_AUT/PuK_SE_AUT erzeugen. Das Schlüsselpaar MUSS für die Anwendung des Algorithmus ECDSA auf Basis der Kurve P-256 geeignet sein. Das Authenticator-Modul MUSS hierbei über die Betriebssystem-APIs die in Abschnitt ML-118528 - Missing cross-reference beschriebenen Parameter zur Durchsetzung der dort genannten Anforderungen und die Schlüssel innerhalb des dort identifizierten Schlüsselspeichers setzen. [<=]"	Quellcodeanalyse	Die verwendeten Schlüssel PrK_SE_AUT und der abgeleitete öffentliche Schlüssel PuK_SE_AUT sind kombatibel mit ECDSA P-256.	AFO umgesetzt	kein Sicherheitsmangel			
A_21590	Beschränkung der Nutzung des PrK_SE_AUT auf Authentisierung gegenüber dem IdP-Dienst	gemSpec_IDP_Frontend	"Das Authenticator-Modul DARF den Schlüssel PrK_SE_AUT ausschließlich zum Zweck der Authentifizierung gegenüber dem IdP-Dienst verwenden. Es DARF dem Nutzer keine andere Option anbieten oder den Schlüssel anderweitig verwenden. [<=]"	Quellcodeanalyse	Es konnte nicht festgestellt werden, dass der PrK_SE_AUT anderweitig als für den biometrischen Login verwendet wird.	AFO umgesetzt	kein Sicherheitsmangel			
A_21591	Erhebung von Geräteinformationen	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS die folgenden Informationen über das verwendete Gerät über Betriebssystem-APIs erheben: - Name des Herstellers, - Name des Produkts, - Name des Modells, - Name des Betriebssystems und - Version des Betriebssystems. Hierbei MUSS der Datentyp ""Device_Type"" gebildet werden. Die hier erhobenen Geräteinformationen MÜSSEN zusammen mit einem vom Nutzer für das Gerät vergebenen Namen zur Datenstruktur ""Device_Informationen"" kombiniert werden. [<=] Hinweis: Die genaue Spezifikation der Schemata ist in den Tabellen ""Schema Datentyp ""Device_Information""""" und ""Schema Datentyp ""Device_Type""""" in [gemSpec_IDP_Dienst], Anhang C dargestellt."	Quellcodeanalyse	In iOS werden die aktuellen Geräteinformationen gemäß der Anforderung erhoben und übermittelt.	AFO umgesetzt	kein Sicherheitsmangel			
A_21595	Lokale Speicherung des C.CH.AUT	gemSpec_IDP_Frontend	Das Authenticator-Modul MUSS das Authentifizierungszertifikat C.CH.AUT nach erfolgreicher Registrierung für die Verwendung in weiteren Authentifizierungsvorgängen lokal auf dem Endgerät speichern. Die Speicherung MUSS so erfolgen, dass eine missbräuchliche Verwendung des	Penetrationstest Quellcodeanalyse	Das entsprechende Zertifikat wird bei der ersten Anmeldung am Fachdienst durch die Anwendung innerhalb des Keyrings gespeichert. Hierbei unterliegt es verschiedenen Sicherungsmaßnahmen und ist nur für die E-Rezept	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
			Zertifikats durch andere Anwendungen in ausreichendem Maß verhindert wird. Das Authenticator-Modul DARF im Fall einer nicht erfolgreichen Registrierung das Authentifizierungszertifikat C.CH.AUT NICHT speichern. [<=]		Anwendung zugänglich. Dies wird über die Einstellungen der Betriebssystemschicht realisiert, die in Verbindung mit einer verschlüsselten Ablage eine missbräuchliche Verwendung des Zertifikats durch andere Anwendung geeignet verhindert. Eine Speicherung des Zertifikats, bei fehlgeschlagener Authentifizierung geschieht.					
A_21598	Löschung von lokalen Daten bei Fehlschlag	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS bei fehlschlagender Registrierung alle lokal erzeugten Daten (einschließlich der erzeugten kryptographischen Schlüssel) über die Betriebssystem-APIs des Geräts löschen. [<=]"	Penetrationstest Quellcodeanalyse	Die generierten Zertifikate/Schlüssel werden bei einem Fehlschlagen des regestrierens eines Fingerabdrucks mittels der vom Betriebsystem zur verfügung gestellten APIs gelöscht. Auch das Zertifikat der eGK wird über das Betriebssystem gelöscht. Da ein ACCESS_TOKEN erst nach erfolgreicher Registrierung erstellt wird und im RAM gehalten wird, ist dieser bei einem Fehler innerhalb des Regestrierungsvorganges nicht vorhanden oder persistent gespeichert, weshalb er nicht gelöscht werden muss.	AFO umgesetzt	kein Sicherheitsmangel			
A_21600	Einholen von aktuellen Geräteinformationen	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS aktuelle Geräteinformationen über die Betriebssystem-APIs einholen und dabei eine Device-Information-Struktur wie in Abschnitt ML-118258 - Missing cross-reference konstruieren [<=]"	Penetrationstest Quellcodeanalyse	Die aktuellen Geräteinformation werden über die Betriebssystem-Apis abgefragt.	AFO umgesetzt	kein Sicherheitsmangel			
A_21603	Ermöglichung der Löschung von alternativen Authentisierungsmitteln und lokal gespeicherten Daten	gemSpec_IDP_Frontend	"Das Authenticator-Modul MUSS dem Nutzer die Möglichkeit geben, lokal gespeicherte Daten dauerhaft zu löschen und über Betriebssystem-APIs des Geräts eine Löschung des PrK_SE_AUT auszulösen. Die Löschung MUSS eventuell vorhandene SSO_TOKEN mit einbeziehen. [<=]"	Quellcodeanalyse	Die Löschung aller mit der Authentifizierung verbundenen Daten erfolgt innerhalb der iOS Anwendung bei Nutzung der Logout Funktion. Hierbei werden auch die Identifier und entsprechenden Schlüssel auf dem Gerät gelöscht.	AFO umgesetzt	Kein Sicherheitsmangel			
A_21275−01	TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake	gemSpec_Krypt	-	Penetrationstest Quellcodeanalyse	Prüfung erfolgte bereits im Rahmen der Prüfungen zu gemSpec_eRp-FdV.	AFO umgesetzt	kein Sicherheitsmangel			
GS−A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt	-	Penetrationstest Quellcodeanalyse	Prüfung erfolgte bereits im Rahmen der Prüfungen zu	AFO umgesetzt	kein Sicherheitsmangel			

Afo-ID	Afo-Bezeichnung	Quelle [Referenz]	Anforderung	Prüfmethode	Umsetzung	Umsetzungsstatus	Sicherheitsmängel	Anmerkung/Empfehlung/ Risiko	Folgemaßnahme/ Auflagen	Termin für Folgemaßnahme
					gemSpec_eRp-FdV.					

Anlage 2: Prüfplan – BSI Prüfvorschrift

Datum: 09. Juni 2021
Stand: Final

ID Prüfaspekt	Kurzfassung des Prüfaspekts	Prüfaspekt	Ergebnis der Prüfung	c	Verweis Gematikprüfung	Datum der Aktivität
O.Purp_1	Informationspflicht des Herstellers zum primären Zweck und Verwendung von personenbezogenen Daten.	Der Hersteller MUSS den primären Zweck der Anwendung und die Verwendung von personenbezogenen Daten vor der Installation offenlegen (etwa in der Beschreibung des App- Stores; vgl. Anhang A) und den Nutzer mindestens bei der erstmaligen Inbetriebnahme darüber informieren.	Pass	Der primäre Einsatzzweck der Anwendung wird innerhalb der Beschreibungstexte auf den jeweiligen offiziellen Storeseiten beschrieben. Auch die verarbeiteten Daten und auch der Zweck für die Verarbeitung wird innerhalb der verlinkten Datenschutzbestimmungen aufgezeigt. Darüber hinaus wurde, da sich die spezifischere Datenschutzerklärung noch in der Abstimmung befinden, vorab die aktuelle Entwurfsfassung bereitgestellt. Beide Fassungen weisen auf die Verarbeitung personenbezogener Daten hin und dieser Hinweis ist darüber hinaus auch beim ersten Aufruf durch einen Dialog realisiert worden.		01.06.2021
O.Purp_2	Zweckgebundene Erhebung und Verarbeitung der Daten.	Die Anwendung DARF KEINE Daten erheben und verarbeiten, die nicht dem primären Zweck der Anwendung dienen.	Pass	Die Anwendung limitiert die Berechtigungen, die angefragt und genutzt werden auf das für die bereitgestellte Funktionen benötigte Minimum. Dies konnte innerhalb von Quellcodeaudits und durch praktische Tests validiert werden. Hierbei werden beispielsweise GPS Daten lediglich bei der Aktivierung der Umkreissuche der Apothekenfunktion oder die Kamera lediglich beim einscannen von Rezepten angefragt.		01.06.2021
O.Purp_3	Einholung einer Einwilligungserklärung des Nutzers.	Die Anwendung MUSS vor jeglicher Erfassung oder Verarbeitung personenbezogener Daten eine Einwilligungserklärung des Nutzers einholen.	Pass	In unserer Quellcodeanalyse sowie in einem Penetrationstest der App konnten wir feststellen, dass personenbezogene Daten innerhalb der App verarbeitet werden. Dies geschieht nur im Rahmen der eGK-Nutzung und wird mittels CAN/PIN im Rahmen einer Abfrage der Rezepte an die gematik Infrastruktur durchgeführt. Hierfür muss der Nutzer zunächst zustimmen. Die Rückantwort enthält Informationen über das Rezept sowie über den Versicherten. Wir konnten in unseren Tests ohne Zustimmung keine personenbezogenen Daten in der App vorfinden, in Verarbeitung bringen oder in sonstiger Weise einsehen.		01.06.2021
O.Purp_4	Nutzung ausschließlich zugestimmter Daten.	Daten, deren Verwendung der Benutzer nicht ausdrücklich zugestimmt hat, DÜRFEN NICHT von der Applikation oder dem Backend erfasst oder genutzt werden.	Pass	Die Datenschutzerklärung, welcher der Nutzer vor der erstmaligen Nutzung der Anwendung zustimmen muss, beinhaltet die Auflistung aller unter O.Purp_3 rückschlüssigen Daten.		
O.Purp_5	Entzug der Einwilligung ermöglichen.	Die Anwendung MUSS ermöglichen, dass der Nutzer seine Einwilligung wieder entziehen kann. Sie MUSS darüber informieren, inwieweit sich das Verhalten der Anwendung dadurch verändert.	Pass	Der Nutzer hat in den Einstellungen der App die Möglichkeit, erteilte Zustimmungen zu widerrufen und wird darüber informiert, welche Auswirkung dies hat (bspw. der Wegfall einiger Funktionen). Diese wurde auch geprüft im Rahmen von A_19982, welche wir als erfüllt bewerten.	A 19982	01.06.2021
O.Purp_6	Führen eines Verzeichnisses der Nutzereinwilligungen.	Der Hersteller MUSS ein Verzeichnis führen, welches erkennen lässt, welche Nutzereinwilligungen vorliegen. Der nutzerspezifische Teil des Verzeichnisses MUSS für den Nutzer automatisiert einsehbar sein.	Pass	Die Berechtigungsverwaltung wird über die Schnittstellen der Betriebssysteme realisiert. Hierbei sind das Anfragen und das Nachhalten der Berechtigungen bereits feste Bestandteile der jeweiligen Betriebssystemversionen.		01.06.2021
O.Purp_7	Nutzung nur erforderlicher Frameworks und Bibliotheken von Dritten.	Setzt die Anwendung Frameworks und Bibliotheken von Dritten ein, SOLLEN alle verwendeten Funktionen für den primären Zweck der Anwendung erforderlich sein. Die Anwendung SOLL anderweitige Funktionen sicher deaktivieren. Im Falle einer geringen Nutzung SOLL abgewägt werden, ob die Nutzung im Verhältnis zur Vergrößerung der Angriffsoberfläche durch die verwendeten Frameworks und Bibliotheken steht.	Pass	Die Prüfung des Einsatzes der Trackingfunktion von PiwickSDK folgt dem Hersteller zufolge der Weiterentwicklung der Anwendung und dem zielgerichteten Einsatz der Ressourcen der Entwicklung. Da hierbei speziell darauzf geachtet wurde keine sensiblen Daten zu erfassen und dem Nutzer die Entscheidung über die Nutzung dieser obliegt, wird die Anforderung mit einem Pass bewertet. Auch die Nutzung weiterer Bibliotheken Dritter folgt einer Abwägung im Entwicklungsprozess und einer Prüfung im Rahmen des Gematik Gutachtens.		01.06.2021
O.Purp_8	Weitergabe von sensiblen Daten nur für den primären Zweck.	Sofern es nicht für den vorgesehenen primären Zweck einer Anwendung erforderlich ist, DÜRFEN sensible Daten NICHT mit Dritten geteilt werden. Dies betrifft auch die Ablage dieser Daten im öffentlichen Teil des Dateisystems. Die Applikation MUSS den Nutzer über die Konsequenzen einer eventuellen Weitergabe von Anwendungsdaten vollumfänglich informieren und sein Einverständnis einholen (OPT-IN).	Pass	Ein Teilen von sensiblen Daten mit Dritten geschieht nur im Rahmen des Usability-Trackings und Crash Reportings via piwik Pro. Die Anforderungen A_19087 bis A_19097 haben dies ausführlich geprüft. Im Ergebnis konnten wir keine prüfaspektwidrige Weitergabe von Daten an Dritte identifizieren, und die bestehende Weitergabe beschränkt sich auf ein Minimum an Daten, bei denen lediglich Stack Traces und zufallsbasierte Identifier genutzt werden. Ein Risiko dahingehend bewerten wir als sehr gering, da der Hersteller technisch lediglich einen Stack Trace und bspw. keinen Memory Dump übermittelt - somit können auch nicht "aus Versehen" kritische Informationen übermittelt werden. Generell sind die im Rahmen der Weitergabe von Daten an Dritte übermittelten Informationen daher minimiert und in ihrer Natur nicht kritisch.	A_19087 bis A_19097	01.06.2021
O.Purp_9	Nur zweckgebundene Darstellung sensibler Daten auf dem Bildschirm.	Die Anwendung DARF sensible Daten NICHT auf dem Bildschirm darstellen, außer dies ist für den Zweck der Anwendung erforderlich.	Pass	In unserer Quellcodeanalyse sowie in einem Penetrationstest der App konnten wir feststellen, dass personenbezogene Daten innerhalb der App verarbeitet werden. Dies geschieht nur im Rahmen der eGK-Nutzung und wird mittels CAN/PIN im Rahmen einer Abfrage der Rezepte an die gematik Infrastruktur durchgeführt. Die Rückantwort enthält Informationen über das Rezept		01.06.2021

O.Arch_1	„Security“ ist Bestandteil des Softwareentwicklungs- und Lebenszyklus.	Security MUSS ein fester Bestandteil des Softwareentwicklungs- und Lebenszyklus‘ für die gesamte Anwendung sein (vgl. iOS Security Framework [iOSSF], beziehungsweise Security for Android Developers [SfAD]).	Pass	Wir konnten im Rahmen einiger Meetings mit den Entwicklern sowie während der Sicherung des Secure Software Development Lifecycles die Relevanz von Security im Entwicklungsprozess und Lebenszyklus verifizieren. Die gematik orientiert sich am Microsoft Security Development Lifecycle. Am Anfang steht hier eine Hauptsicherheitsschulung aller beteiligten Entwickler. Die gesichteten Prozesse bewerten wir als Best Practice gerecht. Im Rahmen der Prüfung der gematik Anforderungen des eRp konnten wir uns von der Verwendung dieses Best Practices auch in der Praxis überzeugen.		01.06.2021
O.Arch_2	Berücksichtigung der Verarbeitung sensibler Daten in der Design-Phase.	Bereits in der Design-Phase der Applikation MUSS berücksichtigt werden, dass die Applikation in der Produktiv-Phase sensible Daten verarbeiten wird. Die Architektur der Anwendung MUSS dafür die sichere Erhebung, Verarbeitung, Speicherung und Löschung der sensiblen Daten in einem Datenlebenszyklus abbilden.	Pass	Bei der Implementierung der Anwendung und zusammenhängenden Datenverarbeitung wurde den Vorgabedokumenten der jeweiligen Produktsteckbriefe und der hierbei entsprechenden geltenden Vorgabedokumenten der Gematik Folge geleistet. Auf Anfrage beim Hersteller wurden die für den Produkttypen vorgeschriebenen Vorgaben dargelegt und auch die unmittelbar umgebenen Systeme, wie beispielsweise der Fachdienst und Identity Provider verwiesen. Da die Architektur und Datenverarbeitung innerhalb der Design Phase bereits vollumfänglich auf die Verarbeitung, Speicherung und Löschung sensibler Daten ausgelegt war und die jeweiligen regulierenden Dokumente für den Zweck als ausreichend eingeschätzt werden.		03.06.2021
O.Arch_3	Dokumentation des Lebenszyklus von kryptographischem Material.	Der Lebenszyklus von kryptographischem Schlüsselmaterial MUSS einer ausgearbeiteten Richtlinie folgen, die Eigenschaften wie die Zufallszahlenquelle, detaillierte Angaben zur Aufgabentrennung von Schlüsseln, Ablauf von Schlüsselzertifikaten, Integritätssicherung durch Hash-Algorithmen, etc., umfasst. Die Richtlinie SOLL auf anerkannten Standards wie [TR02102-1] und [NSP80057] basieren.	Not Applicable	Die E-Rezept App selbst ist nur Nutzer von kryptographischen Schutzmechanismen und muss die Lebenszyklusmodelle der erzwingenden Umsysteme erfüllen. Die Sicherheitsmechanismen des IDP und des FD sind in eigenen Gutachten beschrieben, und zu anderen Teilen im Produktgutachten der E-Rezept App überprüft.		02.06.2021
O.Arch_4	Zertifikat bei Verwendung der Cloud als Backend-System notwendig.	Realisiert die Anwendung die Backend- Komponente in der Cloud, MUSS der Cloud- Anbieter über ein gültiges C5 (Cloud Computing Compliance Controls Catalogue) Testat vom Typ 2 [KCC-C5] oder ein vergleichbares Testat oder Zertifikat verfügen.	Pass	Das eingesetzte Apothekensuche basiert auf dem Apothekenverzeichnis des NGDA und wird innerhalb von Microsoft Azure gehostet. Diese verfügt über ein entsprechendes Zerttifikat. Für den Betrieb des Fachdienstes und des Identityproviders müssen die Anbieter jeweils über eine ISO 27001 Zertifizierung sowie ein Sicherheitsgutachten nachweisen.		02.06.2021
O.Arch_5	Keine unverschlüsselten sensiblen Daten in Backups.	Vom Betriebssystem gesteuerte Backups und Cloud-Backups DÜRFEN KEINE Daten im Klartext beinhalten.	Pass	Innerhalb der Anwendungen sind die entsprechend notwendigen Schritte getroffen worden, um die Sicherung der Anwendungsinformationen zu unterbinden. Durch diese wurde die automatisierte Sicherung der jeweiligen Daten z.B. über ein icloud Backup verhindert. Verweis auf die Gematik Prüfung: A_21579	A 21579	02.06.2021
O.Arch_6	Verteilte Implementierung von Sicherheitsfunktionen.	Sicherheitsfunktionen MÜSSEN immer auf allen Außenschnittstellen und API- Endpunkten implementiert werden.	Pass	Der Hauptkommunikationsweg der Anwendung führt über die Netzwerkschnittstellen, hin zum Identityprovider bzw. Fachdienst der Gematik. Diese sind in die Sicherheitsmechanismen für die erzwingte TLS Kommunikation und die Validierung mittels eigenem Truststore eingebunden, welche eine Prüfung auf eine valide Zertifikatskette des in der Anwendung integrierten Wurzelzertifikats umsetzt. Darüber hinaus werden ausgestauschte Informationen über Signautrverfahren validiert. Die Anbindung an die eGk kann hierbei auch als Schnittstelle der Anwenudng betrachtet werden. Diese erfolgt mittels Systemmitteln und muss über die Eingabe eines Pins und einer CAN durch den Nutzer entsperrt werden. Die Kamera ist eine weitere Anbindung der Anwendung bei der jedoch keine persistente Dateien innerhalb des Datensystems gespeichert werden. Lediglich die Taskid und der entsprechende Access Code wird hierbei innerhalb der Anwendung gespeichert. Im Rahmen des Einlesens wird der Input durch die Anwendungen validiert und ggf. abgelehnt.		03.06.2021
O.Arch_7	Authentizitäts- und Integritätsschutz der Applikation.	Die Anwendung MUSS einen Authentizitäts- und Integritätsschutz für die Applikation und ihre Konfiguration gewährleisten. Die Applikation SOLL dabei regelmäßig eine eigene Authentizitäts- und Integritätsprüfung des Applikations-Binaries, basierend auf einer digitalen Signatur mit Zertifikat, durchführen.	Fail	Nicht erfüllt. Die Nutzung dieser Funktion auf mobilen Geräten hätte den Einsatz von DeviceCheck resp. SaftyNet erfordert. Dieser Einsatz ist aufgrund von Datenschutzbedenken des BfDI nicht eingesetzt worden.		02.06.2021
O.Arch_8	Informierung des Nutzers zu Frameworks oder Bibliotheken von Dritten.	Nutzt die Anwendung Frameworks oder Bibliotheken von Dritten (etwa für Objektserialisierung), MUSS der Hersteller dem Nutzer Informationen über den Nutzungsumfang und die eingesetzten Sicherheitsmechanismen klar darstellen. Die Anwendung MUSS sicherstellen, dass diese Funktionen in sicherer Weise genutzt werden. Die Anwendung MUSS darüber hinaus sicherstellen, dass ungenutzte Funktionen durch Dritte nicht aktiviert werden können.	Fail	Die Anwendung nutzt verschiedene Frameworks/Bibiliotheken von Dritten, hierzu findet eine Aufliustung innerhalb der Datei "3rd party libs in der App.pdf" statt. Über den Nutzungsumfang bzw. die Nutzung derer wird der Nutzer aktuell nicht informiert. Im Rahmen der Gematik Prüfung wurde bereits der sichere Einsatz dieser getestet. .		03.06.2021
O.Arch_9	Zweckgebundener Zugriff auf verschlüsselte Speicher oder Nutzerdaten durch interpretierenden Code.	Interpretierter Code, der in möglichen Interaktionen mit Benutzereingaben steht (Webviews mit JavaScript), DARF KEINEN Zugriff auf verschlüsselte Speicher oder Nutzerdaten haben, sofern es für die Erfüllung des Zwecks der Anwendung nicht zwingend	Pass	Die Anwendungen beinhalten intepretierten Code lediglich in Form der Nutzungs- und Datenschutzbedingungen der Anwendungen. Hierin sind keine Skripte hinterlegt die auf solche Funktionalitäten zugreifen, auch eine solche Schnittstelle konnte im Quellcode nicht aufgefunden werden.		01.06.2021

		erforderlich ist. Nicht gemeint ist Code der plattformspezifischen Programmiersprachen (z. B. Java oder Kotlin bei Android).				
O.Arch_10	Barrierearme Möglichkeit zum Melden von Sicherheitsproblemen.	Der Hersteller MUSS dem Nutzer eine barrierearme Möglichkeit bereitstellen, um Sicherheitsprobleme zu melden. Die Kommunikation SOLL über einen verschlüsselten Kanal stattfinden.	Inconclusive	Sicherheitsprobleme lassen sich Barrierearm über einen Anruf beim Service-Desk oder mittels einer E-Mail melden. Bei einer E-Mail werden die Standard TLS Verschlüsslung der Mailserver verwendet. Der Nutzer sollte jedoch explizit darauf hingewiesen werden, dass er Sicherheitsprobleme dort, und an der offiziellen Seiter der Gematik (https://www.gematik.de/telematikinfrastruktur/datenschutz/), melden kann. Außerdem ist nicht gewährleistet, dass bei einem Anruf die Verbindung gesichert ist.		01.06.2021
O.Arch_11	Applikation fragt Zwangsupdates vom Backend ab	Die Applikation SOLL beim Start auf verfügbare sicherheitsrelevante Updates prüfen. Wenn ein sicherheitsrelevantes Update verfügbar ist, DARF die Applikation ohne dieses Update einzuspielen sensible Daten NICHT mehr verarbeiten.	Fail	Updates werden über den jeweiligen AppStore insofern es der Nutzer eingestellt hat automatisch ausgerollt, es wird beim App-Start keine Überprüfung vorgenommen. Die Kommunikation von veraltete App-Versionen werden, nach Aussage der Gematik, von dem Backend über API-Keys verhindert. Ein Nutzer kann weiterhin die aktuellen Rezepte anschauen/bearbeiten und sich einen ACCESS_TOKEN beim IDP holen. Dies wiederspricht sich mit dem Grundsatz, dass die App die Verarbeitung von sensiblen Daten nicht mehr zulassen darf. Außerdem wird innerhalb des Backends nur auf Existenz des Header Felds geprüft und nicht auch auf tatsächliche Versionsnummer.		01.06.2021
O.Arch_13	Nutzung kryptographischer Maßnahmen bei alternativen Download-Quellen/Mechanismen.	Werden die Applikation und Updates nicht über die normalen Mechanismen des App- Stores der Hardwareplattform eingespielt, MÜSSEN die Authentizität der Datenquelle sowie des Updates vor dessen Anwendung durch kryptographische Maßnahmen positiv bestätigt werden.	Not Applicable	Updates für die Anwendung werden über die jeweiligen offiziellen Stellen bezogen.		01.06.2021
O.Source_1	Prüfung von Eingaben vor Verwendung.	Eingaben aus nicht vertrauenswürdigen Quellen MÜSSEN vor deren Verwendung geprüft werden, um potenziell bösartige Werte vor der Verarbeitung herauszufiltern.	Pass	Die Anwendung implementiert für Ihre Netzwerkschnittstellen und zusammenhängende API Aufrufe eine Prüfung der entsprechenden Zertifikatsketten und führt diese auf die entsprechenden authentischen Roots der Anwendung zurück. Die Authentisierung des Nutzers wird über die Gesundheitskarte und die mit dieser zusammenhängende Abfrage der PIN und CAN realisiert, wodurch das Schlüsselmaterial der Karte für die Authentifizierung nur bei richtiger Einfgabe der jeweiligen Authentisierungsmittel stattfinden kann.		01.06.2021
O.Source_2	Nutzung einer Escape-Syntax bei strukturierten Daten.	Der Hersteller MUSS eingehende Daten maskieren beziehungsweise von potenziell schadhaften Zeichen bereinigen.	Pass	Die Verarbeitung der eingehenden Daten erfolgt über ein JSON Parsing der jeweiligen Aufrufe. Hierbei werden Syntax brechende Zeichen durch Ausnahmenbehandlung verarbeitet. Weiter werden die ausgetauschten Daten über eine Signatur in Form der Bildung eines JWE und der Prüfung der Zertifikatskette realisiert.		01.06.2021
O.Source_3	Keine sensiblen Daten in Meldungen.	Fehlermeldungen und Benachrichtigungen DÜRFEN KEINE sensiblen Daten (z. B. User Identifier) enthalten.	Pass	Die Anwendung zeigt keine Daten des Anwenders, also Rezeptdaten oder personenbezogene Daten des Nutzers, als Fehlermeldungen in der Anwendung. Benachrichtigungen beinhalten auch keine solcher Daten und werden innerhalb der Anwendung nur vereinzelt verwendet.		01.06.2021
O.Source_4	Kontrollierte Behandlung und Dokumentation von Ausnahmen („Exceptions“).	Potenzielle Ausnahmen im Programmablauf (Exceptions) MÜSSEN abgefangen, kontrolliert behandelt und dokumentiert werden.	Pass	Wir haben stichprobenartig das Exceptionhandling der iOS und Android app im Quelltext überprüft. Beim manuellen Testen der Applikation in der aktuell im Android Play Store verfügbaren Version sind keine Ausnahmen aufgetreten.		02.06.2021
O.Source_5	Abbruch des Zugriffs auf sensible Daten bei Exceptions.	Bei Ausnahmen im Programmablauf (Exceptions), mit sicherheitskritischen Auswirkungen, SOLL die Anwendung Zugriffe auf sensible Daten abbrechen und diese im Speicher sicher löschen.	Pass	Im Rahmen der Gematik Prüfung wurde die Ausnahmenbehandlung untersucht und es konnte kein Zugriff auf sensible Daten festgestellt werden. Tretten Ausnahmen im Zusammenhang mit der Authentifizierung an Diensten oder der Registrierung von biometrischen Merkmalen für die alternative Authentifizierung (iOS) auf, so werden alle hiermit zusammenhängenden Daten aus dem Speicher entfernt bzw. verworfen.		03.06.2021
O.Source_6	Nutzung von sicheren Funktionsalternativen beim Zugriff auf Speichersegmente.	Bei Programmumgebungen mit manueller Speicherverwaltung (d.h., die Applikation kann selbst exakt festlegen, wann und wo Speicher gelesen und beschrieben wird) MUSS die Applikation für lesende und schreibende Zugriffe auf Speichersegmente auf sichere Funktionsalternativen (z. B. sprintf_s statt printf) zurückgreifen.	Not Applicable	Die Anwendungen nutzen mit Kotlin und Swift Programmiersprachen, die keine manuelle Speicherverwaltung umfassen		01.06.2021
O.Source_7	Sicheres Löschen von sensiblen Daten nach ihrer Verwendung.	Die Applikation MUSS sicherstellen, dass alle sensible Daten unverzüglich nach ihrer Verwendung sicher gelöscht werden.	Not Applicable	Alle sensiblen Daten, nach Anhang A dieser Prüfvorschrift, werden innerhalb sicherer Datenhaltung nach O.Data_2 behandelt.		03.06.2021
O.Source_8	Deaktivierung von unterstützenden Entwicklungsoptionen in der Produktiv-Version.	Alle Optionen zur Unterstützung der Entwicklung (z. B. Log-Aufrufe, Entwickler- URLs, Testmethoden, etc.) MÜSSEN in der Produktiv-Version mindestens deaktiviert oder besser vollständig entfernt sein.	Pass	Innerhalb der iOS Anwendung werden die entsprechenden Funktionalitäten über die Buildpipeline abgeschaltet und entsprechende Compiler Flags (DEBUG, DEBUG_VIEW_ENABLED). Im Rahmen der Sourcecodeanalyse konnten keine Rückstände für Debuggingfunktionen gefunden werden.		03.06.2021
O.Source_9	Keine Debug-Mechanismen in der Produktiv-Version.	Der Hersteller MUSS sicherstellen, dass keinerlei Überreste von Debug-Mechanismen in der Produktiv-Version verbleiben.	Pass	Innerhalb der iOS Anwendung werden die entsprechenden Funktionalitäten über die Buildpipeline abgeschaltet und entsprechende Compiler Flags (DEBUG, DEBUG_VIEW_ENABLED). Im Rahmen der Sourcecodeanalyse konnten keine Rückstände für Debuggingfunktionen gefunden werden.		03.06.2021
O.Source_10	Aktivierung von modernen Sicherheitsmechanismen der Entwicklungsumgebung.	Die Implementierung der Anwendung SOLL moderne Sicherheitsmechanismen der Entwicklungsumgebung, wie beispielsweise Byte-Code-Minimierung und Stack-Protection, aktivieren.	Pass	Die Anwendungen wurden im Rahmen der Prüfung auf den Einsatz gängiger Sicherheitsmechanismen wie Certifikate Pinning, Input Validierung geprüft.		03.06.2021

O.TrdP_1	Verwendung der aktuellen Version bei externen Bibliotheken und Frameworks.	Externe Bibliotheken und Frameworks SOLLEN in der neusten verfügbaren „Stable“ - Version, bezogen auf das genutzte Betriebssystem der Plattform, verwendet werden. Mit „Stable“-Version wird die Version eines Software-Pakets bezeichnet, welches den aktuellsten, stabil laufend geltenden Zustand abbildet. Typischerweise beinhaltet dieser keine ungetesteten Funktionen.	Pass	In der Android Version wird durch das OWASP dependency-check-gradle bei jedem Compilevorgang überprüft ob veraltete Frameworks und Bibliotheken verwendet werden. Die Prüfung hat dabei ergeben, dass in den verwendeten Abhängikeiten keine bekannten Sicherheitslücken enthalten sind. Für die Android Version der App bewerten wir diese Anforderung daher als "Pass" Für die iOS Version der App haben wir den Source Code der Anwendung geprüft. Dabei haben wir festgestellt, dass die Versionen der referenzierten Abhängigkeiten zumindest so aktuell sind, dass keine Schwachstellen bekannt sind. Weiterhin hat die Gematik durch ihren Software Development Lifecycle (vgl. A_1982) Prozesse definiert die Abhängikeiten auf einem akutellen Stand halten.		01.06.2021
O.TrdP_2	Herstellerprüfung externer Bibliotheken und Frameworks auf Schwachstellen.	Externe Bibliotheken und Frameworks MÜSSEN durch den Hersteller regelmäßig auf Schwachstellen überprüft werden. Funktionen aus Bibliotheken und Frameworks DÜRFEN bei bekannten Schwachstellen NICHT eingesetzt werden.	Pass	Die Gematik verwendet automatisierte Schwachstellenscanner (MicroFocus Fortify) als Teil des Build Prozesses, welche sowohl den Code statisch auf Schwachstellen prüft, als auch nach bekannten Schwachstellen in den verwendeten Bibliothek scannt. vgl. A_19182	A_19182	02.06.2021
O.TrdP_3	Sicherheitskonzept für zeitnahes Einspielen von Sicherheitsupdates für externe Bibliotheken und Frameworks.	Sicherheitsupdates für externe Bibliotheken und Frameworks MÜSSEN zeitnah zur Verfügung gestellt werden. Der Hersteller MUSS ein Sicherheitskonzept vorlegen, das anhand der Kritikalität ausnutzbarer Schwachstellen die geduldete Weiternutzung für die Applikation, bzw. das Backend festlegt. Nachdem die Übergangsfrist (Grace Period) abgelaufen ist, MUSS die Anwendung den Betrieb verweigern.	Pass	Das Bekanntwerden und die entsprechende Eskalation eines solchen Vorfalls ist Teil des Sicherheitsmanagements und hiermit zusammenhängenden Meldeprozess für Datenschutz und Sicherheitsvorfälle. Hierbei würden im Falle einer Routineüberprüfung oder einer besonderen Ticketsituation, beispielsweise aus dem Schwachstellenmanagement heraus, nach einer Validierung der Umstände die in Rufbereitschaft befindlichen Mitarbeiter hinzugezogen werden und über einen dokumentierten Prozess behoben. Dies ist beispielsweise innerhalb des Secure Software Development Lifecycle (SSDL) beschrieben.		03.06.2021
O.TrdP_4	Prüfung auf Vertrauenswürdigkeit der Quelle von externen Bibliotheken und Frameworks.	Vor der Verwendung von externen Bibliotheken und Frameworks MUSS deren Quelle auf Vertrauenswürdigkeit geprüft werden.	Pass	Prinzipiell erfolgt der Einsatz von 3rd party code restriktiv. Der eingesetzte Code wird immer unter 4-Augen-Prinzip reviewed. Weitere Maßnahmen erfolgen situativ, wenn möglich, so z.B. Extraktion der benötigten Codeteile. vgl. A_19182	A_19182	02.06.2021
O.TrdP_5	Keine Weitergabe von sensiblen Daten an Drittanbieter-Software.	Die Anwendung SOLL sensible Daten nicht an Drittanbieter-Software weitergeben.	Pass	Es konnte nicht fesgtestellt werden, dass sensible Daten oder Session Daten (Tokens) an Dritte weitergegeben werden. Siehe A_19480 und A_19979 aus dem orginalem Produktgutachten.	A_19480 und A_19979	02.06.2021
O.TrdP_6	Validierung eingehender Daten über Drittanbieter-Software.	Über Drittanbieter-Software eingehende Daten SOLLEN validiert werden.	Pass	Es konnten mittels Quellcodeanalyse und praktischer Tests keine eingehenden Daten von Dritten (d.h. nicht-gematik, also piwik Pro) identifiziert werden. Dies ist programmatisch nicht vorgesehen und wird weiterhin dadurch unterbunden, dass eine eingehende TLS-Verbindung über ein gültiges Zertifikat abgesichert sein muss, wodurch Quellen stets vertrauenswürdig sind. Ein ausstehendes Risiko, bspw. dadurch, dass jemand etwaige private Schlüssel der vertrauenswürdigen Kommunikationsteilnehmer replizieren kann, bewerten wir dahingehend als niedrig, dass rechenintensive Kalkulationen zum "Erraten" dieser Schlüssel notwendig wären, oder aber diese anderweitig kompromittiert werden müssten.		01.06.2021
O.TrdP_7	Prüfung der Wartung von verwendeter Dirittanbieter-Software.	Drittanbieter-Software, die nicht länger vom Hersteller oder Entwickler gewartet wird, DARF NICHT verwendet werden.	Pass	Die verwendete Drittanbietersoftware piwik Pro wird zum aktuellen Zeitpunkt gepflegt. Der Hersteller des eRp-FdV hat einen laufenden Vertrag mit piwik und steht im Austausch mit dem Anbieter. In der Vergangenheit konnte piwik (geringe) Sicherheitsmangel schnell beseitigen (bspw. CVE-2010-1453).		01.06.2021
O.Cryp_1	Keine fest einprogrammierten Schlüssel oder anderweitige Geheimnisse.	Beim Einsatz von Verschlüsselung in der Applikation DÜRFEN KEINE fest einprogrammierten geheimen, bzw. privaten Schlüssel eingesetzt werden. Ausgenommen sind Techniken, die den verwendeten Schlüssel stark vor Reverse Engineering nach aktuellem Stand der Technik verbergen (Stichwort: „White Box Cryptography“).	Pass	Die Anwendung wurde auf vorhandene private bzw. geheime Schlüsselmaterialien getestet. Hierbei konnte validiert werden das keine solchen vorhanden sind. Lediglich das öffentliche Zertifikat ist für den internen Truststore innerhalb der Anwendung integriert.		03.06.2021
O.Cryp_2	Nur bewährte Implementierungen bei kryptographischen Primitiven.	Die Anwendung MUSS auf bewährte Implementierungen zur Umsetzung kryptographischer Primitive und Protokolle zurückgreifen (vgl. [TR02102-1]).	Pass	Die Gematik verwendet die TLS Bibliothek des jeweiligen Betriebsystems und forciert die Verwendung von mind. TLS 1.2. Vgl. GS-A_4385	GS-A_4385	02.06.2021
O.Cryp_3	Passende Wahl der kryptographischen Primitive.	Die Wahl kryptographischer Primitive MUSS passend zum Anwendungsfall sein und den Vorgaben des aktuellen Stands der Technik (siehe [TR02102-1]) entsprechen.	Pass	Die Gematik erfüllt die Anforderungen von BSI-TR03116-1#3.9 Schlüsselerzeugung welche auf TR-02102-1 verweist. vgl. GS-A_4368	GS-A 4368	02.06.2021
O.Cryp_4	Zweckbindung kryptographischer Schlüssel.	Kryptographische Schlüssel DÜRFEN NICHT für mehr als genau einen Zweck eingesetzt werden.	Pass	Die Prüfung des Quellcodes der Android und iOS App ergab, dass kein Schlüsselmaterial welches gefunden wurde für mehr als einen Zweck verwendet wird. Daher wird die Anforderungen mit "Pass" bewertet.		02.06.2021
O.Cryp_5	Nutzung von starken kryptographischen Schlüsseln.	Die Stärke der kryptographischen Schlüssel MUSS dem aktuellen Stand der Technik entsprechen (siehe [TR02102-1]).	Pass	Die Gematik erfüllt die Anforderungen von BSI-TR03116-1#3.9 Schlüsselerzeugung welche auf TR-02102-1 verweist. vgl. GS-A_4368	GS-A_4368	01.06.2021

O.Cryp_6	Manipulationsschutz kryptographischer Schlüssel durch Umgebung.	Alle kryptographischen Schlüssel SOLLEN in einer vor Manipulation und Offenlegung geschützten Umgebung liegen.	Pass	Die Anwendung verarbeitet kryptografische Schlüssel zum einen innerhalb des Trust Stores, welcher auf Android innerhalb der Shared Preferences und innerhalb von iOS innerhalb der Keychain abgelegt werden. Das Schlüsselmaterial innerhalb von iOS und der Nutzung der elektronischen Gesundheitskarten wird innerhalb dieser und bei biometrischer Anmeldung innerhalb einer SecureEnclave erzeugt, gespeichert und verwendet.		03.06.2021
O.Cryp_7	Manipulationsschutz kryptographischer Operationen durch Umgebung.	Alle kryptographischen Operationen SOLLEN in einer vor Manipulation und Offenlegung geschützten Umgebung stattfinden.	Pass	Die Anwendung verarbeitet kryptografische Schlüssel zum einen innerhalb des Trust Stores, welcher auf Android innerhalb der Shared Preferences und innerhalb von iOS innerhalb der Keychain abgelegt werden. Das Schlüsselmaterial der Nutzung der elektronischen Gesundheitskarten wird innerhalb dieser und bei biometrischer Anmeldung auf iOS innerhalb einer SecureEnclave erzeugt, gespeichert und verwendet.		03.06.2021
O.Rand_1	Erzeugung von Zufallswerten durch sicheren Zufallszahlengenerator.	Alle Zufallswerte MÜSSEN über einen starken kryptographischen Zufallszahlengenerator erzeugt werden.	Pass	Die Generierung der Zufallszahlen in Android mit dem Linux Kernel Version 4.x zu vergleichen sind welche NTG.1 erfüllen, des weiteren erfüllt dieser auch Anforderungen aus FIPS 140-2 zu RNG. Auch Apple erklärt iOS Konform zu FIPS 140-2/3 weshalb auch die Zufallszahlengeneration akzeptiert wird.	GS-A_4367, GS-A_4368	02.06.2021
O.Rand_2	Verwendung eines Zufallszahlengenerators mit hoher Entropie.	Die Anwendung MUSS Zufallszahlen von einem Zufallszahlengenerator mit hoher Entropie beziehen.	Pass	Die im Sinne der BSI [TR-03116-1#3.8] vorgesehene Stärke des Zufallszahlengenerators wird, wie auch in GS-A_4367 und GS-A_4368 geprüft, durch Betriebssystemmittel und vorhandene Sensoren gewährleistet.	GS-A_4367, GS-A_4368	01.06.2021
O.Rand_3	Zusammensetzung des Startwerts (Seed) aus mindestens drei Systemparametern.	Die Anwendung SOLL dem Zufallszahlengenerator einen Startwert (Seed) zuweisen, der sich aus mindestens drei voneinander unabhängigen Systemparametern zusammensetzt. Die Parameter SOLLEN von außerhalb der Anwendung nicht ermittelbar und eindeutig sein. Stellt die Plattform einen Hardware-Zufallszahlengenerator zur Verfügung, welcher keine Vergabe von Startwerten erlaubt, SOLL stattdessen dieser verwendet werden.	Pass	Die Android Applikation verwendet die Klasse "SecureRandom" welche laut Android Dokumentation den "FIPS 140-2, Security Requirements for Cryptographic Modules" entspricht. Dies bewerten wir als ausreichenden Zufallsgenerator, obwohl er keine Vergabe von Startwerten erlaubt. In der iOS App wurde im Quelltext kein Hinweis auf die Verwendung eines nicht kryptografisch sicheren Zufallszahlengenerators gefunden.	GS-A_4367	01.06.2021
O.Rand_4	Nutzung von Backend-Entropie bei Erstellung eines Startwerts (Seed).	Die Applikation SOLL bei Erstellung eines Startwerts (Seed) für den Zufallszahlengenerator einen geeigneten Zufall aus einer geeigneten externen Quelle beziehen.	Pass	Die im Sinne der BSI [TR-03116-1#3.8] vorgesehene Stärke des Zufallszahlengenerators wird, wie auch in GS-A_4367 und GS-A_4368 (und O.Rand_2) geprüft, durch Betriebssystemmittel und vorhandene Sensoren gewährleistet. Der initiale Seed wird mittels der sicheren Bordmittel des Betriebssystems erzeugt (bspw. unter iOS SecRandomCopyBytes: https://developer.apple.com/documentation/security/1399291-secrandomcopybytes).	GS-A_4367, GS-A_4368	01.06.2021
O.Auth_1	Hersteller-Konzept zur Authentifizierung von Anwendungssitzungen.	Der Hersteller MUSS ein Konzept zur Authentifizierung (Zwei-Faktor-basiert), Autorisierung (Rollenkonzept) und zum Beenden einer Anwendungssitzung dokumentieren.	Pass	Das eRp-FdV nutzt als zweiten Faktor zur Authentifizierung des Nutzers die physische eGK samt CAN und PIN. Ohne diese kann ein Abruf der Rezeptdaten nicht erfolgen. Dieser physische zweite Faktor bietet dahingehend ein hohes Maß an Sicherheit, dass er einzigartig ist und die PIN nur dem Besitzer bekannt sein sollte. Außerdem wird empfohlen, den Appstart mit Biometrie abzusichern, um einen zusätzlichen Schutz der Daten zu gewährleisten. Ein Angreifer benötigt also sowohl eGK als auch PIN und biometrische Merkmale des Nutzers, um Zugriff auf die Daten zu gewinnen. Ein Restrisiko dahingehend bewerten wir aufgrund des komplexen Angriffsvektors als sehr gering. Hinsichtlich der Autorisierung nutzt das eRp-FdV kein explizites Rollenkonzept. Ein authentifizierter Nutzer kann nur genau die eigenen Rezepte abrufen und sonst keine weiteren Funktionen mit erhöhten Berechtigungen nutzen. Bei Beenden der Appsitzung werden bestehende Sessiondaten zurückgesetzt. Die Speicherung dieser vglw sensiblen Daten erfolgt in verschlüsselten Datenbanken. Ein Restrisiko hier ist gering, da ein Angriff auf diese verschlüsselten Daten zeitlich sehr aufwändig ist und während der Laufzeit der App erfolgen müsste, da nach Beenden die Sessiondaten gelöscht werden.		01.06.2021
O.Auth_2	Authentifizierung an der Schnittstelle zwischen App und Backend.	Die Anwendung MUSS für die Anbindung eines Backend-Systems eine geeignete Authentifizierung unterstützen.	Pass	Die Validierung der Backenddienste wurde im Rahmen des Gematik Gutachtens geprüft.	A_19739 A_20033	02.06.2021
O.Auth_3	Getrennte Realisierung von Authentifizierungsmechanismen und Autorisierungsfunktionen.	Die Applikation SOLL Authentifizierungsmechanismen und Autorisierungsfunktionen separat realisieren. Sind für die Anwendung verschiedene Rollen notwendig, MUSS eine Autorisierung bei jedem Datenzugriff separat realisiert werden.	Not Applicable	Die Anwendung unterscheidet keine Rollen oder verschiedene Benutzer innerhalb der App.		01.06.2021
O.Auth_4	Zwei-Faktor-Authentifizierung vor Verarbeitung sensibler Daten.	Der Nutzer MUSS mittels zweitem Faktor authentifiziert werden, bevor sensible Daten in der Anwendung verarbeitet werden (Step- Up-Authentisierung).	Fail	Die 2F-Authentifizierung an der E-Rezept App ist nicht zwingend, da es sich um ein single user personal device handelt, dass im Regelfall mit Wissen oder biometrischen Merkmalen vor Fremdzugriff geschützt ist. Eine darüber hinausgehende Abfrage biometrischer Merkmale zum Start der App ist umgesetzt. Um (neue) sensible Daten zu erlangen, ist Wissen und Besitz notwendig (eGK und PIN, zusätzlich zu dem Besitz des Gerätes und dessen Entsperrung).		02.06.2021
O.Auth_5	Erzeugung des zweiten Faktors durch das Backend-System.	Für die Nutzer-Authentifizierung in der Anwendungssitzung KANN der zweite Faktor vom Backend-System erzeugt werden.	Not Applicable	Die Applikation verwendet zum Abruf der sensiblen Gesundsheitsdaten die Authentifizierung über die eGK und PIN. Die beschriebenen Anforderungen an die Zwei-Faktor-Authentifizierung treffen auf diese nicht zu.		02.06.2021

O.Auth_6	Zusätzliche Informationen bei Bewertung des Authentifizierungsvorgangs einbeziehen.	Für die Bewertung eines Authentifizierungsvorgangs SOLLEN zusätzliche Informationen (z. B. das verwendete Endgerät, der verwendete WiFi- Zugangsknoten oder die Zeit des Zugriffs) mit einbezogen werden. Bei einer Abweichung von gewohnten Parametern MUSS eine zusätzliche Authentifizierungsmaßnahme (Step-Up- Authentisierung) erfolgen.	Fail	Es werden keine zusätzlichen Informationen zur Authentifizierung benutzt. Da die Authentifizierung über die eGK und PIN ein hohes Sicherheitsniveau besitzt und die Authentifizierung gegenüber dem Zugriffsschutz gerätespezifisch ist, erreicht die Applikation unserer Auffassung auch ohne diese Anforderung ein sehr hohes Sicherheitsniveau.		02.06.2021
O.Auth_7	Information des Benutzers über ungewöhnliche Anmeldeversuche.	Dem Nutzer SOLL eine Möglichkeit gegeben werden, sich über ungewöhnliche Anmeldevorgänge informieren zu lassen.	Fail	Dies ist nicht in der Anwendung vorgesehen, daher wird die Anfroderung mit Fail bewertet.		03.06.2021
O.Auth_8	Durchsetzung starker Passwortrichtlinien.	Bei einer Authentifizierung mittels Benutzername und Passwort MÜSSEN starke Passwortrichtlinien existieren. Diese SOLLEN sich am aktuellen Stand gängiger Best- Practices orientieren.	Not Applicable	Die eRp verwendet keine Authentifizierung über Passwörter.		01.06.2021
O.Auth_9	Anzeige der Stärke des verwendeten Passworts.	Für die Authentifizierung mittels Benutzername und Passwort KANN die Stärke des verwendeten Passworts dem Nutzer angezeigt werden. Informationen über die Stärke des gewählten Passworts DÜRFEN NICHT im Applikationsspeicher oder im Backend gehalten werden.	Not Applicable	Die eRp verwendet keine Authentifizierung über Passwörter.		01.06.2021
O.Auth_10	Möglichkeit zur Änderung des Passwortes.	Der Nutzer MUSS die Möglichkeit haben, sein Passwort zu ändern.	Not Applicable	Die eRp verwendet keine Authentifizierung über Passwörter. Der Benutzer hat die Möglichkeit einen PIN-basierten Zugriffschutz einzurichten. Hier kann der PIN vom Benutzer gewählt und geändert werden.		01.06.2021
O.Auth_11	Verwendung von kryptographisch sicheren Hashing-Algorithmen und Salts zur Speicherung der Passwörter.	Werden Passwörter gespeichert, MÜSSEN diese mit einer den aktuellen Sicherheitsstandards entsprechenden Hashing-Funktion und unter Verwendung geeigneter Salts gehasht werden.	Not Applicable	Die eRp verwendet keine Authentifizierung über Passwörter.		01.06.2021
O.Auth_12	Verhinderung des Ratens von Login-Parametern.	Die Applikation MUSS Maßnahmen vorsehen, die ein Ausprobieren von Login-Parametern (z. B. Passwörter) verhindern.	Pass	Die Erstanmeldung mittels eGk kann durch den Nutzer lediglich drei Mal mit falschen Zugangsdaten (PIN/CAN) wiederholt werden bevor eine PUK notwendig wird. Die biometrische Authentifizierung nutzt die Betriebssystem Schnittstellen für die alternative Authentifizierung an der Anwendung. Bei dieser werden durch die jeweiligen Betriebssysteme bei Fehlversuchen erhöhte Wartezeiten für den Nutzer erzwungen.		03.06.2021
O.Auth_13	Erneute Authentifizierung bei unterbrochener Anwendung.	Wurde die Anwendung unterbrochen (in den Hintergrundbetrieb versetzt) MUSS eine erneute Authentisierung durchgeführt werden.	Fail	Wenn der Benutzer wählt die App nicht gegen unbefugten Zugriff zu sichern ist nach Unterbrechung der Anwendung keine Authentifizierung notwendig. Der Benutzer kann aber den Zugriffschutz aktivieren, was diese Anforderung umsetzen würde.		01.06.2021
O.Biom_1	Biometrische Sensoren nur als Teil einer Zwei-Faktor-Authentifizierung zulässig.	Die Verwendung biometrischer Sensoren SOLL nicht als alleiniger Authentifizierungsmechanismus eingesetzt werden. Sie ist lediglich als Teil einer Zwei- Faktor-Authentifizierung zulässig.	Fail	Biometrische Sensoren können für den Zugriffschutz verwendet werden. Für den Zugriff auf die TI ist jedoch die TI-Authentisierung notwendig		01.06.2021
O.Biom_2	Qualität und Eigenschaften eingesetzter biometrischer Sensoren.	Der Hersteller MUSS definieren, welche Qualität und Eigenschaften ein biometrischer Sensor mindestens aufweisen muss, um von der Anwendung verwendet werden zu dürfen.	Fail	Eine derartige Spezifikation wurde nicht von der Gematik definiert. Für offizielle Android Gerät existiert der Standard https://source.android.com/security/biometric/measure#strong-weakunlocks		01.06.2021
O.Biom_3	Prüfung des biometrischen Sensors über eine White- oder eine Blacklist.	Die Applikation MUSS die Hardware des biometrischen Sensors, vor dem Einsatz, über eine White- oder eine Blacklist prüfen. Der Hersteller SOLL eine White-/Blacklist mit sicherer/unsicherer Biometrie-Sensorik pflegen. Eine White-/Blacklist MUSS im Backend aktuell verfügbar gehalten werden.	Pass	Für die alternative authentifizierung mittels Biometrie entscheidet der Server über eine Block/Allow Liste welche Geräte erlaubt sind. Ein Prozess für regelmäßige Überprüfung der Liste ist in Zusammenarbeit mit dem BSI in Arbeit.		01.06.2021
O.Biom_4	Prüfung der Bereitstellung biometrischer Referenzmerkmale.	Bevor die Applikation einen biometrischen Sensor nutzt, MUSS sie sicherstellen, dass dem Sensor biometrische Referenzmerkmale des Gerätenutzers zum Vergleich bereit stehen.	Pass	Die Anwendungen beziehen diese Informationen beide aus Schnittstellen der mobilen Betriebsysteme. Dies wurde über praktische Tests der Anwendungen über die Nutzung ohne Merkmale bzw. mit Merkmalen getestet. Hierbei konnte validiert werden das biometrische Merkmale lediglich bei Vorhandensein von Referenzmerkmalen angeboten werden, ansonsten wird eine auf diesen Merkmalen basierende Authentifizierung nicht verwendet.		01.06.2021
O.Biom_5	Ablehnung der Anmeldung bei nachträglich veränderten biometrischen Referenzmerkmalen.	Die Applikation MUSS feststellen, wann die biometrischen Referenzmerkmale verändert wurden und die Anmeldung ablehnen, falls biometrische Referenzmerkmale nachträglich (das heißt seit der Aktivierung des Authentifizierungskontrollmechanismus in der Applikation) verändert worden sind.	Fail	Innerhalb von Android haben praktische Tests aufzeigen können, das die Anmeldung auch mit einem erneut hinterlegten Referenzmerkmal möglich war und auch entsprechend zu einer Anmeldung geführt hatte. Tests unter iOS konnten zeigen, dass das für die Authentisierung verwendete Schlüsselmaterial aufgrund des Setzens der entsprechenden Konfiguration nicht mithilfe neu registrierter Referenzmerkmale möglich ist. Dies ist auch Bestandteil der im Pruefplan der Gematikanforderungen unter A_21586 behandelten Anforderung.	A_21586	01.06.2021
O.Biom_6	Auswertung der biometrischen Authentifizierung durch	Die Applikation MUSS zur Auswertung der biometrischen Authentifizierung auf betriebssystemeigene Funktionalitäten zurückgreifen (z. B. Entsperren KeyChain/KeyStore).	Pass	Die Anwendung nutzt für die Implementierung der biometrischen Authentifizierung lediglich Funktionen des Betriebssystems. Hierzu wurden zum einen die eingesetzten Bibiliotheken auf biometrische Funktionen überprüft und zum anderen die Authentifizierungsprozesse der jeweiligen Anwendungen untersucht.		02.06.2021

	betriebssystemeigene Funktionalitäten.					
O.Sess_1	Sessionhandling durch sicherere Frameworks.	Das Session-Handling SOLL mittels sicherer Frameworks (vgl. O.Ntwk_3) realisiert werden.	Pass	Beide anwendungen nutzen für Ihr Handling der Session Daten, insbesondere für die HTTP-Interaktion etablierte Frameworks. Unter Android wird die okhttp Framework eingesetzt und unter iOS kommen die Funktionen des Betriebssystems zum Einsatz. Weiter verweise wir auf die Prüfung des Gematik Gutachtens und die mit diesem zusammenhängende Prüfung der Authentifizierung gegenüber des Identity Providers für die Handhabung der Authentifizierungsdaten. (vgl. https://raw.githubusercontent.com/gematik/api-erp/master/images/workflowAuthentication.svg)	A_19187 A_20172 A_20309 A_20483	02.06.2021
O.Sess_2	Nutzung des Backend-Zufallszahlengenerator zur Session-Identifier-Erzeugung.	Die Erstellung von Session-Identifiern MUSS durch den Zufallszahlengenerator des Backends erfolgen.	Pass	Die Session-ID für den Einsatz von PiwickSDKpro erfolgt durch das Backend des Anbieters und wird in beiden Anwendungen nicht durch diese gesetzt. Die sonstigen Kommunikationen auf Netzwerkebene nutzen keine Session-Identifier.		02.06.2021
O.Sess_3	Session-Identifier sind sensible Daten.	Session-Identifier MÜSSEN als sensible Daten geschützt werden.	Pass	Die Anforderung wurde im Rahmen der Datenhaltung bereits im Rahmen des Gematik Gutachtens betrachtet. Daher verweisen wir auf dieses.	A_19186	03.06.2021
O.Sess_4	Ablage von Session-Identifiern.	Session-Identifier DÜRFEN NICHT unverschlüsselt auf permanenten Speichermedien abgelegt werden.	Pass	Die Android Anwendung nutzt zur Speicherung von Daten zum einen die von Android bereitgestellten "SharedPreferences" und eine SQLite Datenbank, die verschlüsselt auf dem Gerät abgelegt wird. Der Access Token wird verschlüsselt auf dem Gerätespeicher abgelegt, wohingegen der ID_Token nicht persistent gespeichert wird. Somit sind die Anforderungen für die verschlüsselte Speicherung erfüllt. Unter iOS wird die vom Hersteller bereitgestellte Lösung (Core Data / SQLite) für die persistente Speicherung von Daten genutzt. In dieser werden die Informationen persistent und mit einer Passphrase verschlüsselt im intern geschützten Speicher abgelegt. Somit ist auch für iOS die Erfüllung der Anforderung gegeben. vgl. A_20184	A_20184	02.06.2021
O.Sess_5	Aktive Beendigung der Anwendungssitzung nach Session-Timeout.	Die Anwendung MUSS die Anwendungssitzung nach einem angemessenen Session-Timeout aktiv beenden.	Fail	Innerhalb der Anwendungen ist kein solches Timeout vorhanden.		03.06.2021
O.Sess_6	Aktive Beendigung der Anwendungssitzung nach Logout durch den Benutzer.	Die Anwendung MUSS es dem Nutzer ermöglichen ein oder alle zuvor ausgestellten Session-Identifier ungültig zu machen.	Pass	Per Quellcodeanalyse konnten wir folgendes feststellen: Unter iOS: Mit dem Aufruf der Logout Funktion zur Beendigung einer Session werden auch die zuvor genutzten Session Daten allesamt gelöscht. Dies erfolgt durch ein dereferenzieren der Token innerhalb der Keychain (iOS) bzw. der sicheren Storage Datenbank (Android). Diese werden zurückgesetzt und das access_token wird invalidiert. Android: Auch hier gibt es eine Logout-Funktion, die die IDP Konfigurationstabelle in den Shared Preferences bereinigt (nullt) und somit alle Session Daten löscht. vgl. A_20186	A 20186	03.06.2021
O.Sess_7	Löschen des Session-Identifiers nach Ende der Anwendungssitzung.	Wird eine Anwendungssitzung beendet, MUSS die Anwendung den Session-Identifier sicher löschen und das Backend informieren.	Pass	Dies wurde im Rahmen der Gematik Prüfung nachgewiesen. Daher verweisen wir auf dieses.	A_19095 A_20186	03.06.2021
O.Tokn_1	Ablage des Authentifizierungstokens in einem geschützten Speicherbereich.	Das Authentifizierungstoken SOLL auf dem Endgerät in einem sicheren Speicherbereich liegen (z. B. KeyChain/KeyStore).	Pass	Die Android Anwendung nutzt zur Speicherung von Daten zum einen die von Android bereitgestellten "SharedPreferences" und eine SQLite Datenbank, die verschlüsselt auf dem Gerät abgelegt wird. Der Access Token wird verschlüsselt auf dem Gerätespeicher abgelegt, wohingegen der ID_Token nicht persistent gespeichert wird. Somit sind die Anforderungen für die verschlüsselte Speicherung erfüllt. Unter iOS wird die vom Hersteller bereitgestellte Lösung (Core Data / SQLite) für die persistente Speicherung von Daten genutzt. In dieser werden die Informationen persistent und mit einer Passphrase verschlüsselt im intern geschützten Speicher abgelegt. Somit ist auch für iOS die Erfüllung der Anforderung gegeben. vgl. A_20184	A_20184	
O.Tokn_2	Authentifizierungstoken ohne Einbettung sensibler Daten.	Es DÜRFEN KEINE sensiblen Daten in ein Authentifizierungstoken eingebettet werden.	Pass	Mittels einer Prüfung der Anfragen konnte festgestellt werden, dass der id_token sowie der access_token keine sensiblen Daten in Klarform o.Ä. enthalten.		02.06.2021
O.Tokn_3	Aufbau und Prüfung des Authentifizierungstokens.	Ein Authentifizierungstoken MUSS den voll qualifizierten Namen des Backends umfassen. Die Anwendung MUSS den voll qualifizierten Namen prüfen.	Fail	Es werden standardisierte JWT Token verwendet. Diese enthalten nicht den voll qualifizierten Namen.		02.06.2021
O.Tokn_4	Prüfung der Inhalte des Authentifizierungstokens.	Ein Authentifizierungstoken MUSS ausschließlich die von der Applikation erwarteten Felder enthalten.	Pass	Die Anwendungen implementieren eine Signaturprüfung, die die Integrität und auch die Authentizität des Tokens validiert. Diese konnte im Rahmen der Gematikprüfung nachvollzogen und validiert werden.	A_20625	03.06.2021
O.Tokn_5	Speicherort des Signaturschlüssels des Authentifizierungstokens.	Der private Schlüssel, zum Signieren des Authentifizierungstokens DARF NICHT auf dem Gerät vorliegen.	Pass	Im Rahmen der Prüfung der Authentifizierung wurde sichergestellt, das die für die Authentifizierung notwendigen Schlüssel richtig verarbeitet und gespeichert werden. Hierfür wird die eGk verwendet. Bei Nutzung einer alternativen Authentifizierungsmethode unter iOS werden die erzeugten Schlüsselmatieralien innerhalb einer sicheren Ausführungsumgebung erzeugt und genutzt.		03.06.2021

O.Tokn_6	Bereitstellung bestehender Authentifizierungstoken durch das Backend.	Die Anwendung MUSS dem Nutzer bestehende Authentifizierungstoken, auf Anfrage, zur Verfügung stellen.	Fail	Diese Funktion ist nicht vorhanden.		02.06.2021
O.Tokn_7	Invalidierung bereits ausgestellter Authentifizierungstoken.	Die Anwendung MUSS es dem Nutzer ermöglichen ein oder alle zuvor ausgestellten Authentifizierungstoken ungültig zu machen.	Fail	Diese Funktion ist nicht vorhanden.		02.06.2021
O.Data_1	Datenschutz und Sicherheit bei Werkseinstellung.	Die Werkseinstellung der Anwendung MUSS den maximalen Datenschutz und die maximale Sicherheit bieten.	Pass	Die Anwendungen sind bei der Installation mit den minimalsten Berechtigungen im jeweiligen System hinterlegt. Die notwendigen Berechtigungen werden erst beim Aufruf des jeweiligen Funktion erfragt, z.B. die Kameraberechtigung beim Einscanner der Rezepte. Verwiesen wird hierüber auf die geprüften Gematik Anforderungen A_20193, A_20194.	A_20193, A_20194	01.06.2021
O.Data_2	Verschlüsselung aller sensiblen Daten.	Sensible Daten MÜSSEN verschlüsselt gespeichert werden. Das Schlüsselmaterial für diese Verschlüsselung DARF NICHT unverschlüsselt persistiert werden. Dies gilt sowohl für flüchtiges Ablegen (z. B. im Arbeitsspeicher), als auch für dauerhaftes Speichern (z. B. in einer Cloud-Umgebung). Eine hardwareunterstützte Schlüsselverwaltung der Plattform SOLL bevorzugt verwendet werden.	Pass	Die Anwendungen speichern sensible Daten entsprechend der Anforderung an abgesicherten Speicherorten bzw. mittels zusätzlicher Schutzmaßnahmen (z.B. SecureEnclave oder verschlüsselten SqlLite Datenbanken). Hierbei werden Session Daten innerhalb von Android und iOS in den Shared Preferences bzw. Keyring abgelegt. Die Schlüsselmaterialien für eine alternative Biometrische Authentifizierung werden in iOS innerhalb der Secure Enclave erzeugt und verlassen diese nicht. Weiter verweisen wir auf die Prüfungen im Gematik Gutachten.	A_19186 A_21579	03.06.2021
O.Data_3	Ablage sensibler Daten.	Die Applikation SOLL sensible Daten in einer vor Einsicht und Manipulation geschützten Umgebung ablegen (z. B. embedded Secure Element/Trusted Execution Environment).	Pass	Die iOS-Anwendung implementiert die Nutzung einer Secure Enclave für die Ablage, Erzeugung und Nutzung der Authentifizierungsmerkmale bei biometrischer Anmeldung. Die reguläre Anmeldungf speichert Schlüsselmaterial auf der eGk. Andere Sensible Daten werden in einer durch das Betriebssystem geschützten Umgebung abgelegt.	A_19186 A_21579	03.06.2021
O.Data_4	Zugriff auf sensible Daten durch Dritte.	Die Applikation DARF Ressourcen, die einen Zugriff auf sensible Daten gemäß Anhang A ermöglichen, gegenüber Dritten NICHT verfügbar machen.	Pass	DIe Prüfung auf eine Offenlegung von sensiblen Daten wurde im Rahmen des Gematik Gutachtens durchgeführt. Hierbei konnten keine von der Anforderung genannten Umstände identifiziert werden.	A_19480 A_19979	03.06.2021
O.Data_5	Löschung aller erhobenen sensiblen Daten nach Abschluss der Verwendung durch die Applikation.	Alle erhobenen sensiblen Daten DÜRFEN NICHT über die Dauer ihrer jeweiligen Verwendung hinaus in der Anwendung gehalten werden.	Pass	Die eRezept App speichert eRezepte über den Verwendungszeitraum hinweg, jedoch wird dies als Kernfunktionalität der App angesehen, alle zusätzlichen Zertifikate, Schlüssel o.Ä. werden nach dem Verwendungszeitraum aus ihrer sicheren Aufbewahrungsumgebung gelöscht.		02.06.2021
O.Data_6	Erhebung, Speicherung und Verarbeitung von ausschließlich für den Zweck der Applikation notwendigen Daten.	Die Applikation MUSS die Grundsätze der Datensparsamkeit und Zweckbindung berücksichtigen.	Pass	Die App verfolgt den Grundsatz der Datensparsamkeit und erhebt aktuell keine personenbezogenen oder sensiblen Daten in Logging oder Tracking.		02.06.2021
O.Data_7	Speicherung und Verarbeitung von sensiblen Daten.	Die Speicherung und Verarbeitung von sensiblen Daten SOLL im Backend erfolgen.	Fail	Die Speicherung von sensiblen Daten ist eine Kernfunktion der eRezept App. Die Daten werden verschlüsselt und vor Zugriff geschützt gespeichert.		03.06.2021
O.Data_8	Entfernung von Metadaten mit Datenschutzrelevanz	Bei der Verwendung von Aufnahmegeräten (z. B. Kamera) MÜSSEN sämtliche Metadaten mit Datenschutz-Relevanz, wie etwa Rückschlüsse auf den GPS-Koordinaten des Aufnahmeorts, eingesetzte Hardware, etc., entfernt werden.	Pass	Es werden keine Bilder oder Dokumente welche Metadaten enthalten an das Backend gesendet. Das Scannen eines eRezepts erfolgt ohne fotografieren und verwendet die Kamera nur als "Scanner". Auf dem System wird lediglich ein Json-Wert eingelesen, welcher das Rezept beinhaltet.		02.06.2021
O.Data_9	Zugriffsbeschränkung bei der Erhebung von sensiblen Daten.	Bei der Erhebung von sensiblen Daten, durch die Verwendung von Aufnahmegeräten (z. B. Kamera), MUSS vorgebeugt werden, dass andere Anwendungen darauf Zugriff erlangen könnten, etwa über eine Mediengalerie.	Pass	Die Erhebung von sensiblen Daten erfolgt im Rahmen der Anwendung beim Einscannen verschiedener Rezepte, die der Nutzer von seinem Arzt in Papierform ausgehändigt hat. Die Handhabung der Daten erfolgt hierbei lediglich im Rahmen der Anwendung und es werden keine Daten auf dem Dateisystem des Gerätes gespeichert.		02.06.2021
O.Data_10	Keine Aufzeichnungen bei der Eingabe sensibler Daten über die Tastatur.	Bei der Eingabe sensibler Daten über die Tastatur SOLL die Anwendung unterbinden, dass Aufzeichnungen für Dritte erkennbar werden. Dies schließt insbesondere Caches, Autokorrektur- und Autovervollständigungsverfahren, Eingabegeräte von Drittanbietern und jegliche für Dritte auswertbare Speicherung, aus.	Inconclusive	Der Nutzer kann Tastaturen von Dritten installieren, weder iOS noch Android ermöglichen es das zu erkennen oder zu verhindern. Die Felder sind jeweils als Password Feld gesetzt womit verhindert wird, dass diese in den normalen Tastaturen in Caches oder Autokorrektur gespeichert werden. Der Nutzer sollte klarer auf die Gefahren von Betriebssystem fremden Tastaturen hingewiesen werden oder eine eigene Eingabetastatur sollte erstellt werden um das Problem zu beheben. Somit gilt diese Anforderung als "Inconclusive" da das Benutzen von Tastaturen dritter eine Entscheidung des Nutzers ist und die Hersteller der App das Verhalten nicht beeinflussen können.		02.06.2021
O.Data_11	Kein Export sensibler Daten in die Zwischenablage.	Bei der Eingabe sensibler Daten SOLL der Export in die Zwischenablage unterbunden werden. Die Anwendung KANN alternativ eine eigene Zwischenablage implementieren, welche vor dem Zugriff durch andere Apps geschützt ist.	Fail	Die Anwendung umfasst die Eingabe der jeweiligen PIN und CAN Nummern der elektronischen Gesundheitskarte des Anwenders. Die Felder sind jeweils als Password Feld gesetzt womit verhindert wird, dass diese in die jeweiligen Zwischenablagen des Gerätes kopiert werden. Da jedoch das Kopieren von Rezeptdetails innerhalb der Anwendung das Kopieren sensibler Daten beinhalten kann, wird die Anforderung mit Inconclusive gewertet. Hierbei sollten dem Anwender entsprechende Warnhinweise angezeigt werden um Ihn in die Lage zu versetzen das Risiko einschätzen zu können.		02.06.2021

O.Data_12	Kein Export von biometrische Daten oder privaten Schlüssel aus der Quelle.	Sensible Daten wie biometrische Daten oder private Schlüssel DÜRFEN NICHT aus der Komponente, auf der sie erzeugt wurden, exportiert werden.	Pass	Biometrische Daten werden nicht von der App gespeichert. Erzeugte Schlüssel werden sicher abgelegt und können nicht exportiert werden.		02.06.2021
O.Data_13	Keine Speicherung des Bildschirminhaltes oder Zugriff Dritter bei Anzeige sensibler Daten.	Die Anwendung SOLL beim Anzeigen sensibler Daten den Zugriff für Dritte und die Speicherung des Bildschirms (z. B. Screenshots und Anzeigen für das App- Switching) unterbinden.	Pass	Die Erstellung von Screenshots ist innerhalb der Anwendungen von beiden Betriebssystemen unterbunden worden. Hierbei werden auch Inhalte bei der Ansicht im jeweiligen App-Switcher ausgeblendet.		03.06.2021
O.Data_14	Keine sensiblen Daten in Logfiles oder anderen Meldungen oder Nachrichten.	Die Anwendung DARF KEINE sensiblen Daten in Logfiles oder anderen Meldungen oder Benachrichtigungen, die nicht vom Benutzer explizit eingeschaltet wurden (siehe O.Plat_4), schreiben.	Not Applicable	Es werden keine Logfiles o.ä. generiert. In den Analytics werden keine sensiblen Daten verwendet.		
O.Data_15	Verschlüsselung aller sensiblen Daten im gesperrten Zustand.	Die Anwendung MUSS sicherstellen, dass im gesperrten Zustand des Endgeräts alle sensiblen Daten verschlüsselt sind.	Pass	Die Android Anwendung verbietet das Verschieben der Dateien nicht explizit. Die Datenhaltung der Anwendung verhindert jedoch eine Ablage der Daten in einem unverschlüsselten Zustand. Hierfür verweisen wir auf die Gematik Prüfung.	A_21322 A_20184 A_19186	03.06.2021
O.Data_16	Gerätebindung lokal gespeicherter Daten.	Die Applikation MUSS lokal gespeicherte Daten mit einer sicheren Gerätebindung versehen.	Not Applicable	Die Anwendung verwendet keine lokal gespeicherte Daten im Dateisystemen gespeichert und kann somit auch nicht auf einem anderen Gerät getestet werden.		03.06.2021
O.Data_17	Hinweis bei Auswahl bestimmter Speichermedien.	Schützt die Plattform das gewählte Speichermedium nicht vor Diebstahl (z.B. unverschlüsselte SD-Karten), MUSS die Applikation bei einer Auswahl des betreffenden Speichermediums den Nutzer auf das erhöhte Risiko hinweisen.	Not Applicable	Die Anwendung unterstützt nicht die Verwendung von externen Speichermedien bzw. die Ablage der Anwendungsinformationen auf einem Dateisystem.		02.06.2021
O.Data_18	Unzugänglichmachen aller sensiblen Daten auf dem Endgerät bei Deinstallation der Anwendung.	Die Anwendung MUSS sicherstellen, dass bei ihrer Deinstallation alle sensiblen Daten und anwendungsspezifischen Anmeldeinformationen auf dem Endgerät nicht mehr zugreifbar sind.	Pass	Die Anwendungen speichern Daten lediglich in den vom System bereitgestellten und durch dieses geschützten Speicherbereiche. Nach getesteten Deintsallationen konnten keine Rückschlüsse auf sensible Datein vollzogen werden. Die unter iOS innerhalb der Secure Enclavce gespeicherten Daten werden nicht durch die Deinstallation der Anwendung gelöscht, jedoch sind die für den Zugriff benötigten Identifier von einer Deinstallation betroffen.		02.06.2021
O.Data_19	Löschung aller sensiblen Daten im Backend bei Deinstallation der Anwendung.	Die Anwendung MUSS dem Nutzer die Möglichkeit geben, dass bei ihrer Deinstallation alle sensiblen Daten und anwendungsspezifischen Anmeldeinformationen auch im Backend vollständig gelöscht werden. Entscheidet sich der Nutzer, die Daten im Backend nicht zu löschen, MUSS eine für den Zweck angemessene maximale Verweildauer definiert sein. Der Nutzer MUSS über die Verweildauer informiert werden. Nach Ablauf der maximalen Verweildauer MÜSSEN alle sensiblen Daten und anwendungsspezifischen Anmeldeinformationen vollständig gelöscht werden. Dem Nutzer MUSS die Möglichkeit gegeben werden alle Daten auch vor Ablauf der Verweildauer vollständig zu löschen.	Fail	Die Rezepte bleiben im Backend gespeichert, unabhängig vom Status der Applikation auf dem Endgerät des Benutzers.		02.06.2021
O.Data_20	Sicheres Überschreiben von Nutzerdaten im Gerät durch den Anwender über das Backend.	Um dem Missbrauch von sensiblen Daten nach einem Geräteverlust entgegenzuwirken, KANN die Anwendung einen Kill-Switch realisieren, d. h. ein absichtliches, sicheres Überschreiben von Nutzerdaten im Gerät auf Applikationsebene, ausgelöst durch das Backend. Der Hersteller MUSS die Auslösung des Kill-Switches durch den Anwender über das Backend durch starke Authentifizierungsmechanismen vor missbräuchlicher Nutzung schützen.	Not Applicable	Für die Anwendung gibt es keinen Kill-Switch, der die Daten der Anwendung über eine Funktion im Backend auslösen könnte.		01.06.2021
O.Paid_1	Anzeige kostenpflichtiger Leistungen.	Die Applikation MUSS für den Nutzer kenntlich machen, welche Leistungen mit zusätzlichen Kosten vergütet werden.	Not Applicable	Die Applikation verfügt über keine kostentplfichtigen Leistungen.		01.06.2021
O.Paid_2	Einverständnis des Nutzers vor dem Ausführen kostenpflichtiger Aktionen.	Die Anwendung MUSS vor dem Ausführen kostenpflichtiger Aktionen das Einverständnis des Nutzers einholen.	Not Applicable	Die Applikation verfügt über keine kostentplfichtigen Leistungen.		01.06.2021
O.Paid_3	Einverständnis des Nutzers vor einer Zugriffsanforderung auf kostenpflichtige Ressourcen.	Die Anwendung MUSS, vor einer Zugriffsanforderung (z. B. Android-Berechtigungen) auf kostenpflichtige Ressourcen, das Einverständnis des Nutzers einholen. Anwendungshinweis/Beispiel: Das Versenden von SMS kann Kosten verursachen und benötigt daher ein Einverständnis.	Not Applicable	Die Applikation verfügt über keine kostentplfichtigen Leistungen.		01.06.2021
O.Paid_4	Dauerhaftes Einverständnis des Nutzers auf häufig verwendete, kostenpflichtige Ressourcen.	Die Anwendung KANN, für den Zugriff auf häufig verwendete, kostenpflichtige Ressourcen, ein dauerhaftes Einverständnis des Nutzers einholen, soweit dies dem Zweck der Anwendung angemessen ist.	Not Applicable	Die Applikation verfügt über keine kostentplfichtigen Leistungen.		01.06.2021

O.Paid_5	Entzug des Einverständnisses ermöglichen.	Die Anwendung MUSS den Nutzer in die Lage versetzen zuvor erteilte Einverständnisse zurückzuziehen.	Not Applicable	Die Applikation verfügt über keine kostentplfichtigen Leistungen.		01.06.2021
O.Paid_6	Ablage der sensiblen Transaktionshistorie im Backend.	Die Anwendung SOLL die Transaktionshistorie von zahlungspflichtigen Ressourcen und Funktionen im Backend ablegen. Die Transaktionshistorie, einschließlich der Metadaten, MUSS als sensibles Datum gemäß O.Purp_8 behandelt werden.	Not Applicable	Die Applikation verfügt über keine kostentplfichtigen Leistungen.		01.06.2021
O.Paid_7	Profilbildung durch Nachverfolgung der Zahlungsströme durch Dritte.	Falls die Anwendung kostenpflichtige Funktionen anbietet, MUSS der Hersteller ein Konzept vorlegen, welches vorbeugt, dass Dritte die Zahlungsströme zur Nutzung von Anwendungsfunktionen zurückverfolgen können.	Not Applicable	Die Applikation verfügt über keine kostentplfichtigen Leistungen.		01.06.2021
O.Paid_8	Anzeige der Übersicht der entstandenen Kosten.	Die Anwendung MUSS dem Nutzer eine Übersicht der entstandenen Kosten anbieten. Falls die Kosten aufgrund einzelner Zugriffe erfolgt sind, MUSS die Anwendung einen Überblick der Zugriffe aufführen.	Not Applicable	Die Applikation verfügt über keine kostentplfichtigen Leistungen.		01.06.2021
O.Paid_9	Validierung von getätigten Bezahlvorgängen im Backend.	Die Validierung von getätigten Bezahlvorgängen MUSS im Backend vorgenommen werden.	Not Applicable	Die Applikation verfügt über keine kostentplfichtigen Leistungen.		01.06.2021
O.Paid_10	Anforderungen bei Zahlverfahren von Drittanbietern.	Zahlverfahren von Drittanbietern MÜSSEN die Anforderungen an Drittanbieter-Software erfüllen (vgl. Kapitel 3.1.4).	Not Applicable	Die Applikation verfügt über keine kostentplfichtigen Leistungen.		01.06.2021
O.Ntwk_1	Netzwerkkommunikation ausschließlich TLS verschlüsselt.	Jegliche Netzwerkkommunikation der Anwendung MUSS durchgängig mit TLS verschlüsselt werden.	Pass	Im Rahmen der Prüfung des Gematik Gutachtens sind alle verwendeten Netzwerkprotokolle auf den Einsatz von TLS untersucht worden. Hierbei konnte festgestellt werden, das bei jeglicher Netzwerkkommunikation TLS zum Einsatz kommt. vgl. A_20606, A_19215, A_20206	A_20606 A_19215 A_20206 A_21332	
O.Ntwk_2	TLS-Konfiguration gemäß aktuellem Stand der Technik.	Die Konfiguration der TLS-Verbindungen MUSS dem aktuellen Stand der Technik entsprechen und aktuellen Best-Practice- Empfehlungen folgen (vgl. [TR02102-2]).	Not Applicable	Die TLS Verbindungen werden nach dem aktuellen Stand der Technik gesichert. Wir haben das über Quellcodeanalysen festgestellt. Vgl. A_17124	A_17124	01.06.2021
O.Ntwk_3	Sichere Kommunikationskanäle nur mit Betriebssystem-Funktionen oder sicherheitsüberprüfter Drittsoftware.	Die Anwendung MUSS entweder die Sicherheitsfunktionalität der jeweilig verwendeten Betriebssystem-Plattform oder sicherheitsüberprüfte Frameworks oder Bibliotheken verwenden, um sichere Kommunikationskanäle aufzubauen.	Pass	Innerhalb der iOS Anwendung kommen lediglich Betriebssystemfunktionalitäten und die hiermit verbundenen Sicherheitsmaßnahmen (ATS) zum Einsatz. Hierbei wird auch die jeweilige Mindestversion von TLS aktiv durch die Entwickler gesetzt. Innerhalb von Android werden, mittels Framework (okHttp), die einzusetzenden TLS-Versionen und Cipher Suiten limitiert. Hierbei wurden die ausgewählten Optionen anhand von Gematikvorgaben, welche wiederum auf Vorgaben des BSI basieren, festgelegt.	GS-A_4385 GS-A_4387 GS-A_5035 GS-A_5322 GS-A_5339 GS-A_5526 GS-A_5542	01.06.2021
O.Ntwk_4	Unterstützung von Zertifikatspinning.	Die Applikation MUSS Zertifikatspinning unterstützen, d. h. sie DARF Zertifikate NICHT akzeptieren, deren Zertifikatskette dem Hersteller nicht vertrauenswürdig erscheint [RFC7469].	Pass	Im Rahmen der Prüfung des Gematik Gutachtens wurde der eingesetzte Truststore und die mit diesem realisierte Prüfung auf den in der Anwendung integrierten Root durchgeführt.	A_21218 A_20161-01 A_20623 A_20624 A_20625	01.06.2021
O.Ntwk_5	Validierung des Server-Zertifikats des Backends.	Die Applikation MUSS das Server-Zertifikat des Backends überprüfen.	Pass	Im Rahmen der Prüfung des Gematik Gutachtens wurde der eingesetzte Truststore und die mit diesem realisierte Prüfung auf den in der Anwendung integrierten Root durchgeführt.	A_21218 A_20161-01 A_20623 A_20624 A_20625	01.06.2021
O.Ntwk_6	Validierung der Integrität und Authentizität der Antworten des Backends.	Die Applikation MUSS die Integrität und Authentizität der Antworten des Backends validieren.	Pass	Im Rahmen des Gematik Gutachtens wurde die Komunikation mit dem Backend betrachtet und die umgesetzte Prüfung der Signaturen dieser Dienste validiert.	A_20623 A_20624 A_20625	01.06.2021
O.Ntwk_7	Keine plattformspezifischen Fallback-Mechanismen zulässig.	Die Applikation MUSS plattformspezifische Fallback-Mechanismen (z. B. clear Text traffic Opt-out bzw. analog In-App Transport Security) deaktivieren.	Pass	Durch die Konfigurationen und jeweilige Mitschnitte des Netzwerkverkehrs konnte validiert werden, das keine schwächeren Cipher-Suiten bzw. Fallback-Mechanismen innerhalb der Anwendungen vorhanden sind.	GS-A_5322 A_17124 GS-A_5322	01.06.2021
O.Ntwk_8	Vorhaltung von vollständigen Log-Dateien für alle aufgebauten Verbindungen.	Die Anwendung SOLL für alle aufgebauten Verbindungen Log-Dateien auf dem Backend vorhalten.	Not Applicable	Das Gesamtkonzept E-Rezept ist nicht Teil dieser Prüfung.		01.06.2021
O.Ntwk_9	Protokollierung bestimmter Sicherheitsereignisse im Backend.	Ein abgebrochener Start MUSS als Sicherheitsereignis im Backend protokolliert werden.	Not Applicable	Das Gesamtkonzept E-Rezept ist nicht Teil dieser Prüfung.		01.06.2021

O.Plat_1	Geräteschutz für die Nutzung der Anwendung erforderlich.	Für die Nutzung der Anwendung SOLL das Endgerät über einen aktivierten Geräteschutz (Passwort, Mustersperre, o. ä.) verfügen. Im Fall eines nicht aktivierten Geräteschutzes MUSS der Hersteller den Nutzer über die damit verbundenen Risiken aufklären.	Fail	Die Authentisierung der Anwendungssitzungen wird beim Start der Anwendung ohne entsprechenden Geräteschutz realisiert. Wenn auf dem Gerät kein entsprechender Schutz aktiviert ist, wird keine Warnmeldung auf diesem angezeigt.		01.06.2021
O.Plat_2	Nur Anforderung der für den primären Zweck notwendigen Berechtigungen.	Die Anwendung DARF Berechtigungen, die für die Erfüllung ihres primären Zwecks nicht notwendig sind, NICHT einfordern.	Pass	Die Umsetzung dieser Anforderung erfolgte bereits im Rahmen des Gematik Gutachtens. Hierbei werden lediglich Berechtigungen angefragt, die für die jeweils erstmals aufgerufene Funktionalität notwendig sind.	A_20193	01.06.2021
O.Plat_3	Hinweis auf Zweck der Berechtigungen und Auswirkungen bei Nichterteilung.	Die Applikation MUSS den Nutzer auf den Zweck der anzufragenden Berechtigungen und auf die Auswirkungen hinweisen, die eintreten, falls der Nutzer diese nicht gewährt.	Pass	Die Anwendungen erbitten den Zugriff auf die Kamera des Gerätes. Hierbei wird dem Nutzer beim Anklicken der Funkionalität diese über einen kurzen Einleitungstext erläutert. Wenn der Anwender sich gegen die Erteilung der Freigabe entscheidet, wird ihm ein entsprechender Erklärungstext angezeigt, die Ihn über den umstand aufklärt.		
O.Plat_4	Option zur Anzeige von Meldungen/Benachrichtigungen mit sensiblen Inhalten.	Die Applikation KANN dem Nutzer die Optionen bieten, Meldungen und Benachrichtigungen, ggf. auch mit sensiblen Inhalten, anzuzeigen. Bei Werkseinstellung MUSS diese deaktiviert sein.	Not Applicable	Die Anwendung hat nicht die Möglichkeit sensible Informationen in Notifications anzuzeigen.		02.06.2021
O.Plat_5	Nur Nutzung von vorgesehenen Dateipfaden.	Die Applikation SOLL den Zugriff auf vorgesehene Dateipfade beschränken.	Not Applicable	Die Anwendungen speichern entsprechende Daten lediglich innerhalb von geschützten Bereichen und bieten dem Anwender auch keine Möglichkeit diese Datenhaltung anzupassen.		01.06.2021
O.Plat_6	Zugriffsbeschränkungen auf sämtliche Daten.	Die Anwendung MUSS Zugriffsbeschränkungen auf sämtliche Daten realisieren.	Pass	Die Anwendung setzt einen Schutz der Anwendungsdaten (z.B. Sessiondaten, Zugangs-Credentials und biometrischen Daten) geeignet um. Der entsprechende Umgang mit diesen war Teil des Gematik Gutachtens. Aggregierte Anwendungsdaten wie beispielsweise Therapieberichte im PDF Format sind nicht Teil der Anwendungen.	A_21322 A_19186	02.06.2021
O.Plat_7	Beschränkung von Broadcast-Nachrichten auf autorisierte Applikationen.	Die Applikation MUSS Broadcast-Nachrichten auf autorisierte Applikationen beschränken.	Not Applicable	Innerhalb der Prüfung kontte keine aktive Funktionalität zum Versand von Brodcastnachrichten aufgefunden werden. Im Rahmen des Gematik Gutachtens wurde auch auf eine fehlerhafte Datenhaltung hin geprüft, die eine Interprozesskommunikation über shared Storage.	A_19186	02.06.2021
O.Plat_8	Keine sensiblen Daten in Broadcast-Nachrichten.	Die Anwendung DARF in Broadcast- Nachrichten KEINE sensiblen Daten versenden.	Not Applicable	Die Anwendung sendet keine Broadcastnachrichten.		02.06.2021
O.Plat_9	Nutzung von sensiblen Funktionalitäten über Interprozesskommunikation.	Das Anbieten von sensiblen Funktionalitäten über Interprozesskommunikation SOLL unterbunden werden. Ist das Anbieten zur Erfüllung des Zwecks erforderlich, MÜSSEN die angebotenen Funktionalitäten angemessen geschützt werden.	Not Applicable	Innerhalb der Prüfung kontte keine aktive Funktionalität zum Versand von Brodcastnachrichten aufgefunden werden. Im Rahmen des Gematik Gutachtens wurde auch auf eine fehlerhafte Datenhaltung hin geprüft, die eine Interprozesskommunikation über shared Storage.	A_19186	02.06.2021
O.Plat_10	JavaScript bei Nutzung von WebView.	Die Applikation SOLL verhindern, dass JavaScript während der Nutzung von WebView aktiv ist. Falls JavaScript für die Realisierung der Anwendung unabdingbar ist, MUSS die Applikation JavaScript aus Quellen außerhalb der Kontrolle des Herstellers ablehnen.	Pass	Es wurden Schutzmechanismen innerhalb der Anwendung implementiert die den Einsatz von javascript verbieten. Da abseits hiervon keine interpretierbare Sprache gefunden wurde, wird die Anforderung mit Pass bewertet.		01.06.2021
O.Plat_11	Entfernung von sensiblen Daten bei Wechsel in den Hintergrundbetrieb.	Wechselt die Anwendung in den Hintergrundbetrieb, MUSS diese alle sensiblen Daten aus der aktuellen Ansicht (Views in iOS bzw. Activities in Android) entfernen.	Pass	Konnte in der Android und iOS App erfolgreich getestet werden.		02.06.2021
O.Plat_12	Deaktivierung nicht benötigter Protokoll-Handler in WebViews.	Die Applikation MUSS alle nicht benötigten Protokoll-Handler in WebViews deaktivieren.	Pass	Es wurden Schutzmechanismen innerhalb der Anwendung implementiert die den Einsatz von javascript verbieten.		01.06.2021
O.Plat_13	Löschen anwendungsspezifischer Cookies beim Beenden der Anwendung.	Die Applikation MUSS nach Beenden der Anwendung anwendungsspezifische Cookies gelöscht haben.	Not Applicable	Die Applikation verwendet lediglich lokale Webviews. Da nur HTML Seiten innerhalb der Anwendung aufgerufen werden, werden keine Cookies verwendet.		01.06.2021
O.Plat_14	Überschreiben aller nutzerspezifischen Daten bei Ende der Anwendung.	Die Applikation SOLL nach Beenden alle nutzerspezifischen Daten im Arbeitsspeicher sicher überschrieben haben.	Fail	Die Applikation überschreibt nicht explizit den Arbeitsspeicher.		01.06.2021
O.Plat_15	Information des Nutzers über erforderliche Sicherheitsmaßnahmen zur App, Bibliotheken und Plattformen.	Der Nutzer MUSS über Sicherheitsmaßnahmen informiert werden, sofern diese durch den Nutzer umsetzbar sind.	Pass	Das eRp-FdV informiert den Nutzer über die relevanten Sicherheitsmaßnahmen, die der Nutzer selbst umsetzen kann. Bspw. wird empfohlen, einen Login via Biometrie einzurichten (bspw Fingerprint, Face ID). Der Nutzer wird hierüber kurz aufgeklärt. Auch das Vorgehen mittels eGK wird erklärt. Die Maßnahmen, insb. die Nutzung von Biometrie, dienen dem Schutz der Informationen in der App und minimieren ein Restrisiko hinsichtlich eines unbefugten Zugriffs auf die App.		01.06.2021
O.Resi_1	Informationen zum sicheren Umgang mit der Anwendung.	Die Anwendung MUSS dem Nutzer barrierearme Best-Practice-Empfehlungen zum sicheren Umgang mit der Anwendung und ihrer Konfiguration bereitstellen.	Pass	Der Hersteller gibt im Rahmen des App-Onboardings sowie im Einstellungsmenü Hinweise zu Sicherheits-Best-Practices, bspw. im Umgang mit der Biometrie. Auch wird darauf hingewiesen, dass eine Installation auf gejailbreakten Geräten nicht durchgeführt werden soll,		01.06.2021

				wie auch in Emulatoren o.ä. Die gegebenen Security Best Practices entsprechen aus unserer Sicht dem Stand der Technik und sind für den Nutzer klar verständlich.		
O.Resi_2	Erkennung von gerooteten oder gejailbreakten Geräte.	Die Anwendung MUSS gerootete oder gejailbreakte Geräte entsprechend dem aktuellen Stand der Technik erkennen und angemessen darauf reagieren. Die Applikation MUSS dem Nutzer darstellen, welche Risiken für die Daten des Nutzers bei einer Fortsetzung der App bestehen (z. B. dass diese offengelegt werden könnten) oder die Fortsetzung unterbinden.	Fail	Diese Prüfung findet nicht statt.		01.06.2021
O.Resi_3	Erkennung und Unterbindung des Starts in einer Entwicklungs-/Debugumgebung.	Die Anwendung MUSS den Start in einer Entwicklungs-/Debugumgebung sicher erkennen und unterbinden.	Not Applicable	Die Prüfung auf eine Entwicklungsumgebung findet nicht statt. Die zugrundeliegenden Sicherheitsprobleme sind hiervon, da die Anwendung Open Source wird, nicht betroffen		01.06.2021
O.Resi_4	Abbruch des Starts der Anwendung bei ungewöhnlichen Benutzerrechten.	Die Anwendung MUSS ihren Start abbrechen, falls sie unter ungewöhnlichen Benutzerrechten gestartet wird (z. B. root oder nobody).	Fail	Diese Prüfung findet nicht statt.		01.06.2021
O.Resi_5	Überprüfung der Integrität des Endgeräts vor Verarbeitung sensibler Daten.	Die Anwendung MUSS die Integrität des Endgeräts überprüfen, bevor sensible Daten verarbeitet werden.	Fail	Diese Prüfung findet nicht statt.		01.06.2021
O.Resi_6	Überprüfung der Integrität des Backend vor Zugriff.	Die Anwendung MUSS vor dem Zugriff auf das Backend dessen Integrität überprüfen (siehe auch O.Ntwk_4).	Pass	Die Anwendungen implementieren einen Trust-Store, der in Verbindung mit dem in der Anwendung hinterlegtem Trust-Anchor, eine Prüfung des Backends durchführt. Die Implementierung konnte mittels praktischer Tests wie beispielsweise durch Zwischenschaltung einer Proxy validiert werden. Somit bewerten wir diese Anforderung mit Pass.		01.06.2021
O.Resi_7	Integration von Härtungsmaßnahmen vor Verarbeitung sensibler Daten.	Die Applikation SOLL Härtungsmaßnahmen, wie etwa eine Integritätsprüfung vor jeder Verarbeitung sensibler Daten innerhalb des Programmablaufs, realisieren.	Fail	Diese Prüfung findet nicht statt.		01.06.2021
O.Resi_8	Umsetzung von Maßnahmen gegen Reverse Engineering.	Die Applikation MUSS starke Maßnahmen gegen Reverse Engineering umsetzen.	Not Applicable	Die Applikation schützt sich nicht gegen Reverse Engineering. Da die Applikation in Zukunft OpenSource veröffentlich werden soll ist dies auch nicht sinnvoll.		01.06.2021
O.Resi_9	Berücksichtigung von Plattformen und Versionen bei Zugriffskontrollmechanismen.	Die Anwendung MUSS Zugriffskontrollmechanismen unter der Berücksichtigung von unterschiedlichen Plattformen und Plattformversionen implementieren, so dass ein missbräuchlicher Zugriff auf Ressourcen durch eine Änderung der Plattformversion ausgeschlossen ist und somit in jeder Ausführungsumgebung ein hinreichender Schutz aller Assets erzielt wird.	Pass	Die Zugriffsmaßnahmen sind zum einen biometrisch und somit von Anforderung O.Biom_6 betroffen. Die von jeden Nutzer zwingend durchzuführende Authentifizierung wird mittels Gesundheitskarte durchgeführt. Bei dieser sind jedoch mehrere Faktoren (Pin,CAN, EGk) für die Aktualisierung der Rezepte notwendig und greift nicht für die Einsicht der bereits erhaltenen Rezepte. Weiter wurde unter Android auf eine Implementierung der alternativen Authentifizierung verzichtet, welche eine Behandlung verschiedener Plattformen und Betriebssystemversionen abkürzt. Da die beschriebenen Kontrollmechanismen zum einen anderen Anforderungen unterliegen und im Falle der eGk, für Aktualisierungen, auch über das Backend verifiziert werden, wird die Anforderung mit Pass bewertet.		03.06.2021

Anlage 3: Allgemeine Auftragsbedingungen

Allgemeine Auftragsbedingungen
für
Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften
vom 1. Januar 2017

1. Geltungsbereich

(1) Die Auftragsbedingungen gelten für Verträge zwischen Wirtschaftsprüfern oder Wirtschaftsprüfungsgesellschaften (im Nachstehenden zusammenfassend „Wirtschaftsprüfer" genannt) und ihren Auftraggebern über Prüfungen, Steuerberatung, Beratungen in wirtschaftlichen Angelegenheiten und sonstige Aufträge, soweit nicht etwas anderes ausdrücklich schriftlich vereinbart oder gesetzlich zwingend vorgeschrieben ist.

(2) Dritte können nur dann Ansprüche aus dem Vertrag zwischen Wirtschaftsprüfer und Auftraggeber herleiten, wenn dies ausdrücklich vereinbart ist oder sich aus zwingenden gesetzlichen Regelungen ergibt. Im Hinblick auf solche Ansprüche gelten diese Auftragsbedingungen auch diesen Dritten gegenüber.

2. Umfang und Ausführung des Auftrags

(1) Gegenstand des Auftrags ist die vereinbarte Leistung, nicht ein bestimmter wirtschaftlicher Erfolg. Der Auftrag wird nach den Grundsätzen ordnungsmäßiger Berufsausübung ausgeführt. Der Wirtschaftsprüfer übernimmt im Zusammenhang mit seinen Leistungen keine Aufgaben der Geschäftsführung. Der Wirtschaftsprüfer ist für die Nutzung oder Umsetzung der Ergebnisse seiner Leistungen nicht verantwortlich. Der Wirtschaftsprüfer ist berechtigt, sich zur Durchführung des Auftrags sachverständiger Personen zu bedienen.

(2) Die Berücksichtigung ausländischen Rechts bedarf – außer bei betriebswirtschaftlichen Prüfungen – der ausdrücklichen schriftlichen Vereinbarung.

(3) Ändert sich die Sach- oder Rechtslage nach Abgabe der abschließenden beruflichen Äußerung, so ist der Wirtschaftsprüfer nicht verpflichtet, den Auftraggeber auf Änderungen oder sich daraus ergebende Folgerungen hinzuweisen.

3. Mitwirkungspflichten des Auftraggebers

(1) Der Auftraggeber hat dafür zu sorgen, dass dem Wirtschaftsprüfer alle für die Ausführung des Auftrags notwendigen Unterlagen und weiteren Informationen rechtzeitig übermittelt werden und ihm von allen Vorgängen und Umständen Kenntnis gegeben wird, die für die Ausführung des Auftrags von Bedeutung sein können. Dies gilt auch für die Unterlagen und weiteren Informationen, Vorgänge und Umstände, die erst während der Tätigkeit des Wirtschaftsprüfers bekannt werden. Der Auftraggeber wird dem Wirtschaftsprüfer geeignete Auskunftspersonen benennen.

(2) Auf Verlangen des Wirtschaftsprüfers hat der Auftraggeber die Vollständigkeit der vorgelegten Unterlagen und der weiteren Informationen sowie der gegebenen Auskünfte und Erklärungen in einer vom Wirtschaftsprüfer formulierten schriftlichen Erklärung zu bestätigen.

4. Sicherung der Unabhängigkeit

(1) Der Auftraggeber hat alles zu unterlassen, was die Unabhängigkeit der Mitarbeiter des Wirtschaftsprüfers gefährdet. Dies gilt für die Dauer des Auftragsverhältnisses insbesondere für Angebote auf Anstellung oder Übernahme von Organfunktionen und für Angebote, Aufträge auf eigene Rechnung zu übernehmen.

(2) Sollte die Durchführung des Auftrags die Unabhängigkeit des Wirtschaftsprüfers, die der mit ihm verbundenen Unternehmen, seiner Netzwerkunternehmen oder solcher mit ihm assoziierten Unternehmen, auf die die Unabhängigkeitsvorschriften in gleicher Weise Anwendung finden wie auf den Wirtschaftsprüfer, in anderen Auftragsverhältnissen beeinträchtigen, ist der Wirtschaftsprüfer zur außerordentlichen Kündigung des Auftrags berechtigt.

5. Berichterstattung und mündliche Auskünfte

Soweit der Wirtschaftsprüfer Ergebnisse im Rahmen der Bearbeitung des Auftrags schriftlich darzustellen hat, ist alleine diese schriftliche Darstellung maßgebend. Entwürfe schriftlicher Darstellungen sind unverbindlich. Sofern nicht anders vereinbart, sind mündliche Erklärungen und Auskünfte des Wirtschaftsprüfers nur dann verbindlich, wenn sie schriftlich bestätigt werden. Erklärungen und Auskünfte des Wirtschaftsprüfers außerhalb des erteilten Auftrags sind stets unverbindlich.

6. Weitergabe einer beruflichen Äußerung des Wirtschaftsprüfers

(1) Die Weitergabe beruflicher Äußerungen des Wirtschaftsprüfers (Arbeitsergebnisse oder Auszüge von Arbeitsergebnissen – sei es im Entwurf oder in der Endfassung) oder die Information über das Tätigwerden des Wirtschaftsprüfers für den Auftraggeber an einen Dritten bedarf der schriftlichen Zustimmung des Wirtschaftsprüfers, es sei denn, der Auftraggeber ist zur Weitergabe oder Information aufgrund eines Gesetzes oder einer behördlichen Anordnung verpflichtet.

(2) Die Verwendung beruflicher Äußerungen des Wirtschaftsprüfers und die Information über das Tätigwerden des Wirtschaftsprüfers für den Auftraggeber zu Werbezwecken durch den Auftraggeber sind unzulässig.

7. Mängelbeseitigung

(1) Bei etwaigen Mängeln hat der Auftraggeber Anspruch auf Nacherfüllung durch den Wirtschaftsprüfer. Nur bei Fehlschlagen, Unterlassen bzw. unberechtigter Verweigerung, Unzumutbarkeit oder Unmöglichkeit der Nacherfüllung kann er die Vergütung mindern oder vom Vertrag zurücktreten; ist der Auftrag nicht von einem Verbraucher erteilt worden, so kann der Auftraggeber wegen eines Mangels nur dann vom Vertrag zurücktreten, wenn die erbrachte Leistung wegen Fehlschlagens, Unterlassung, Unzumutbarkeit oder Unmöglichkeit der Nacherfüllung für ihn ohne Interesse ist. Soweit darüber hinaus Schadensersatzansprüche bestehen, gilt Nr. 9.

(2) Der Anspruch auf Beseitigung von Mängeln muss vom Auftraggeber unverzüglich in Textform geltend gemacht werden. Ansprüche nach Abs. 1, die nicht auf einer vorsätzlichen Handlung beruhen, verjähren nach Ablauf eines Jahres ab dem gesetzlichen Verjährungsbeginn.

(3) Offenbare Unrichtigkeiten, wie z.B. Schreibfehler, Rechenfehler und formelle Mängel, die in einer beruflichen Äußerung (Bericht, Gutachten und dgl.) des Wirtschaftsprüfers enthalten sind, können jederzeit vom Wirtschaftsprüfer auch Dritten gegenüber berichtigt werden. Unrichtigkeiten, die geeignet sind, in der beruflichen Äußerung des Wirtschaftsprüfers enthaltene Ergebnisse infrage zu stellen, berechtigen diesen, die Äußerung auch Dritten gegenüber zurückzunehmen. In den vorgenannten Fällen ist der Auftraggeber vom Wirtschaftsprüfer tunlichst vorher zu hören.

8. Schweigepflicht gegenüber Dritten, Datenschutz

(1) Der Wirtschaftsprüfer ist nach Maßgabe der Gesetze (§ 323 Abs. 1 HGB, § 43 WPO, § 203 StGB) verpflichtet, über Tatsachen und Umstände, die ihm bei seiner Berufstätigkeit anvertraut oder bekannt werden, Stillschweigen zu bewahren, es sei denn, dass der Auftraggeber ihn von dieser Schweigepflicht entbindet.

(2) Der Wirtschaftsprüfer wird bei der Verarbeitung von personenbezogenen Daten die nationalen und europarechtlichen Regelungen zum Datenschutz beachten.

9. Haftung

(1) Für gesetzlich vorgeschriebene Leistungen des Wirtschaftsprüfers, insbesondere Prüfungen, gelten die jeweils anzuwendenden gesetzlichen Haftungsbeschränkungen, insbesondere die Haftungsbeschränkung des § 323 Abs. 2 HGB.

(2) Sofern weder eine gesetzliche Haftungsbeschränkung Anwendung findet noch eine einzelvertragliche Haftungsbeschränkung besteht, ist die Haftung des Wirtschaftsprüfers für Schadensersatzansprüche jeder Art, mit Ausnahme von Schäden aus der Verletzung von Leben, Körper und Gesundheit, sowie von Schäden, die eine Ersatzpflicht des Herstellers nach § 1 ProdHaftG begründen, bei einem fahrlässig verursachten einzelnen Schadensfall gemäß § 54a Abs. 1 Nr. 2 WPO auf 4 Mio. € beschränkt.

(3) Einreden und Einwendungen aus dem Vertragsverhältnis mit dem Auftraggeber stehen dem Wirtschaftsprüfer auch gegenüber Dritten zu.

(4) Leiten mehrere Anspruchsteller aus dem mit dem Wirtschaftsprüfer bestehenden Vertragsverhältnis Ansprüche aus einer fahrlässigen Pflichtverletzung des Wirtschaftsprüfers her, gilt der in Abs. 2 genannte Höchstbetrag für die betreffenden Ansprüche aller Anspruchsteller insgesamt.

(5) Ein einzelner Schadensfall im Sinne von Abs. 2 ist auch bezüglich eines aus mehreren Pflichtverletzungen stammenden einheitlichen Schadens gegeben. Der einzelne Schadensfall umfasst sämtliche Folgen einer Pflichtverletzung ohne Rücksicht darauf, ob Schäden in einem oder in mehreren aufeinanderfolgenden Jahren entstanden sind. Dabei gilt mehrfaches auf gleicher oder gleichartiger Fehlerquelle beruhendes Tun oder Unterlassen als einheitliche Pflichtverletzung, wenn die betreffenden Angelegenheiten miteinander in rechtlichem oder wirtschaftlichem Zusammenhang stehen. In diesem Fall kann der Wirtschaftsprüfer nur bis zur Höhe von 5 Mio. € in Anspruch genommen werden. Die Begrenzung auf das Fünffache der Mindestversicherungssumme gilt nicht bei gesetzlich vorgeschriebenen Pflichtprüfungen.

(6) Ein Schadensersatzanspruch erlischt, wenn nicht innerhalb von sechs Monaten nach der schriftlichen Ablehnung der Ersatzleistung Klage erhoben wird und der Auftraggeber auf diese Folge hingewiesen wurde. Dies gilt nicht für Schadensersatzansprüche, die auf vorsätzliches Verhalten zurückzuführen sind, sowie bei einer schuldhaften Verletzung von Leben, Körper oder Gesundheit sowie bei Schäden, die eine Ersatzpflicht des Herstellers nach § 1 ProdHaftG begründen. Das Recht, die Einrede der Verjährung geltend zu machen, bleibt unberührt.

10. Ergänzende Bestimmungen für Prüfungsaufträge

(1) Ändert der Auftraggeber nachträglich den durch den Wirtschaftsprüfer geprüften und mit einem Bestätigungsvermerk versehenen Abschluss oder Lagebericht, darf er diesen Bestätigungsvermerk nicht weiterverwenden.

Hat der Wirtschaftsprüfer einen Bestätigungsvermerk nicht erteilt, so ist ein Hinweis auf die durch den Wirtschaftsprüfer durchgeführte Prüfung im Lagebericht oder an anderer für die Öffentlichkeit bestimmter Stelle nur mit schriftlicher Einwilligung des Wirtschaftsprüfers und mit dem von ihm genehmigten Wortlaut zulässig.

(2) Widerruft der Wirtschaftsprüfer den Bestätigungsvermerk, so darf der Bestätigungsvermerk nicht weiterverwendet werden. Hat der Auftraggeber den Bestätigungsvermerk bereits verwendet, so hat er auf Verlangen des Wirtschaftsprüfers den Widerruf bekanntzugeben.

(3) Der Auftraggeber hat Anspruch auf fünf Berichtsausfertigungen. Weitere Ausfertigungen werden besonders in Rechnung gestellt.

11. Ergänzende Bestimmungen für Hilfeleistung in Steuersachen

(1) Der Wirtschaftsprüfer ist berechtigt, sowohl bei der Beratung in steuerlichen Einzelfragen als auch im Falle der Dauerberatung die vom Auftraggeber genannten Tatsachen, insbesondere Zahlenangaben, als richtig und vollständig zugrunde zu legen; dies gilt auch für Buchführungsaufträge. Er hat jedoch den Auftraggeber auf von ihm festgestellte Unrichtigkeiten hinzuweisen.

(2) Der Steuerberatungsauftrag umfasst nicht die zur Wahrung von Fristen erforderlichen Handlungen, es sei denn, dass der Wirtschaftsprüfer hierzu ausdrücklich den Auftrag übernommen hat. In diesem Fall hat der Auftraggeber dem Wirtschaftsprüfer alle für die Wahrung von Fristen wesentlichen Unterlagen, insbesondere Steuerbescheide, so rechtzeitig vorzulegen, dass dem Wirtschaftsprüfer eine angemessene Bearbeitungszeit zur Verfügung steht.

(3) Mangels einer anderweitigen schriftlichen Vereinbarung umfasst die laufende Steuerberatung folgende, in die Vertragsdauer fallenden Tätigkeiten:

a) Ausarbeitung der Jahressteuererklärungen für die Einkommensteuer, Körperschaftsteuer und Gewerbesteuer sowie der Vermögensteuererklärungen, und zwar auf Grund der vom Auftraggeber vorzulegenden Jahresabschlüsse und sonstiger für die Besteuerung erforderlicher Aufstellungen und Nachweise

b) Nachprüfung von Steuerbescheiden zu den unter a) genannten Steuern

c) Verhandlungen mit den Finanzbehörden im Zusammenhang mit den unter a) und b) genannten Erklärungen und Bescheiden

d) Mitwirkung bei Betriebsprüfungen und Auswertung der Ergebnisse von Betriebsprüfungen hinsichtlich der unter a) genannten Steuern

e) Mitwirkung in Einspruchs- und Beschwerdeverfahren hinsichtlich der unter a) genannten Steuern.

Der Wirtschaftsprüfer berücksichtigt bei den vorgenannten Aufgaben die wesentliche veröffentlichte Rechtsprechung und Verwaltungsauffassung.

(4) Erhält der Wirtschaftsprüfer für die laufende Steuerberatung ein Pauschalhonorar, so sind mangels anderweitiger schriftlicher Vereinbarungen die unter Abs. 3 Buchst. d) und e) genannten Tätigkeiten gesondert zu honorieren.

(5) Sofern der Wirtschaftsprüfer auch Steuerberater ist und die Steuerberatervergütungsverordnung für die Bemessung der Vergütung anzuwenden ist, kann eine höhere oder niedrigere als die gesetzliche Vergütung in Textform vereinbart werden.

(6) Die Bearbeitung besonderer Einzelfragen der Einkommensteuer, Körperschaftsteuer, Gewerbesteuer, Einheitsbewertung und Vermögensteuer sowie aller Fragen der Umsatzsteuer, Lohnsteuer, sonstigen Steuern und Abgaben erfolgt auf Grund eines besonderen Auftrags. Dies gilt auch für

a) die Bearbeitung einmalig anfallender Steuerangelegenheiten, z.B. auf dem Gebiet der Erbschaftsteuer, Kapitalverkehrsteuer, Grunderwerbsteuer,

b) die Mitwirkung und Vertretung in Verfahren vor den Gerichten der Finanz- und der Verwaltungsgerichtsbarkeit sowie in Steuerstrafsachen,

c) die beratende und gutachtliche Tätigkeit im Zusammenhang mit Umwandlungen, Kapitalerhöhung und -herabsetzung, Sanierung, Eintritt und Ausscheiden eines Gesellschafters, Betriebsveräußerung, Liquidation und dergleichen und

d) die Unterstützung bei der Erfüllung von Anzeige- und Dokumentationspflichten.

(7) Soweit auch die Ausarbeitung der Umsatzsteuerjahreserklärung als zusätzliche Tätigkeit übernommen wird, gehört dazu nicht die Überprüfung etwaiger besonderer buchmäßiger Voraussetzungen sowie die Frage, ob alle in Betracht kommenden umsatzsteuerrechtlichen Vergünstigungen wahrgenommen worden sind. Eine Gewähr für die vollständige Erfassung der Unterlagen zur Geltendmachung des Vorsteuerabzugs wird nicht übernommen.

12. Elektronische Kommunikation

Die Kommunikation zwischen dem Wirtschaftsprüfer und dem Auftraggeber kann auch per E-Mail erfolgen. Soweit der Auftraggeber eine Kommunikation per E-Mail nicht wünscht oder besondere Sicherheitsanforderungen stellt, wie etwa die Verschlüsselung von E-Mails, wird der Auftraggeber den Wirtschaftsprüfer entsprechend in Textform informieren.

13. Vergütung

(1) Der Wirtschaftsprüfer hat neben seiner Gebühren- oder Honorarforderung Anspruch auf Erstattung seiner Auslagen; die Umsatzsteuer wird zusätzlich berechnet. Er kann angemessene Vorschüsse auf Vergütung und Auslagenersatz verlangen und die Auslieferung seiner Leistung von der vollen Befriedigung seiner Ansprüche abhängig machen. Mehrere Auftraggeber haften als Gesamtschuldner.

(2) Ist der Auftraggeber kein Verbraucher, so ist eine Aufrechnung gegen Forderungen des Wirtschaftsprüfers auf Vergütung und Auslagenersatz nur mit unbestrittenen oder rechtskräftig festgestellten Forderungen zulässig.

14. Streitschlichtungen

Der Wirtschaftsprüfer ist nicht bereit, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle im Sinne des § 2 des Verbraucherstreitbeilegungsgesetzes teilzunehmen.

15. Anzuwendendes Recht

Für den Auftrag, seine Durchführung und die sich hieraus ergebenden Ansprüche gilt nur deutsches Recht.

Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik, 55133 Bonn

gematik GmbH
Friedrichstrasse 136
10117 Berlin

[redacted]
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn

Postanschrift:
Postfach 20 03 06
53133 Bonn

Tel. +49 228 99 9582-[redacted]
Fax +49 228 99 10 9582-[redacted]

Referat-di24@bsi.bund.de

Betreff: Bestätigung gemäß § 360 Abs. 10 SGB V
Bezug: 1. Produktgutachten zum FdV E-Rezept (gematik, [redacted], 10.06.2021)
2. Produktgutachten zum Fachdienst E-Rezept (gematik, [redacted], 17.06.2021)
3. Produktgutachten zum Fachdienst IDP (gematik, [redacted], 18.06.2021)
4. Ergänzende Sicherheitsaussagen zum Fachdienst IDP (gematik, [redacted], 21.06.2021)

Berichterstatter: [redacted]
Datum: 25.06.2021

Sehr geehrte Damen und Herren,

das Bundesamt für Sicherheit in der Informationstechnik bestätigt das „Produktgutachten eRp-Frontend des Versicherten (FdV)“, erstellt durch PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft (PwC) am 31.05.2021.

Die Bestätigung erfolgt unter Berücksichtigung der unter Bezügen 2+3 vorgelegten Produktgutachten zu den Fachdiensten E-Rezept und IDP.
Da es sich bei dem Produktgutachten zum Fachdienst IDP um ein Teilgutachten handelt, danken wir Ihnen für die freundlicherweise zu Verfügung gestellten zusätzlichen Hinweise zu den Sicherheitseigenschaften des Fachdienstes IDP (Bezug 4.).
Wir danken im Voraus dafür, dass Sie uns die Ergebnisse der noch erfolgenden PEN-Tests zu Bezügen 1-3 zu Verfügung stellen werden.

Im o.a. Produktgutachten wurde festgestellt, dass Anforderungen der „BSI Prüfvorschrift für den Produktgutachter des „ePA-Frontend des Versicherten“ und des „E-Rezept Frontend des Versicherten“ nicht erfüllt wurden.

Die Dokumentation des Verfahrens der Risikobewertung des Produktgutachtens bei den nicht erfüllten Anforderungen im Prüfteil zur Prüfvorschrift des BSI entspricht nicht den

Anforderungen des BSI. Eine differenzierte Angabe der Höhe des Restrisikos und eine transparente Beschreibung wie das Prüflabor aus Basis von Wertungskriterien wie beispielsweise dem zu erwartendem Schaden und der Eintrittswahrscheinlich zu dieser Einstufung kommt, ist für ein solches Verfahren essenziell. Die Angabe „akzeptabel“ ist nach Ansicht des BSI nicht ausreichend. Das Prüflabor MUSS der gematik ein überarbeitetes Produktgutachten bis zum 31.12.2021 vorlegen.

Bei einem Teil dieser nicht erfüllten Anforderungen wird unterstellt, dass hierdurch Restrisiken für den Versicherten entstehen können.

Diese Restrisiken sind in einem begrenzten Test- oder Probebetrieb hinnehmbar unter der Voraussetzung, dass alle Teilnehmer an der Testphase darüber informiert werden, dass das FdV noch nicht in seiner endgültigen Fassung vorliegt und deshalb vom BSI Sicherheitsrisiken niedrigen Umfangs festgestellt wurden, die bis zum Produktivbetrieb zu beheben sind. Die Gefahr eines Datenverlusts bzw. Datenabflusses durch die Restrisiken wird seitens BSI als sehr gering eingeschätzt.

Das BSI bestätigt das o.a. Gutachten deshalb unter der Auflage, folgende Anforderungen bis zum 31.12.2021 zu erfüllen:

1. O.Auth_7
2. O.Token_6
3. O.Token_7
4. O.Plat_1
5. O.Arch_7
6. O.Data_3
7. O.Resi_4
8. O.Resi_5
9. O.Resi_7
10. O.Auth_13
11. O.Auth_6

Zusätzlich sollen folgende Anforderungen bis zum 31.12.2021 umgesetzt werden:

12. O.Resi_2
13. O.Tokn_3

Mit freundlichen Grüßen
Im Auftrag
gez.

Dr. Silke Bargstädt-Franke

Prüfbericht über FdV E-Rezept der gematik

1. Prüfung FdV E-Rezept

Prüfgegenstand: Produktgutachten eRezept-Frontend des Versicherten, Version 1.1 vom 31.05.2021,
Produktgutachter PwC,
eingereicht von der gematik GmbH, [redacted] beim BSI am 10.06.2021.

1.1 Prüfteil der Anforderungen nach Produkttypsteckbrief:

Der Produktgutachter hat insgesamt 134 Anforderungen geprüft.
Lediglich eine Anforderung wurde als "teilweise umgesetzt" bewertet, alle anderen Anforderungen wurden als "umgesetzt" oder "entbehrlich" bewertet.
Die Anforderung, die "teilweise umgesetzt" bewertet wurde, ist die Anforderung lfd. Nr. 114, A_21576 Löschung bestehender alternativer
Authentisierungsmittel. Zu dieser Anforderung spricht der Produktgutachter folgende Empfehlung aus.

Der Produktgutachter kommt unter 3.9 zu folgendem Prüfurteil:
"Als Ergebnis unserer Prüfungshandlungen wurden keine Sicherheitsmängel identifiziert, die den gesetzten Anforderungen
gemäß Prüfgrundlage widersprechen. Die erforderlichen Prozesse sind grundsätzlich angemessen etabliert. Verbleibende
geringfügige Abweichungen ohne Sicherheitsmangel sind aus Sicht der Gutachter nicht zulassungsverhindernd und sollten im
Rahmen der regelmäßigen Begutachtungen erneut geprüft werden. Es wurden acht (8) Empfehlungen ausgesprochen, die
jedoch keinen wesentlichen Sicherheitsmangel des Prüfobjektes adressieren.
Die Produktgutachter sind somit der Auffassung, dass das eRp-Frontend des Versicherten (FdV) nach reiflicher
Begutachtung und Bewertung den sicherheitstechnischen und datenschutzrechtlichen Anforderungen der gematik
entsprechen und somit geeignet sind, Teil der Telematikinfrastruktur der elektronischen Gesundheitskarte zu werden. Einer
kontrollierten Inbetriebnahme in den Produktionsbetrieb steht aus Sicht der Gutachter nichts im Wege."

Es wurden keine Auflagen zum Prüfurteil erteilt und acht Empfehlungen ausgesprochen.

Bewertung des BSI:

Das FdV E-Rezept erfüllt die Anforderungen des Produkttypsteckbriefs der gematik.
Die AFO A_21576 ist eine MUSS-Vorgabe.
Da keine Kritikalität für die IT-Sicherheit gesehen wird, ist die Bewertung des Produktgutachters und dessen Empfehlung hierzu für das BSI akzeptabel.

Zustell- und Lieferanschrift: Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189, 53175 Bonn

1.2 Prüfteil der Anforderungen nach BSI-Prüfvorschrift für den Produktgutachter des „ePA-Frontend des Versicherten“ und des „E-Rezept Frontend des Versicherten“ in der Entwurfsversion 1.2.6 vom 30.03.2021:

Der Produktgutachter hat alle 145 Prüfaspekte geprüft, davon wurden
• 85 Prüfaspekte mit „Pass“ bewertet,
• 25 Prüfaspekte mit „Fail“ bewertet,
• 33 Prüfaspekte als „Not Applicable“ bewertet und
• zwei Prüfaspekte konnten nicht abschließend bewertet werden („Inconclusive“).

Die Prüfer [redacted], alle BSI, Referat DI24) haben sich am 15.06.2021 konsultiert und sind zu folgendem einstimmigen Ergebnis gekommen:

Die Anforderungen, die mit "pass" bewertet wurden sind kursorisch geprüft worden und sind nicht zu beanstanden.

Prüfung zu den Anforderungen, die mit "fail" oder "inconclusive" bewertet wurden:

1. O.Auth_7 FAIL. Die Prüftiefe ist check. Die Vorgabe Prüfaspekt ist SOLL. Die Begründung, warum das FAIL kein relevantes Risiko darstellt ist unvollständig. Sie stellt nur auf die Protokollierung, nicht aber auf die Umsetzung der Benachrichtigungsfunktion für den Nutzer ab.
Die Risikobetrachtung enthält keinen Hinweis auf das vorgesehene white-Listing für die Gerätefreigabe.
BSI: Es besteht ein signifikantes Restrisiko. Das Restrisiko wird dennoch für die Testphase E-Rezept vom 01.07.-31.12.2021 als tragbar angesehen. Auflage: Die gematik MUSS die Funktion(serweiterung) bis 31.12.2021 umsetzen.

2. O.Token_6 FAIL. Die Prüftiefe ist check. Die Vorgabe Prüfaspekt ist MUSS. Die Begründung, warum das FAIL kein relevantes Risiko darstellt ist nicht vollständig, bzw. nicht zutreffend, weil für den Aufruf einer neuen Session die eGk nicht zwingend genutzt werden muss (z.B. Biometrie).
BSI: Es handelt sich um eine MUSS-Vorgabe. Das Restrisiko wird dennoch für die Testphase E-Rezept vom 01.07.-31.12.2021 als tragbar angesehen. Auflage: Die gematik MUSS die Vorgabe bis zum 31.12.2021 umsetzen.

3. O.Token_7 FAIL. Die Prüftiefe ist check. Die Vorgabe Prüfaspekt ist MUSS. Die Funktion dient dazu, dem Nutzer zu ermöglichen die Session sicher zu beenden, ohne die App zu schließen.
BSI: wie 2..

4. O.Resi_2 FAIL. Die Prüftiefe ist EXAMINE. Die Vorgabe Prüfaspekt ist MUSS. Die Funktion dient dazu, in erster Linie den Nutzer zu informieren. Es ist der Fall denkbar, dass der

Nutzer nicht weiß, dass sein Smartphone gerootet wurde. In dem Fall ist die Rückmeldung an den Nutzer nicht nur eine Information, sondern auch WARNUNG.
BSI: Es handelt sich um eine MUSS-Vorgabe. Das Restrisiko wird dennoch für die Testphase E-Rezept vom 01.07.-31.12.2021 als tragbar angesehen. Auflage: Die gematik SOLL die Vorgabe bis zum 31.12.2021 umsetzen.

5. O.Plat_1 FAIL. Die Prüftiefe ist check. Die Vorgabe Prüfaspekt ist SOLL/MUSS. Die Funktion dient dazu, in erster Linie den Nutzer zu WARNEN. Die Bewertung des Prüfers ist nur zum Teil schlüssig, weil die nicht umgesetzte Warnung sich nicht wegdiskutieren lässt.
BSI: wie 2..

6. O.Plat_14 FAIL. Die Prüftiefe ist check. Die Vorgabe Prüfaspekt ist SOLL.
BSI: OK.

7. O.Data_7 FAIL. Die Prüftiefe ist check. Die Vorgabe Prüfaspekt ist SOLL.
BSI: OK.

8. O.Data_11 FAIL. Die Prüftiefe ist check. Die Vorgabe Prüfaspekt ist KANN.
BSI: OK.

9. O.Arch_7 FAIL. Die Prüftiefe ist EXAMINE. Die Vorgabe Prüfaspekt ist MUSS. Die Begründung des Prüfers ist schlüssig.
BSI: Es wird die Klärung mit dem BfDI empfohlen. Grundsätzlich sieht das BSI keine Bedenken aus Sicht der IT-Sicherheit gegen google safetynet. Im Bankensektor ist der Einsatz des service bei Apps üblich.

10. O.Data_3 FAIL. Die Prüftiefe ist EXAMINE. Die Vorgabe Prüfaspekt ist SOLL. Der vorgegebene Prüfumfang wurde nicht ausgeführt, bzw. nicht dokumentiert. Der e-Gk-Schlüssel wird im secure-element abgelegt.
BSI: wie 2..

11. O.Resi_3 FAIL. Die Prüftiefe ist check. Die Vorgabe Prüfaspekt ist MUSS.
BSI: -not applicable-

12. O.Resi_4 FAIL. Die Prüftiefe ist CHECK. Die Vorgabe Prüfaspekt ist MUSS.
BSI: wie 2..

13. O.Resi_5 FAIL. Die Prüftiefe ist EXAMINE. Die Vorgabe Prüfaspekt ist MUSS. Die Anforderung weitergehender Integritätschecks beinhaltet einen aufwändigen Prüfauftrag, der nicht durchgeführt wurde.
BSI: wie 9..

14. O.Resi_7 FAIL. Die Prüftiefe ist EXAMINE. Die Vorgabe Prüfaspekt ist MUSS.
BSI: wie 2..

15. O.Resi_8 FAIL.
BSI: -not applicable-

16. O.Auth_13. FAIL. Die Prüftiefe ist check. Die Vorgabe Prüfaspekt ist MUSS. Es könnte sein, dass der Versicherte das smartphone unbeabsichtigt offen liegen lässt.
BSI: wie 2..

17. O.Arch_11. FAIL. Die Prüftiefe ist EXAMINE. Die Vorgabe Prüfaspekt ist MUSS. Der Umfang des Prüfauftrags wurde nicht ausgeführt. Zwangsupdates ist keine Standard-Anforderung, sondern etwas sehr Spezielles im App-Umfeld.
BSI: OK.

18. O.Arch._8. FAIL. Die Prüftiefe ist EXAMINE. Die Vorgabe Prüfaspekt ist MUSS.
BSI: OK.

19. O.Auth_6. FAIL. Die Prüftiefe ist EXAMINE. Die Vorgabe Prüfaspekt ist MUSS. Nachbesserung erforderlich.
BSI: wie 9..

20. O.Sess_5. FAIL. Die Prüftiefe ist EXAMINE. Die Vorgabe ist MUSS. Die ANWENDUNG muss nach Timeout die Session beenden, nicht der Nutzer.
BSI: -not applicable-.

21. O.Auth_13 doppelt siehe 16.

22. O.Auth_4. FAIL. Die Prüftiefe ist EXAMINE. Die Vorgabe Prüfaspekt ist MUSS.
BSI: OK.

23. O.Biom_1. FAIL. . Die Prüftiefe ist check. Die Vorgabe Prüfaspekt ist SOLL.
BSI: OK.

24. O.Tokn_3. FAIL. Die Prüftiefe ist check. Die Vorgabe Prüfaspekt ist MUSS.
BSI: wie 4..

25. O.Biom_2. FAIL. Die Prüftiefe ist check. Die Vorgabe Prüfaspekt ist MUSS. siehe 24. und Absprache Biometrie mit gematik.
BSI: OK.

26. O.Arch_10. Inconclusive. Die Prüftiefe ist check. Die Vorgabe Prüfaspekt ist MUSS.
BSI: OK.

27. O.Data_10. Inconclusive. Die Prüftiefe ist EXAMINE. Die Vorgabe Prüfaspekt ist SOLL. Anforderung gegen Expertenwissen checken.
BSI: OK.

Grundlage für das Prüfurteil soll ein dokumentiertes Risikomanagementverfahren sein. Als allgemeine Referenz werden ISO 27005 und Anhang B der Common Criteria Evaluation Methodology in der Prüfvorschrift genannt. Das Prüflabor darf nach Abstimmung jedoch auch ein vergleichbares, auf eine IT-Sicherheitsanwendung ausgerichtetes Risikomanagementverfahren einsetzen. Das BSI ist der Ansicht, dass das Prüflabor bei der Risikobewertung auf ein akzeptables Risikomanagementverfahren zurückgegriffen hat. Jedoch

entspricht die Dokumentation des Verfahrens nicht den Anforderungen des BSI. Eine differenzierte Angabe der Höhe des Restrisikos und eine transparente Beschreibung wie das Prüflabor aus Basis von Wertungskriterien wie beispielsweise dem zu erwartendem Schaden und der Eintrittswahrscheinlich zu dieser Einstufung kommt, ist für ein solches Verfahren essenziell. Die Angabe „akzeptabel“ ist nach Ansicht des BSI nicht ausreichend. Das Prüflabor MUSS dem BSI ein überarbeitetes Produktgutachten bis zum 31.12.2021 vorlegen.

1.3 Bewertung:

Die Anforderungen der Prüfvorschrift des BSI wurden nur teilweise erfüllt.
Es wurden keine wesentliche Mängel festgestellt, deshalb kann der Testbetrieb des E-Rezept wie vorgesehen zum 01.07.2021 starten unter der Maßgabe, dass die Teilnehmer im Testbetrieb darüber informiert werden, dass die App noch nicht fertig ist und noch Restrisiken bestehen, die vom BSI im eingeschränkten Testbetrieb als nicht kritisch gesehen werden.

Der Live-Betrieb am 01.01.2022 kann starten, wenn die o.a. Auflagen vorher umgesetzt wurden.

Im Auftrag

Gez.
[redacted]

Bericht zum Penetrationstest des E-Rezeptes der gematik

gematik
25.06.2021

Version 1.0

pwc

Vertraulich

Änderungshistorie

Version	Datum	Beschreibung
0.1	17.05.2021	Initiale Version
0.9	24.06.2021	QS Version
1.0	25.06.2021	Finale Version

Abkürzungsverzeichnis

Abkürzung	Beschreibung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CVSS	Common Vulnerability Scoring System 3.1
DoS	Denial of Service
HTTP	Hypertext Transfer Protocol
JSON	JavaScript Object Notation
PwC	PricewaterhouseCoopers
TNV	Teilnehmerverwaltung
URL	Uniform Resource Locator

Tabelle 1: Abkürzungsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Inhaltsverzeichnis

1. Auftrag und Auftragsdurchführung

Im Rahmen der im März 2021 erfolgten Beauftragung zur Produktbegutachtung der E-Rezept-App hat uns die

gematik GmbH

Berlin, Deutschland

(nachfolgend „gematik“ oder Auftraggeber)

weiterhin mit der Durchführung eines Security Penetration Tests (nachfolgend „SPT“) beauftragt.

Testgegenstand waren die gematik E-Rezept-App für iOS und Android und die beiden Backendkomponenten E-Rezept-Fachdienst (eRp-FD) und Identity-Provider (IDP).

Ziel des SPT war die Suche nach Schwachstellen mit Hilfe von automatisierten Werkzeugen und manuellen Analysen.

Den Test haben wir im Zeitraum vom 22.06.2021 bis zum 25.06.2021 durchgeführt. Gegenstand unseres Auftrags waren weder die Aufdeckung und Aufklärung strafrechtlicher Tatbestände, wie Untreuehandlungen oder Unterschlagungen, noch die Beurteilung der Effektivität und Wirtschaftlichkeit der Vorgehensweisen, Verfahren und Systeme der Gesellschaft. Soweit wir aufgrund unserer Analysen Verbesserungsmöglichkeiten sehen, weisen wir gleichwohl in diesem Bericht darauf hin.

Die Beurteilung der Analysegebiete erfolgte auf Grundlage, der uns von Mitarbeitern der gematik erteilten Auskünfte und Dokumente sowie anhand eigener Tests. Auskünfte und die benötigten Unterlagen zur Durchführung unserer Tätigkeit erhielten wir im gewünschten Umfang.

Über Art und Umfang sowie über das Ergebnis unserer Tätigkeiten berichten wir im Folgenden.

Für die Durchführung des Auftrags und unsere Verantwortlichkeit sind, auch im Verhältnis zu Dritten, die diesem Bericht beigefügten Allgemeinen Auftragsbedingungen vom 1. Januar 2017 vereinbart.

2. Management Zusammenfassung

Die gematik hat die PwC mit der Durchführung eines Security Penetration Tests gegen die gematik E-Rezept-App für iOS und Android und die beiden Backendkomponenten E-Rezept-Fachdienst (eRp-FD) und Identity-Provider (IDP) beauftragt. Die Untersuchungen haben wir in der Zeit vom 22.06.2021 bis 25.06.2021 durchgeführt.

Im Rahmen der Untersuchung konnten wir insgesamt vier Feststellungen treffen. Davon haben wir zwei mit **niedrig** und zwei als **informativ** bewertet (siehe Abbildung 1).

Abbildung 1 - Aufteilung der Feststellungen

Fehlendes Rate Limiting auf der API (FD und IDP)

Sowohl der Fachdienst als auch der Identity-Provider implementieren kein Rate Limiting. Das bedeutet, dass beliebig viele Anfragen an den Server geschickt werden können. Dies kann zu einer Überlastung des Servers führen und erleichtert es einem Angreifer, andere Angriffe durchzuführen. Wir empfehlen daher, die Anzahl der Anfragen pro IP-Adresse und Zeiteinheit zu begrenzen.

Erstellen von Screenshots möglich (iOS)

In der iOS App ist es möglich, Screenshots von sensiblen Daten anzufertigen. So kann der Nutzer sensible Daten abfotografieren und in der Fotobibliothek speichern, wo sie nicht mehr geschützt sind. Wir empfehlen, die Möglichkeit Screenshots zu machen zu deaktivieren oder die Benutzer explizit auf die Risiken hinzuweisen.

Die detaillierte Darstellung samt Informationen zur Reproduktion und empfohlenen Maßnahmen zur Behebung der Schwachstellen folgt in den Kapiteln 3 bis 5.

Wir weisen darauf hin, dass unsere Sicherheitsanalysen im Wesentlichen darauf ausgerichtet sind, durch realistische Tests Schwachstellen zu entdecken und mittels dieser Schwachstellen in die als unzugänglich definierten Netzbereiche und Serversysteme vorzudringen. Sie sind daher nur bedingt geeignet, sämtliche Kontroll- und Sicherheitsmechanismen zu analysieren oder alle potenziellen Schwachstellen im Gesamtnetz der gematik aufzudecken, wie dies etwa im Rahmen einer weiterführenden Untersuchung möglich wäre. Unsere Analyseergebnisse beziehen sich auf den Entwicklungsstand der E-Rezept-App zum Zeitpunkt unserer Untersuchungen.

Da unser Bericht mögliche Angriffspunkte beinhaltet, empfehlen wir, diesen vertraulich zu behandeln.

3. iOS Anwendung

3.1 Feststellungen

3.1.1 Erstellen von Screenshots möglich

Während des Security Penetration Tests konnte festgestellt werden, dass Screenshots nicht in der Anwendung deaktiviert sind, so kann der Nutzer kritische Daten abfotografieren und in der Fotobibliothek speichern.

Alle innerhalb der Anwendung angezeigten Informationen können gestohlen werden, da diese nicht explizit geschützt sind. Das Risiko im Zusammenhang mit dieser Art von Schwachstelle besteht hauptsächlich im Diebstahl sensibler Informationen.

Mobile Anwendungen sollten Mechanismen zur Verhinderung von Screenshots implementieren, um zu verhindern, dass ein Angreifer sensible Daten, wie z. B. Zugangsdaten oder private Informationen, die während der Ausführung der Anwendung auf dem Bildschirm angezeigt werden, stehlen kann.

Evidenz

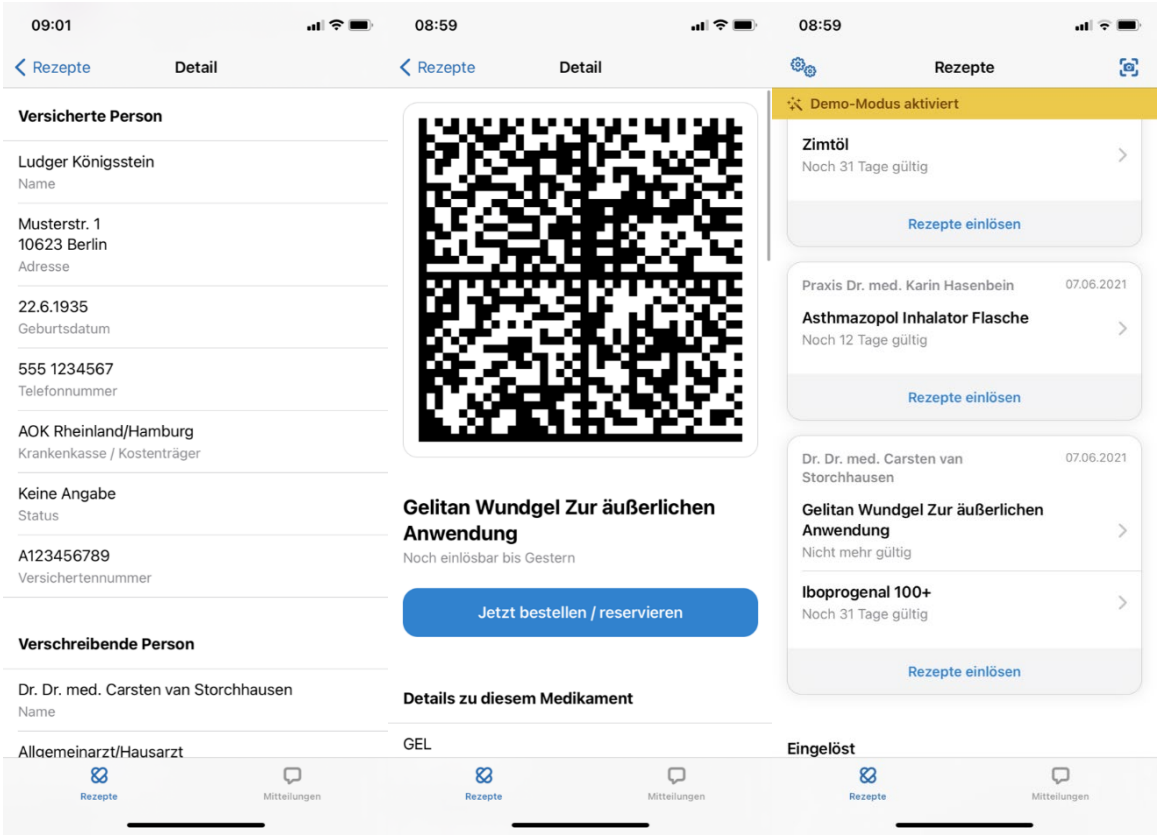

Abbildung 2: Screenshots der iOS Anwendung

Bewertung der Feststellung

Risiko: Niedrig

Die Anwendung zeigt einerseits sensible Daten an, andererseits benötigt eine Ausnutzung eine explizite Interaktion des Anwenders. Wir bewerten diese Feststellung daher mit einem niedrigen Risiko.

Empfehlungen

Die Funktion für die Erstellung von Screenshots sollte in der Anwendung geeignet deaktiviert bzw. unterbunden werden.

3.2 Beobachtungen

Die iOS-Anwendung hat ein sehr gutes Sicherheitsniveau, es wurde nur eine Schwachstelle mit niedrigem Risiko gefunden. Während des Tests hat der Prüfer keine kritische Schwachstelle gefunden.

- Die Berechtigungen der Anwendung sind klar dokumentiert und beinhalten lediglich für den Betrieb notwendige Berechtigungen.
- Die FaceID-Authentifizierung ist sicher implementiert, um unbefugte Zugriffe zu erschweren.
- Die Datenspeicherung entspricht den Sicherheitsstandards. Typische Schwachstellen wie Injektion oder Datenlecks sind uns in unseren Tests nicht aufgefallen.
- In unseren Tests konnten wir keine OWASP Mobile Top 10 Schwachstellen im Rahmen der App vorfinden.

4. Android Anwendung

4.1 Feststellungen

4.1.1 AES-Konfiguration

Es wurde der Blockchiffre-Modus ECB verwendet: Blockbasierte Verschlüsselung wird an diskreten Eingabeblöcken durchgeführt (AES hat bspw. 128-Bit Blöcke). Wenn der Klartext größer als die Blockgröße ist, wird der Klartext intern in Blöcke der gegebenen Eingabegröße aufgeteilt und an jedem Block wird verschlüsselt. Ein Blockmodus bestimmt, ob sich das Ergebnis der Verschlüsselung des vorherigen Blocks auf nachfolgende Blöcke auswirkt.

Im Code wurde der ECB Modus entdeckt. Dieser unterteilt die Eingabe in Blöcke fester Größe, die separat mit demselben Schlüssel verschlüsselt werden. Wenn mehrere geteilte Blöcke denselben Klartext enthalten, werden sie in identische Geheimtextblöcke verschlüsselt, wodurch Muster in den Daten leichter identifiziert werden können. So könnten Angreifer in manchen Situationen auch die verschlüsselten Daten wiedergeben.

Bewertung der Feststellung

Bewertung: informativ

Die Art wie der ECB-Modus in der Android App verwendet wird stellt aus der Sicht des Gutachters keine Sicherheitsgefährdung da. Daher bewerten wir diese Feststellung als rein informativ.

4.2 Beobachtungen

- Es wurden keine hardcodierten Secrets wie Keys, IP-Adressen, Passwörter, etc. im Code bzw. in den Dateien entdeckt.

- Die Backup und Debugging Funktion der App ist ausgeschaltet, welche sonst von diversen Tools ausgenutzt und einen Datenabfluss von sensiblen Daten ermöglicht bzw. Rückschlüsse zur internen Datenstruktur freigeben könnte.

- Es wurden keine unnötigen Genehmigungen oder sonstigen Freigaben festgestellt — ein Missbrauch würde auch hier zu einem Sicherheitsfaktor führen.

- Positiv anzumerken ist die Nutzung der AES Verschlüsselung im Allgemeinen, da sie aktuell als de-facto Standard für sichere Kryptographieverfahren gilt.

- Die Konfiguration von AES selbst erfolgt im Code größtenteils mit dem GCM Modus, welcher standardmäßig von diversen Behörden empfohlen wird und aktuell als sicher eingestuft wird.

- Zudem ist die durchgehende Einhaltung der Standards für sichere Cipher Suites mit zusätzlicher Unterteilung in TLS1.2 & TLS1.3 erwähnenswert, da oft Fehlkonfigurationen bei der Implementierung für die unterschiedlichen TLS Versionen entstehen können.

- Die DataMatrix Code Scan-Funktion erfasste durchweg die für die Funktion gedachten Rezepte ausnahmslos und wies zum Zeitpunkt des Tests keine Fehlfunktionen auf, auch nach mehreren Bypassing-Versuchen.

- Umgehungsversuche der Screenshot-Funktion waren erfolglos und ein Screenshotschutz für die Android Version ist aktuell in einem funktionsfähigen Zustand.

5. Fachdienst und Identity Provider

Wir haben jeweils die Test- und Produktivversion des Fachdienstes und des Identity Providers getestet. Die Schnittstellen werden jeweils von der IBM Deutschland GmbH und der Research Industrial Systems Engineering GmbH (kurz RISE) betrieben.

Die Endpunkte für die Systeme sind im Folgenden gelistet:

Testsystem

- erp-test.app.ti-dienste.de
- idp-test.app.ti-dienste.de
- idp-test.zentral.idp.splitdns.ti-dienste.de
- idp-pairing-test.zentral.idp.splitdns.ti-dienste.de

Produktivsystem

- erp.app.ti-dienste.de
- idp.app.ti-dienste.de
- idp.zentral.idp.splitdns.ti-dienste.de
- idp-pairing.zentral.idp.splitdns.ti-dienste.de

Eine Authentifizierung gegenüber dem Identity Provider innerhalb der Produktivumgebung war aufgrund von fehlender, valider Gesundheitskarten nicht möglich. Daher wurden authentifizierte Tests innerhalb der Testumgebung durchgeführt, die mit einer Testkarte authentifiziert wurden. Das Produktivsystem wurde daher nur anonym getestet. Der Betreiber hat versichert das in beiden Systemen der gleiche Softwarestand vorhanden ist.

5.1 Feststellungen

Im Folgenden wird näher auf die Feststellungen des SPT für den Fachdienst und Identityprovider eingegangen.

5.1.1 Fehlendes Rate Limiting auf der API

Während des Tests konnte kein Rate-Limiting an der API erkannt werden. Dies erlaubt es einem Angreifer eine beliebige Anzahl an Anfragen an die API zu senden, was potenziell zur Überlastung der Endpunkte und des Backend führen kann. Im Weiteren eröffnet fehlendes Rate-Limiting die Möglichkeit für Brute-Force Angriffe, z.B. das Erraten von Object-IDs.

Alle Anfragen mit der ID 7615 – 7466 wurden innerhalb derselben Sekunde verschickt. Daraus geht hervor, dass 149 Request pro Sekunde an die API gesendet werden konnten.

Wir stufen diese Feststellung mit einer niedrigen Kritikalität ein.

Betroffene Endpunkte

- https://erp-test.app.ti-dienste.de
- https://idp-test.app.ti-dienste.de

Evidenz

In folgenden Abbildungen ist eine Liste an abgeschickten Anfragen an den Server zu sehen.

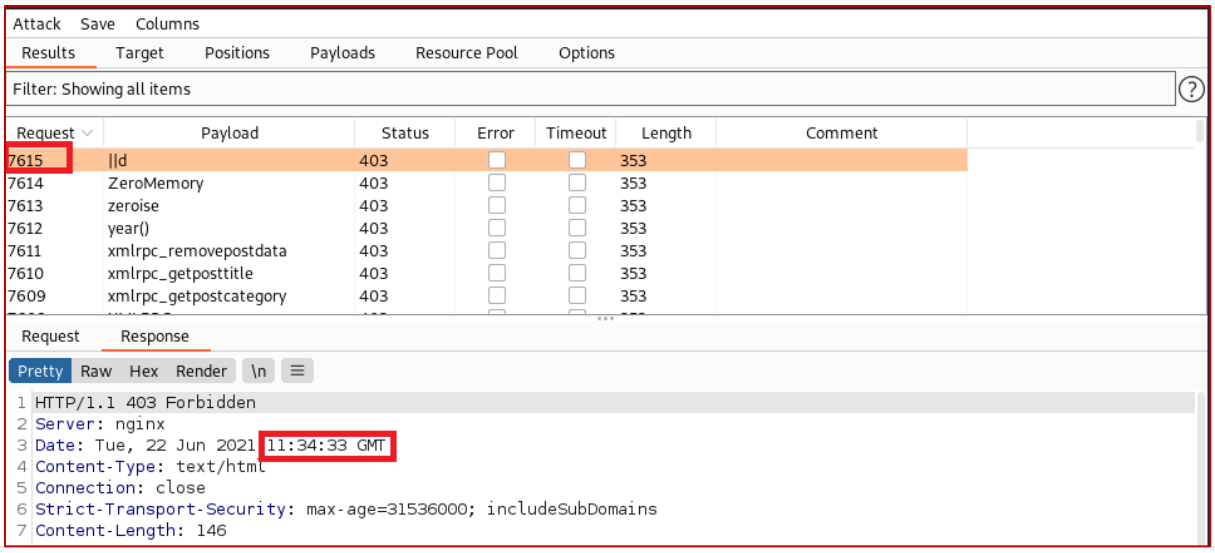

Abbildung 3: Request 7615 wurde um 11:34:33 GMT gesendet.

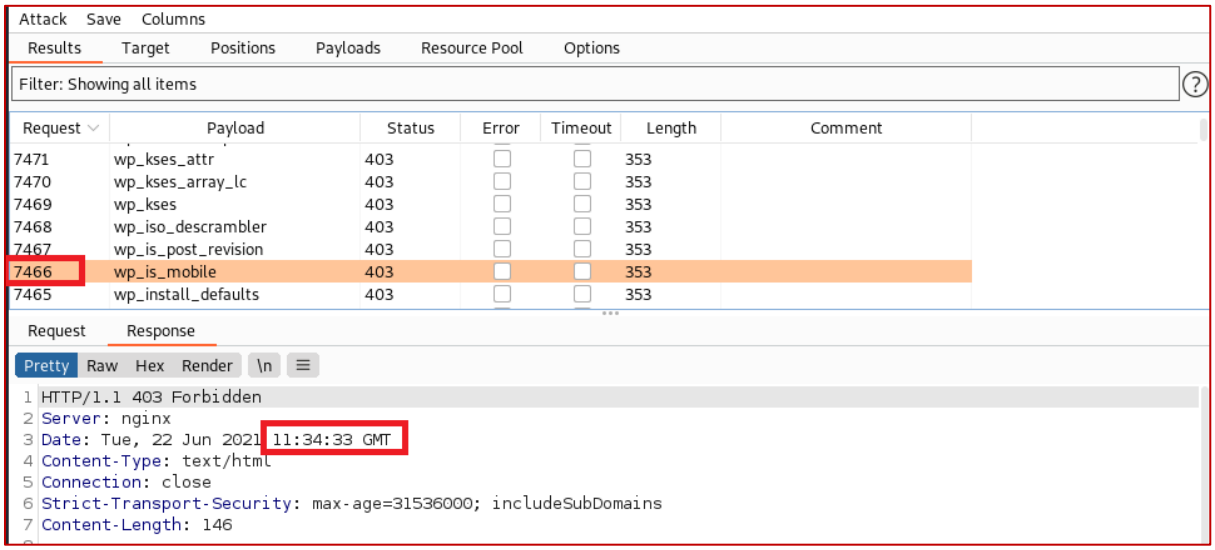

Abbildung 4: Request 7466 wurde um 11:34:33 GMT versendet.

Bewertung der Feststellung

Risiko: Niedrig

Das Fehlen eines Rate-Limitings stellt einen Angriffsvektor dar, der einem potentiellen Angreifer die Möglichkeit bietet, zum Beispiel das Authentifizierungsprotokoll mittels „Brute-Force“-Angriffen zu brechen. Weitere Tests konnten jedoch keine Anzeichen für die Umsetzbarkeit eines solchen Angriffs aufzeigen (siehe Kapitel 5.2). Daher bewerten wir diese Feststellung mit einem niedrigen Risiko.

Empfehlung

Es wird empfohlen, ein Rate-Limiting für die API einzustellen.

5.1.2 Fehlende HSTS Header

Um zu verhindern, dass sensible Informationen von einem Angreifer abgehört werden können, sollte zu jedem Zeitpunkt ein verschlüsselter Kommunikationskanal genutzt werden. Der HSTS-Header weist

einen Client an, mit einem Endpunkt nur mittels HTTPS zu kommunizieren, wenn bereits erfolgreich eine Verbindung mittels HTTPS hergestellt wurde. Dies erlaubt es bestimmte Arten von Man-in-the-Middle Angriffen zu mitigieren, bei denen ein Angreifer Datenverkehr abfängt und die Kommunikation mit dem Client auf eine unverschlüsselte HTTP Verbindung umstellt. Dabei könnten sensible Daten unverschlüsselt übertragen werden.

Da die Endpunkte ausschließlich zur Verwendung durch die mobilen Applikationen gedacht sind, stellen die fehlenden HSTS Header kein Sicherheitsrisiko da.

Betroffene Endpunkte

- https://erp-test.app.ti-dienste.de

Evidenz

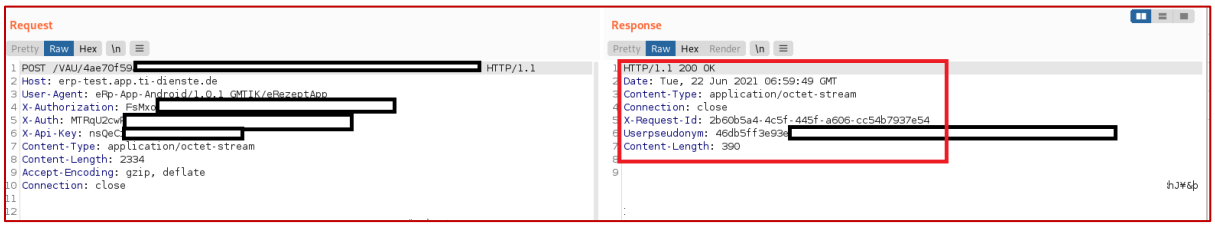

Abbildung 5: Fehlender HSTS-Header. In der Response des API Endpunktes fehlt der Strict-Transport-Security-Header.

Bewertung der Feststellung

Risiko: informativ

Ein Anwender wird zu keiner Zeit auf den Dienst über einen Webserver zugreifen, sondern über die Mobile Anwendung verwenden, die eine HTTPS Verbindung erzwingt. Daher bewerten wir diese Feststellung als informativ.

Empfehlung

Wir empfehlen, den Server so zu konfigurieren, dass dieser Strict-Transport-Security in der Kommunikation erzwingt.

5.2 Beobachtungen

Im Rahmen des SPT wurden verschiedene Aspekte des Fachdienstes und Identity-Providers geprüft. Hierbei konnten wir zusätzlich positive Aspekte der betrachteten Implementierungen beobachten. Eine Auswahl derer ist im Folgenden aufgeführt.

1. Während des Authentifizierungs-Prozesses wird dem Identity Provider eine Redirect URI gesendet. Während des Tests war es nicht möglich diese zu manipulieren und somit eine Weiterleitung auf ungewünschte Ressourcen zu erreichen.
2. In der Kommunikation mit dem Fachdienst war es nicht möglich die GET-Request, welche von der App gesendet wird, so zu manipulieren, dass der Endpunkt dadurch beeinflusst wird. Jeder Versuch, eine manipulierte GET-Request an den Endpunkt zu senden wurde mit einer “405 Method not allowed” Fehlermeldung beantwortet.
3. Während des Tests konnten keine weiteren öffentlichen Endpunkte gesichtet werden, welche nicht in der regulären Kommunikation zwischen Endpunkt und App verwendet werden.
4. Die zur Authentifizierung genutzten JSON Web Token (JWT) konnten weder erfolgreich manipuliert werden, noch war es im zeitlichen Rahmen des Tests möglich die Signatur der Token zu brechen. Die Signatur der JWT wurde vom Server geprüft und manipulierte Tokens wurden erfolgreich abgelehnt.

6. Schlussbemerkung

Wir haben für die gematik einen Security Penetration Test der E-Rezept-App durchgeführt. Das Ergebnis unserer Analyse und unsere empfohlenen Maßnahmen, Hinweise und Anregungen haben wir in diesem Bericht dargestellt. Das zusammengefasste Untersuchungsergebnis aus der Management Zusammenfassung in Kapitel 2 ist je Prüfungsgegenstand in den Kapiteln 3 bis 5 enthalten.

Dieser Bericht basiert auf unseren Untersuchungen, den uns erteilten Auskünften sowie zur Verfügung gestellten Unterlagen. In diesem Zusammenhang möchten wir uns für die angenehme Zusammenarbeit und die Unterstützung durch die Mitarbeiter der gematik, der RISE und IBM bedanken.

Zu den Feststellungen haben wir jeweils Maßnahmen empfohlen und erläutert.

Für eine weitergehende Unterstützung stehen wir gerne zur Verfügung.

XXXXXX, 25.06.2021

XXXXXXXXXXXXXXX

XXXXXX, 25.06.2021

XXXXXXXXXXXXXXX

7. Referenzen

- HSTS Header:
  https://www.globalsign.com/de-de/blog/was-ist-hsts-wie-fuehren-sie-es-ein
- API Rate-Limiting:
  https://apisecurity.io/encyclopedia/content/owasp/api4-lack-of-resources-and-rate-limiting.htm
- Padding Oracle Crypto Attack:
  https://cve.circl.lu/capec/463
- CWE-649: Verschlüsselung ohne Integritätscheck:
  https://cwe.mitre.org/data/definitions/649.html
- CWE-327: Nutzung von riskanten Krypto-Algorithmen:
  https://cwe.mitre.org/data/definitions/649.html
- Related CVEs:
  https://nvd.nist.gov/vuln/detail/CVE-2019-8919 (CVSS 7.5 - High)
  https://nvd.nist.gov/vuln/detail/CVE-2020-8911 (CVSS 5.6 Medium).

8. Allgemeine Auftragsbedingungen

Allgemeine Auftragsbedingungen
für
Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften
vom 1. Januar 2017

1. Geltungsbereich

(1) Die Auftragsbedingungen gelten für Verträge zwischen Wirtschaftsprüfern oder Wirtschaftsprüfungsgesellschaften (im Nachstehenden zusammenfassend „Wirtschaftsprüfer" genannt) und ihren Auftraggebern über Prüfungen, Steuerberatung, Beratungen in wirtschaftlichen Angelegenheiten und sonstige Aufträge, soweit nicht etwas anderes ausdrücklich schriftlich vereinbart oder gesetzlich zwingend vorgeschrieben ist.

(2) Dritte können nur dann Ansprüche aus dem Vertrag zwischen Wirtschaftsprüfer und Auftraggeber herleiten, wenn dies ausdrücklich vereinbart ist oder sich aus zwingenden gesetzlichen Regelungen ergibt. Im Hinblick auf solche Ansprüche gelten diese Auftragsbedingungen auch diesen Dritten gegenüber.

2. Umfang und Ausführung des Auftrags

(1) Gegenstand des Auftrags ist die vereinbarte Leistung, nicht ein bestimmter wirtschaftlicher Erfolg. Der Auftrag wird nach den Grundsätzen ordnungsmäßiger Berufsausübung ausgeführt. Der Wirtschaftsprüfer übernimmt im Zusammenhang mit seinen Leistungen keine Aufgaben der Geschäftsführung. Der Wirtschaftsprüfer ist für die Nutzung oder Umsetzung der Ergebnisse seiner Leistungen nicht verantwortlich. Der Wirtschaftsprüfer ist berechtigt, sich zur Durchführung des Auftrags sachverständiger Personen zu bedienen.

(2) Die Berücksichtigung ausländischen Rechts bedarf – außer bei betriebswirtschaftlichen Prüfungen – der ausdrücklichen schriftlichen Vereinbarung.

(3) Ändert sich die Sach- oder Rechtslage nach Abgabe der abschließenden beruflichen Äußerung, so ist der Wirtschaftsprüfer nicht verpflichtet, den Auftraggeber auf Änderungen oder sich daraus ergebende Folgerungen hinzuweisen.

3. Mitwirkungspflichten des Auftraggebers

(1) Der Auftraggeber hat dafür zu sorgen, dass dem Wirtschaftsprüfer alle für die Ausführung des Auftrags notwendigen Unterlagen und weiteren Informationen rechtzeitig übermittelt werden und ihm von allen Vorgängen und Umständen Kenntnis gegeben wird, die für die Ausführung des Auftrags von Bedeutung sein können. Dies gilt auch für die Unterlagen und weiteren Informationen, Vorgänge und Umstände, die erst während der Tätigkeit des Wirtschaftsprüfers bekannt werden. Der Auftraggeber wird dem Wirtschaftsprüfer geeignete Auskunftspersonen benennen.

(2) Auf Verlangen des Wirtschaftsprüfers hat der Auftraggeber die Vollständigkeit der vorgelegten Unterlagen und der weiteren Informationen sowie der gegebenen Auskünfte und Erklärungen in einer vom Wirtschaftsprüfer formulierten schriftlichen Erklärung zu bestätigen.

4. Sicherung der Unabhängigkeit

(1) Der Auftraggeber hat alles zu unterlassen, was die Unabhängigkeit der Mitarbeiter des Wirtschaftsprüfers gefährdet. Dies gilt für die Dauer des Auftragsverhältnisses insbesondere für Angebote auf Anstellung oder Übernahme von Organfunktionen und für Angebote, Aufträge auf eigene Rechnung zu übernehmen.

(2) Sollte die Durchführung des Auftrags die Unabhängigkeit des Wirtschaftsprüfers, die der mit ihm verbundenen Unternehmen, seiner Netzwerkunternehmen oder solcher mit ihm assoziierten Unternehmen, auf die die Unabhängigkeitsvorschriften in gleicher Weise Anwendung finden wie auf den Wirtschaftsprüfer, in anderen Auftragsverhältnissen beeinträchtigen, ist der Wirtschaftsprüfer zur außerordentlichen Kündigung des Auftrags berechtigt.

5. Berichterstattung und mündliche Auskünfte

Soweit der Wirtschaftsprüfer Ergebnisse im Rahmen der Bearbeitung des Auftrags schriftlich darzustellen hat, ist alleine diese schriftliche Darstellung maßgebend. Entwürfe schriftlicher Darstellungen sind unverbindlich. Sofern nicht anders vereinbart, sind mündliche Erklärungen und Auskünfte des Wirtschaftsprüfers nur dann verbindlich, wenn sie schriftlich bestätigt werden. Erklärungen und Auskünfte des Wirtschaftsprüfers außerhalb des erteilten Auftrags sind stets unverbindlich.

6. Weitergabe einer beruflichen Äußerung des Wirtschaftsprüfers

(1) Die Weitergabe beruflicher Äußerungen des Wirtschaftsprüfers (Arbeitsergebnisse oder Auszüge von Arbeitsergebnissen – sei es im Entwurf oder in der Endfassung) oder die Information über das Tätigwerden des Wirtschaftsprüfers für den Auftraggeber an einen Dritten bedarf der schriftlichen Zustimmung des Wirtschaftsprüfers, es sei denn, der Auftraggeber ist zur Weitergabe oder Information aufgrund eines Gesetzes oder einer behördlichen Anordnung verpflichtet.

(2) Die Verwendung beruflicher Äußerungen des Wirtschaftsprüfers und die Information über das Tätigwerden des Wirtschaftsprüfers für den Auftraggeber zu Werbezwecken durch den Auftraggeber sind unzulässig.

7. Mängelbeseitigung

(1) Bei etwaigen Mängeln hat der Auftraggeber Anspruch auf Nacherfüllung durch den Wirtschaftsprüfer. Nur bei Fehlschlagen, Unterlassen bzw. unberechtigter Verweigerung, Unzumutbarkeit oder Unmöglichkeit der Nacherfüllung kann er die Vergütung mindern oder vom Vertrag zurücktreten; ist der Auftrag nicht von einem Verbraucher erteilt worden, so kann der Auftraggeber wegen eines Mangels nur dann vom Vertrag zurücktreten, wenn die erbrachte Leistung wegen Fehlschlagens, Unterlassung, Unzumutbarkeit oder Unmöglichkeit der Nacherfüllung für ihn ohne Interesse ist. Soweit darüber hinaus Schadensersatzansprüche bestehen, gilt Nr. 9.

(2) Der Anspruch auf Beseitigung von Mängeln muss vom Auftraggeber unverzüglich in Textform geltend gemacht werden. Ansprüche nach Abs. 1, die nicht auf einer vorsätzlichen Handlung beruhen, verjähren nach Ablauf eines Jahres ab dem gesetzlichen Verjährungsbeginn.

(3) Offenbare Unrichtigkeiten, wie z.B. Schreibfehler, Rechenfehler und formelle Mängel, die in einer beruflichen Äußerung (Bericht, Gutachten und dgl.) des Wirtschaftsprüfers enthalten sind, können jederzeit vom Wirtschaftsprüfer auch Dritten gegenüber berichtigt werden. Unrichtigkeiten, die geeignet sind, in der beruflichen Äußerung des Wirtschaftsprüfers enthaltene Ergebnisse infrage zu stellen, berechtigen diesen, die Äußerung auch Dritten gegenüber zurückzunehmen. In den vorgenannten Fällen ist der Auftraggeber vom Wirtschaftsprüfer tunlichst vorher zu hören.

8. Schweigepflicht gegenüber Dritten, Datenschutz

(1) Der Wirtschaftsprüfer ist nach Maßgabe der Gesetze (§ 323 Abs. 1 HGB, § 43 WPO, § 203 StGB) verpflichtet, über Tatsachen und Umstände, die ihm bei seiner Berufstätigkeit anvertraut oder bekannt werden, Stillschweigen zu bewahren, es sei denn, dass der Auftraggeber ihn von dieser Schweigepflicht entbindet.

(2) Der Wirtschaftsprüfer wird bei der Verarbeitung von personenbezogenen Daten die nationalen und europarechtlichen Regelungen zum Datenschutz beachten.

9. Haftung

(1) Für gesetzlich vorgeschriebene Leistungen des Wirtschaftsprüfers, insbesondere Prüfungen, gelten die jeweils anzuwendenden gesetzlichen Haftungsbeschränkungen, insbesondere die Haftungsbeschränkung des § 323 Abs. 2 HGB.

(2) Sofern weder eine gesetzliche Haftungsbeschränkung Anwendung findet noch eine einzelvertragliche Haftungsbeschränkung besteht, ist die Haftung des Wirtschaftsprüfers für Schadensersatzansprüche jeder Art, mit Ausnahme von Schäden aus der Verletzung von Leben, Körper und Gesundheit, sowie von Schäden, die eine Ersatzpflicht des Herstellers nach § 1 ProdHaftG begründen, bei einem fahrlässig verursachten einzelnen Schadensfall gemäß § 54a Abs. 1 Nr. 2 WPO auf 4 Mio. € beschränkt.

(3) Einreden und Einwendungen aus dem Vertragsverhältnis mit dem Auftraggeber stehen dem Wirtschaftsprüfer auch gegenüber Dritten zu.

(4) Leiten mehrere Anspruchsteller aus dem mit dem Wirtschaftsprüfer bestehenden Vertragsverhältnis Ansprüche aus einer fahrlässigen Pflichtverletzung des Wirtschaftsprüfers her, gilt der in Abs. 2 genannte Höchstbetrag für die betreffenden Ansprüche aller Anspruchsteller insgesamt.

(5) Ein einzelner Schadensfall im Sinne von Abs. 2 ist auch bezüglich eines aus mehreren Pflichtverletzungen stammenden einheitlichen Schadens gegeben. Der einzelne Schadensfall umfasst sämtliche Folgen einer Pflichtverletzung ohne Rücksicht darauf, ob Schäden in einem oder in mehreren aufeinanderfolgenden Jahren entstanden sind. Dabei gilt mehrfaches auf gleicher oder gleichartiger Fehlerquelle beruhendes Tun oder Unterlassen als einheitliche Pflichtverletzung, wenn die betreffenden Angelegenheiten miteinander in rechtlichem oder wirtschaftlichem Zusammenhang stehen. In diesem Fall kann der Wirtschaftsprüfer nur bis zur Höhe von 5 Mio. € in Anspruch genommen werden. Die Begrenzung auf das Fünffache der Mindestversicherungssumme gilt nicht bei gesetzlich vorgeschriebenen Pflichtprüfungen.

(6) Ein Schadensersatzanspruch erlischt, wenn nicht innerhalb von sechs Monaten nach der schriftlichen Ablehnung der Ersatzleistung Klage erhoben wird und der Auftraggeber auf diese Folge hingewiesen wurde. Dies gilt nicht für Schadensersatzansprüche, die auf vorsätzliches Verhalten zurückzuführen sind, sowie bei einer schuldhaften Verletzung von Leben, Körper oder Gesundheit sowie bei Schäden, die eine Ersatzpflicht des Herstellers nach § 1 ProdHaftG begründen. Das Recht, die Einrede der Verjährung geltend zu machen, bleibt unberührt.

10. Ergänzende Bestimmungen für Prüfungsaufträge

(1) Ändert der Auftraggeber nachträglich den durch den Wirtschaftsprüfer geprüften und mit einem Bestätigungsvermerk versehenen Abschluss oder Lagebericht, darf er diesen Bestätigungsvermerk nicht weiterverwenden.

Hat der Wirtschaftsprüfer einen Bestätigungsvermerk nicht erteilt, so ist ein Hinweis auf die durch den Wirtschaftsprüfer durchgeführte Prüfung im Lagebericht oder an anderer für die Öffentlichkeit bestimmter Stelle nur mit schriftlicher Einwilligung des Wirtschaftsprüfers und mit dem von ihm genehmigten Wortlaut zulässig.

(2) Widerruft der Wirtschaftsprüfer den Bestätigungsvermerk, so darf der Bestätigungsvermerk nicht weiterverwendet werden. Hat der Auftraggeber den Bestätigungsvermerk bereits verwendet, so hat er auf Verlangen des Wirtschaftsprüfers den Widerruf bekanntzugeben.

(3) Der Auftraggeber hat Anspruch auf fünf Berichtsausfertigungen. Weitere Ausfertigungen werden besonders in Rechnung gestellt.

11. Ergänzende Bestimmungen für Hilfeleistung in Steuersachen

(1) Der Wirtschaftsprüfer ist berechtigt, sowohl bei der Beratung in steuerlichen Einzelfragen als auch im Falle der Dauerberatung die vom Auftraggeber genannten Tatsachen, insbesondere Zahlenangaben, als richtig und vollständig zugrunde zu legen; dies gilt auch für Buchführungsaufträge. Er hat jedoch den Auftraggeber auf von ihm festgestellte Unrichtigkeiten hinzuweisen.

(2) Der Steuerberatungsauftrag umfasst nicht die zur Wahrung von Fristen erforderlichen Handlungen, es sei denn, dass der Wirtschaftsprüfer hierzu ausdrücklich den Auftrag übernommen hat. In diesem Fall hat der Auftraggeber dem Wirtschaftsprüfer alle für die Wahrung von Fristen wesentlichen Unterlagen, insbesondere Steuerbescheide, so rechtzeitig vorzulegen, dass dem Wirtschaftsprüfer eine angemessene Bearbeitungszeit zur Verfügung steht.

(3) Mangels einer anderweitigen schriftlichen Vereinbarung umfasst die laufende Steuerberatung folgende, in die Vertragsdauer fallenden Tätigkeiten:

a) Ausarbeitung der Jahressteuererklärungen für die Einkommensteuer, Körperschaftsteuer und Gewerbesteuer sowie der Vermögensteuererklärungen, und zwar auf Grund der vom Auftraggeber vorzulegenden Jahresabschlüsse und sonstiger für die Besteuerung erforderlicher Aufstellungen und Nachweise

b) Nachprüfung von Steuerbescheiden zu den unter a) genannten Steuern

c) Verhandlungen mit den Finanzbehörden im Zusammenhang mit den unter a) und b) genannten Erklärungen und Bescheiden

d) Mitwirkung bei Betriebsprüfungen und Auswertung der Ergebnisse von Betriebsprüfungen hinsichtlich der unter a) genannten Steuern

e) Mitwirkung in Einspruchs- und Beschwerdeverfahren hinsichtlich der unter a) genannten Steuern.

Der Wirtschaftsprüfer berücksichtigt bei den vorgenannten Aufgaben die wesentliche veröffentlichte Rechtsprechung und Verwaltungsauffassung.

(4) Erhält der Wirtschaftsprüfer für die laufende Steuerberatung ein Pauschalhonorar, so sind mangels anderweitiger schriftlicher Vereinbarungen die unter Abs. 3 Buchst. d) und e) genannten Tätigkeiten gesondert zu honorieren.

(5) Sofern der Wirtschaftsprüfer auch Steuerberater ist und die Steuerberatervergütungsverordnung für die Bemessung der Vergütung anzuwenden ist, kann eine höhere oder niedrigere als die gesetzliche Vergütung in Textform vereinbart werden.

(6) Die Bearbeitung besonderer Einzelfragen der Einkommensteuer, Körperschaftsteuer, Gewerbesteuer, Einheitsbewertung und Vermögensteuer sowie aller Fragen der Umsatzsteuer, Lohnsteuer, sonstigen Steuern und Abgaben erfolgt auf Grund eines besonderen Auftrags. Dies gilt auch für

a) die Bearbeitung einmalig anfallender Steuerangelegenheiten, z.B. auf dem Gebiet der Erbschaftsteuer, Kapitalverkehrsteuer, Grunderwerbsteuer,

b) die Mitwirkung und Vertretung in Verfahren vor den Gerichten der Finanz- und der Verwaltungsgerichtsbarkeit sowie in Steuerstrafsachen,

c) die beratende und gutachtliche Tätigkeit im Zusammenhang mit Umwandlungen, Kapitalerhöhung und -herabsetzung, Sanierung, Eintritt und Ausscheiden eines Gesellschafters, Betriebsveräußerung, Liquidation und dergleichen und

d) die Unterstützung bei der Erfüllung von Anzeige- und Dokumentationspflichten.

(7) Soweit auch die Ausarbeitung der Umsatzsteuerjahreserklärung als zusätzliche Tätigkeit übernommen wird, gehört dazu nicht die Überprüfung etwaiger besonderer buchmäßiger Voraussetzungen sowie die Frage, ob alle in Betracht kommenden umsatzsteuerrechtlichen Vergünstigungen wahrgenommen worden sind. Eine Gewähr für die vollständige Erfassung der Unterlagen zur Geltendmachung des Vorsteuerabzugs wird nicht übernommen.

12. Elektronische Kommunikation

Die Kommunikation zwischen dem Wirtschaftsprüfer und dem Auftraggeber kann auch per E-Mail erfolgen. Soweit der Auftraggeber eine Kommunikation per E-Mail nicht wünscht oder besondere Sicherheitsanforderungen stellt, wie etwa die Verschlüsselung von E-Mails, wird der Auftraggeber den Wirtschaftsprüfer entsprechend in Textform informieren.

13. Vergütung

(1) Der Wirtschaftsprüfer hat neben seiner Gebühren- oder Honorarforderung Anspruch auf Erstattung seiner Auslagen; die Umsatzsteuer wird zusätzlich berechnet. Er kann angemessene Vorschüsse auf Vergütung und Auslagenersatz verlangen und die Auslieferung seiner Leistung von der vollen Befriedigung seiner Ansprüche abhängig machen. Mehrere Auftraggeber haften als Gesamtschuldner.

(2) Ist der Auftraggeber kein Verbraucher, so ist eine Aufrechnung gegen Forderungen des Wirtschaftsprüfers auf Vergütung und Auslagenersatz nur mit unbestrittenen oder rechtskräftig festgestellten Forderungen zulässig.

14. Streitschlichtungen

Der Wirtschaftsprüfer ist nicht bereit, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle im Sinne des § 2 des Verbraucherstreitbeilegungsgesetzes teilzunehmen.

15. Anzuwendendes Recht

Für den Auftrag, seine Durchführung und die sich hieraus ergebenden Ansprüche gilt nur deutsches Recht.

Zusammenfassung der Ergebnisse der Produktbegutachtung (1. Teilgutachten)

über den

Identity Provider-Dienst

für die Version vom 21.05.2021
der Research Industrial Systems Engineering Forschungs-, Entwicklungs- und Groß-projektberatung GmbH (RISE)
Concorde Business Park F
2320 Schwechat
Österreich

von SRC Security Research & Consulting GmbH
Emil-Nolde-Str. 7, 53113 Bonn

Version:	1.0
Dateiname:	Zusammenfassung Gutachten RISE IDP-Dienst 2021-06-30_v1_0
Stand:	30.06.2021
Status:	Final
Gutachter:	Randolf-Heiko Skerka, SRC Security Research & Consulting GmbH
Zweit-/Produktgutachter:	Dr. Jens Putzka, SRC Security Research & Consulting GmbH

Inhalt

Dokumentenhistorie

Datum	Version	Änderung
28.06.2021	0.1	Initiale Version, Beschreibung des Dienstes
30.06.2021	1.0	Finale Version

Tabelle 1: Dokumentenhistorie

Verfahrensinformationen

Antragsteller	Research Industrial Systems Engineering Forschungs-, Entwicklungs- und Großprojektberatung GmbH (RISE) Concorde Business Park F 2320 Schwechat Österreich
Prüfobjekt	Identity Provider-Dienst
Titel des Gutachtens	Teil-Produktgutachten zum Identity Provider-Dienst der Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH
Version des Gutachtens	1.0
Stand des Gutachtens	07.06.2021
Nummer des Gutachtens	SRC-2021-04
Steckbrief	Produkttypsteckbrief - Identity Provider-Dienst gemäß gemProdT_IDP-Dienst_PTV_2.2.0.xlsx, Stand 21.04.2021
Sicherheitsgutachter	Randolf-Heiko Skerka randolf.skerka@src-gmbh.de Tel. +49 (0)228 2806 136
Produktgutachter	Dr. Jens Putzka jens.putzka@src-gmbh.de Tel. +49 (0)228 2806 162
Standort(e) der Entwicklung	Research Industrial Systems Engineering Forschungs-, Entwicklungs- und Großprojektberatung GmbH (RISE) Concorde Business Park F 2320 Schwechat Österreich
Beginn der Begutachtung	06.04.2021
Ende der Begutachtung	31.05.2021
Stand der Zusammenfassung	30.06.2021

Tabelle 2: Verfahrensinformationen

1 Zusammenfassung

Das nachfolgende Dokument fasst die wesentlichen Ergebnisse der Begutachtung des Prüfobjektes

- Identity Provider-Dienst

der Research Industrial Systems Engineering Forschungs-, Entwicklungs- und Großprojektberatung GmbH (RISE) zusammen. Die vollständigen Ergebnisse der Begutachtung sind im folgenden Gutachten niedergelegt:

Titel	Teil-Produktgutachten zum Identity Provider-Dienst der Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH
Version	1.0
Stand	07.06.2021
Nummer	SRC-2021-04
Prüfobjekt	Identity Provider-Dienst in der Version vom 21.05.2021

Tabelle 3: Gutachten

1.1 Aufgabenstellung

Die Research Industrial Systems Engineering Forschungs-, Entwicklungs- und Großprojektberatung GmbH (RISE) entwickelt und betreibt Systeme, die im Kontext der Telematikinfrastruktur (TI) der gematik eingesetzt werden.

Der IdP-Dienst ermöglicht Anwendungsfrontends über die Authentifizierung des Nutzers am IdP-Dienst Zugriff zu den von den Fachdiensten, wie dem E-Rezept, angebotenen Daten zu erhalten. Die wesentliche Aufgabe des IdP-Dienstes ist somit die Authentifizierung des Nutzers und das Ausstellen entsprechender Bestätigungen.

SRC wurde mit der Begutachtung des oben genannten Prüfobjektes beauftragt und hat hierzu einen durch die gematik zugelassenen Sicherheitsgutachter eingesetzt. Das Ziel der Begutachtung war es festzustellen, ob das Prüfobjekt

- Identity Provider-Dienst

der RISE die in der Exceldatei

gemProdT_IDP-Dienst_PTV_2.2.0.xlsx, Stand 21.04.2021

zum „Produkttypsteckbrief - Identity Provider-Dienst“ niedergelegten und mit der gematik abgestimmten Anforderungen erfüllt und damit den Vorgaben der gematik entspricht, um Teil der Telematikinfrastruktur zu werden.

Eine Prüfung außerhalb der oben genannten gematik-Anforderungen fand nicht statt.

> **Hinweis:** Der Prüfung lag die unveröffentlichte Version 2.2.0 vom 21.4.2021 des gemProdT_IDP-Dienst_PTV zugrunde und nicht die mittlerweile veröffentliche Version gemProdT_IDP-Dienst_PTV_2.2.0-0_V1.0.0 vom 14.6.2021.

Hinweis:
In Abstimmung mit der gematik wurde für die erste Version des Teil-Gutachtens eine Priorisierung der Anforderungen vorgenommen, die für das 1. Teilgutachten begutachtet werden mussten. Diese Teilmenge umfasst folgende 19 Anforderungen:
A_20313-01, A_20314, A_20318, A_20323, A_20327-02, A_20464, A_20465, A_20521-02, A_20695-01, A_20696, A_20948-01, A_20949, A_20951, A_21317, A_21318, A_21319, A_21321, GS-A_4357, GS-A_4359
Darüber hinaus konnten zusätzlich bereits die folgenden Anforderungen begutachtet werden:
A_17207, A_20315-01, A_20462, A_20463, A_20522, A_20692-01, A_20697, A_20731, A_20947, A_20950-01, GS-A_4389, GS-A_4390.
Somit umfasst das Teil-Gutachten insgesamt 31 von den im Produkttypsteckbrief definierten 63 Anforderungen.

Die Beurteilung erfolgte auf der Grundlage des für das Prüfobjekt relevanten Produkttypsteckbriefs sowie der in den Anforderungen referenzierten Spezifikationen und folgt, dem in der

Richtlinie zur Prüfung der Sicherheitseignung
Version: 2.1.0
Stand: 27.04.2020
Referenzierung: gemRL_PruefSichEig_DS

durch die gematik vorgegebenen, vorliegenden Handlungsleitfaden für Gutachten in der TI.

Die Begutachtung erstreckt sich auf den Zeitraum vom 06.04.2021 bis zum 31.05.2021

Aktivität	Zeitraum
Beginn der Prüfung (Erstlieferung zum Gutachten)	06.04.2021
Finalisierung Teil-Produktgutachten Version 1.0	07.06.2021
Auslieferung Teil-Produktgutachten Version 1.0	07.06.2021
Ende der Prüfung für Teil-Produktgutachten Version 1.0	31.05.2021

Tabelle 4: Zeitraum der Prüfung / Timeline

2 Zusammenfassung der Prüfergebnisse

2.1.1 Umsetzung der Anforderungen

Der Begutachtung zugrunde gelegte Produkttypsteckbrief führt in Kapitel 3.2.1 insgesamt 31 Anforderungen auf, deren Einhaltung im Rahmen einer Begutachtung zu prüfen ist. Eine Anforderung kann hierbei die folgenden Status umfassen (gem. Kapitel 5.5 der Richtlinie zur Prüfung der Sicherheitseignung):

Umgesetzt	Alle der Anforderung gegenübergestellten Maßnahmen sind vollständig, wirksam und angemessen umgesetzt. Die umgesetzten Maßnahmen mitigieren das Risiko in ausreichendem Maße.
Teilweise umgesetzt	Einige Teile der Anforderung gegenübergestellten Maßnahmen sind umgesetzt, andere noch nicht oder nur teilweise.
Nicht umgesetzt	Die der Anforderung gegenübergestellten Maßnahmen sind größtenteils noch nicht umgesetzt. Die umgesetzten Maßnahmen decken die Anforderung nicht ab.
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).

Tabelle 5: Definition der möglichen Umsetzungsstatus

Die insgesamt 31 Anforderungen verteilen sich beim Prüfobjekt wie folgt auf die vier möglichen Status:

Status	Anzahl Anforderungen
Umgesetzt	29
Teilweise umgesetzt	0
Nicht umgesetzt	0
Nicht relevant	2
Summe	**31**

Tabelle 6: Zusammenfassung des Umsetzungsstatus

Im Detail haben die 31 Anforderungen die folgenden Umsetzungsstatus:

AFO-ID	Zusammenfassung	Umsetzungsstatus
A_17207	A_17207 - Signaturen binärer Daten (ECC-Migration)	AFO umgesetzt
A_20313-01	A_20313-01 - Inhalte des Claims	AFO umgesetzt
A_20314	A_20314 - Maximale Gültigkeitsdauer des "AUTHORIZATION_CODE"	AFO umgesetzt
A_20315-01	A_20315-01 - "AUTHORIZATION_CODE" nach Gültigkeitsende nicht mehr verwenden	AFO umgesetzt
A_20318	A_20318 - Keine Token für widerrufene Entitäten	AFO umgesetzt
A_20323	A_20323 - TOKEN-Ausgabe Protokollierung in allen Fällen	AFO umgesetzt
A_20327-02	A_20327-02 - Signatur des "ID_TOKEN" und "ACCESS_TOKEN"	AFO umgesetzt
A_20462	A_20462 - Maximale Gültigkeitsdauer des "ID_TOKEN"	AFO umgesetzt
A_20463	A_20463 - Maximale Gültigkeitsdauer des "ACCESS_TOKEN"	AFO umgesetzt
A_20464	A_20464 - Token-Endpunkt (Datensparsamkeit)	AFO umgesetzt
A_20465	A_20465 - Zertifikatsprüfung gegen OCSP-Responder	AFO umgesetzt

AFO-ID	Zusammenfassung	Umsetzungsstatus
A_20521-02	A_20521-02 - Inhalt des CHALLENGE_TOKENS an das Authenticator-Modul	AFO umgesetzt
A_20522	A_20522 - Erstellen einer "SESSION_ID"	AFO umgesetzt
A_20692-01	A_20692-01 - Maximale Gültigkeitsdauer eines "SSO_TOKEN"	AFO umgesetzt
A_20695-01	A_20695-01 - Signieren des "SSO_TOKEN"	AFO umgesetzt
A_20696	A_20696 - Verschlüsselung des "SSO_TOKEN"	AFO umgesetzt
A_20697	A_20697 - Zusammenstellung des "AUTHORIZATION_CODE"	AFO umgesetzt
A_20731	A_20731 - Verwendung des Attributes "auth_time"	AFO umgesetzt
A_20947	A_20947 - Entschlüsselung des "SSO_TOKEN"	AFO umgesetzt
A_20948-01	A_20948-01 - Validierung des "SSO_TOKEN"	AFO umgesetzt
A_20949	A_20949 - Anforderung einer Authentisierung bei negativer Validierung des "SSO_TOKEN"	AFO umgesetzt
A_20950-01	A_20950-01 - Positive Validierung des "SSO_TOKEN"	AFO umgesetzt
A_20951	A_20951 - Validierung der Signatur und des Zertifikats der "CHALLENGE"	AFO umgesetzt
A_21317	A_21317 - Verschlüsselung des "AUTHORIZATION_CODE"	AFO umgesetzt
A_21318	A_21318 - Prüfung des „AUTHORIZATION_CODE“	AFO umgesetzt
A_21319	A_21319 - Prüfung des CODE_VERIFIER	AFO umgesetzt
A_21321	A_21321 - Verschlüsselung von "ACCESS_TOKEN" und „ID_TOKEN“	AFO umgesetzt
GS-A_4357	GS-A_4357 - X.509-Identitäten für die Erstellung und Prüfung digitaler nicht-qualifizierter elektronischer Signaturen	AFO umgesetzt
GS-A_4359	GS-A_4359 - X.509-Identitäten für die Durchführung einer TLS-Authentifizierung	AFO umgesetzt
GS-A_4389	GS-A_4389 - Symmetrischer Anteil der hybriden Verschlüsselung binärer Daten	AFO nicht relevant
GS-A_4390	GS-A_4390 - Asymmetrischer Anteil der hybriden Verschlüsselung binärer Daten	AFO nicht relevant

Tabelle 7: Übersicht Umsetzung der Anforderungen

2.1.2 Notwendige Folgemaßnahmen und Auflagen zur Erfüllung der Anforderungen, sofern der Umsetzungsstatus „Umgesetzt“ nicht erreicht worden ist

Im Ergebnis der Begutachtung wurden 0 Anforderungen nicht und 0 Anforderungen teilweise umgesetzt. Entsprechend der *Richtlinie zur Prüfung der Sicherheitseignung* müssen notwendige Folgemaßnahmen und Auflagen zur Erfüllung der Anforderungen definiert werden, sofern der Umsetzungsstatus „umgesetzt“ nicht erreicht worden ist.

Folgende Auflagen / Folgemaßnahmen wurden durch die Gutachter empfohlen:

- Es sind keine Folgemaßnahmen notwendig.

Hinweis:
Über die endgültig, durch die RISE für den Identity Provider-Dienst umzusetzenden Folgemaßnahmen entscheidet die gematik im Rahmen des Zulassungsprozesses, in den neben dem Produktgutachten weitere durch den Hersteller zu erbringende Nachweise eingehen. Die gematik legt die Begründung der Zulassungsentscheidung schriftlich im Zulassungsbescheid nieder.

Zusammenfassung der Ergebnisse der Produktbegutachtung

über den

E-Rezept-Fachdienst

für die Version vom 11.6.2021
der IBM Deutschland GmbH (IBM)
IBM Allee 1
71139 Ehningen
Deutschland

von SRC Security Research & Consulting GmbH
Emil-Nolde-Str. 7, 53113 Bonn

Version	1.1
Dateiname	Zusammenfassung Gutachten IBM eRezept 2021-06-30_v1_1
Stand	30.06.2021
Status	Final
Gutachter	Randolf-Heiko Skerka, SRC Security Research & Consulting GmbH
Zweit-/Produktgutachter	Ansgar Tessmer, SRC Security Research & Consulting GmbH

Inhalt

Dokumentenhistorie

Datum	Version	Änderung
30.06.2021	ENTWURF-0.1	Initiale Version, Beschreibung des Dienstes
30.06.2021	1.1	Finale Version

Tabelle 1: Dokumentenhistorie

Verfahrensinformationen

Antragsteller	IBM Deutschland GmbH (IBM) IBM Allee 1 71139 Ehningen
Prüfobjekt	E-Rezept-Fachdienst
Titel des Gutachtens	Produktgutachten über das Produkt E-Rezept-Fachdienst (eRp FD) der IBM Deutschland GmbH
Version des Gutachtens	1.1
Stand des Gutachtens	11.06.2021
Nummer des Gutachtens	SRC-2021-07
Steckbrief	Produkttypsteckbrief - E-Rezept-Fachdienst gemProdT_eRp_FD_PTV_1.2.0-0 -0, Stand 19.02.2021
Sicherheitsgutachter	Randolf-Heiko Skerka randolf.skerka@src-gmbh.de Tel. +49 (0)228 2806 136
Produktgutachter	Ansgar Tessmer ansgar.tessmer@src-gmbh.de Tel. +49 (0)228 2806 228
Standort(e) der Entwicklung	IBM Deutschland GmbH Beim Strohhause 17 20097 Hamburg IBM Romania STR. GARII NR. 21 CLUJ-NAPOCA, RO 400267, ro
Beginn der Begutachtung	18.01.2021
Ende der Begutachtung	11.06.2021
Stand der Zusammenfassung	30.06.2021

Tabelle 2: Verfahrensinformationen

1 Zusammenfassung

Das nachfolgende Dokument fasst die wesentlichen Ergebnisse der Begutachtung des Prüfobjektes

- E-Rezept-Fachdienst

der IBM Deutschland GmbH (IBM) zusammen. Die vollständigen Ergebnisse sind im folgenden Gutachten niedergelegt:

Titel	Produktgutachten über das Produkt E-Rezept-Fachdienst (eRp FD) der IBM Deutschland GmbH
Version	1.1
Stand	11.06.2021
Nummer	SRC-2021-07
Prüfobjekt	E-Rezept-Fachdienst in der Version vom 11.06.2021

Tabelle 3: Gutachten

1.1 Aufgabenstellung

Die IBM Deutschland GmbH (IBM) entwickelt Systeme für den E-Rezept-Fachdienste (eRp FD) der Telematikinfrastruktur der gematik. Die Fachanwendung E-Rezept ermöglicht eine Übermittlung von ärztlichen und zahnärztlichen Verordnungen für apothekenpflichtige Arzneimittel in elektronischer Form.
Der E-Rezept-Fachdienst verwaltet E-Rezepte in der Telematikinfrastruktur als ein zentraler Ressourcenserver auf Basis des FHIR-Standards mit einer RESTful API. Die Rezepte werden dabei über eine eindeutige Ressourcen-ID (Rezept-ID) adressiert. Zusätzlich protokolliert der E-Rezept-Fachdienst alle Zugriffe auf ein E-Rezept für den Versicherten und verwaltet die Statusübergänge eines E-Rezepts. Für einen Nachrichtenaustausch zwischen Apotheken und Versicherten über die Verfügbarkeit von Medikamenten, die Belieferung von E-Rezepten und der Vertretung beim Einlösen eines E-Rezepts ist zusätzlich eine Kommunikation über den E-Rezept-Fachdienst möglich.
Der E-Rezept-Fachdienst realisiert die Vertraulichkeit und Integrität der verarbeiteten Daten über das Konzept der vertrauenswürdigen Ausführungsumgebung (VAU), die eine durchgängige Verschlüsselung der E-Rezepte und der dazu gehörigen Daten aus einer Kombination kryptografischer Verfahren während des Transports, der vertrauenswürdigen Verarbeitung und in der verschlüsselten Persistierung der Daten sicherstellt.

SRC wurde mit der Begutachtung des oben genannten Prüfobjektes beauftragt und hat hierzu einen durch die gematik zugelassenen Sicherheitsgutachter eingesetzt. Das Ziel der Begutachtung war es festzustellen, ob das Prüfobjekt

- E-Rezept-Fachdienst

der IBM die in Kapitel 3.2.1 des zugehörigen Produkttypsteckbriefes

- Produkttypsteckbrief - E-Rezept-Fachdienst
  gemProdT_eRp_FD_PTV_1.2.0-0 -0, Stand 19.02.2021

sowie den Änderungseinträgen C_10485, C_10498, C_10516, C_10519, C_10523, C_10588, C_10608, C_10609, C_10610, C_10611, C_10658 und C_10687

niedergelegten und mit der gematik abgestimmten Anforderungen erfüllt und damit den Vorgaben der gematik entspricht, um Teil der Telematikinfrastruktur zu werden. In Abstimmung mit der gematik bildeten die in Tabelle 7 aufgeführten Anforderungen die Grundlage der Begutachtung.

Die Beurteilung erfolgte auf der Grundlage des für das Prüfobjekt relevanten Produkttypsteckbriefs sowie der in den Anforderungen referenzierten Spezifikationen und folgt, dem in der

Richtlinie zur Prüfung der Sicherheitseignung
Version: 2.1.0
Stand: 27.04.2020
Referenzierung: gemRL_PruefSichEig_DS

durch die gematik vorgegebenen, vorliegenden Handlungsleitfaden für Gutachten in der TI.

Die Begutachtung erstreckt sich auf den Zeitraum vom 18.01.2021 bis zum 11.06.2021

Aktivität	Zeitraum
Beginn der Prüfung (Erstlieferung zum Gutachten)	18.01.2021
Finalisierung Teil-Produktgutachten Version 1.1	11.06.2021
Auslieferung Teil-Produktgutachten Version 1.1	11.06.2021
Ende der Prüfung für Produktgutachten Version 1.1	11.06.2021

Tabelle 4: Zeitraum der Prüfung / Timeline

2 Zusammenfassung der Prüfergebnisse

2.1 Umsetzung der Anforderungen

Der der Begutachtung zugrundeliegende Produkttypsteckbrief führt in Kapitel 3.2.3 diejenigen Anforderungen auf, deren Einhaltung im Rahmen einer Begutachtung zu prüfen ist. Eine Anforderung kann hierbei die folgenden Status umfassen (gem. Kapitel 5.5 der Richtlinie zur Prüfung der Sicherheitseignung):

Umgesetzt	Alle der Anforderung gegenübergestellten Maßnahmen sind vollständig, wirksam und angemessen umgesetzt. Die umgesetzten Maßnahmen mitigieren das Risiko in ausreichendem Maße.
Teilweise umgesetzt	Einige Teile der Anforderung gegenübergestellten Maßnahmen sind umgesetzt, andere noch nicht oder nur teilweise.
Nicht umgesetzt	Die der Anforderung gegenübergestellten Maßnahmen sind größtenteils noch nicht umgesetzt. Die umgesetzten Maßnahmen decken die Anforderung nicht ab.
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).

Tabelle 5: Definition der möglichen Umsetzungsstatus

Die insgesamt 98 Anforderungen verteilen sich beim Prüfobjekt wie folgt auf die vier möglichen Status:

Status	Anzahl Anforderungen
Umgesetzt	92
Teilweise umgesetzt	0
Nicht umgesetzt	0
Nicht relevant	6
Summe	**98**

Tabelle 6: Zusammenfassung des Umsetzungsstatus

Im Detail haben die 98 Anforderungen die folgenden Umsetzungsstatus:

AFO-ID	Zusammenfassung	Umsetzungsstatus
A_17205	A_17205 - Signatur der TSL: Signieren und Prüfen (ECC-Migration)	AFO umgesetzt
A_17207	A_17207 - Signaturen binärer Daten (ECC-Migration)	AFO entbehrlich
A_17359	A_17359 - Signaturen binärer Daten (Dokumente) (ECC-Migration)	AFO entbehrlich
A_19018	A_19018 - E-Rezept-Fachdienst - Rollenprüfung Verordnender stellt Rezept ein	AFO umgesetzt
A_19021	A_19021 - E-Rezept-Fachdienst - Generierung AccessCode	AFO umgesetzt

AFO-ID	Zusammenfassung	Umsetzungsstatus
A_19022	A_19022 - E-Rezept-Fachdienst - Rollenprüfung Verordnender aktiviert Rezept	AFO umgesetzt
A_19026	A_19026 - E-Rezept-Fachdienst - Rollenprüfung Nutzer löscht Rezept	AFO umgesetzt
A_19027-01	A_19027-01 - E-Rezept-Fachdienst - Rezept löschen	AFO umgesetzt
A_19113-01	A_19113-01 - E-Rezept-Fachdienst - Rollenprüfung Versicherter oder Apotheker liest Rezept	AFO umgesetzt
A_19115	A_19115 - E-Rezept-Fachdienst - Filter Tasks auf KVNR des Versicherten	AFO umgesetzt
A_19116	A_19116 - E-Rezept-Fachdienst - Prüfung AccessCode bei KVNR-Missmatch	AFO umgesetzt
A_19127	A_19127 - E-Rezept-Fachdienst - Übernahme der KVNR des Patienten	AFO umgesetzt
A_19130	A_19130 - E-Rezept-Fachdienst - Authentifizierung erforderlich LEI-Endpunkt	AFO umgesetzt
A_19131	A_19131 - E-Rezept-Fachdienst - Authentifizierung ungültig	AFO umgesetzt
A_19132	A_19132 - E-Rezept-Fachdienst - Authentifizierung Signaturprüfung	AFO umgesetzt
A_19166	A_19166 - E-Rezept-Fachdienst - Rollenprüfung Abgebender ruft Rezept ab	AFO umgesetzt
A_19169	A_19169 - E-Rezept-Fachdienst - Generierung Secret, Statuswechsel in Abgabe und Rückgabewert	AFO umgesetzt
A_19170-01	A_19170-01 - E-Rezept-Fachdienst - Rollenprüfung Abgebender weist zurück	AFO umgesetzt
A_19230	A_19230 - E-Rezept-Fachdienst - Rollenprüfung Abgebender vollzieht Abgabe des Rezepts	AFO umgesetzt
A_19252	A_19252 - E-Rezept-Fachdienst - Löschfrist abgelaufener Rezepte	AFO umgesetzt
A_19253	A_19253 - E-Rezept-Fachdienst - Löschfrist veraltete Nachrichten	AFO umgesetzt
A_19255	A_19255 - E-Rezept-Fachdienst Löschen veralteter MedicationDispense	AFO umgesetzt
A_19256-01	A_19256-01 - E-Rezept-Fachdienst - Löschfrist veraltete Protokolleinträge	AFO umgesetzt
A_19260	A_19260 - E-Rezept-Fachdienst – Ausschluss unbekannter FdV-Versionsnummern von der Kommunikation	AFO umgesetzt
A_19262	A_19262 - E-Rezept-Fachdienst - Transportverschlüsselte Übertragung von Daten mit PVS	AFO umgesetzt
A_19263	A_19263 - E-Rezept-Fachdienst - Transportverschlüsselte Übertragung von Daten mit AVS	AFO umgesetzt
A_19264	A_19264 - E-Rezept-Fachdienst - Transportverschlüsselte Übertragung von Daten mit FdV	AFO umgesetzt
A_19265	A_19265 - E-Rezept-Fachdienst – vertrauliche Kommunikation	AFO umgesetzt
A_19266	A_19266 - E-Rezept-Fachdienst - Berücksichtigung OWASP-Top-10-Risiken	AFO umgesetzt
A_19267	A_19267 - E-Rezept-Fachdienst - Authentisierung gegenüber Clients	AFO umgesetzt
A_19283	A_19283 - E-Rezept-Fachdienst - Systemprotokoll ohne personenbezogene und ohne medizinische Daten	AFO umgesetzt

AFO-ID	Zusammenfassung	Umsetzungsstatus
A_19389	A_19389 - E-Rezept-Fachdienst - Authentifizierung erforderlich Vers-Endpunkt	AFO umgesetzt
A_19390	A_19390 - E-Rezept-Fachdienst - Authentifizierung Nutzerrolle	AFO umgesetzt
A_19395	A_19395 - E-Rezept-Fachdienst - Rollenprüfung Versicherter liest AuditEvent	AFO umgesetzt
A_19396	A_19396 - E-Rezept-Fachdienst - Filter AuditEvent auf KVNR des Versicherten	AFO umgesetzt
A_19400	A_19400 - E-Rezept-Fachdienst - unzulässige Operationen MedicationDispense	AFO umgesetzt
A_19401	A_19401 - E-Rezept-Fachdienst - unzulässige Operationen Communication	AFO umgesetzt
A_19402	A_19402 - E-Rezept-Fachdienst - unzulässige Operationen AuditEvent	AFO umgesetzt
A_19405	A_19405 - E-Rezept-Fachdienst - Rollenprüfung Versicherter liest MedicationDispense	AFO umgesetzt
A_19406	A_19406 - E-Rezept-Fachdienst - Filter MedicationDispense auf KVNR des Versicherten	AFO umgesetzt
A_19439	A_19439 - E-Rezept-Fachdienst - Authentifizierung Authentifizierungsstärke	AFO umgesetzt
A_19446	A_19446 - E-Rezept-Fachdienst - Rollenprüfung Versicherter oder Apotheker liest Rezept	AFO umgesetzt
A_19450	A_19450 - E-Rezept-Fachdienst - Nachricht einstellen Schadcodeprüfung	AFO umgesetzt
A_19520	A_19520 - E-Rezept-Fachdienst - Nachrichten für Empfänger filtern	AFO umgesetzt
A_19683	A_19683 - E-Rezept-Fachdienst – Umsetzung der fachlichen Operationen in einer Vertrauenswürdigen Ausführungsumgebung (VAU)	AFO umgesetzt
A_19684	A_19684 - E-Rezept-Fachdienst – Verarbeitungskontext der VAU	AFO umgesetzt
A_19688	A_19688 - E-Rezept-Fachdienst – Verschlüsselung von außerhalb des Verarbeitungskontextes der VAU gespeicherten Daten	AFO umgesetzt
A_19694	A_19694 - E-Rezept-Fachdienst – Geschützte Weitergabe von Daten an autorisierte Nutzer durch die VAU	AFO umgesetzt
A_19699	A_19699 - E-Rezept-Fachdienst – Ableitung der Persistenzschlüssel durch ein HSM	AFO umgesetzt
A_19700	A_19700 - E-Rezept-Fachdienst - Ableitung der Persistenzschlüssel aus Merkmal der E-Rezepte	AFO umgesetzt
A_19702	A_19702 - E-Rezept-Fachdienst – Isolation zwischen Datenverarbeitungsprozessen mehrerer Verarbeitungskontexte der VAU	AFO umgesetzt
A_19704	A_19704 - E-Rezept-Fachdienst – Isolation der VAU von Datenverarbeitungsprozessen des Anbieters	AFO umgesetzt
A_19706	A_19706 - vE-Rezept-Fachdienst – Ausschluss von Manipulationen an der Software der VAU	AFO umgesetzt
A_19707	A_19707 - E-Rezept-Fachdienst – Ausschluss von Manipulationen an der Hardware der VAU	AFO umgesetzt
A_19708	A_19708 - E-Rezept-Fachdienst – Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU	AFO umgesetzt
A_19709	A_19709 - E-Rezept-Fachdienst – Kein physischer Zugang des Anbieters zu Systemen der VAU	AFO umgesetzt

AFO-ID	Zusammenfassung	Umsetzungsstatus
A_19710	A_19710 - E-Rezept-Fachdienst – Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU	AFO umgesetzt
A_19711-01	A_19711-01 - E-Rezept-Fachdienst – Private Schlüssel von Dienstzertifikaten im HSM	AFO umgesetzt
A_19712	A_19712 - E-Rezept-Fachdienst – Einsatz zertifizierter HSM	AFO umgesetzt
A_19713	A_19713 - E-Rezept-Fachdienst – HSM-Kryptographie-schnittstelle verfügbar nur für Instanzen der VAU	AFO umgesetzt
A_19714	A_19714 - E-Rezept-Fachdienst – Sicherer Kanal vom Client zum Verarbeitungskontext der VAU	AFO umgesetzt
A_19715	A_19715 - E-Rezept-Fachdienst – Konsistenter System-zustand des Verarbeitungskontextes der VAU	AFO umgesetzt
A_19716	A_19716 - E-Rezept-Fachdienst – Datenschutzkonfor-mes Logging und Monitoring des Verarbeitungskontextes der VAU	AFO umgesetzt
A_19722	A_19722 - E-Rezept-Fachdienst – Automatisierter Abbau des sicheren Kanals	AFO umgesetzt
A_19813	A_19813 - E-Rezept-Fachdienst – Sicherung zum Trans-portnetz Internet durch Paketfilter	AFO umgesetzt
A_19814	A_19814 - E-Rezept-Fachdienst – Platzierung des Pa-ketfilters Internet	AFO umgesetzt
A_19815	A_19815 - E-Rezept-Fachdienst – Richtlinien für den Pa-ketfilter zum Internet	AFO umgesetzt
A_19824	A_19824 - E-Rezept-Fachdienst – Verhalten bei Vollaus-lastung	AFO umgesetzt
A_19992	A_19992 - E-Rezept-Fachdienst - Blocklisting zu häufig verwendeter ACCESS_TOKEN	AFO umgesetzt
A_19993	A_19993 - E-Rezept-Fachdienst - Prüfung eingehender ACCESS_TOKEN	AFO umgesetzt
A_20019	A_20019 - Blacklisting von IP-Adressen	AFO umgesetzt
A_20022	A_20022 - E-Rezept-Fachdienst - OCSP-Status für das OCSP-Stapling	AFO umgesetzt
A_20158-01	A_20158-01 - E-Rezept-Fachdienst - Prüfung Signatur-zertifikat IDP	AFO umgesetzt
A_20159	A_20159 - E-Rezept-Fachdienst - QES Prüfung Signatur-zertifikat des HBA	AFO umgesetzt
A_20160-01	A_20160-01 - E-Rezept-VAU, Schlüsselpaar und Zertifi-kat	AFO umgesetzt
A_20162	A_20162 - E-Rezept-FD, Webschnittstellen, VAU-Re-quests	AFO umgesetzt
A_20163	A_20163 - E-Rezept-VAU, Nutzeranfrage, Ent- und Ver-schlüsselung	AFO umgesetzt
A_20365-01	A_20365-01 - Die Signatur des "ACCESS_TOKEN" ist zu prüfen	AFO umgesetzt
A_20372	A_20372 - Prüfung der zeitlichen Gültigkeit des "AC-CESS_TOKEN"	AFO umgesetzt
A_20504	A_20504 - Reaktion bei ungültiger oder fehlender Signa-tur des "ACCESS_TOKEN"	AFO umgesetzt
A_20967	A_20967 - E-Rezept-VAU, Erstellung und Pflege der Schlüssel im Mehr-Augen-Prinzip	AFO umgesetzt
A_20974	A_20974 - E-Rezept-Fachdienst - Prüfungsintervall Sig-naturzertifikat E-Rezept-Fachdienst	AFO umgesetzt

AFO-ID	Zusammenfassung	Umsetzungsstatus
A_21215	A_21215 - E-Rezept-FD, Random-Operation	AFO umgesetzt
A_21217	A_21217 - E-Rezept-FD, Zertifikatslisten und OCSP-Response für Clients	AFO umgesetzt
A_21332	A_21332 - E-Rezept: TLS-Vorgaben	AFO umgesetzt
A_21520	A_21520 - Prüfung des "aud" Claim des ACCESS_TOKEN" mit der vom Fachdienst registrierten URI	AFO umgesetzt
A_21521	A_21521 - Fachdienst: Prüfung der Signatur des Discovery Document	AFO entbehrlich
GS-A_4062-01	GS-A_4062-01 - Sicherheitsanforderungen für Netzübergänge zu Fremdnetzen	AFO umgesetzt
GS-A_4357	GS-A_4357 - X.509-Identitäten für die Erstellung und Prüfung digitaler nicht-qualifizierter elektronischer Signaturen	AFO umgesetzt
GS-A_4359	GS-A_4359 - X.509-Identitäten für die Durchführung einer TLS-Authentifizierung	AFO umgesetzt
GS-A_4361	GS-A_4361 - X.509-Identitäten für die Erstellung und Prüfung digitaler Signaturen	AFO umgesetzt
GS-A_4367	GS-A_4367 - Zufallszahlengenerator	AFO umgesetzt
GS-A_4368	GS-A_4368 - Schlüsselerzeugung	AFO umgesetzt
GS-A_4389	GS-A_4389 - Symmetrischer Anteil der hybriden Verschlüsselung binärer Daten	AFO entbehrlich
GS-A_4390	GS-A_4390 - Asymmetrischer Anteil der hybriden Verschlüsselung binärer Daten	AFO entbehrlich
GS-A_4750-01	GS-A_4750-01 - TUC_PKI_030 „QES-Zertifikatsprüfung“	AFO umgesetzt
GS-A_5016	GS-A_5016 - Symmetrische Verschlüsselung binärer Daten	AFO entbehrlich
GS-A_5484	GS-A_5484 - TUC_PKI_036 „BNetzA-VL-Aktualisierung“	AFO umgesetzt

Tabelle 7: Übersicht Umsetzung der Anforderungen

2.2 Notwendige Folgemaßnahmen und Auflagen zur Erfüllung der Anforderungen, sofern der Umsetzungsstatus „Umgesetzt“ nicht erreicht worden ist

Im Ergebnis der Begutachtung wurden 0 Anforderungen nicht und 0 Anforderungen teilweise umgesetzt. Entsprechend der *Richtlinie zur Prüfung der Sicherheitseignung* müssen notwendige Folgemaßnahmen und Auflagen zur Erfüllung der Anforderungen definiert werden, sofern der Umsetzungsstatus „umgesetzt“ nicht erreicht worden ist.
Aus den Ergebnissen der Begutachtung ergeben sich – vorbehaltlich der abschließenden Einschätzung der gematik – die nachfolgenden Folgemaßnahmen, die aus Sicht des Gutachters zur Gewährleistung eines sicheren Betriebes erforderlich sind:

1. Penetrationstests

Sachverhalt:

Im Rahmen der Begutachtung wurden Penetrationstests durchgeführt. Da diese zu einem sehr frühen Zeitpunkt, noch während der Entwicklungs- und Testphase der Anwendung erfolgten, wurden hier mehrere Auffälligkeiten und Sicherheitslücken identifiziert und als Findings in einem Bericht vermerkt.

Der Hersteller hat jedes einzelne dieser Findings ausgewertet und einen Behandlungsplan mit Maßnahmen zur Behebung dieser Findings erstellt. Der Behandlungsplan wurde dem Gutachter zur Prüfung vorgelegt und die darin definierten Maßnahmen als geeignet bewertet, den identifizierten Risiken wirksam zu begegnen und die genannten Sicherheitslücken effektiv zu schließen. Im Rahmen der Nachbegutachtung konnte der Hersteller die Umsetzung der vorgestellten Maßnahmen durch die Einlieferung von Evidenzen wie angepasste Konfigurationsdateien, Skripte, Screenshots und begleitende Tests durch den Hersteller glaubhaft belegen.

Das Votum dieses Gutachtens berücksichtigt die Auswertung der Findings durch den Gutachter hinsichtlich ihrer Art und Kritikalität sowie die durch den Hersteller umgesetzten Maßnahmen, diesen Findings zu begegnen. Eine abschließende Überprüfung durch eine Wiederholung des Penetrationstestes im finalen System konnte aus zeitlichen Gründen nicht mehr erfolgen.

Auflage:

Es muss ein abschließender Penetrationstest durchgeführt und die Ergebnisse durch den Gutachter bewertet werden, der alle internen und externen Schnittstellen im finalen System auf Schwachstellen untersucht und die Wirksamkeit der umgesetzten Maßnahmen bestätigt.

Hinweis:
Über die endgültig, durch die IBM für den E-Rezept-Fachdienst umzusetzenden Folgemaßnahmen entscheidet die gematik im Rahmen des Zulassungsprozesses, in den neben dem Produktgutachten weitere durch den Hersteller zu erbringende Nachweise eingehen. Die gematik legt die Begründung der Zulassungsentscheidung schriftlich im Zulassungsbescheid nieder.