Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Technische Richtlinie TR-03161: Anforderungen an Anwendungen im Gesundheitswesen

Teil 1: Mobile Anwendungen

Version 3.0

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
1.0	15.04.2020	Kleinmanns (DI 24)	Erste Version
2.0	15.02.2022	Referat DI 24	Anpassungen für Erweiterung auf TR-Familie Überarbeitung Kapitel 3 Erstellung Prüfschritte (Kap. 4) Erstellung Risikoanalyse (Kap. 5) Erstellung Anhang A, B und C Formelle Überarbeitung
3.0	25.03.2024	Referat DI 24	Überarbeitung Kapitel 3 Überarbeitung Kapitel 4 Überarbeitung Anhang A, B und C Formelle Überarbeitung

Bundesamt für Sicherheit in der Informationstechnik Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: referat-di24@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

Tabellenverzeichnis

1 Einleitung

1.1 Gegenstand der Technischen Richtlinie

Anwendungen im Gesundheitswesen (E-Health) haben das allgemeine Ziel bei „der Behandlung und Betreuung von Patientinnen und Patienten“ zu unterstützen und „die Möglichkeiten [zu] nutzen, die moderne Informations- und Kommunikationstechnologien (IKT) bieten“ [BMG-EH]. Besonders hervorzuheben sind im Kontext dieser Technischen Richtlinie (TR) digitale Gesundheitsanwendungen und digitale Pflegeanwendungen:

Nach § 33a Sozialgesetzbuch Fünf (SGB V) haben gesetzlich Krankenversicherte unter bestimmten Voraussetzungen einen Anspruch auf Versorgung mit sogenannten digitalen Gesundheitsanwendungen. Sie sind dazu bestimmt, die „Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten oder die Erkennung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen zu unterstützen“ [SGBV33a].

Nach § 40a Sozialgesetzbuch Elf (SGB XI) haben Pflegebedürftige in der sozialen Pflegeversicherung unter bestimmten Voraussetzungen einen Anspruch auf Versorgung mit sogenannten digitalen Pflegeanwendungen. Sie beabsichtigen die „Beeinträchtigungen der Selbständigkeit oder der Fähigkeiten des Pflegebedürftigen zu mindern und einer Verschlimmerung der Pflegebedürftigkeit entgegenzuwirken“ [SGBXI40a].

Die TR richtet sich an Hersteller von Anwendungen im Gesundheitswesen für mobile Endgeräte. Zusätzlich kann sie als Richtlinie für mobile Anwendungen betrachtet werden, welche sensible Daten verarbeiten oder speichern.

1.2 Zielsetzung der Technischen Richtlinie

Die Digitalisierung aller Lebensbereiche, sei es im Beruf, in Heimumgebungen, im Individual- oder im öffentlichen Personenverkehr, schreitet stetig voran. Bereits im Jahr 2018 überschritt die Anzahl der Internetnutzer die Grenze von vier Milliarden Menschen. Zwei Drittel der zurzeit 7,6 Milliarden Menschen zählenden Weltbevölkerung nutzen ein Mobiltelefon. Mehr als drei Milliarden Menschen nutzen soziale Netzwerke und tun dies in neun von zehn Fällen über ihr Smartphone (vgl. [GDR18]). Diese Entwicklung setzt sich im Gesundheitswesen mit dem Trend zum „Self-Tracking“, aber auch mit der zunehmenden Forderung nach der effizienten Nutzung einmal erhobener medizinischer Daten, fort. Insbesondere im Gesundheitswesen ist es dabei komfortabel, dass orts- und zeitunabhängig auf die eigenen medizinischen Daten zugegriffen werden kann. Mobile Anwendungen speichern in diesem Fall sensible und persönliche Daten, von der Pulsfrequenz, über Aufzeichnungen des Schlafrhythmus bis hin zu Medikationsplänen sowie ärztlichen Verordnungen und Bescheinigungen. Sie verbinden den Nutzer mit entsprechenden Services und fungieren als Kommunikations-Knotenpunkte. Ein kompromittiertes Smartphone kann somit das gesamte digitale Leben des Nutzers ungewollt offenlegen und zu hohem finanziellen Schaden führen. Das Einhalten von geeigneten Sicherheitsstandards, gerade im Bereich der mobilen Anwendungen, kann dies wesentlich erschweren und möglicherweise sogar verhindern. Schon während der Entwicklungsphase sollten Hersteller sehr verantwortungsvoll planen, wie eine mobile Anwendung personenbezogene und andere sensible Daten verarbeitet, speichert und schützt.

Die IT-Sicherheit verfolgt im Wesentlichen drei Schutzziele: Vertraulichkeit, Integrität und Verfügbarkeit.

Gerade bei mobilen Anwendungen im Gesundheitswesen ist die Einhaltung dieser Anforderungen von besonderer Wichtigkeit. Im Besonderen im Gesundheitswesen ist die Vertraulichkeit von Gesundheitsdaten, die unwillentlich offenbart werden, für immer verloren. Der Patient könnte hierfür zwar Schadensersatz erhalten, die unwillentliche Offenbarung kann allerdings nicht ungeschehen gemacht werden.

Darüber hinaus können durch das ungewollte Bekanntwerden von Gesundheitsdaten, im sozialen, wie auch im beruflichen Umfeld, unerwünschte Folgen mit erheblichen Auswirkungen entstehen.

Sollte ein Angreifer in der Lage sein, sensible Daten des Anwenders einer Gesundheitsanwendung zu manipulieren und damit deren Integrität zu verletzen, könnte er wesentlichen Einfluss auf Therapieentscheidungen und letztlich die Gesundheit des Betroffenen haben. Neben der Manipulation von sensiblen Daten ist die Manipulation der gesamten Anwendung als Risiko für solche Anwendungen anzusehen, da so die Anzeige für den Nutzenden falsch dargestellt werden kann.

Diese Technische Richtlinie soll als Leitfaden dienen, um Entwickler von mobilen Anwendungen bei der Erstellung sicherer mobiler Applikationen im Gesundheitswesen zu unterstützen. Greift die Anwendung auf Funktionalitäten eines Hintergrundsystems zurück, ist für eine vollumfängliche sicherheitstechnische Begutachtung ebenfalls die Sicherheit des Hintergrundsystems unerlässlich (vgl. Kapitel. 2.3).

1.3 Übersicht der Technischen Richtlinie

1.3.1 Methodik

Anwendungen im Sinne dieser TR sind Applikationen auf mobilen Endgeräten. Dies schließt insbesondere digitale Gesundheitsanwendungen im Sinne des § 33a SGB V (siehe [SGBV33a]) und mobile digitale Pflegeanwendungen nach § 40a SGB XI (siehe [SGBXI40a]) mit ein. Der Betrieb kann autonom durch die Anwendung auf dem Endgerät oder in Kombination mit einem sicheren Hintergrundsystem umgesetzt werden. Wird im Folgenden der Begriff Hintergrundsystem verwendet, ist insbesondere auch der Einsatz von Cloud-Computing gemeint. Auf Grund des rasanten technischen Fortschritts und der Diversität mobiler Endgeräte sowie ihrer Plattformen, erhebt die Technische Richtlinie keinen Anspruch auf Vollständigkeit. Sie kann als Mindestanforderung für den sicheren Betrieb einer Anwendung betrachtet werden.

Die Technische Richtlinie formuliert eine Security Problem Definition (SPD), welche potentielle Bedrohungsszenarien aufweist. Aus der SPD werden Prüfaspekte für mobile Anwendungen und deren Plattformen bzw. Einsatzumgebungen abgeleitet, um vor diesen Bedrohungen zu schützen.

Die in dieser Technischen Richtlinie formulierten Bedrohungsszenarien und Prüfaspekte basieren auf Erfahrungen, die das BSI bei bisherigen Untersuchungen von mobilen Anwendungen im Gesundheitswesen gesammelt hat. Darüber hinaus orientiert sie sich an internationalen Standards, wie den „Smartphone Secure Development Guidelines“ [SSDG] und dem „Mobile AppSec Verification Standard“ [MASVS], mit seinem dazugehörigen „Mobile Security Testing Guide“ [MSTG].

Eine Grundanforderung an Anwendungen im Sinne der Technischen Richtlinie ist die Orientierung an Best-Practice-Empfehlungen und anderen allgemeinen Anforderungen an sichere, verteilte Anwendungen. Dazu zählen die Durchführung intensiver funktionaler Tests, Integrationstests sowie insbesondere Tests zum Verhalten der Anwendung bei erwarteten und unerwarteten (Nutzer-)Eingaben (Positiv-/Negativ-Tests). Die TR stellt darüber hinaus zusätzliche, spezifische Anforderungen.

1.3.2 Begriffe

Diese Technische Richtlinie verwendet folgende Begriffe:

Tabelle 1: Begriffe der Technischen Richtlinie

Begriff	Beschreibung
MUSS	Die Anwendung muss eine bestimmte Eigenschaft zwingend aufweisen.
DARF NICHT / DARF KEIN(E)	Die Anwendung darf eine bestimmte Eigenschaft unter keinen Umständen aufweisen.

Begriff	Beschreibung
SOLL	Die Anwendung muss eine bestimmte Eigenschaft aufweisen, außer es wird dargelegt, dass durch ein Nicht-Umsetzen kein Risiko für den sicheren Betrieb besteht, bzw. eine Umsetzung, aufgrund von technischen Einschränkungen, derzeit nicht möglich ist.
KANN	Die Anwendung kann eine bestimmte Eigenschaft aufweisen, wobei ein Umsetzen dieser Eigenschaft vom Lösungsanbieter anzuzeigen ist.
primärer Zweck	Der primäre Zweck einer Anwendung im Sinne der Technischen Richtlinie ist ein Zweck des bestimmungsgemäßen Gebrauchs sowie alle Zwecke, die unmittelbar auf die Verankerung der Anwendung im geltenden Rechtsrahmen abzielen. (Für digitale Gesundheitsanwendungen nach § 33a SGB V bilden die Zwecke nach § 4 Absatz 2 Satz 1 Nummer 1 bis 3 [DIGAV] zusammen mit den Verpflichtungen aus dem Medizinprodukterecht den primären Zweck.)
rechtmäßiger Zweck	Der rechtmäßige Zweck einer Anwendung im Sinne der Technischen Richtlinie ist ein Zweck, der durch geltendes Recht als Grundlage zur Verarbeitung personenbezogener Daten zulässig ist. (Für digitale Gesundheitsanwendungen nach § 33a SGB V sind diese Zwecke in der Rechtsverordnung nach § 4 Abs. 2 und Abs. 4 [DIGAV]definiert.)

2 Überblick der Sicherheitsanforderungen an Anwendungen im Gesundheitswesen

2.1 Anwendungskonzepte auf mobilen Endgeräten

Der Begriff „mobile Anwendung“ bezeichnet ein Programm, das auf einer mobilen Plattform ausgeführt wird. Grundsätzlich lassen sich solche Anwendungen in drei Kategorien unterteilen. Die erste Kategorie bilden die nativen Anwendungen (Kapitel 2.1.1), welche direkt auf die Plattform, auf der sie ausgeführt werden, zugeschnitten sind, ab. Dem gegenüber stehen die Web-Anwendungen (Kapitel 2.2). Ihre Implementierung ist völlig unabhängig von der Plattform und sie laufen innerhalb des Web-Browsers des Endgeräts. In die dritte Kategorie fallen die hybriden Ansätze (Kapitel 2.1.2). Sie spiegeln alle möglichen Kombinationen aus nativen Anwendungen und Web-Anwendungen wider.

Da Web-Anwendungen weit über den allgemeinen Einsatz auf mobilen Endgeräten hinausgehen, liegt der Fokus dieser Publikation auf nativen Anwendungen und dem nativen Teil von hybriden Ansätzen. Für zusätzliche Hinweise zur sicheren Entwicklung und zum sicheren Betrieb von Web-Anwendungen empfiehlt das BSI „TR-03161 Anforderungen an Anwendungen im Gesundheitswesen Teil 2: Web-Anwendungen“ [TR03161-2] zu Rate zu ziehen.

2.1.1 Native-Anwendungen

Eine native Anwendung ist passend auf eine Plattform und deren Betriebssystem zugeschnitten. Sie basiert auf den von der Plattform (beispielsweise Android oder iOS) bereitgestellten Programmierwerkzeugen (Software Development Kits - SDKs). Diese ermöglichen einen direkten Zugriff auf Gerätekomponenten, wie beispielsweise GPS, Kamera oder Mikrofon. Aufgrund ihrer Nähe zum Betriebssystem können sie eine sehr gute Performanz, eine hohe Zuverlässigkeit und eine intuitive Bedienbarkeit erreichen. Die Anwendungen werden beispielsweise über den plattformeigenen App-Store installiert und können oft auch offline betrieben werden.

Mit der Nähe zum Betriebssystem sind allerdings auch Nachteile verbunden. Änderungen am Betriebssystem, beispielsweise durch Updates, können dazu führen, dass Anpassungen an der Anwendung vorgenommen werden müssen. Sollte dies nicht erfolgen, kann es zu Beeinträchtigungen der Funktionsfähigkeit der Anwendung kommen. Darüber hinaus ist es nicht möglich sie auf anderen Betriebssystemen zu installieren. Soll die gleiche Anwendung auf mehreren Betriebssystemen publiziert werden, so muss jeweils eine eigene Codebasis[1] existieren. Dies ist häufig mit einem hohen Aufwand und somit auch hohen Kosten verbunden.

2.1.2 Hybride Ansätze

Hybride Anwendungen verbinden sowohl die Vor-, als auch die Nachteile von nativen Anwendungen sowie Web-Anwendungen und Web-Services. Mit Hilfe des SDKs wird eine Rahmen-Anwendung geschaffen, welche alle Vor- und Nachteile von nativen Anwendungen aufweist. Sie kann auf Gerätekomponenten zugreifen und über einen App-Store bezogen werden, jedoch nicht auf anderen Plattformen installiert werden, ohne Anpassungen am Quellcode vorzunehmen. Darüber hinaus beinhalten die Rahmen-Anwendungen einen eingebetteten Web-Browser, mit dessen Hilfe Web-Anwendungen in native Anwendungen eingebunden werden können. Dadurch ist es auch Web-Anwendungen möglich, auf die sonst nur den nativen Anwendungen vorbehaltenen Gerätekomponenten zuzugreifen. Darüber hinaus

[1] Es existieren auch plattformübergreifende Implementierungsansätze, welche die Entwicklung einer Anwendung für verschiedene Plattformen gleichzeitig unterstützen. Allerdings verschiebt sich dadurch die Abhängigkeit lediglich in diese sehr umfangreiche Middleware, die alle Zielplattformen abdecken muss.

kann es durch den Einsatz unterschiedlicher Benutzerschnittstellen zu einer negativen Beeinträchtigung der User-Experience kommen. Die Plattformabhängigkeit der Anwendung bezieht sich nun lediglich auf die Rahmen-Anwendung, womit der Aufwand für eine Migration auf andere Plattformen deutlich reduziert wird.

2.2 Web-Anwendungen

Web-Anwendungen sind Anwendungsprogramme, meist Webseiten, die in Kombination mit einem Hintergrundsystem (Kapitel 2.3) ohne Installation auf einem lokalen System betrieben werden können. Solche Webseiten sind oft so programmiert, dass sie wie eine native Anwendung für klassische Desktop-Systeme oder mobile Endgeräte aussehen und sich vergleichbar verhalten. Im Gegensatz zu nativen Anwendungen basieren sie nicht auf einem SDK der zugrundeliegenden Plattformen, sondern auf klassischen Programmierwerkzeugen der Web-Entwicklung. In den meisten Fällen kommen HTML5 und JavaScript zum Einsatz. Aus diesem Grund ist mit ihnen nur ein sehr eingeschränkter Zugriff auf Gerätekomponenten möglich. Ihr größter Vorteil besteht darin, dass sie unabhängig vom Betriebssystem sind. Da die Anwendungen innerhalb eines Web-Browsers laufen, können sie auf jeder Plattform gleichermaßen eingesetzt werden, ohne Anpassungen an der Codebasis vornehmen zu müssen.

Da der Fokus dieser Publikation auf mobilen Anwendungen liegt, beziehen sich die nachfolgenden Bedrohungsanalysen und die Prüfaspekte auf den Schutz nativer Anwendungen für mobile Endgeräte und zusätzlich lediglich auf jene Eigenschaften von Web-Anwendungen, welche direkten Einfluss auf die Sicherheit der mobilen Anwendung haben. Für weiterführende Hinweise zum sicheren Betrieb und der sicheren Entwicklung von Web-Anwendungen wird auf „TR-03161 Anforderungen an Anwendungen im Gesundheitswesen Teil 2: Web-Anwendungen“ verwiesen [TR03161-2].

2.3 Hintergrundsysteme

Die meisten Anwendungen verlassen sich für die Verarbeitung und Speicherung von Daten nicht ausschließlich auf die von der Laufzeitumgebung bereitgestellten Ressourcen. Sie lagern diese Aufgaben auf ein Server-System aus. Weil diese Server aus Nutzersicht nicht sichtbar sind, werden sie auch Hintergrundsysteme oder Backend-Services genannt (als Abgrenzung zu der Anwendung, die der Nutzer sieht, welche Frontend genannt wird). Neben der fachspezifischen Verarbeitung und Speicherung von Daten übernehmen diese Systeme oft Aufgaben zur Authentifizierung und Autorisierung von Nutzern oder andere zentrale Tätigkeiten. Dies erlaubt es, dass nicht alle Funktionalitäten der Anwendungen auf den Endgeräten umgesetzt werden müssen. Oft beschränken sie sich lediglich auf eine grafische Nutzerführung. Eine generelle Aussage darüber, wie viel Funktionalität in der Anwendung selbst umgesetzt und wie viel auf einen Server ausgelagert wird, kann nicht getroffen werden. Die Ausprägungen können von Anwendung zu Anwendung variieren. Daher ist bei einer vollumfänglichen sicherheitstechnischen Betrachtung der gesamten Anwendung die Sicherheit des Hintergrundsystems ein essentieller Teil.

Für die Nutzung von Anwendungen, die an ein Hintergrundsystem angeschlossen sind, ist meistens eine aktive Internetverbindung zwingend erforderlich. Dabei wird für die Kommunikation zwischen Vorder- und Hintergrundsystemen meist eine über TLS gesicherte Transportverbindung eingesetzt. Der Einsatz von Hintergrundsystemen beschränkt sich nicht nur auf den Bereich der mobilen Anwendungen, sondern spiegelt den aktuellen Stand der Technik für fast alle Anwendungen wider. Hierbei werden im wesentlich drei Szenarien unterschieden:

- Der Hersteller der Anwendung verwaltet die Infrastruktur des Hintergrundsystems selbst (siehe Kapitel 2.3.1).
- Der Hersteller der Anwendung lässt die Infrastruktur von einem externen Dienstleister verwalten (siehe Kapitel 2.3.2).
- Das gesamte Hintergrundsystem der Anwendung wird bei einem Cloud-Dienstleister gehostet (siehe Kapitel 2.3.3).

Abhängig von der Art des Betriebs und den damit verbundenen unterschiedlichen Angriffsvektoren stehen dem Hersteller unterschiedliche Möglichkeiten zur Verfügung, die Sicherheit der Gesamtlösung und der gespeicherten und zu verarbeitenden Daten zu gewährleisten.

Da der Fokus dieser Publikation auf mobilen Anwendungen liegt, beziehen sich die nachfolgenden Bedrohungsanalysen und die Prüfaspekte auf den Schutz der mobilen Anwendung und zusätzlich lediglich auf jene Eigenschaften des Hintergrundsystems, welche direkten Einfluss auf die Sicherheit der Anwendung haben. Für weiterführende Hinweise zum sicheren Betrieb und der sicheren Entwicklung von Hintergrundsystemen wird auf „TR-03161 Anforderungen an Anwendungen im Gesundheitswesen Teil 3: Hintergrundsysteme“ verwiesen [TR03161-3].

2.3.1 Selbst gehostete Systeme

Bei selbst gehosteten Systemen agiert der Entwickler des Hintergrundsystems auch als Betreiber. Damit hat er den direkten Zugriff auf die Systeme und deren Umgebung. Die Server, auf denen das Hintergrundsystem betrieben wird, sind innerhalb der Betriebsumgebung des Herstellers untergebracht und die physische, technische und organisatorische Absicherung der Systeme erfolgt durch ihn alleine. Der größte Vorteil dieser Lösung besteht darin, dass der Hersteller die alleinige Hoheit über die Systeme hat und schnell und direkt auf jegliche Vorgänge reagieren kann. Da er die Systeme auch selber verwaltet und die Softwarekomponenten darauf selber auswählt bzw. entwickelt, hat er auch am meisten Wissen über die mögliche Verwundbarkeit der Systeme. Allerdings lastet in diesem Fall auch die alleinige Verantwortung auf dem Hersteller, sodass er z.B. dauerhaft Personal abstellen muss, um Sicherheitsvorfälle zu überwachen und angemessen darauf zu reagieren. Je nach geschäftlicher Ausrichtung des Herstellers, besitzt dieser möglicherweise zwar viel Wissen im fachlichen Bereich seiner jeweiligen Anwendung, aber weniger im Bereich der IT-Sicherheit.

2.3.2 Extern gehostete Systeme

Bei dieser Variante werden die Server in einem Datacenter eines externen Dienstleisters gehostet, der sich üblicherweise auf Hosting spezialisiert hat. Die sicherheitstechnischen Vorteile bei dieser Lösung bestehen darin, dass der Dienstleister in der Regel mehr Erfahrung mit dem Betrieb solcher Systeme hat, was einen positiven Einfluss vor allem auf die Verfügbarkeit hat. Je nach Ausgestaltung der Dienstleitung übernimmt der externe Hoster auch weitergehende Aufgaben, wie z.B. die Versorgung der Betriebssysteme mit Sicherheitsupdates, Datensicherung und Backups, sowie Überwachung und Monitoring, um rechtzeitig auf verdächtige Aktivitäten reagieren zu können.

Der Betreiber muss dem Hoster ein gewisses Maß an Vertrauen entgegenbringen. So kann er selber z.B. die Integrität der Hardware nicht überwachen, weil mit einem direkten physischen Zugang Software-Überwachungsmaßnahmen immer umgangen werden können. Außerdem besitzt der Hoster in der Regel viele Kunden, die alle auf technischer Ebene voneinander separiert werden müssen um unbeabsichtigten Informationsabfluss, etwa zu Konkurrenten oder an die Öffentlichkeit, zu verhindern. Nicht zuletzt können durch die Aufteilung der Zuständigkeitsbereiche Reibungsverluste entstehen, die gerade bei kritischen Situationen wertvolle Zeit kosten können.

2.3.3 Cloud Computing

Cloud Computing beschreibt ein Modell, das bei Bedarf – meist über das Internet und geräteunabhängig – zeitnah und mit wenig Aufwand geteilte Computerressourcen als Dienstleistung, etwa in Form von Servern, Datenspeicher oder Anwendungen, bereitstellt und nach Nutzung abrechnet. Je nach Bedarf des Kunden können Ressourcen flexibel angepasst werden. Dadurch hat der Hersteller der Anwendung weniger Einfluss auf die Ausführungsumgebung als bei einem einfachen Hosting. Es ist beispielsweise nicht mehr möglich, zu erkennen, auf welchem Gerät eine bestimmte Operation ausgeführt wird. Der Betreiber muss sich hier voll und ganz auf den Anbieter der Cloud-Lösung verlassen können. Deswegen empfiehlt das BSI beim

Einsatz von Cloud Computing für Anwendungen im Sinne der TR auf Anbieter zurückzugreifen, welche die Anforderungen aus dem „Kriterienkatalog Cloud Computing“ des BSI ([KCC-C5]) erfüllen. Hierbei muss der Betreiber auf Basis des vorgelegten Testats prüfen, ob die Anforderungen der TR durch die genutzten Cloud-Dienste erfüllt werden. Alternativ zum C5-Testat sind auch Anbieter mit vergleichbaren Testaten oder Zertifikaten zulässig (vgl. [TR03161-3]).

2.4 Security Problem Definition

Die Security Problem Definition beschreibt Annahmen, Bedrohungen und organisatorische Sicherheitspolitiken, die für Anwendungen im Gesundheitswesen zur Erbringung der Sicherheitsleistung relevant sind.

2.4.1 Annahmen

A.Device Das Gerät, auf der die Anwendung genutzt wird, wird vom Nutzer selbst betrieben und vor Schwachstellen geschützt, etwa durch Aktualisieren des Betriebssystems nach Bereitstellung der jeweiligen Updates. Die Sicherheit des Gerätes wurde nicht durch Veränderungen durch den Nutzer beeinträchtigt. Geräte, welche durch den Hersteller nicht weiterhin mit Sicherheitsupdates versorgt werden, werden nicht verwendet.

A.Source Der Bezug der Anwendung und Ihrer Updates erfolgt ausschließlich über sichere Quellen, die der Hersteller zur Veröffentlich seiner Anwendung bestimmt hat (z.B. App-Stores, herstellereigene Website, öffentliche Stellen wie zuständigen Behörden und Krankenkassen). Die installierten Anwendungen werden regelmäßig auf Updates geprüft und aktualisiert.

A.Backend Das Hintergrundsystem befindet sich in einer geschützten Umgebung. Es ist durch organisatorische und technische Maßnahmen sichergestellt, dass Angreifer sich keinen physischen Zugriff auf die Infrastruktur des Hintergrundsystems verschaffen können. Das Hintergrundsystem erfüllt die Anforderungen der „TR-03161 Anforderungen an Anwendungen im Gesundheitswesen Teil 3: Hintergrundsysteme“ [TR03161-3].

A.OperatingSystem Es werden nur die vom Betriebssystem bereitgestellten Funktionen und Komponenten genutzt, die für den rechtmäßigen Zweck der Anwendung erforderlich sind. Die mittels der erteilten Berechtigungen des Betriebssystems genutzten Funktionen vergrößern die Angriffsoberfläche nicht und werden als sicher angenommen. Dies trifft insbesondere für die kryptographischen Funktionen und Protokolle zu. Das Betriebssystem teilt keine sensiblen Daten der Anwendung ohne vorherige Zustimmung des Nutzers mit Dritten.

2.4.2 Bedrohungen

T.SensitiveData Sensible Daten in der Technischen Richtlinie sind im Sinne des Anhang A zu verstehen. Ein Unbefugter erhält Zugriff auf solche sensiblen Daten in der Anwendung, etwa auf sensible Benachrichtigungen im Sperrbildschirm, unverschlüsselt gespeicherte Daten im Dateisystem oder Arbeitsspeicher. Dies umfasst auch, dass ein Angreifer auf verschlüsselte, sensible Daten, nach Analyse des Verschlüsselungsmechanismus, im Klartext zugreifen kann.

T.Auth Ein Angreifer erhält unter einer fremden Nutzerkennung oder der Verwendung fremder Rollen- oder Gruppenzugehörigkeit Zugriff auf sensible Daten anderer Nutzer.

T.Eavesdropping Einem Angreifer gelingt es, z.B. über eine unzureichend verschlüsselte/nicht-authentisierte Verbindung, über unzureichend authentisierte Interprozess-Kommunikation (IPC)-Aufrufe[2] den Nutzer zu belauschen. Beispielsweise kann ein Angreifer aufgrund mangelnder Prüfung von Zertifikatseigenschaften den Aufbau eine Transportverbindung ausnutzen, um an sensible Daten zu gelangen.

T.DevFunctions Ein Angreifer nutzt in der Anwendung versteckte oder verbliebene Entwickler- bzw. Debuggingfunktionen zur Unterwanderung von Sicherheitsmaßnahmen.

T.Expense Die Anwendung verursacht unvorhergesehene, zusätzliche Kosten für den Nutzer oder Betreiber.

T.Impersonation Ein Angreifer erhält durch fehlende oder fehlerhafte Zugriffskontrollen oder durch Erraten von Zugriffsparametern unberechtigten Zugriff auf sensible Daten oder kostenpflichtige Funktionen eines anderen Nutzers.

T.InfoDisclosure Ein Angreifer führt eine Analyse der Anwendung durch und findet Referenzen auf z.B. Entwicklerinstanzen, hartkodierte Testaccounts oder Daten zur Verwendung in Verschlüsselungsroutinen.

T.Integrity Ein Angreifer ist in der Lage, Daten innerhalb eines Speichers oder über den Transportweg unbemerkt zu manipulieren oder zu löschen.

T.MemoryStructures Ein Angreifer führt ein Reverse Engineering auf die Anwendung durch und ermittelt dadurch ungeschützte Datenstrukturen im Speicher, wodurch der Zugriff auf Schlüssel und sensible Daten möglich wird.

T.VisibleAsset Der Angreifer kann durch „Schulter-Surfen“[3] sensible Daten, die auf der Anwendung dargestellt werden mitlesen.

2.4.3 Organisatorische Sicherheitspolitiken

OSP.Authorization Der Hersteller entwickelt ein Autorisierungskonzept, welches sowohl den lesenden, als auch den schreibenden Zugriff auf sensible Daten steuert. Die Zugriffsberechtigungen müssen so gewählt werden, dass ausschließlich für die Erfüllung des primären bzw. rechtmäßigen Zwecks erforderliche Rechte erteilt werden. Das Autorisierungskonzept muss unabhängig von der Authentifizierung implementiert werden.

OSP.Biometry Wird Biometrie zur Authentisierung angewendet, ist die Eignung der Plattform sowie des hinterlegten Referenzwerts vor jeder Anwendungssitzung zu überprüfen.

OSP.CriticalUpdates Der Hersteller überprüft und überwacht die Anwendung sowie die genutzte Drittanbieter-Software [4] dauerhaft auf ausnutzbare Schwachstellen. Der Hersteller muss bei bekannt werden von Schwachstellen kurzfristig ein Update bereitstellen. Das Hintergrundsystem muss die Anwendung über das Update informieren und nach einer Übergangsfrist (Grace Period) die Benutzung der Anwendung in einer veralteten Version unterbinden.

OSP.DataSovereignty Die Anwendung stellt die Datenhoheit des Nutzers sicher. Die Anwendung weist den Nutzer auf bestehende Risiken durch die Konfiguration seines Endgeräts hin und

[2] IPC (vgl. englisch: *Interprocess Communication*) wird auf mobilen Geräten als Kommunikationskanal zwischen verschiedenen Anwendungen genutzt.

[3] Beim Schulter-Surfen blickt der Angreifer unbemerkt über die Schulter auf das Gerät um Informationen zu erhalten.

[4] Unter einer Drittanbieter-Software soll die Zusammenfassung von Funktionalitäten verstanden werden, die nicht in der Hoheit des Entwicklers der Anwendung entstanden sind und die auch nicht Teil der Funktionalität der verwendeten Betriebssystemplattform ist.

lässt ihn entscheiden, die Nutzung abzubrechen. Auf Anforderung des Nutzers löscht die Anwendung bereits erfasste Daten auf allen lokalen Speichermedien. Sofern eine Anbindung der App an ein Hintergrundsystem besteht, fragt die App ein Löschen der Daten beim Hintergrundsystem an.

OSP.Disclosure Der Hersteller bietet einen niederschwelligen Prozess zum Melden von Schwachstellen an. Das heißt, er stellt leicht auffindbare Kontaktinformationen zur Sicherheits-Abteilung bereit und bietet eine Möglichkeit, um Schwachstellen anonym zu melden.

OSP.LibsIn Von Drittanbieter-Software eingehende Daten sollen vor einer Verwendung in der Anwendung validiert werden (z. B. XML-Schemavalidierung, Prüfung auf ungültiges Encoding etc.). Ziel ist es, die Anwendung vor Angriffen durch bösartige Eingaben zu schützen.

OSP.LibsOut Die Anwendung soll sensible Daten nicht im Klartext an Drittanbieter-Software weitergeben. Zulässig ist die Nutzung entsprechender Drittanbieter-Software für die Sicherung eines Kommunikationskanals oder eines lokalen Speichercontainers.

OSP.Purpose Jegliche Datenerhebung, -verarbeitung, -speicherung, -weitergabe und –löschung darf nur mit einer Zweckbindung erfolgen. Der Hersteller veröffentlicht dafür den rechtmäßigen Zweck der Anwendung und darüber hinaus welche Daten wie verarbeitet werden und wo und wie lange sie gespeichert werden. Ausgehend vom rechtmäßigen Zweck ist das zulässige Kommunikationsverhalten sowie die verwendete interne und externe Sensorik auszuwählen.

Anwendungshinweis: Ortungsdaten wie WiFi-SSID, GPS u. ä. dürfen nur verarbeitet werden, wenn diese für die Funktion der Anwendung von essentiellem Nutzen sind. Die so erhobenen Daten dürfen ausschließlich zweckgebunden verarbeitet werden. Sie dürfen nicht direkt oder indirekt (etwa in Bildaufnahmen) im Gerät persistiert werden, sofern dies nicht unmittelbar durch den Verarbeitungszweck erforderlich ist.

OSP.RNG Zufallszahlen sind aus einem Zufallszahlengenerator zu beziehen, der eine hohe Entropie besitzt. Die Anwendung soll initial einmalig Entropie vom Nutzer in den Zufallszahlengenerator der Plattform einbringen. Anschließend bezieht die Anwendung Zufall vom Hintergrundsystem und bringt diese in den lokalen Zufallszahlengenerator ein.

OSP.SecurityLifeCycle Der Hersteller realisiert einen Entwicklungszyklus, dessen Teilschritte darauf ausgelegt sind, die Sicherheit der Anwendung zu stärken. Darunter fallen Maßnahmen, mit denen bösartige Aktivitäten erkannt werden und der Betreiber angemessene Gegenmaßnahmen einleiten kann.

OSP.SecurityLog Sofern eine Anbindung der App an ein Hintergrundsystem besteht, werden Logs zu Sicherheitsvorfällen an das Hintergrundsystem geschickt.

2.4.4 Restrisiken

Der Betrieb von Anwendungen im Gesundheitswesen hat besonders hohe Anforderungen, die mit bestehenden Endgeräten und Cloud-Lösungen nur unzureichend abzudecken sind. Daher weist die Technische Richtlinie auf bestehende Restrisiken hin.

Mobile Endgeräte sind besonders anfällig für Diebstahl. Auch bei der Nutzung der sicheren Quellen (s.o.) ist nicht ausgeschlossen, dass auf diesen Quellen Schadsoftware zum Download angeboten wird. Installierte Schadsoftware kann bestehende Schwachstellen ausnutzten.

Der Betrieb des Hintergrundsystems bei Public Cloud-Anbietern beinhaltet besondere Risiken für die sensiblen Daten der Nutzer. Während hohe Entropie, sichere Kommunikations- und

Verschlüsselungsverfahren Risiken abmildern, sind Daten in der Cloud während der Verarbeitung potenziell ungeschützt. Dies stellt höchste Anforderungen an den Betreiber der Cloud, sowie an andere Anwender, die eventuell gleichzeitig Ressourcen derselben physischen Maschine benutzen dürfen. Durch Überwinden von Trennungsmechanismen erhält ein Angreifer Zugriffsmöglichkeiten außerhalb seines Mandantenbereichs und kann unter Umständen sensible Daten eines anderen Mandanten (hier: der Anwendungen im Gesundheitswesen), während deren Verarbeitung, einsehen und manipulieren.

Der Schutz von Kommunikationsverbindungen zwischen der Plattform, der Anwendung und dem Hintergrundsystem erfolgt mittels des kryptographisch gesicherten TLS-Protokolls. Im vorliegenden Szenario geht die TR von einer einseitigen Authentisierung aus, wobei die Anwendung die Authentizität des Hintergrundsystems prüft. Die Anwendung fügt in den Prozess des TLS-Verbindungsaufbaus eigenen Zufall ein, um damit zu erschweren, dass ein Angreifer in die TLS-Verbindung eindringt. Zufallszahlen auf Smartphone-Plattformen erreichen im Allgemeinen jedoch nicht die notwendige Qualität, die für den Schutz sensibler Daten innerhalb einer Anwendung im Gesundheitswesen notwendig sind. Das Restrisiko während des Verbindungsaufbaus besteht darin, dass der Angreifer die Authentizität eigener Nachrichten vortäuschen kann. Dadurch könnte der Angreifer sensible Daten, welche von der Anwendung an das Hintergrundsystem übermittelt werden, einsehen und manipulieren.

Im Allgemeinen ist auf Grund der in Kapitel 2.1 und 2.3 beschriebenen Einschränkungen, bezogen auf den Umfang der Technischen Richtlinie, eine gesamtheitliche Aussage über die Sicherheit der Anwendung, selbst unter Berücksichtigung aller aufgeführten Prüfaspekte, nicht möglich. Um die Sicherheit der gesamten Anwendung zu erhöhen, ist es erforderlich weitere Literatur zu studieren. Dies gilt insbesondere für den Schutz vor Angriffen, welche direkt das eingesetzte Hintergrundsystem als Ziel haben und bei der Verbindung von digitalen Gesundheitsanwendungen mit IoT-Geräten.

3 Prüfaspekte für Anwendungen im Gesundheitswesen

3.1 Prüfaspekte

Die Prüfung nach der Technischen Richtlinie deckt die minimalen Sicherheitseigenschaften von Anwendungen auf mobilen Endgeräten ab. Die zu prüfende Sicherheitsfunktionalität lässt sich in folgende Prüfaspekte gliedern:

(1) Prüfung des Anwendungszwecks

(2) Prüfung der Architektur

(3) Prüfung des Quellcodes

(4) Prüfung der Drittanbieter-Software

(5) Prüfung der kryptographischen Umsetzung

(6) Prüfung der Authentisierung und Authentifizierung

(7) Prüfung der Datenspeicherung und des Datenschutzes

(8) Prüfung der kostenpflichtigen Ressourcen

(9) Prüfung der Netzwerkkommunikation

(10) Prüfung der plattformspezifischen Interaktionen

(11) Prüfung der Resilienz

Der Hersteller dokumentiert für jeden Prüfaspekt, sofern die zu schützende Funktionalität verwendet wird, wie dessen Anforderung durch die Implementierung sichergestellt wird.

3.1.1 Prüfaspekt (1): Anwendungszweck

O.Purp_1	Der Hersteller MUSS die rechtmäßigen Zwecke der Anwendung und die Verarbeitung 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.
O.Purp_2	Die Anwendung DARF KEINE Daten erheben und verarbeiten, die nicht dem rechtmäßigen Zweck der Anwendung dienen.
O.Purp_3	Die Anwendung MUSS vor jeglicher Erfassung oder Verarbeitung personenbezogener Daten eine aktive und eindeutige Einwilligungserklärung des Nutzers einholen.
O.Purp_4	Daten, deren Verarbeitung der Nutzer nicht ausdrücklich zugestimmt hat, DÜRFEN NICHT von der Anwendung oder dem Hintergrundsystem erfasst, erhalten oder genutzt werden.
O.Purp_5	Die Anwendung MUSS ermöglichen, dass der Nutzer eine bereits erteilte Einwilligung wieder entziehen kann. Der Nutzer MUSS vor der Einwilligung über die Möglichkeit des Widerrufs und die sich daraus ergebenden Veränderungen im Verhalten der Anwendung informiert werden.
O.Purp_6	Der Hersteller MUSS ein Verzeichnis führen, welches erkennen lässt, welche Nutzereinwilligungen vorliegen. Der nutzerspezifische Teil des Verzeichnisses MUSS für den Nutzer automatisiert einsehbar sein. Es SOLL eine Historie dieses Verzeichnisses angefordert werden können.

O.Purp_7 Setzt die Anwendung Drittanbieter-Software ein, MÜSSEN alle verwendeten Funktionen für die rechtmäßigen Zwecke der Anwendung erforderlich sein. Die Anwendung SOLL anderweitige Funktionen sicher deaktivieren. Wird nur eine einzige oder sehr wenige Funktionen der Drittanbieter-Software benötigt, MUSS abgewogen werden, ob die Einbindung der gesamten Drittanbieter-Software im Verhältnis zur Vergrößerung der Angriffsoberfläche durch die verwendete Drittanbieter-Software steht.

O.Purp_8 Sofern es nicht für den vorgesehenen primären oder rechtmäßigen Zweck einer Anwendung erforderlich ist, DÜRFEN sensible Daten NICHT mit Dritten geteilt werden. Dies betrifft auch die Ablage dieser Daten in Teilen des Dateisystems, auf die auch andere Anwendungen Zugriff haben. Die Anwendung MUSS den Nutzer über die Konsequenzen einer eventuellen Weitergabe von Anwendungsdaten, die dem primären oder rechtmäßigen Zweck dienen, vollumfänglich informieren und sein Einverständnis einholen (OPT-IN).

O.Purp_9 Die Anwendung DARF sensible Daten NICHT auf dem Bildschirm darstellen, außer dies ist für den primären Zweck der Anwendung erforderlich.

3.1.2 Prüfaspekt (2): Architektur

O.Arch_1 „Security“ MUSS ein fester Bestandteil des Softwareentwicklungs- und Lebenszyklus‘ für die gesamte Anwendung sein (vgl. „iOS Security Framework” [iOSSF], beziehungsweise „Design for Safety“ [DfS]).

O.Arch_2 Bereits in der Designphase der Anwendung MUSS berücksichtigt werden, dass die Anwendung in der Produktivphase sensible Daten verarbeiten wird. Die Architektur der Anwendung MUSS dafür die sichere Erhebung, Verarbeitung, Speicherung und Löschung der sensiblen Daten in einem Datenlebenszyklus gewährleisten.

O.Arch_3 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 [TR02102-2] und [NIST80057] basieren.

O.Arch_4 In Backups gespeicherte sensiblen Daten MÜSSEN gemäß dem aktuellen Stand der Technik verschlüsselt sein.

O.Arch_5 Sicherheitsfunktionen MÜSSEN immer auf allen Außenschnittstellen und API-Endpunkten implementiert werden.

O.Arch_6 Die Anwendung MUSS die Überprüfung der Integrität durch eine digitale Signatur ermöglichen. Die Authentizität der Anwendung ist durch die Vertrauenswürdigkeit der Bezugsquelle (s. A.Source) sichergestellt.

O.Arch_7 Nutzt die Anwendung Drittanbieter-Software (etwa für Objektserialisierung), MUSS der Hersteller sicherstellen[8], dass nur solche Drittanbieter-Software zum Einsatz kommen, deren zu nutzenden Funktionen sicher genutzt werden können und dem Nutzer Informationen über den Nutzungsumfang und die eingesetzten Sicherheitsmechanismen klar darstellen. Die Anwendung MUSS diese Funktionen sicher nutzen. Der Hersteller MUSS darüber hinaus sicherstellen[8], dass ungenutzte Funktionen durch Dritte nicht aktiviert werden können.

O.Arch_8 Interpretierter Code[5], der in möglichen Interaktionen mit Benutzereingaben steht (WebViews mit JavaScript), DARF KEINEN Zugriff auf verschlüsselte Speicher oder

[5] Nicht gemeint ist Code der plattformspezifischen Programmiersprachen.

Nutzerdaten haben, sofern es für die Erfüllung des primären Zwecks der Anwendung nicht zwingend erforderlich ist.

O.Arch_9 Der Hersteller MUSS dem Nutzer eine barrierearme Möglichkeit bereitstellen, um Sicherheitsprobleme zu melden. Die Kommunikation SOLL über einen verschlüsselten Kanal stattfinden.

O.Arch_10 Die Anwendung SOLL beim Start auf verfügbare sicherheitsrelevante Updates prüfen. Wenn ein sicherheitsrelevantes Update verfügbar ist, DARF die Anwendung sensible Daten NICHT mehr verarbeiten, ohne dieses Update einzuspielen. Der Nutzer MUSS über die Möglichkeit eines Updates und über ein durchgeführtes Update informiert werden.

O.Arch_11 Der Hersteller MUSS für die Veröffentlichung der Anwendung (und ihrer Updates) eine Quelle wählen, auf der die Anwendung gegen Manipulation durch Unbefugte geschützt ist und die einen vertrauenswürdigen Kanal zum Bezug der Anwendung zur Verfügung stellt.

O.Arch_12 Der Hersteller MUSS dem App-Nutzer einfach und sicher zugängliche Wege zum Bezug der Anwendung bereitstellen (z.B. in Form einer Link-Liste auf seiner Website, als individuell zugestellter QR-Code, o. Ä.).

3.1.3 Prüfaspekt (3): Quellcode

O.Source_1 Die Anwendung MUSS alle Eingaben vor deren Verarbeitung prüfen, um potenziell bösartige Werte vor der Verarbeitung herauszufiltern.

O.Source_2 Die Anwendung MUSS eingehende und ausgehende Daten maskieren beziehungsweise von potenziell schadhaften Zeichen bereinigen oder deren Verarbeitung ablehnen.

O.Source_3 Fehlermeldungen und Log-Dateien DÜRFEN KEINE sensiblen Daten (z. B. User Identifier) enthalten.

O.Source_4 Potenzielle Ausnahmen im Programmablauf (Exceptions) MÜSSEN abgefangen, kontrolliert behandelt und dokumentiert werden. Technische Fehlerbeschreibungen (z.B. Stack Traces) DÜRFEN dem Nutzer NICHT angezeigt werden.

O.Source_5 Bei Ausnahmen im Programmablauf (Exceptions) SOLL die Anwendung Zugriffe auf sensible Daten abbrechen und diese im Speicher sicher löschen.

O.Source_6 Bei Programmumgebungen mit manueller Speicherverwaltung (d.h., die Anwendung kann selbst exakt festlegen, wann und wo Speicher gelesen und beschrieben wird) MUSS die Anwendung für lesende und schreibende Zugriffe auf Speichersegmente auf sichere Funktionsalternativen (z. B. printf_s statt printf) zurückgreifen.

O.Source_7 Die Anwendung MUSS sicherstellen[8], dass alle sensiblen Daten unverzüglich nach der Erfüllung ihres Verarbeitungszwecks sicher gelöscht werden.

O.Source_8 Alle Optionen zur Unterstützung der Entwicklung (z. B. Entwickler-URLs, Testmethoden, Überreste von Debugmechanismen etc.) MÜSSEN in der Produktiv-Version vollständig entfernt sein.

O.Source_9 Für den Bau der Anwendung SOLLEN moderne Sicherheitsmechanismen, wie beispielsweise Obfuskation und Stack-Protection aktiviert werden.

O.Source_10 Für die Entwicklung der Anwendung SOLLEN Werkzeuge zur statischen Codeanalyse eingesetzt werden.

3.1.4 Prüfaspekt (4): Drittanbieter-Software

O.TrdP_1 Der Anbieter[6] MUSS eine zentrale und vollständige Liste von Abhängigkeiten durch Drittanbieter-Software führen.

O.TrdP_2 Drittanbieter-Software MUSS in der neusten oder der ihr vorhergehenden, für die Veröffentlichung vorgesehenen Version verwendet werden.

O.TrdP_3 Drittanbieter-Software MUSS durch den Hersteller regelmäßig (durch Auswertung öffentlich verfügbarer Informationen oder durch statische/dynamische Testmethoden) auf Schwachstellen überprüft werden. Überreste von Optionen zur Unterstützung der Entwicklung (vgl. O.Source_8) sind hierbei als Schwachstelle zu werten. Der Hersteller MUSS für alle öffentlich bekannten Schwachstellen analysieren, inwieweit die Schwachstelle die Sicherheit des Gesamtsystems beeinträchtigt. Software, bzw. Funktionen aus Drittanbieter-Software DARF bei bekannten Schwachstellen, die die Sicherheit des Gesamtsystems betreffen NICHT eingesetzt werden.

O.TrdP_4 Sicherheitsupdates für Drittanbieter-Software MUSS zeitnah integriert und per Update dem Nutzer zur Verfügung gestellt werden. Der Hersteller MUSS ein Sicherheitskonzept vorlegen, das anhand der Kritikalität ausnutzbarer Schwachstellen die geduldete Weiternutzung für die Anwendung, bzw. das Hintergrundsystem festlegt. Nachdem die Übergangsfrist (Grace Period) abgelaufen ist, MUSS die Anwendung den Betrieb verweigern.

O.TrdP_5 Vor der Verwendung von Drittanbieter-Software MUSS deren Quelle auf Vertrauenswürdigkeit geprüft werden.

O.TrdP_6 Die Anwendung SOLL sensible Daten nicht an Drittanbieter-Software weitergeben.

O.TrdP_7 Über Drittanbieter-Software eingehende Daten MÜSSEN validiert werden.

O.TrdP_8 Drittanbieter-Software, die nicht mehr gewartet wird, DARF NICHT verwendet werden.

3.1.5 Prüfaspekt (5): Kryptographische Umsetzung

O.Cryp_1 Beim Einsatz von Verschlüsselung in der Anwendung DÜRFEN KEINE fest einprogrammierten geheimen, bzw. privaten Schlüssel eingesetzt werden.

O.Cryp_2 Die Anwendung MUSS auf bewährte Implementierungen zur Umsetzung kryptographischer Primitive und Protokolle zurückgreifen (vgl. [TR02102-2]).

O.Cryp_3 Die Wahl kryptographischer Primitive MUSS passend zum Anwendungsfall sein und dem aktuellen Stand der Technik (siehe [TR02102-1]) entsprechen.

O.Cryp_4 Kryptographische Schlüssel DÜRFEN NICHT für mehr als genau einen Zweck eingesetzt werden.

O.Cryp_5 Die Stärke der kryptographischen Schlüssel MUSS dem aktuellen Stand der Technik entsprechen (siehe [TR02102-1]).

O.Cryp_6 Alle kryptographischen Schlüssel SOLLEN in einer vor Manipulation und Offenlegung geschützten Umgebung liegen.

O.Cryp_7 Alle kryptographischen Operationen SOLLEN in einer vor Manipulation und Offenlegung geschützten Umgebung stattfinden.

[6] Anbieter beschreibt die für die Inhalte des Produktes verantwortliche juristische Person.

3.1.5.1 Zufallszahlen

O.Rand_1 Alle Zufallswerte MÜSSEN über einen starken kryptographischen Zufallszahlengenerator erzeugt werden, welcher mit ausreichend Entropie geseedet wurde (vgl. [TR02102-1]).

3.1.6 Prüfaspekt (6): Authentisierung und Authentifizierung

O.Auth_1 Der Hersteller MUSS ein Konzept zur Authentisierung auf angemessenem Vertrauensniveau (vgl. [TR03107-1]), zur Autorisierung (Rollenkonzept) und zum Beenden einer Anwendungssitzung dokumentieren.

O.Auth_2 Die Anwendung SOLL Authentisierungsmechanismen und Autorisierungsfunktionen separat realisieren. Sind für die Anwendung verschiedene Rollen notwendig, MUSS eine Autorisierung bei jedem Datenzugriff separat realisiert werden.

O.Auth_3 Jeder Authentifizierungsvorgang des Nutzers MUSS in Form einer Zwei-Faktor-Authentisierung umgesetzt werden.

O.Auth_4 Zusätzlich zu der in O.Auth_1 definierten Authentisierung auf einem angemessenen Vertrauensniveau, KANN der Hersteller dem Nutzer gemäß § 139e Abs. 10 SGB V, nach umfassender Information und Einwilligung, eine Authentisierungsmöglichkeit auf einem niedrigeren Vertrauensniveau anbieten. Dies schließt das Anbieten zusätzlicher Verfahren basierend auf den digitalen Identitäten im Gesundheitswesen gemäß § 291 Abs. 8 SGB V mit ein.

O.Auth_5 Für die Bewertung eines Authentisierungsvorgangs SOLLEN zusätzliche Informationen (z. B. das verwendete Endgerät, der verwendete WiFi-Zugangsknoten oder die Zeit des Zugriffs) mit einbezogen werden.

O.Auth_6 Dem Nutzer SOLL eine Möglichkeit gegeben werden, sich über ungewöhnliche Anmeldevorgänge informieren zu lassen.

O.Auth_7 Die Anwendung MUSS Maßnahmen umsetzen, die ein Ausprobieren von Login-Parametern (z. B. Passwörter) erschweren.

O.Auth_8 Wurde die Anwendung unterbrochen (in den Hintergrundbetrieb versetzt), MUSS nach Ablauf einer angemessenen Frist (Grace Period) eine erneute Authentisierung durchgeführt werden.

O.Auth_9 Die Anwendung MUSS nach einer angemessenen Zeit in der sie nicht aktiv verwendet wurde (idle time) eine erneute Authentisierung fordern.

O.Auth_10 Die Anwendung MUSS nach einer angemessenen Zeit in der sie aktiv verwendet wurde (active time) eine erneute Authentisierung zur Reaktivierung der Serversitzung fordern.

O.Auth_11 Die Authentisierungsdaten DÜRFEN NICHT ohne eine erneute Authentifizierung des Nutzers geändert werden.

O.Auth_12 Die Anwendung MUSS für die Anbindung eines Hintergrundsystems eine dem Stand der Technik entsprechende Authentifizierung verwenden.

O.Auth_13 Authentisierungsdaten, wie bspw. Session-Identifier bzw. Authentisierungstoken, MÜSSEN als sensible Daten geschützt werden.

O.Auth_14 Die Anwendung MUSS es dem Nutzer ermöglichen einen oder alle zuvor ausgestellten Session-Identifier bzw. Authentisierungstoken zu invalidieren.

O.Auth_15 Wird eine Anwendungssitzung ordnungsgemäß beendet, MUSS die Anwendung das Hintergrundsystem darüber informieren, sodass Session-Identifier bzw.

Authentisierungstoken sicher gelöscht werden. Dies gilt sowohl für das aktive Beenden durch den Benutzer (log-out), als auch für das automatische Beenden durch die Anwendung (vgl. O.Auth_9 und O.Auth_10).

3.1.6.1 Authentisierung über Passwort

O.Pass_1 Bei einer Authentisierung mittels Benutzername und Passwort MÜSSEN starke Passwortrichtlinien existieren. Diese SOLLEN sich am aktuellen Stand gängiger „Best-Practices“ orientieren.

O.Pass_2 Für die Einrichtung der Authentisierung mittels Benutzername und Passwort KANN die Stärke des verwendeten Passworts dem Nutzer angezeigt werden. Informationen über die Stärke des gewählten Passworts DÜRFEN NICHT gespeichert werden.

O.Pass_3 Der Nutzer MUSS die Möglichkeit haben, sein Passwort zu ändern.

O.Pass_4 Wird die Anwendung zusammen mit einem Hintergrundsystem genutzt, MUSS das Ändern und Zurücksetzen von Passwörtern protokolliert werden. Das Hintergrundsystem SOLL den Nutzer über das Ändern und Zurücksetzen von Passwörtern informieren, dabei MUSS ein separater Kanal genutzt werden.

O.Pass_5 Werden Passwörter gespeichert, MÜSSEN diese mit einer den aktuellen Sicherheitsstandards entsprechenden Hash-Funktion und unter Verwendung geeigneter Salts gehasht werden.

3.1.7 Prüfaspekt (7): Datensicherheit

O.Data_1 Die Werkseinstellung der Anwendung MUSS die maximale Sicherheit bieten.

O.Data_2 Die Anwendung MUSS sensible Daten verschlüsselt speichern. Die betriebssystemeigene Verschlüsselung des Dateisystems genügt nicht. 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.

O.Data_3 Die Anwendung SOLL sensible Daten in einem vor Einsicht und Manipulation besonders geschützten Bereich ablegen.

O.Data_4 Die Anwendung DARF Ressourcen, die einen Zugriff auf sensible Daten ermöglichen, gegenüber Dritten NICHT verfügbar machen.

O.Data_5 Alle erhobenen sensiblen Daten DÜRFEN NICHT über die Dauer ihrer jeweiligen Verarbeitung hinaus in der Anwendung gehalten werden.

O.Data_6 Die Anwendung MUSS die Grundsätze der Datensparsamkeit und Zweckbindung berücksichtigen.

O.Data_7 Sofern die Anwendung an ein Hintergrundsystem angebunden ist, SOLL die Speicherung und Verarbeitung von sensiblen Daten im Hintergrundsystem erfolgen.

O.Data_8 Bei der Verwendung von Aufnahmegeräten (z. B. Kamera) MÜSSEN sämtliche Metadaten mit Datenschutz-Relevanz, wie etwa Rückschlüsse auf die GPS-Koordinaten des Aufnahmeorts, eingesetzte Hardware etc., entfernt werden.

O.Data_9 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.

O.Data_10	Bei der Eingabe sensibler Daten über die Tastatur SOLL die Anwendung unterbinden, dass Aufzeichnungen für Dritte erkennbar werden.
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 Anwendungen geschützt ist.
O.Data_12	Sensible Daten wie biometrische Daten oder private Schlüssel DÜRFEN NICHT aus der Komponente, auf der sie erzeugt wurden, exportiert werden.
O.Data_13	Die Anwendung MUSS Funktionen des Betriebssystems zur Unterbindung der Anzeige sensibler Daten und des Zugriffs für Dritte und der Speicherung des Bildschirms (z. B. Screenshots und Anzeigen für das App-Switching) nutzen.
O.Data_14	Die Anwendung MUSS sicherstellen[8], dass im gesperrten Zustand des Endgeräts alle sensiblen Daten verschlüsselt sind.
O.Data_15	Die Anwendung MUSS lokal gespeicherte Daten verschlüsselt mit einer sicheren Gerätebindung versehen.
O.Data_16	Es MUSS vom Hersteller sichergestellt werden, dass bei der Deinstallation der Anwendung alle sensiblen Daten und anwendungsspezifischen Anmeldeinformationen auf dem Endgerät nicht mehr zugreifbar sind.
O.Data_17	Die Anwendung MUSS dem Nutzer die Möglichkeit geben, dass alle sensiblen Daten und anwendungsspezifischen Anmeldeinformationen vollständig gelöscht bzw. unzugänglich gemacht werden.
O.Data_18	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 Anwendungsebene, ausgelöst durch das Hintergrundsystem. Der Hersteller MUSS die Auslösung des Kill-Switches durch den Anwender über das Hintergrundsystem durch starke Authentifizierungsmechanismen vor missbräuchlicher Nutzung schützen.

3.1.8 Prüfaspekt (8): Kostenpflichtige Ressourcen

O.Paid_1	Die Anwendung MUSS für den Nutzer kenntlich machen, welche kostenpflichtigen Leistungen (z.B. Zusatzfunktionalitäten oder Premiumzugriffe) und welche kostenpflichtigen Ressourcen (z.B. SMS, Telefonate, mobile Daten) von der Anwendung angeboten oder verwendet werden.
O.Paid_2	Die Anwendung MUSS vor der Verwendung kostenpflichtiger Leistungen das Einverständnis des Nutzers einholen.
O.Paid_3	Die Anwendung MUSS vor einer Zugriffsanforderung (z. B. Android-Berechtigungen) auf kostenpflichtige Ressourcen, das Einverständnis des Nutzers einholen.
O.Paid_4	Die Anwendung KANN für den Zugriff auf häufig verwendete, kostenpflichtige Ressourcen oder kostenpflichtige Leistungen ein dauerhaftes Einverständnis des Nutzers einholen.
O.Paid_5	Die Anwendung MUSS den Nutzer in die Lage versetzen zuvor erteilte Einverständnisse zurückzuziehen.
O.Paid_6	Die Anwendung SOLL die Transaktionshistorie von kostenpflichtigen Leistungen im Hintergrundsystem ablegen. Die Transaktionshistorie, einschließlich der Metadaten, MUSS als sensibles Datum gemäß O.Purp_8 behandelt werden.

O.Paid_7	Falls die Anwendung kostenpflichtige Leistungen anbietet, MUSS der Hersteller ein Konzept vorlegen, welches vorbeugt, dass Dritte die Zahlungsströme zur Nutzung von Anwendungsfunktionen zurückverfolgen können.
O.Paid_8	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.
O.Paid_9	Die Validierung von getätigten Bezahlvorgängen SOLL im Hintergrundsystem vorgenommen werden.
O.Paid_10	Zahlverfahren von Drittanbietern MÜSSEN die Anforderungen an Drittanbieter-Software erfüllen (vgl. Kapitel 3.1.4).

3.1.9 Prüfaspekt (9): Netzwerkkommunikation

O.Ntwk_1	Jegliche Netzwerkkommunikation der Anwendung MUSS durchgängig mit gegenseitiger Authentisierung verschlüsselt (zum Beispiel mittels mTLS) werden.
O.Ntwk_2	Die Konfiguration der verschlüsselten Verbindungen MUSS dem aktuellen Stand der Technik entsprechen (vgl. [TR02102-2]).
O.Ntwk_3	Die Anwendung MUSS sicherheitsüberprüfte Drittanbieter-Software verwenden, um sichere Kommunikationskanäle aufzubauen. Dies schließt die im Betriebssystem mitgelieferte Bibliothek mit ein.
O.Ntwk_4	Die Anwendung MUSS Zertifikats-Pinning anwenden.
O.Ntwk_5	Die Anwendung MUSS das Server-Zertifikat des Hintergrundsystems überprüfen.
O.Ntwk_6	Die Anwendung MUSS die Integrität und Authentizität der Antworten des Hintergrundsystems validieren.
O.Ntwk_7	Plattformspezifische Optionen, wie beispielsweise „Cleartext Traffic Opt-out“ und „In-App Transport Security“ MÜSSEN verwendet werden.
O.Ntwk_8	Die Anwendung MUSS für alle Verbindungen Log-Dateien vorhalten. Diese SOLLEN an das Hintergrundsystem übermittelt werden.

3.1.10 Prüfaspekt (10): Plattformspezifische Interaktionen

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.
O.Plat_2	Die Anwendung DARF Berechtigungen, die für die Erfüllung ihres primären Zwecks nicht notwendig sind, NICHT einfordern.
O.Plat_3	Die Anwendung MUSS den Nutzer auf den Zweck der anzufragenden Berechtigungen und auf die Auswirkungen hinweisen, die eintreten, falls der Nutzer diese nicht gewährt.
O.Plat_4	Die Anwendung DARF KEINE sensiblen Daten in Meldungen oder Benachrichtigungen, die nicht vom Benutzer explizit eingeschaltet wurden (siehe O.Plat_5), schreiben.
O.Plat_5	Die Anwendung KANN dem Nutzer die Optionen bieten, Meldungen und Benachrichtigungen, ggf. auch mit sensiblen Daten, anzuzeigen. Bei Werkseinstellung MUSS diese deaktiviert sein.
O.Plat_6	Die Anwendung MUSS Zugriffsbeschränkungen auf sensible Daten realisieren.

O.Plat_7	Die plattformspezifischen Mechanismen zu Interprozesskommunikation DÜRFEN NICHT zum Austausch von sensiblen Daten genutzt werden, sofern sie nicht zur Erfüllung des primären Zwecks der Anwendung erforderlich sind.
O.Plat_8	Verwendet die Anwendung für die Erfüllung ihres primären Zwecks eine Rendering Engine, MUSS sie diese so konfigurieren, dass aktive Inhalte nicht ausgeführt werden. Falls aktive Inhalte für die Realisierung der Anwendung unabdingbar sind, MUSS die Anwendung das Nachladen von Inhalten auf Quellen beschränken, die unter der Kontrolle des Herstellers sind oder durch den Hersteller autorisiert wurden.
O.Plat_9	Wechselt die Anwendung in den Hintergrundbetrieb, MUSS diese alle sensiblen Daten aus der aktuellen Ansicht („Views“ in iOS bzw. „Activities“ in Android) entfernen.
O.Plat_10	Die Anwendung MUSS alle nicht benötigten Protokoll-Handler in Rendering-Engines deaktivieren.
O.Plat_11	Die Anwendung MUSS vor dem ordnungsgemäßen Beenden das Löschen aller anwendungsspezifischen Sitzungsdaten (bspw. Cookies) bei der genutzten Rendering Engine anfordern.
O.Plat_12	Die Anwendung SOLL nach Beenden alle nutzerspezifischen Daten im Arbeitsspeicher sicher überschrieben haben.
O.Plat_13	Der Nutzer MUSS über Sicherheitsmaßnahmen informiert werden, sofern diese durch den Nutzer umsetzbar sind.
O.Plat_14	Ein abgebrochener Start[7] SOLL als Sicherheitsereignis protokolliert werden. Die Protokollierung SOLL im Hintergrundsystem stattfinden.

3.1.11 Prüfaspekt (11): Resilienz

O.Resi_1	Die Anwendung MUSS dem Nutzer barrierearme Best-Practice-Empfehlungen zum sicheren Umgang mit der Anwendung und ihrer Konfiguration bereitstellen.
O.Resi_2	Die Anwendung MUSS mittels Betriebssystem-Funktion abfragen, ob sich das Betriebssystem in einem Betriebszustand befindet, der den Anforderungen des Betriebssystemherstellers entspricht. Befindet sich das Betriebssystem in keinem vom Betriebssystemhersteller vorgesehenen Zustand, MUSS die Anwendung angemessen darauf reagieren. Die Anwendung MUSS dem Nutzer darstellen, welche Risiken für die Daten des Nutzers bei einer Fortsetzung der Anwendung bestehen (z. B., dass diese offengelegt werden könnten) oder die Fortsetzung unterbinden.
O.Resi_3	Die Anwendung MUSS eigene Prüfmechanismen implementieren, die beim Start der Anwendung feststellen, ob sie in einer Entwicklungs-/Debug-Umgebung ausgeführt wird. Wenn die Anwendung feststellt, dass sie in einer Entwicklungs-/Debug-Umgebung ausgeführt wird, MUSS sie sich sofort beenden.
O.Resi_4	Die Anwendung MUSS eigene Prüfmechanismen implementieren, die beim Start der Anwendung feststellen, ob sie unter ungewöhnlichen Benutzerrechten gestartet ist. Wenn die Anwendung feststellt, dass dies der Fall ist, MUSS sie sich sofort beenden.
O.Resi_5	Die Anwendung SOLL die Integrität des Endgeräts sicherstellen[8], bevor sensible Daten verarbeitet werden.

[7] Als abgebrochener Start ist jede Unterbrechung beim Öffnen der Anwendung zu verstehen. Dies schließt ebenfalls ein erneutes in den Vordergrund holen (aufwecken) der Anwendung mit ein.

[8] Sicherstellen meint das Abfragen einer Eigenschaft oder eines Zustands und anschließende Prüfen der Abfrage auf ein positives Ergebnis.

O.Resi_6	Die Anwendung MUSS vor dem Zugriff auf das Hintergrundsystem dessen Authentizität überprüfen (siehe auch O.Ntwk_4).
O.Resi_7	Die Anwendung SOLL Härtungsmaßnahmen, wie etwa eine Integritätsprüfung vor jeder Verarbeitung sensibler Daten innerhalb des Programmablaufs, realisieren.
O.Resi_8	Die Anwendung MUSS dem Stand der Technik entsprechende Maßnahmen gegen Reverse Engineering umsetzen.
O.Resi_9	Die Anwendung MUSS unterschiedliche Ausprägungen einer Plattform (bspw. Android) bei unterschiedlichen Herstellern berücksichtigen. Sie muss so gebaut sein, dass solche unterschiedlichen Plattformen bzw. unterschiedliche Plattformversionen zu keinem Fehlverhalten führt. Insbesondere MUSS ein missbräuchlicher Zugriff auf Ressourcen durch unterschiedliche Ausprägungen einer Plattform ausgeschlossen werden.
O.Resi_10	Die Anwendung MUSS robust gegenüber Störungen sein.

4 Prüfschritte einer Anwendung im Gesundheitswesen

4.1 Anforderungen an die Prüfung

Die TR-Prüfung von Anwendungen im Gesundheitswesen orientiert sich an den Prüfaspekten, die in Kapitel 3.1 aufgeführt sind. Kapitel 4.3 leitet aus den Prüfaspekten Testcharakteristika ab, welche die Anforderungen um eine Prüftiefe und Hinweise für TR-Prüfer erweitert. Unterstützend kann der Hersteller Aussagen tätigen, in denen er die betreffende Umsetzung skizziert und eine Referenz auf die jeweilige Implementierung angibt. Bei komplexen Testcharakteristika stellt der Hersteller eine umfassende Liste der Vorkommen zur Verfügung. Abhängig von der umgesetzten Prüftiefe unterstützen diese Herstelleraussagen die TR-Prüfung. Die untenstehende Tabelle legt dar, welche Prüfschritte mindestens für die jeweilige Prüftiefe gefordert sind.

Tabelle 2: Prüftiefen und Mindestanforderungen

Prüftiefe	Mindestanforderungen an die Prüfung
CHECK	Der Evaluator validiert (englisch „check“, analog zu Begriffsverwendung in der Common Criteria Evaluation Methodology) die vom Hersteller beschriebene Maßnahme im Hinblick auf ihre Wirksamkeit und räumt bestehende Zweifel (Plausibilitätsprüfung) aus, ob der Prüfaspekt und die damit verbundene Sicherheitsproblematik umfassend durch die beschriebenen Maßnahmen adressiert wird. Hierbei MUSS der Evaluator den aktuellen Stand der Technik für die jeweilige Plattform mitberücksichtigen. Die Validierung KANN weitergehende Schritte, wie z.B. eine Quelltextanalyse, umfassen, falls der Evaluator diese für eine umfassende Einschätzung benötigt.
EXAMINE	Der Evaluator untersucht (englisch „examine“, analog zu Begriffsverwendung in der Common Criteria Evaluation Methodology) die betreffende Testcharakteristik. Der Evaluator MUSS in seiner Prüfung über die Mindestanforderungen für „CHECK“ hinausgehen: In der Regel wird dies durch umfassende Quelltextanalyse der relevanten Implementierungsanteile und Penetrationstests geschehen. Die Unterstützung durch den Hersteller kann genutzt werden. „EXAMINE“ erfordert in jedem Fall eine eigenständige Beurteilung durch den Evaluator.

Aus den Prüftiefen folgt auch der Einsatz einer Quelltextanalyse bei der Begutachtung. Bei „CHECK“ wählt der TR-Prüfer aus, wie hoch die Abdeckung der Analyse für seine Einschätzung notwendig ist. Für „EXAMINE“ muss der TR-Prüfer erläutern, inwiefern sämtliche relevanten Codezeilen in Betracht gezogen wurden.

4.2 Protokollierung der Ergebnisse

Die Protokollierung der Testergebnisse ist so zu gestalten, dass unbeteiligte Dritte in die Lage versetzt werden, anhand der Angaben aus dem Prüfbericht die vorgenommen Prüfschritte zu wiederholen und dabei das gleiche Ergebnis zu erzielen. Hierzu ist es neben der Beschreibung der einzelnen Prüfschritte notwendig, dass die verwendeten Prüfwerkzeuge in den verwendeten Versionen in dem Prüfbericht ersichtlich sind. Die untenstehende Tabelle definiert die zulässigen Prüfergebnisse, welche sich aus der Prüfung einer Charakteristik ergeben können. Der TR-Prüfer begründet, wie er zu einem entsprechenden Ergebnis gekommen ist.

Tabelle 3: Mögliche Prüfergebnisse

Ergebnis	Notwendige Angaben
PASS	Der Prüfer erläutert sein Verständnis, warum die Hersteller-Implementierung das geforderte Sicherheitsziel erfüllt. Der Prüfbericht führt die durchgeführten Prüfschritte sowie das Prüfergebnis aus.
INCONCLUSIVE	Der Prüfbericht spezifiziert/referenziert die fehlenden oder inkonsistenten Informationen, damit der Hersteller die Nicht-Konformität zu dem betreffenden Aspekt des Sicherheitsziel bereinigen kann.
FAIL	Die geprüfte Anwendung verfehlt das betreffende Sicherheitsziel. Der Prüfer dokumentiert, inwiefern Angriffe durch Sicherheitsmaßnahmen in der Umgebung der Anwendung (z.B. operative Maßnahmen) verhindert werden können. Der Prüfer nimmt eine Evidenz der Verletzung der Prüfcharakteristik in die Protokollierung auf. Der Prüfer nimmt das durch die Verletzung der Testcharakteristik entstehende Risiko in die Risikoabschätzung mit auf.
NOT APPLICABLE (N/A)	Die geprüfte Anwendung verfügt über keinerlei Implementierung der durch den Prüfaspekt zu schützenden Funktionalitäten. Daher kann die betreffende Testcharakteristik nicht auf die zu prüfende Anwendung angewandt werden.

Die TR-Prüfer identifizieren bestehende Restrisiken beim Einsatz der Anwendung im Gesundheitswesen. Mit der Aufdeckung bestehender Restrisiken wird dem Umstand Rechnung getragen, dass der Verlust von Gesundheitsdaten sofort zu einem Schaden für den Nutzer führt und ausreichende Schutzmaßnahmen zum Zeitpunkt der TR-Prüfung nicht identifiziert werden konnten. Die Risikobewertung muss mindestens folgende Aspekte umfassen:

- Identifikation von Risiken aus der unterlassenen oder unzureichenden Umsetzung von „SOLL"-Anforderungen in Sicherheitszielen.
- Implementierungsspezifische Risiken.
- Risiken durch Integration in der geplanten Betriebsumgebung.
- Die Eignung des Monitorings sowie im Produkt vorgesehene Reaktionsmöglichkeiten für den Betreiber in der Produktprüfung berücksichtigen.

4.3 Testcharakteristika

Die Testcharakteristiken erweitern die Prüfaspekte aus Kapitel 3 um ihre Prüftiefe und ergänzende Informationen für Evaluatoren. Der Evaluator soll über die einzelnen Prüfschritte hinaus sicherstellen, dass das betreffende Sicherheitsziel insgesamt erfüllt wird. Dies umfasst möglicherweise weitere, hier nicht aufgeführte Testcharakteristika.

4.3.1 Testcharakteristik zu Prüfaspekt (1): Anwendungszweck

Tabelle 4: Testcharakteristik: Anwendungszweck

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Purp_1	Informationspflicht des Herstellers zum rechtmäßigen Zweck und Verarbeitung von personenbezogenen Daten.	CHECK	Der Evaluator prüft, ob eine Beschreibung vorhanden ist und diese den rechtmäßigen Zwecken der Anwendung entspricht. Dabei werden die vom Hersteller definierten rechtmäßige Zwecke als Grundlage genutzt. Eine juristische Prüfung der Rechtmäßigkeit ist nicht erforderlich.
O.Purp_2	Zweckgebundene Erhebung und Verarbeitung der Daten.	CHECK	Die Nutzung von Sensordaten ist nur soweit zulässig, wie sie etwa zur Erhebung des Seeds dient. Der Evaluator prüft anhand der Permisison-Policy, welche Daten in der Anwendung verarbeitet werden und ob diese den rechtmäßigen Zwecken der Anwendung entsprechen. Dabei werden die vom Hersteller definierten rechtmäßige Zwecke als Grundlage genutzt. Eine juristische Prüfung der Rechtmäßigkeit ist nicht erforderlich.
O.Purp_3	Einholung einer Einwilligungserklärung des Nutzers.	CHECK	Der Evaluator prüft, ob ohne Zustimmung des Nutzers personenbezogene Daten verarbeitet werden können.
O.Purp_4	Nutzung ausschließlich zugestimmter Daten.	CHECK	Der Evaluator gleicht die in O.Purp_2 gewonnen Erkenntnisse mit den erteilten Zustimmungen ab.
O.Purp_5	Entzug der Einwilligung ermöglichen.	CHECK	Der Evaluator prüft, ob dem Nutzer die Möglichkeit gegeben wird erteilte Einwilligungen wieder zu entziehen. Darüber hinaus validiert er, dass der Nutzer beim Entzug von Einwilligungen auf die daraus resultierenden Konsequenzen hingewiesen wird.
O.Purp_6	Führen eines Verzeichnisses der Nutzereinwilligungen.	CHECK	Der Evaluator prüft das Vorhandensein, die Aktualität und die Vollständigkeit des Verzeichnisses.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Purp_7	Nutzung nur erforderlicher Drittanbieter-Software.	CHECK	Der Evaluator prüft die Abwägungen des Herstellers bei Funktionen, die nicht dem rechtmäßigen Zweck für die Anwendung dienen. So dürfte beispielsweise eine API für soziale Netzwerke nur verwendet werden, wenn dies mit dem rechtmäßigen Zweck der Anwendung vereinbar ist. Die Risikobewertung erfasst die Auswirkungen auf den Schutz der Gesundheitsdaten, beispielsweise bei dem für Dritte erkennbaren Nutzungsverhalten in Logging Frameworks.
O.Purp_8	Weitergabe von sensiblen Daten nur für den primären oder rechtmäßigen Zweck.	CHECK	Der Evaluator prüft die Abwägungen des Herstellers, ob die Weitergabe von sensiblen Daten an Dritte dem primären oder rechtmäßigen Zweck für die Anwendung dient. Darüber hinaus prüft er, ob die Weitergabe immer explizit durch den Nutzer erlaubt werden muss (Opt-In). Die Weitergabe an Dienste, deren primärer Zweck die Verarbeitung von Daten für Werbezwecke ist, ist generell verboten. Die Risikobewertung berücksichtigt, wie die Weitergabe von Daten an Dritte im Verhältnis zum Schutzbedarf der weitergeleiteten Informationen (Daten) und der daraus resultierenden Gefahr der Preisgabe von Informationen steht.
O.Purp_9	Nur zweckgebundene Darstellung sensibler Daten auf dem Bildschirm.	CHECK	Der Evaluator prüft die Abwägungen des Herstellers, ob die Darstellung von sensiblen Daten zum gegebenen Zeitpunkt für die Erfüllung des Zwecks der Anwendung erforderlich ist. Für die Risikobewertung ist zu berücksichtigen, wie die Anwendung den Nutzer davor schützt, sensible Daten anzuzeigen (vergleiche T.VisibleAsset).

4.3.2 Testcharakteristik zu Prüfaspekt (2): Architektur

Tabelle 5: Testcharakteristik: Architektur

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Arch_1	„Security“ ist Bestandteil des Softwareentwicklungs- und Lebenszyklus.	CHECK	Der Evaluator prüft, ob der Quelltext und die Design-Dokumente auf die Verwendung aktueller „Best-Practices“ bei der Entwicklung schließen lassen.
O.Arch_2	Berücksichtigung der Verarbeitung sensibler Daten in der Design-Phase.	CHECK	Der Evaluator prüft Design- und Architektur-Dokumente auf die Berücksichtigung der Verarbeitung sensibler Daten inkl. des Datenlebenszyklus.
O.Arch_3	Dokumentation des Lebenszyklus von kryptographischem Material.	CHECK	Der Evaluator bewertet die ausgearbeitete Richtlinie des Herstellers und deren Berücksichtigung in der Risikobewertung.
O.Arch_4	Keine unverschlüsselten sensiblen Daten in Backups.	EXAMINE	Der Evaluator prüft durch Quelltextanalyse und praktische Tests, ob sensible Daten unverschlüsselt in Backups vorhanden sind.
O.Arch_5	Verteilte Implementierung von Sicherheitsfunktionen.	EXAMINE	Der Evaluator prüft das Vorhandensein und die Güte von Sicherheitsfunktionen durch Quelltextanalyse und praktische Tests. Als Sicherheitsfunktionen sind unter anderem Authentifizierung, Autorisierung, Input-Validierung und die Verwendung von Escape-Syntaxen zu verstehen.
O.Arch_6	Authentizitäts- und Integritätsschutz der Anwendung.	EXAMINE	Der Evaluator prüft das Vorhandensein und die Güte des eingesetzten Authentizitäts- und Integritätsschutzes durch Quelltextanalyse und praktische Tests. Hierbei ist auf die Aktualität (siehe [TR02102-1]) der eingesetzten Signaturverfahren zu achten. Die Wirksamkeit gegen eine Manipulation der Anwendung (siehe T.MemoryStructures) ist in der Risikobewertung zu betrachten.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Arch_7	Sichere Nutzung der Funktionen von Drittanbieter-Software.	EXAMINE	Der Evaluator prüft, durch Quelltextanalyse und praktische Tests, dass Funktionalitäten sicher verwendet werden und ungenutzte Funktionalitäten nicht zugänglich sind. Darüber hinaus prüft er, ob der Nutzer ausreichend über die Verwendung von Drittanbieter-Software informiert wird.
O.Arch_8	Zweckgebundener Zugriff auf verschlüsselte Speicher oder Nutzerdaten durch interpretierten Code.	EXAMINE	Der Evaluator prüft durch Quelltextanalyse und praktische Tests, ob ein Zugriff auf verschlüsselte Speicher oder Nutzerdaten über interpretierten Code möglich ist. Falls dies der Fall ist, prüft er die Abwägungen des Herstellers zur zwingenden Notwendigkeit für die Erfüllung des primären Zwecks und die Berücksichtigung in der Risikobewertung.
O.Arch_9	Barrierearme Möglichkeit zum Melden von Sicherheitsproblemen.	CHECK	Der Evaluator prüft, ob eine entsprechende Möglichkeit vorhanden ist. Falls kein verschlüsselter Kanal bereitgestellt wird, ist dies in der Risikobewertung zu berücksichtigen.
O.Arch_10	Anwendung fragt Zwangsupdates vom Hintergrundsystem ab.	EXAMINE	Der Evaluator prüft die Güte der Implementierung der entsprechenden Funktionalität in der Anwendung. Falls diese nicht vorhanden ist, prüft er die Abwägungen des Herstellers zu den Auswirkungen auf die Sicherheit der Anwendung. Dies ist in der Risikobewertung zu berücksichtigen. Falls die Funktionalität vorhanden ist, prüft der Evaluator mit praktischen Tests, ob das Blockieren einzelner Anfragen eine weitere Nutzung der Anwendung wirksam unterbindet.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Arch_11	Bereitstellung von Updates über einen eigenen App-Store.	CHECK	Der Evaluator prüft, ob der Hersteller einen eigenen App-Store zur Verfügung stellt. Daraus resultierende Abwägungen und Auswirkungen auf die Sicherheit sind in der Risikobewertung zu berücksichtigen.
O.Arch_12	Nutzung kryptographischer Maßnahmen bei alternativen Download-Quellen/Mechanismen.	CHECK	Der Evaluator prüft durch Quelltextanalyse das Vorhandensein und die Güte der eingesetzten Verfahren.

4.3.3 Testcharakteristik zu Prüfaspekt (3): Quellcode

Tabelle 6: Testcharakteristik: Quellcode

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Source_1	Prüfung von Eingaben vor Verarbeitung.	CHECK	Der Evaluator prüft, ob für alle Eingaben aus nicht vertrauenswürdigen Quellen Sicherheitsfunktionen gemäß O.Arch_5 vorhanden sind. Eingaben meinen jegliche Art von Daten, die in die Anwendung hineinfließen. Das sind zum Beispiel Nutzereingaben, Eingaben aus Drittanbieterkomponenten etc.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Source_2	Nutzung einer Escape-Syntax bei strukturierten Daten.	CHECK	Der Evaluator prüft, ob eine Escape-Syntax von strukturierten Daten für alle Eingaben gemäß O.Arch_5 vorhanden ist. Schadhafte Zeichen sind kontextabhängig zu betrachten. Im Datenbank-Kontext sind beispielsweise Hochkommata oder Prozentzeichen gegebenenfalls schadhaft, während im Web/HTML Kontext eher Tag-Klammern (<) schadhaft sind. Grundsätzlich muss die Input-Validierung daher kontextbezogen stattfinden. Wird eine potenziell schädliche Eingabe erkannt, muss sie entweder bereinigt/maskiert oder abgelehnt/verworfen werden. Das Verwerfen sollte dem Bereinigen vorgezogen werden. Sofern vorher maskierte oder bereinigte Eingaben weitergegeben werden, müssen diese so maskiert oder enkodiert werden, dass sie im Kontext der Weitergabe keine schädlichen Effekte haben.
O.Source_3	Keine sensiblen Daten in Meldungen.	CHECK	Der Evaluator prüft, ob sensible Daten über Fehlermeldungen oder Benachrichtigungen einsehbar werden.
O.Source_4	Kontrollierte Behandlung und Dokumentation von Ausnahmen (Exceptions).	EXAMINE	Der Evaluator prüft durch Quelltextanalyse und praktische Tests die kontrollierte Behandlung und Dokumentation von Exceptions.
O.Source_5	Abbruch des Zugriffs auf sensible Daten bei Exceptions.	EXAMINE	Der Evaluator prüft den Zugriff auf sensible Daten bei Ausnahmen im Programmablauf. Jeglicher identifizierte Zugriff muss in der Risikobewertung betrachtet werden.
O.Source_6	Nutzung von sicheren Funktionsalternativen beim Zugriff auf Speichersegmente.	EXAMINE	Der Evaluator prüft durch Quelltextanalyse, ob die Anwendung auf unsichere Funktionen zum Zugriff auf den Speicher zurückgreift. Die Prüfung umfasst sämtlichen vom Hersteller implementierten Quelltext. Externe Drittanbieter-Software wird in den O.TrdP Testcharakteristiken behandelt.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Source_7	Sicheres Löschen von sensiblen Daten nach ihrer Verarbeitung.	EXAMINE	Der Evaluator prüft durch Quelltextanalyse und praktische Tests, ob alle sensiblen Daten, welche nicht durch O.Data_2 geschützt sind, unverzüglich nach ihrer Verarbeitung sicher gelöscht werden. „Sicheres Löschen“ erfordert ein Überschreiben der Daten im Speicher. Hier ist auch auf eventuelle Kopien der Daten zu achten. Dies beinhaltet bei Programmiersprachen ohne manuelle Speicherverwaltung unter anderem das Ersetzen von Strings durch Byte-Arrays.
O.Source_8	Vollständige Entfernung von unterstützenden Entwicklungsoptionen und Debugmechanismen in der Produktiv-Version.	EXAMINE	Der Evaluator überprüft die produktive Anwendung auf Rückstände von Optionen zur Unterstützung der Entwicklung sowie Rückstände von Zeichenketten, Debugmechanismen und Debuginformationen.
O.Source_9	Aktivierung von modernen Sicherheitsmechanismen der Entwicklungsumgebung.	CHECK	Der Evaluator prüft, ob auf moderne Sicherheitsmechanismen der Entwicklungsumgebungen zurückgegriffen wurde. Sollten entsprechende Sicherheitsmechanismen nicht umgesetzt werden können, muss dies in der Risikobewertung betrachtet werden.
O.Source_10	Verwendung von Werkzeugen zur statischen Codeanalyse.	CHECK	Der Evaluator prüft durch Quelltextanalyse und Befragung des Herstellers, ob bei der Entwicklung Werkzeuge zur statischen Codeanalyse eingesetzt wurden. Wurden keine Werkzeuge zur statischen Codeanalyse verwendet, muss dies in der Risikobewertung betrachtet werden.

4.3.4 Testcharakteristik zu Prüfaspekt (4): Drittanbieter-Software

Tabelle 7: Testcharakteristik: Drittanbieter-Software

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.TrdP_1	Abhängigkeiten durch Drittanbieter-Software.	CHECK	Der Hersteller stellt eine Liste der eingesetzten Drittanbieter-Software inkl. der verwendeten Versionen bereit. Der Evaluator prüft die bereitgestellte Liste auf Vollständigkeit.
O.TrdP_2	Verwendung der aktuellen Version bei Drittanbieter-Software.	CHECK	Der Evaluator prüft die in O.TrdP_1 bereitgestellte Liste auf Aktualität der verwendeten Drittanbieter-Software-Versionen. Diese Abwägungen zu den gewählten Versionen werden in der Risikobewertung berücksichtigt.
O.TrdP_3	Herstellerprüfung Drittanbieter-Software auf Schwachstellen.	CHECK	Der Hersteller stellt eine Übersicht der letzten Schwachstellenanalyse der eingesetzten Drittanbieter-Softwarebereit. Diese wird vom Evaluator geprüft und in der Risikobewertung berücksichtigt. Zusätzlich prüft der Evaluator, ob der Hersteller bei Auftreten von Schwachstellen eine Mitigationsstrategie im Rahmen einer angemessenen Grace-Period bereitstellt.
O.TrdP_4	Sicherheitskonzept für zeitnahes Einspielen von Sicherheitsupdates für Drittanbieter-Software.	CHECK	Der Evaluator prüft das Vorhandensein eines solchen Konzeptes. Eine inhaltliche Prüfung ist im Rahmen der TR nicht erforderlich. Zusätzlich prüft der Evaluator, ob der Hersteller eine Mitigationsstrategie bereitstellt.
O.TrdP_5	Prüfung auf Vertrauenswürdigkeit der Quelle von Drittanbieter-Software.	CHECK	Der Evaluator prüft die Maßnahmen des Herstellers zur Verifikation der Vertrauenswürdigkeit von Drittanbietern.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.TrdP_6	Keine Weitergabe von sensiblen Daten an Drittanbieter-Software.	EXAMINE	Der Evaluator prüft durch eine Quelltextanalyse und praktische Tests, dass keine Weitergabe von sensiblen Daten an Drittanbieter-Software vorgenommen wird. Eine Ausnahme hierzu bietet die Weitergabe von Daten, die für den primären oder rechtmäßigen Zweck der Anwendung erforderlich ist (beispielsweise Drittanbieter-Software zur Transportverschlüsselung). Risiken, die aus einer Nichteinhaltung resultieren, sind in der Risikobewertung zu berücksichtigen.
O.TrdP_7	Validierung eingehender Daten über Drittanbieter-Software.	CHECK	Der Evaluator prüft, ob eingehende Daten über Drittanbieter-Software gemäß O.Source_1 behandelt werden und Sicherheitsfunktionen gemäß O.Arch_5 vorhanden sind.
O.TrdP_8	Prüfung der Wartung von verwendeter Drittanbieter-Software.	CHECK	Der Evaluator prüft, ob die verwendete Drittanbieter-Software vom Hersteller aktiv gepflegt wird. Eine Software gilt als nicht mehr gewartet, sofern sicherheitskritische Verwundbarkeiten bekannt sind, jedoch nicht innerhalb einer angemessenen Frist repariert worden sind.

4.3.5 Testcharakteristik zu Prüfaspekt (5): Kryptographische Umsetzung

Tabelle 8: Testcharakteristik: Kryptographische Umsetzung

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Cryp_1	Keine fest einprogrammierten Schlüssel oder anderweitige Geheimnisse.	EXAMINE	Der Evaluator prüft, ob fest einprogrammierte geheime, bzw. private Schlüssel eingesetzt werden. Ausgenommen sind Techniken, die den verwendeten Schlüssel stark vor Reverse Engineering nach aktuellem Stand der Technik verbergen (Stichwort: „White Box Cryptography“). Wird eine kaskadierte Verschlüsselung eingesetzt, soll mindestens eine Verschlüsselungsebene stark gegen Reverse Engineering geschützt sein und mindestens ein nicht-statischer Schlüssel eingesetzt werden.
O.Cryp_2	Nur bewährte Implementierungen bei kryptographischen Primitiven.	EXAMINE	Der Evaluator prüft die Liste der verwendeten Krypto-Implementierungen gegen den aktuellen Stand der Technik (vgl.[TR02102-2]).
O.Cryp_3	Passende Wahl der kryptographischen Primitive.	EXAMINE	Der Evaluator prüft die Abwägungen des Herstellers zur Wahl der kryptographischen Primitive und prüft, ob diese dem aktuellen Stand der Technik entsprechen (vgl. [TR02102-1]).
O.Cryp_4	Zweckbindung kryptographischer Schlüssel.	EXAMINE	Der Evaluator prüft die verwendeten kryptographischen Schlüssel auf ihre Zweckgebundenheit. Es wird der Zweck nach Schutz durch Verschlüsselung und Authentisierung unterschieden.
O.Cryp_5	Nutzung von starken kryptographischen Schlüsseln.	EXAMINE	Der Evaluator prüft die Stärke der verwendeten Schlüssel gegen den aktuellen Stand der Technik (vgl. [TR02102-1]).

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Cryp_6	Manipulationsschutz kryptographischer Schlüssel durch Umgebung.	EXAMINE	Der Evaluator prüft die Umgebung für die Ablage kryptographischer Schlüssel. Als sichere Umgebung gelten beispielsweise Secure Enclave, embedded Secure Element, Trusted Execution Environment etc. Hierbei ist der Betrieb auf allen zugelassenen Hardware-Plattformen zu berücksichtigen. Bei Nichteinhaltung prüft der Evaluator die Abwägungen des Herstellers zu den Auswirkungen auf die Sicherheit der Anwendungen bzw. diskutiert einen fehlenden Schutz in der Risikobewertung.
O.Cryp_7	Manipulationsschutz kryptographischer Operationen durch Umgebung.	EXAMINE	Der Evaluator prüft die Umgebung für die Durchführung kryptographischer Operationen analog zu O.Cryp_6. Der Betrieb auf allen zugelassenen Hardware-Plattformen ist dabei zu berücksichtigen.
O.Rand_1	Erzeugung von Zufallswerten durch sicheren Zufallszahlengenerator.	EXAMINE	Der Evaluator prüft durch Quelltextanalyse und praktische Tests die Güte des kryptographischen Zufallszahlengenerators. Informationen zu ausreichend sicheren Zufallszahlengeneratoren sind [TR02102-1] Kapitel 10 zu entnehmen. Für die Nachbearbeitung der Zufallszahlen sind die vom BSI als ausreichend sicher angesehen Algorithmen (s.[AIS20], [TR03107-1] und [TR03116-4]) zu verwenden.

4.3.6 Testcharakteristik zu Prüfaspekt (6): Authentisierung und Authentifizierung

Tabelle 9: Testcharakteristik: Authentisierung, Authentifizierung und Autorisierung

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Auth_1	Herstellerkonzept zur Authentisierung , Autorisierung und Beenden von Anwendungssitzungen.	CHECK	Der Evaluator prüft das vom Hersteller bereitgestellt Konzept zur Authentisierung, Autorisierung und Beenden der Anwendungssitzung. Er bewertet die Güte der eingesetzten Verfahren Anhand des aktuellen Standes der Technik. Nach Einschätzung des BSI existieren aktuell keine Verbraucherendgeräte, die in einem unüberwachten Anwendungsszenario Biometrie zur Identifikation oder Authentisierung auf einem Vertrauensniveau „hoch“ einsetzen können.
O.Auth_2	Getrennte Realisierung von Authentifizierungsmechanismen und Autorisierungsfunktionen.	EXAMINE	Der Evaluator prüft und bewertet die getroffenen Maßnahmen zur Trennung von Autorisierungs- und Authentifizierungsmechanismen. Sollte keine Trennung der Mechanismen vorgenommen sein, sind die Abwägungen des Herstellers zu prüfen und in der Risikobewertung zu berücksichtigen.
O.Auth_3	Zwei-Faktor-Authentisierung.	EXAMINE	Der Evaluator prüft durch Quelltextanalyse und praktische Tests das Vorhandensein und die Güte der Zwei-Faktor-Authentisierung. Insbesondere prüft er, ob die verwendeten Faktoren aus unterschiedlichen Kategorien stammen (Wissen und Besitz) und mit dem in O.Auth_1 beschriebenem Konzept übereinstimmen.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Auth_4	Authentisierung über zusätzliche Verfahren, welche einem niedrigeren Sicherheitsniveau entsprechen.	EXAMINE	Der Evaluator prüft das Vorhandensein von Authentisierungsmöglichkeiten mit einem niedrigeren Sicherheitsniveau. Sollten solche Verfahren angeboten werden, prüft der Evaluator durch Quelltextanalyse und praktische Tests, ob diese eine angemessene Sicherheit bieten. Angemessene Sicherheitsanforderungen für niederschwellige Verfahren sind der jeweils aktuellen Version der „Spezifikation Sektoraler Identity Provider“ der gematik GmbH zu entnehmen [gemSpec_IDP_Sek]. Die Abwägungen des Herstellers, zum Bereitstellen zusätzlicher Authentisierungsmöglichkeiten und der gewählten Implementierung, sind in der Risikobewertung zu berücksichtigen.
O.Auth_5	Zusätzliche Informationen bei Bewertung des Authentifizierungsvorgangs einbeziehen.	EXAMINE	Der Evaluator prüft das Vorhandensein und die Güte von zusätzlichen Informationen zur Bewertung eines Authentifizierungsvorgangs. Solche Informationen können beispielsweise über die Invalidierung/Löschung von Schlüsseln bei Änderung von Merkmalen biometrischer Systeme oder eine Prüfung auf Änderung von biometrischen Metadaten umgesetzt werden. Eine Prüfung auf Konformität zum Datenschutz der erhobenen Informationen ist im Rahmen der TR nicht erforderlich, eine zusätzliche Prüfung ist daher empfehlenswert. Werden keine zusätzlichen Informationen zur Bewertung verwendet, prüft der Evaluator die Abwägungen des Herstellers. Diese sind in der Risikobewertung zu berücksichtigen.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Auth_6	Information des Benutzers über ungewöhnliche Anmeldeversuche.	CHECK	Der Evaluator prüft, ob dem Nutzer leicht zugänglich die Möglichkeit gegeben wird, Informationen zu Anmeldevorgängen nachzuvollziehen. Ist das nicht der Fall, sind die Abwägungen des Herstellers zu prüfen und in der Risikobewertung zu berücksichtigen.
O.Auth_7	Verhinderung des Ausprobierens von Login-Parametern.	CHECK	Der Evaluator validiert, dass ein Ausprobieren von Login-Parametern verhindert wird. Dies kann beispielsweise durch Verzögerung nachfolgender Login-Versuche oder den Einsatz von sogenannten Captchas erreicht werden.
O.Auth_8	Erneute Authentifizierung bei unterbrochener Anwendung.	CHECK	Der Evaluator validiert, dass nach einer der Anwendung angemessenen Zeit, in der sie in den Hintergrundmodus versetzt wurde, eine erneute Authentifizierung erfolgen muss. Die Güte der geforderten Authentifizierung muss dem Vertrauensniveau angemessen sein (vgl. O.Auth_3).
O.Auth_9	Erneute Authentifizierung nach angemessenen Zeit in der die Anwendung nicht aktiv verwendet wurde.	CHECK	Der Evaluator validiert, dass nach einer der Anwendung angemessenen Zeit, in der sie nicht aktiv verwendet wurde, eine erneute Authentifizierung erfolgen muss. Die Güte der geforderten Authentifizierung muss dem Vertrauensniveau angemessen sein (vgl. O.Auth_3).
O.Auth_10	Erneute Authentifizierung nach angemessenen Zeit in der die Anwendung dauerhaft aktiv verwendet wurde.	CHECK	Der Evaluator validiert, dass nach einer der Anwendung angemessenen Zeit, in der sie dauerhaft aktiv verwendet wurde, eine erneute Authentifizierung erfolgen muss. Die Güte der geforderten Authentifizierung muss dem Vertrauensniveau angemessen sein (vgl. O.Auth_3).

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Auth_11	Ausreichende Authentifizierung des Nutzers für Änderung der Authentisierungsdaten.	EXAMINE	Der Evaluator prüft, ob er ohne angemessene Authentifizierung die Authentisierungsdaten verändern kann. Dies betrifft auch einen Ablauf zum Passwort zurücksetzen. Beruht dieser Ablauf bspw. auf Sicherheitsabfragen, darf die Antwort nicht einfach zu erraten oder gar aus möglicherweise öffentlichen Informationen ermittelbar sein (z.B. Mädchenname der Mutter).
O.Auth_12	Authentifizierung an der Schnittstelle zwischen Anwendung und Hintergrundsystem.	CHECK	Der Evaluator prüft, ob die Anwendung eine Authentifizierung des Hintergrundsystems unterstützt.
O.Auth_13	Schutz von Authentisierungsdaten.	CHECK	Der Evaluator prüft, ob Authentisierungsdaten als sensible Daten gemäß den Anforderungen der TR behandelt werden.
O.Auth_14	Invalidierung von Authentisierungsdaten durch den Anwender.	CHECK	Der Evaluator prüft, ob die Anwendung dem Nutzer ermöglicht, ein oder alle zuvor ausgestellten Authentisierungsdaten ungültig zu machen.
O.Auth_15	Benachrichtigung des Hintergrundsystems über beendete Anwendungssitzungen durch die Anwendung	CHECK	Der Evaluator prüft, ob das Hintergrundsystem bei einer ordnungsgemäßen Beendigung der Anwendungssitzung durch die Anwendung informiert wird.
O.Pass_1	Durchsetzung starker Passwortrichtlinien.	CHECK	Der Evaluator prüft, ob Passwortrichtlinien, welche dem aktuellen Stand der Technik entsprechen, eingesetzt werden. Andernfalls sind die Abwägungen des Herstellers zu prüfen und in der Risikobewertung zu berücksichtigen.
O.Pass_2	Anzeige der Stärke des verwendeten Passworts.	EXAMINE	Der Evaluator prüft, ob dem Nutzer die Stärke des verwendeten Passworts angezeigt wird. Ist dies der Fall, prüft er durch Quelltextanalyse und praktische Tests, ob dadurch Informationen über das Password oder dessen Güte im Anwendungsspeicher verbleiben.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Pass_3	Möglichkeit zur Änderung des Passwortes.	CHECK	Der Evaluator prüft, ob der Nutzer die Möglichkeit hat, sein Passwort zu ändern und verifiziert, dass diese Funktionalität nicht zweckentfremdet werden kann.
O.Pass_4	Protokollierung und Information über Änderungen und Zurücksetzen von Passwörtern.	CHECK	Der Evaluator prüft das Vorhandensein und die Güte von zusätzlichen Informationen zur Protokollierung von Änderungen und dem Zurücksetzen von Passwörtern.
O.Pass_5	Verwendung von kryptographisch sicheren Hashing-Algorithmen und Salts zur Speicherung der Passwörter.	EXAMINE	Der Evaluator prüft, ob Passwörter in der Anwendung gespeichert werden. Er verifiziert, dass die verwendeten Schutzmechanismen dem aktuellen Stand der Technik und den Anforderungen an Hash-Funktionen, Anzahl an Iterationen und Salts genügen (vgl. [TR02102-1]). In der Risikobewertung werden Maßnahmen, die Brute-Force-Angriffe verlangsamen, berücksichtigt.

4.3.7 Testcharakteristik zu Prüfaspekt (7): Datensicherheit

Tabelle 10: Testcharakteristik: Datenspeicherung und Datenschutz

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Data_1	Maximale Sicherheit bei Werkseinstellung.	CHECK	Der Evaluator prüft die Standardeinstellungen der Anwendung bei ihrer Installation. Das umfasst unter anderem die Berechtigungen des Betriebssystems, welche die Anwendung einfordert. Die Berechtigungen müssen dem Zweck der Anwendung dienen und dürfen erst angefragt werden, sobald sie Verwendung finden.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Data_2	Verschlüsselung aller sensiblen Daten.	EXAMINE	Der Evaluator validiert, dass sensible Daten (s. Anhang A) von der Anwendung nur verschlüsselt gespeichert werden können. Der Evaluator prüft weiterhin, ob eine hardwaregestützte Schlüsselverwaltung des Betriebssystems für die Speicherung der hierfür notwendigen Schlüssel verwendet wird. Ist ein hinreichender Schutz der Schlüssel durch die Plattform sichergestellt (z. B. in einem embedded Secure Element/Trusted Execution Environment), muss die Anwendung diese Schlüssel wirksam gegen Offenlegung schützen. Der Evaluator nimmt die Wirksamkeit gegenüber Reverse Engineering in die Risikobewertung auf.
O.Data_3	Ablage sensibler Daten.	EXAMINE	Der Evaluator prüft, ob hardwaregestützte Maßnahmen (wie z.B. Trusted Execution Environment) zur Speicherung sensibler Daten verwendet werden. Sollte dies nicht der Fall sein, nimmt der Evaluator die Abwägungen der Wirksamkeit gegenüber Reverse Engineering in die Risikobewertung auf.
O.Data_4	Zugriff auf sensible Daten durch Dritte.	EXAMINE	Der Evaluator prüft, ob die Anwendung Ressourcen zur Verfügung stellt, über die Dritte Zugriff auf sensible Daten erhalten können. Dies umfasst Daten in geteilten Speicherbereichen, Dienste oder Interfaces über die sensible Daten bereitgestellt werden.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Data_5	Löschung aller erhobenen sensiblen Daten nach Abschluss der Verarbeitung durch die Anwendung.	CHECK	Der Evaluator prüft, ob Daten über den Zeitraum ihrer Verarbeitung hinaus in der Anwendung gehalten werden. Daten, die nicht mehr genutzt werden, müssen sicher gelöscht werden.
O.Data_6	Erhebung, Speicherung und Verarbeitung von ausschließlich für den Zweck der Anwendung notwendigen Daten.	CHECK	Der Evaluator prüft, welche Daten von der Anwendung erhoben, gespeichert und verarbeitet werden und stellt diese dem Zweck der Anwendung gegenüber.
O.Data_7	Speicherung und Verarbeitung von sensiblen Daten.	CHECK	Der Evaluator prüft, welche Daten die Anwendung permanent speichert bzw. verarbeitet. Er ermittelt das Risiko, das durch eine solche Speicherung und Verarbeitung in der Anwendung entsteht und nimmt es in die Risikobewertung mit auf.
O.Data_8	Entfernung von Metadaten mit Datenschutzrelevanz.	CHECK	Der Evaluator prüft, ob die Anwendung Daten erheben kann, die Metadaten enthalten. In diesem Fall prüft der Evaluator, ob Metadaten mit Datenschutzrelevanz vor der Weiterverarbeitung, wie beispielsweise dem Transfer an das Hintergrundsystem, entfernt werden.
O.Data_9	Zugriffsbeschränkung bei der Erhebung von sensiblen Daten.	EXAMINE	Der Evaluator prüft, ob erhobene sensible Daten anderen Anwendungen auf dem Gerät verfügbar gemacht werden oder Daten in öffentlichen Verzeichnissen gespeichert werden.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Data_10	Keine Aufzeichnungen bei der Eingabe sensibler Daten über die Tastatur.	EXAMINE	Der Evaluator prüft, ob sensible Daten über Softwaretastaturen des Betriebssystems oder von Drittanbietern eingegeben werden können. Dies schließt insbesondere Caches, Autokorrektur- und Autovervollständigungs-verfahren, Eingabegeräte von Drittanbietern und jegliche für Dritte auswertbare Speicherung, mit ein. Ist dies der Fall, prüft der Evaluator die Abwägungen des Herstellers und berücksichtigt diese in der Risikobewertung.
O.Data_11	Kein Export sensibler Daten in die Zwischenablage.	CHECK	Falls die Anwendung einen Export sensibler Daten in die Zwischenablage des Betriebssystems erlaubt, muss der Abfluss dieser Daten in der Risikobewertung berücksichtigt werden.
O.Data_12	Kein Export von sensiblen Daten aus der Quelle.	EXAMINE	Der Evaluator prüft ob sensible Daten, bei denen keine Notwendigkeit für einen Export besteht, trotzdem exportierbar sind. Dies umfasst unter anderem biometrische Daten oder private kryptografische Schlüssel.
O.Data_13	Keine Speicherung des Bildschirminhaltes oder Zugriff Dritter bei Anzeige sensibler Daten.	CHECK	Der Evaluator prüft, ob die Anwendung das Erzeugen von Screenshots verbietet. Dies umfasst sowohl das aktive, als auch das passive Erzeugen von Screenshots wie es beispielsweise für die Vorschau im Task-Manager durchgeführt wird. Der Evaluator prüft außerdem, ob sensible Daten nicht länger als notwendig in der Anwendung angezeigt werden. Das Restrisiko der Anzeige sensibler Daten wird in der Risikobewertung berücksichtigt.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Data_14	Verschlüsselung aller sensiblen Daten im gesperrten Zustand.	EXAMINE	Ältere Plattformversionen erlauben teilweise die Speicherung der Anwendung auf externen Speichermedien, die nicht der Speicherverschlüsselung unterliegen. Der Evaluator prüft, ob die Anwendung solche oder vergleichbare Vorgehensweisen untersagt.
O.Data_15	Gerätebindung lokal gespeicherter Daten.	EXAMINE	Der Evaluator prüft, ob Daten, die von der Anwendung gespeichert werden, auf anderen Geräten verarbeitet werden können. Von dieser Einschränkung ausgenommen sind Daten, die vom Nutzer explizit zur Verarbeitung auf anderen Geräten exportiert werden.
O.Data_16	Enterfernen oder anderweitiges unzugänglich machen aller sensiblen Daten auf dem Endgerät bei Deinstallation der Anwendung.	CHECK	Der Evaluator prüft, ob nach der Deinstallation der Anwendung Daten auf dem Endgerät zurückbleiben. Ist dies der Fall, prüft der Evaluator weiterhin, ob diese Daten sensible Informationen beinhalten oder Rückschlüsse auf sensible Daten zulassen.
O.Data_17	Möglichkeit zum Löschen oder anderweitigen unzugänglich machen aller sensiblen Daten der Anwendung.	EXAMINE	Der Evaluator validiert, dass dem Nutzer die Möglichkeit gegeben wird alle sensiblen Daten vollständig zu löschen oder unzugänglich zu machen. Darüber hinaus prüft er die Wirksamkeit der getroffenen Maßnahmen durch praktische Tests.
O.Data_18	Sicheres Überschreiben von Nutzerdaten im Gerät durch den Anwender über das Hintergrundsystem.	EXAMINE	Der Evaluator führt eine Löschung der Daten über das Hintergrundsystem durch und validiert, dass keine Nutzerdaten mehr auf dem Gerät lesbar sind.

4.3.8 Testcharakteristik zu Prüfaspekt (8): Kostenpflichtige Ressourcen

Tabelle 11: Testcharakteristik: Kostenpflichtige Ressourcen

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Paid_1	Anzeige kostenpflichtiger Leistungen und Ressourcen.	CHECK	Der Evaluator validiert, dass alle kostenpflichtigen Leistungen und Ressourcen eindeutig als solche erkennbar sind.
O.Paid_2	Einverständnis des Nutzers vor dem Ausführen kostenpflichtiger Leistungen.	CHECK	Der Evaluator validiert, dass alle kostenpflichtigen Leistungen ausschließlich nach Bestätigung durch den Nutzer erbracht werden können.
O.Paid_3	Einverständnis des Nutzers vor einer Zugriffsanforderung auf kostenpflichtige Ressourcen.	CHECK	Der Evaluator validiert, dass die Nutzung von Diensten, die zusätzliche Kosten für den Nutzer verursachen können (z.B. das Versenden von SMS), ausschließlich nach Abgabe einer Einverständniserklärung des Nutzers möglich ist.
O.Paid_4	Dauerhaftes Einverständnis des Nutzers auf häufig verwendete, kostenpflichtige Leistungen oder Ressourcen.	CHECK	Falls die Anwendung ein dauerhaftes Einverständnis des Nutzers für den Zugriff auf kostenpflichtige Ressourcen fordert, prüft der Evaluator, ob dies für den primären Zweck der Anwendung erforderlich ist (vgl. O.Purp_1).
O.Paid_5	Entzug des Einverständnisses ermöglichen.	CHECK	Der Evaluator prüft, ob die Anwendung eine Liste mit allen vom Nutzer gegebenen Einverständniserklärungen anzeigt und diese nachträglich geändert werden kann.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Paid_6	Ablage der sensiblen Transaktionshistorie im Hintergrundsystem.	EXAMINE	Der Evaluator prüft über praktische Tests und Quelltextanalyse, ob eine Transaktionshistorie in der Anwendung vorgehalten wird. Die Transaktionshistorie sollte im Hintergrundsystem sicher gespeichert werden und aus der Anwendung einsehbar sein. Wenn die Transaktionshistorie in der Anwendung selber gespeichert wird, ist in einer Risikobewertung darzustellen, inwieweit die Sicherheit der gespeicherten Daten gewährleistet werden kann.
O.Paid_7	Profilbildung durch Nachverfolgung der Zahlungsströme durch Dritte.	CHECK	Der Evaluator prüft, ob über die Nachverfolgung von Zahlungsströmen Rückschlüsse auf die Eigenschaften oder das Verhalten des Nutzers möglich sind. Die Abwägungen des Herstellers bei potenziellen Rückschlüssen sind in der Risikobewertung zu berücksichtigen.
O.Paid_8	Anzeige der Übersicht der entstandenen Kosten.	CHECK	Der Evaluator prüft, ob die Anwendung dem Nutzer eine Übersicht der entstandenen Kosten anbietet. Falls die Kosten aufgrund einzelner Zugriffe erfolgt sind, prüft der Evaluator, ob die Anwendung einen Überblick der Zugriffe aufführt.
O.Paid_9	Validierung von getätigten Bezahlvorgängen im Hintergrundsystem.	EXAMINE	Der Evaluator prüft durch Quelltextanalyse und praktische Tests, ob die Anwendung eigenständig Bezahlungen validiert und beispielsweise kostenpflichtige Funktionen freischalten kann.
O.Paid_10	Anforderungen bei Zahlverfahren von Drittanbietern.	CHECK	Der Evaluator prüft die Zahlverfahren durch Drittanbieter. Sowohl bei Drittanbieter-Software, als auch bei Web-Diensten wird geprüft, dass keine sensiblen Nutzerdaten an den Zahlungsdienstleister abfließen (z.B., dass der Titel der gebuchten Leistung keine sensiblen Informationen enthält).

4.3.9 Testcharakteristik zu Prüfaspekt (9): Netzwerkkommunikation

Tabelle 12: Testcharakteristik: Netzwerkkommunikation

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Ntwk_1	Netzwerkkommunikation durchgängig mit gegenseitiger Authentisierung verschlüsselt.	EXAMINE	Der Evaluator validiert, dass ausschließlich mit gegenseitiger Authentisierung verschlüsselte Kommunikation zwischen der Anwendung und anderen Komponenten möglich ist.
O.Ntwk_2	Konfiguration der verschlüsselten Verbindung gemäß aktuellem Stand der Technik.	EXAMINE	Der Evaluator validiert, dass die in O.Ntwk_1 beschriebene Kommunikation dem Stand der Technik (siehe [TR02102-2]) entspricht.
O.Ntwk_3	Sichere Kommunikationskanäle nur mit Betriebssystem-Funktionen oder sicherheitsüberprüfter Drittsoftware.	EXAMINE	Der Evaluator prüft, wie ein sicherer Kommunikationskanal aufgebaut wird. Wenn keine Betriebssystem-Funktionen verwendet werden, validiert der Evaluator, dass die Drittanbieter-Software, welche zum Verbindungsabbau verwendet wird, den in Kapitel 3.1.4 beschriebenen Anforderungen genügt. Eigene Implementierungen zum Aufbau sicherer Kommunikationskanäle sind nicht zulässig. Gemäß A.OperatingSystem werden die Funktionen zum Aufbau von sicheren Kommunikationskanäle im Betriebssystem als sicher angenommen. Sicherheitsüberprüft bedeutet, dass alle sicherheitsrelevanten Bereiche der Software durch eine weitere Partei auf ihre Sicherheitseigenschaften hinuntersucht worden sind.
O.Ntwk_4	Unterstützung von Zertifikats-Pinning.	EXAMINE	Der Evaluator validiert, dass die Anwendung Zertifikats-Pinning unterstützt und dieses wirksam umsetzt.
O.Ntwk_5	Validierung des Server-Zertifikats des Hintergrundsystems.	EXAMINE	Der Evaluator prüft, wie die Anwendung das Zertifikat des Hintergrundsystems validiert.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Ntwk_6	Validierung der Integrität und Authentizität der Antworten des Hintergrundsystems.	EXAMINE	Der Evaluator bestätigt, dass die Integrität und Authentizität der Nachrichten des Hintergrundsystems von der Anwendung validiert werden.
O.Ntwk_7	Verwendung plattformspezifischer Optionen.	EXAMINE	Der Evaluator bestätigt, dass die plattformspezifischen Optionen zur Gewährleistung einer sicheren Kommunikation umgesetzt wurden.
O.Ntwk_8	Vorhaltung von vollständigen Log-Dateien für alle aufgebauten Verbindungen.	CHECK	Der Evaluator überprüft die von dem Hersteller bereitgestellten Log-Dateien und validiert, dass die HTTP-Header vollständig miterfasst sind. Wenn kein Logging sicherheitsrelevanter Ereignisse auf dem Hintergrundsystem stattfindet, muss dieser Aspekt in der Risikobewertung berücksichtigt werden.

4.3.10 Testcharakteristik zu Prüfaspekt (10): Plattformspezifische Interaktionen

Tabelle 13: Testcharakteristik: Plattformspezifische Interaktionen

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Plat_1	Geräteschutz für die Nutzung der Anwendung erforderlich.	CHECK	Der Evaluator prüft, ob der Hersteller eine Nutzung ohne aktivierten Geräteschutz zulässt. Ist das der Fall, prüft der Evaluator, ob der Nutzer angemessen über die daraus resultierenden Risiken aufgeklärt wird, und er berücksichtigt die Abwägungen des Herstellers in der Risikobewertung. Gemäß A.OperatingSystem wird insbesondere angenommen, dass das Betriebssystem über Funktionen verfügt, die es der Anwendung ermöglichen, die Einstellung des Geräteschutzes abzufragen.
O.Plat_2	Nur Anforderung der für den primären Zweck notwendigen Berechtigungen.	CHECK	Der Evaluator prüft die von der Anwendung geforderten Berechtigungen und bestätigt, dass diese für die Erfüllung des primären Zwecks der Anwendung (O.Purp_1) erforderlich sind.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Plat_3	Hinweis auf Zweck der Berechtigungen und Auswirkungen bei Nichterteilung.	CHECK	Der Evaluator prüft, ob die Anwendung auf den Zweck der geforderten Berechtigungen hinweist.
O.Plat_4	Keine sensiblen Daten in Meldungen oder Benachrichtigungen.	EXAMINE	Der Evaluator prüft anhand von Quelltextanalyse und generierten Log-Nachrichten, ob die Anwendung sensible Daten in diese Nachrichten schreibt. Sollten die geloggten Daten Rückschlüsse auf den Nutzer zulassen, muss dieser Datenabfluss in der Risikobewertung berücksichtigt werden.
O.Plat_5	Option zur Anzeige von Meldungen/Benachrichtigungen mit sensiblen Daten.	CHECK	Falls die Anwendung die Möglichkeit zur Anzeige von Meldungen mit sensiblen Daten bietet, prüft der Evaluator, ob diese standardmäßig deaktiviert sind. Weiterhin prüft er, ob der Nutzer bei Aktivierung dieser Option angemessen über die daraus resultierenden Risiken aufgeklärt wird. Die Abwägungen des Herstellers, solche Optionen anzubieten, sind in der Risikobewertung zu berücksichtigen.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Plat_6	Zugriffsbeschränkungen auf sensible Daten.	EXAMINE	Der Evaluator prüft, ob die Anwendung den Zugriff auf sämtliche Daten beschränkt, solange sie unter der Kontrolle der Anwendung sind. Dies schließt eine Beschränkung des Zugriffs auf vorgesehene Dateipfade zum Schutz sensibler Daten durch automatisches Speichern oder unbeabsichtigtes Speichern durch den Nutzer mit ein. Darüber hinaus ist zu validieren, dass die Anwendung keine Broadcast-Nachrichten verschicken kann, die von allen auf dem Gerät installierten Anwendungen gelesen werden können. Die Anwendung darf Nachrichten ausschließlich an autorisierte Anwendungen verschicken. Wenn die Anwendung diese Vorgabe nicht umsetzt, müssen die Abwägungen des Herstellers in die Risikobewertung mitaufgenommen werden. Gemäß A.OperatingSystem wird angenommen, dass das Betriebssystem über wirksame Funktionen verfügt, die einzelne Anwendungen untereinander und gegenüber dem Betriebssystem isolieren. Die Isolation muss durchgängig sein und mindestens die Prozessebene, Arbeitsspeicherinhalte und Dateisystemebene umfassen.
O.Plat_7	Nutzung von sensiblen Funktionalitäten über Interprozesskommunikation.	CHECK	Bietet die Anwendung Schnittstellen an, berücksichtigt der TR-Prüfer deren Ausnutzbarkeit in der Risikoanalyse. Gemäß A.OperatingSystem wird insbesondere angenommen, dass für das Betriebssystem Funktionen zur Interprozesskommunikation bereitstehen, für die Regeln zur Isolation der Kommunikation gesetzt werden können.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Plat_8	Nutzung von Rendering Engines zum Nachladen aktiver Inhalte.	CHECK	Wenn die Anwendung Rendering Engines einsetzt, prüft der Evaluator, ob die Komponenten das Nachladen aktiver Inhalte unterbinden oder auf Quellen unter der Kontrolle des Herstellers beschränken. Die Auswahl der zugelassenen Quellen wird in der Risikoanalyse berücksichtigt.
O.Plat_9	Entfernung von sensiblen Daten bei Wechsel in den Hintergrundbetrieb.	EXAMINE	Der Evaluator prüft, ob die Anwendung sensible Daten aus den entsprechenden Anzeigeelementen der Anwendung entfernt.
O.Plat_10	Deaktivierung nicht benötigter Protokoll-Handler in Rendering Engines.	CHECK	Wenn die Anwendung Rendering Engines einsetzt, prüft der Evaluator, ob die Komponenten nicht benötigte Protokoll-Handler deaktivieren.
O.Plat_11	Löschen anwendungsspezifischer Sitzungsdaten beim Beenden der Anwendung.	EXAMINE	Wenn die Anwendung Rendering Engines oder andere Arten zur Darstellung von Webinhalten einsetzt, prüft der Evaluator, ob anwendungsspezifische Sitzungsdaten nach Beenden der Anwendung gelöscht werden.
O.Plat_12	Überschreiben aller nutzerspezifischen Daten beim Beenden der Anwendung.	EXAMINE	Die Anwendung darf sich bei der Beendigung nicht rein auf das Betriebssystem und den Garbage Collector der Laufzeitumgebung verlassen. Sensible Daten müssen aktiv gelöscht bzw. überschrieben werden. Der Evaluator ermittelt die Risiken für die einzelnen betroffenen Daten und berücksichtigt diese in der Risikobewertung.
O.Plat_13	Information des Nutzers über erforderliche Sicherheitsmaßnahmen zur Anwendung, Drittanbieter-Software und Plattformen.	CHECK	Der Evaluator prüft, ob der Nutzer über selbst durchführbare Sicherheitsmaßnahmen informiert und ggf. angeleitet wird. Der Evaluator bewertet, ob die Maßnahmen ausreichend sind, um Restrisiken zu begrenzen.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Plat_14	Protokollierung bestimmter Sicherheitsereignisse.	CHECK	Der Evaluator überprüft die von dem Hersteller bereitgestellten Logdateien und validiert, dass ein abgebrochener Start und andere Sicherheitsereignisse der Anwendung protokolliert werden. Die Informationen dienen der Post-Mortem-Analyse von Sicherheitsvorfällen und sollten daher Informationen über alle ausgehenden Verbindungen enthalten, unter anderem Metainformationen über verwendete Proxys und überprüfte Server-Zertifikate.

4.3.11 Testcharakteristik zu Prüfaspekt (11): Resilienz

Tabelle 14: Testcharakteristik: Resilienz

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Resi_1	Informationen zum sicheren Umgang mit der Anwendung.	CHECK	Der Evaluator prüft, ob die Anwendung „Best-Practices“ bereitstellt. Er bestätigt, dass vorhandene „Best-Practices“ dem aktuellen Stand der Technik entsprechen.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Resi_2	Erkennung vom Betriebszustand des verwendeten Endgerätes.	EXAMINE	Der Evaluator überprüft durch praktische Tests die Wirksamkeit der Maßnahmen zur Erkennung, ob sich das Betriebssystem außerhalb eines Betriebszustand befindet, der den Anforderungen des Betriebssystemherstellers entspricht (z.B. Root-/Jailbreak-Erkennung). Weiterhin prüft er, ob die Anwendung angemessen auf das Erkennen reagiert. Dies kann beispielsweise eine Terminierung der Anwendung sein (vergleiche O.Resi_5). Gemäß A.OperatingSystem wird angenommen, dass das Betriebssystem Funktionen bereitstellt, mit denen eine Anwendung die Konformität des Betriebszustandes bezüglich der Anforderungen des Betriebssystemherstellers an das Betriebssystem abfragen kann.
O.Resi_3	Erkennung und Unterbindung des Starts in einer Entwicklungs-/Debug-Umgebung.	CHECK	Der Evaluator prüft die Wirksamkeit der Debug-Erkennung durch praktische Tests. (vergleiche O.Resi_5).
O.Resi_4	Abbruch des Starts der Anwendung bei ungewöhnlichen Benutzerrechten.	CHECK	Der Evaluator prüft die Wirksamkeit der Erkennung durch praktische Tests (vergleiche O.Resi_5).
O.Resi_5	Überprüfung der Integrität des Endgeräts vor Verarbeitung sensibler Daten.	EXAMINE	Der Evaluator untersucht, welche Integritätsprüfung durch die Anwendung vorgenommen wird. Wenn die Prüfung durch externe Tools durchgeführt wird, zu dem der Evaluator keinen Quelltext besitzt, führt er einen Penetrationstest durch (vergleiche O.Resi_2 bis O.Resi_4). Ein Integritätscheck muss mindestens folgende Aspekte abdecken: • Einsatz von „custom firmware“. • Aktualität der Betriebssystemversion. • Vorhandensein von verdächtigen Werkzeugen oder Anwendungen auf dem Gerät.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Resi_6	Überprüfung der Authentizität des Hintergrundsystems vor Zugriff.	EXAMINE	Der Evaluator prüft die Wirksamkeit der Authentizitätsprüfung (beispielsweise Zertifikats-Pinning) durch praktische Tests.
O.Resi_7	Integration von Härtungsmaßnahmen vor Verarbeitung sensibler Daten.	EXAMINE	Der Evaluator prüft, ob die Anwendung eine Integritätsprüfung bei jedem Programmstart oder bei sensiblen Operationen durchführt. Andernfalls werden die daraus resultierenden Restrisiken in der Risikobewertung berücksichtigt.
O.Resi_8	Umsetzung von Maßnahmen gegen Reverse Engineering.	EXAMINE	Der Evaluator prüft, ob starke Maßnehmen gegen Reverse Engineering getroffen werden. „Starke Maßnahmen“ müssen sämtliche Strings, Dateinamen und interne Namen von Klassen und Methoden innerhalb der Anwendung, die einem Angreifer Hinweise auf den Programmablauf geben können, verschleiern. Der Evaluator prüft die Wirksamkeit des Schutzes vor Reverse Engineering durch praktische Tests und dokumentiert den Prozess. Der Evaluator bewertet die bestehenden Restrisiken der Implementierung unter anderem in Bezug auf T.MemoryStructures, T.InfoDisclosure und T.SensitiveData.
O.Resi_9	Berücksichtigung von Plattformen und Versionen bei Zugriffskontrollmechanismen.	EXAMINE	Der Evaluator bestätigt, dass sich die Implementierung der Zugriffsmaßnahmen nicht allein auf das Betriebssystem verlässt und damit evtl. durch einen Downgrade-Angriff auf das Betriebssystem verwundbar ist.
O.Resi_10	Robustheit gegenüber Störungen.	EXAMINE	Der Evaluator prüft durch Quelltextanalyse und praktischen Tests, ob Störungen (z.B. in der Stromversorgung, Internetverbindung) oder Fehlbedienung zu einem Verlust der Daten führen können.

5 Sicherheitsstufen und Risikoanalyse

Grundlage für das Prüfurteil soll ein dokumentiertes Risikomanagementverfahren sein. Als allgemeine Referenz werden BSI Standard 200-3 [BSI200-3], ISO 27005 [ISO27005] und Anhang B der Common Criteria Evaluation Methodology [CEM] genannt. Das Prüflabor darf nach Abstimmung ein vergleichbares, auf eine IT-Sicherheitsanwendung ausgerichtetes, Risikomanagementverfahren einsetzen.

Die TR-Prüfer führen eine methodische Risikoanalyse durch, die mindestens folgende Schritte umfassen muss:

1. Sicherheitsproblem vollständig aufarbeiten – Ausgangspunkt der Risikoanalyse sind die Bedrohungen, Annahmen und Policies der Anwendung (Kapitel 2.4). Der TR-Prüfer etabliert eine vollständige Liste aller sensiblen Daten, die in der Anwendung erfasst, erzeugt oder genutzt werden. Sensible Daten, die alleine im Hintergrundsystem verarbeitet werden, sind durch die Annahme A.Backend abgedeckt.
2. Schutzbedarf feststellen – die IT-Sicherheit betrachtet generell den Schutzbedarf hinsichtlich Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit. Der TR-Prüfer klassifiziert den jeweiligen Schutzbedarf aller verarbeiteten Daten, vgl. Anhang B in [ISO27005]. Die Daten im Rahmen der TR werden anhand ihrer Kritikalität unterschieden (vgl. Tabelle 15).
3. Risikoszenarien bewerten – Der TR-Prüfer führt unter Berücksichtigung der etablierten Gegenmaßnahmen eine Bewertung von Risikoszenarien durch. Es muss dafür ein dokumentierter, ganzheitlicher Ansatz auf die sensiblen Daten der Anwendung durchgeführt werden, beispielsweise [ISO27005], Abschnitt 8.3 und Anhänge C/D/E.

In die Bewertung durch den TR-Prüfer geht ein, welche Schutzmaßnahmen im Produkt realisiert sind, und deren Effektivität (Beispielsweise Maßnahmen gegen Brute-Force Angriffe auf Login Credentials). Ebenfalls werden Vorgaben für die sichere Nutzung berücksichtigt, sofern diese dem Nutzer ausreichend dargelegt sind. Ob das Sicherheitsproblem angemessen behandelt wird, schätzen die TR-Prüfer anhand der Schwierigkeit ermittelter Angriffspfade ein. (Die Schwierigkeit eines Angriffs ersetzt dabei die in der ISO 27005 referenzierte Eintrittswahrscheinlichkeit eines Risikos.)

Häufig werden für die Angriffsbewertung auf mobile Anwendungen folgende Bewertungsprinzipien eingesetzt:

1. Zeitbasierter Ansatz – Der Prüfer schätzt den zeitlichen Aufwand eines Angreifers die bestehenden Gegenmaßnahmen auszuhebeln. Der Hersteller versichert, dass vor Ablauf dieser Zeit eine neue Produktversion mit neuem Schlüsselmaterial bereitgestellt wird (z.B. spätestens monatlich) und die Anwendung ist so beschaffen, dass Angriffe nur an der aktuellsten Produktversion ausgeführt werden können. In diesem Szenario wird eine Ausnutzung des Angriffspfads durch ein rechtzeitiges Update unterbunden.
2. Reaktiver Ansatz – Hier analysiert der Prüfer die effektive Bekämpfung der Risikoszenarien mittels proaktiven Monitorings / Reaktion. Beispielsweise werden Betriebsparameter erfasst und der Zugriff auf sensible Daten wird abgewehrt, sofern diese auf absichtliche Modifikationen hindeuten. Extern vom Hersteller selbst-realisierte Schutzmechanismen müssen im Rahmen der TR-Prüfung mitbetrachtet werden.

Der Prüfer muss aufgrund der ermittelten Restrisiken ein Urteil abgeben, inwiefern das von der TR adressierte Sicherheitsproblem adäquat erfüllt wird. Tabelle 15 zeigt die Anforderungen je Datum. Eine Zertifizierung kann nur erteilt werden, falls die TR-Prüfung ergibt, dass die Anforderungen für alle Daten erfüllt werden.

Diese TR dient primär der Bewertung von Anwendungen, wie sie in Kapitel 1.3.1 definiert sind. Bei solchen Anwendungen ist der Schaden beim Verlust Gesundheitsdaten oft nicht zu beziffern, unter anderem weil eine einmal stattgefundene Offenbarung nicht mehr rückgängig gemacht werden kann. Anwendungen, die nach dieser TR evaluiert werden, können allerdings auch andere sensible Daten enthalten, die gegen

Offenbarung geschützt werden müssen. Das Sicherheitsniveau dieser Daten kann ggf. unter dem der Gesundheitsdaten liegen (vgl. Tabelle 15). Die Klassifizierung der Sicherheitsstufen für die einzelnen Daten ist mit dem BSI im Einzelfall abzustimmen. Hierbei kann auf Risikoabschätzungen basierend auf etablierten Standards zurückgegriffen werden.

Tabelle 15: Anforderung anhand der Daten-Kritikalität

Kritikalität	Beschreibung	Anforderung
Sehr hoch	Eine Verletzung des Schutzbedarfs führt zu einem nicht zu beziffernden oder potenziell schwerwiegenden Schaden für den Dateninhaber.	Die realisierten Maßnahmen werden als wirksam erachtet, sämtliche Risikoszenarien ohne Restrisiken auszuräumen.
Hoch	Eine Verletzung des Schutzbedarfs führt zu einem hohen oder mittleren Schaden für den Dateninhaber.	Die realisierten Maßnahmen reduzieren die Risikoszenarien erheblich. Der TR-Prüfer muss die Durchführung verbleibender Angriffe bewerten und deren Auswirkungen dokumentieren. Im Einzelfall ist das Restrisiko darzustellen und kann Auflagen in der Nutzung der Zertifizierung verursachen.
Normal	Es kann höchstens ein geringer Schaden eintreten.	Die realisierten Maßnahmen reduzieren die Risikoszenarien. Der TR-Prüfer muss die Durchführung verbleibender Angriffe bewerten und Restrisiken offenlegen.

Anhang A: Schutzbedarf sensibler Datenelemente

Abhängig von der realisierten Anwendung und der Kritikalität der jeweils verarbeiteten Datenelemente kann ein unterschiedlicher Schutzbedarf notwendig sein. Personenbezogene Daten unterliegen dem Datenschutz und dürfen nur bei Zweckbindung und nach Einverständnis verarbeitet werden, vgl. Abschnitt 3.1.1. Die Sensibilität verarbeiteter Datenelemente wird in der folgenden Tabelle bestimmt.

Tabelle 16: Schutzbedarf sensibler Datenelemente

Information	Sensibel	Übertragung an Hintergrundsystem erlaubt	Ablage außerhalb einer sicheren Umgebung erlaubt	Bemerkungen
Anwendungsdaten	Ja	Ja	Ja	-
Eingabedaten (von extern, dritter Partei, einer Drittanbieter-Software, über Tastatur oder von Gerätesensoren)	Nein, falls nicht in anderer Kategorie speziell erfasst	Ja	Ja	Vorbehandlung, u.a. Größenprüfung, Escaping-Sequenzen (je nach Weiterverarbeitung)
Zugangsdaten	Ja	Ja	Ja	z.B. salted hashing. Zulässig ist Drittanbieter-Software für Authentifizierung.
Kryptographische Schlüssel der Anwendung	Ja	Nein	Nein[9]	Zulässig ist die Nutzung in Drittanbieter-Software zur Kryptographie und Session-Handling.

[9] Ausgenommen sind Public Keys oder kryptografische Schlüssel von Drittanbietersoftware, sofern diese nicht der Kontrolle des Anwendungs-Entwicklers unterliegen und mobile Endgeräte, die nicht über eine sichere Umgebung (z. B. embedded Secure Element/Secure Enclave/Trusted Execution Environment) verfügen.

Information	Sensibel	Übertragung an Hintergrundsystem erlaubt	Ablage außerhalb einer sicheren Umgebung erlaubt	Bemerkungen
Aggregierte Anwendungsdaten z.B. Therapiebericht als PDF	Ja	Ja	Ja	Eine Anzeige darf nur mit integriertem Viewer erfolgen. Die Implementierung soll eine Speicherung auf dem Gerät vermeiden. Eine Speicherung ist ausschließlich verschlüsselt erlaubt. Die für die Therapieform erforderliche Ausleitung soll über einen sicheren Kanal erfolgen.
Biometrische Daten	Ja	Nein	Nein[10]	Biometrische Daten sind der Anwendung nicht zugänglich, außer einem Referenzmerkmal (z.B. User 1).
Öffentliche Zertifikate sowie Information für das Zertifikats-Pinning	Nein	Ja	Ja	-

[10] Automatisch erfüllt, wenn das Betriebssystem der Anwendung diese Daten nicht zur Verfügung stellt, andernfalls müssen die Daten als sensible Daten von der Anwendung geschützt werden

Abkürzungsverzeichnis

API	Application Programming Interface (Anwendungs-/Programmierschnittstelle)
App	Applikation
A.*	Assumption (Annahme)
BSI	Bundesamt für Sicherheit in der Informationstechnik
GPS	Global Positioning System
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IKT	Informations- und Kommunikationstechnologien
iOS	Betriebssystem des Unternehmens Apple für mobile Geräte
IoT	Internet of Things
IPC	Interprozess Kommunikation
O.*	Objective (Prüfaspekt)
OSP.*	Organizational Security Policies (Organisatorische Sicherheitspolitiken)
R.*	Empfehlung (Recommendation)
SDK	Software Development Kit
SGB V	Sozialgesetzbuch (SGB) Fünftes Buch (V)
SGB XI	Sozialgesetzbuch (SGB) Elftes Buch (XI)
SMS	Short Message Service
SPD	Security Problem Definition
SSID	Service Set Identifier
T.*	Threat (Bedrohung)

TR	Technische Richtlinie
TLS	Transport Layer Security
URL	Uniform Resource Locator
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
XML	Extensible Markup Language

Literaturverzeichnis

[AIS20]

Bundesamt für Sicherheit in der Informationstechnik, „AIS 20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren“, 15.05.2013, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_pdf.pdf?__blob=publicationFile&v=1

[BMG-EH]

Bundesministerium für Gesundheit, „Glossar: E-Health“, Version 2023, verfügbar unter https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/e/e-health.html

[BSI200-3]

Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 200-3 Risikoanalyse auf der Basis von IT-Grundschutz“, Version 1.0, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2

[CEM]

„Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, April 2017, Version 3.1, Revision 5, verfügbar unter https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf

[DIGAV]

„Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesundheitsanwendungen-Verordnung - DiGAV)“, Version 2023, verfügbar unter https://www.gesetze-im-internet.de/digav/__4.html

[DfS]

Google Developers, „Design for Safety“, Version 2023, verfügbar unter https://developer.android.com/quality/security-and-privacy

[GDR18]

we are social, „Global Digital Report 2018“, Version Januar 2018, verfügbar unter https://wearesocial.com/de/blog/2018/01/global-digital-report-2018

[gemSpec_IDP_Sek]

gematik, „Spezifikation Sektoraler Identity Provider“, verfügbar unter https://gemspec.gematik.de/docs/gemSpec/gemSpec_IDP_Sek/latest/

[iOSSF]

Apple Inc. „iOS Security Framework“, verfügbar unter https://developer.apple.com/documentation/security

[ISO27005]

BS ISO/IEC 27005:2011, Information technology - Security techniques – Information security risk management

[KCC-C5]

Bundesamt für Sicherheit in der Informationstechnik, „Kriterienkatalog Cloud Computing“, Version 2020, verfügbar unter

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020.pdf?__blob=publicationFile&v=2

[MASVS]

The OWASP Foundation, „ Mobile AppSec Verification Standard“, Version 2.0, verfügbar unter https://github.com/OWASP/owasp-masvs/releases/tag/v2.0.0

[MSTG]

The OWASP Foundation, „Mobile Security Testing Guide“, Version 1.6, verfügbar unter https://github.com/OWASP/owasp-mastg/releases/tag/v1.6.0

[NIST80057]

National Institute of Standards and Technology, „Recommendation for Key Management“, Revision 5, verfügbar unter https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

[SGBV33a]

Bundesanzeiger, „Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung - § 33a Digitale Gesundheitsanwendungen”, Version 2023, verfügbar unter https://www.gesetze-im-internet.de/sgb_5/__33a.html

[SGBXI40a]

Bundesanzeiger, „Sozialgesetzbuch (SGB) Elftes Buch (XI) - Soziale Pflegeversicherung - § 40a Digitale Pflegeanwendungen”, Version 2023, verfügbar unter https://www.gesetze-im-internet.de/sgb_11/__40a.html

[SSDG]

European Union Agency For Network And Information Security, „Smartphone Secure Development Guidelines“, Version December 2016, verfügbar unter https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016/at_download/fullReport

[TR02102-1]

Bundesamt für Sicherheit in der Informationstechnik, „Kryptographische Verfahren: Empfehlungen und Schlüssellängen”, Version 2023-01, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=8

[TR02102-2]

Bundesamt für Sicherheit in der Informationstechnik, „Kryptographische Verfahren: Empfehlungen und Schlüssellängen Teil 2 – Verwendung von Transport Layer Security (TLS)”, Version 2023-01, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=6

[TR03107-1]

Bundesamt für Sicherheit in der Informationstechnik, „Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1“, Version 1.1.1, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.html

[TR03116-4]

Bundesamt für Sicherheit in der Informationstechnik, “Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4: Kommunikationsverfahren in Anwendungen”, 07. März 2023, verfügbar unter

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.pdf?__blob=publicationFile&v=5

[TR03161-2]

Bundesamt für Sicherheit in der Informationstechnik, „Anforderungen an Anwendungen im Gesundheitswesen Teil 2: Web-Anwendungen", Version 2.0, verfügbar unter https://www.bsi.bund.de/dok/TR-03161-2

[TR03161-3]

Bundesamt für Sicherheit in der Informationstechnik, „Anforderungen an Anwendungen im Gesundheitswesen Teil 3: Hintergrundsysteme", Version 2.0, verfügbar unter https://www.bsi.bund.de/dok/TR-03161-3