Spitzenverband Digitale Gesundheitsversorgung

SVDGV | Pappelallee 78/79 | 10437 Berlin

Bundesministerium für Gesundheit
11055 Berlin

via Email

Berlin, 01.07.2025

Antworten zu Pain Points und Fakten zur BSI TR-03161

1. Welche Verfahren [zur Authentisierung] sind denn erlaubt?

- Gemäß der FAQ aus dem Mai 2025 sind die Verfahren aus der untenstehenden Tabelle erlaubt, allerdings mit etlichen Einschränkungen. Die linke Spalte enthält Verfahren mit dem Sicherheitsniveau “hoch”. Die Verfahren der rechten Spalte sind erst nach einer (für Laien abschreckenden) Aufklärung über ein Sicherheitsrisiko erlaubt und entsprechen dem Sicherheitsniveau “substantiell”. Dieses ist immer noch sehr sicher. Das Sicherheitsniveau “niedrig” steht hier nicht zur Auswahl (z.B. sicheres Passwort und Benutzername oder E-Mail-OTP). Die autonome Entscheidung, welches Sicherheitsniveau Patient:innen nutzen wollen, beschränkt sich also auf “sehr hoch” und “substantiell”, wobei schon bei hohem Schutz einschüchternde Warnungen angezeigt werden müssen.

- Die “benutzerfreundliche Lösung”, die oft vom BSI zitiert wird, also Gerätebindung + Biometrie, zwingt Patient:innen bereits zur Einwilligung in ein niedrigeres Sicherheitsniveau (siehe Tabelle unten), da Biometrie nicht in der linken Spalte unter “geeignet sicher” eingestuft wird. Von den 56 zugelassenen DiGA sind 28 als Webanwendung verfügbar, 14 DiGA sind ausschließlich im Browser und nicht als native App nutzbar. Für diese Anwendungen kann Biometrie nicht einfach verwendet werden, sondern setzt einen komplexen Einrichtungsprozess voraus, der Patient:innen überfordert.

- Eine weitere bedeutende Einschränkung ist bei der Gerätebindung zu finden: in der “Spezifikation Sektoraler Identity Provider” gibt es keinen geeigneten Prozess, um eine Gerätebindung auf ein anderes Gerät zu übertragen und ebenso keinen Prozess, mit dem DiGA-Hersteller im Falle des Geräteverlusts die Identität ihrer Patient:innen rechtskonform

prüfen können, sofern nicht unpraktikable weitere Verfahren eingerichtet wurden. Andere Methoden, wie beispielsweise eine Identifikation mit Post-Ident, sind durch die gesetzliche Verpflichtung zur anonymen Nutzbarkeit für DiGA-Hersteller nicht möglich.

Authentisierungsfaktor (im Rahmen einer Zwei-Faktor-Authentisierung)	geeignet sicher (ohne Einwilligung)	mit niedrigerem Sicherheitsniveau (mit Einwilligung)
Wissen		
Benutzername+Passwort	nein	ja
System-PIN / System-Passwort	ja*	ja*
Karten-PIN (eGK oder nPA)	ja	ja
Besitz		
Externes FIDO 2-Token	nein	ja
Passkey	nein	ja
Speichern von ACCESS- oder REFRESH_TOKEN im lokalen Speicher	nein	nein
Gerätebindung mit asymmetrischer Verschlüsselung	ja*	ja*
One-Time Password per E-Mail	nein	nein
One-Time Password per SMS	nein	nein
Timebased One-Time Password (Authenticator Apps)	nein	ja
elektronische Gesundheitskarte (eGK)	ja	ja
Personalausweis (nPA)	ja	ja

	Inhärenz	
Biometrie	nein	ja*

* unter Berücksichtigung der technischen Rahmenbedingungen aus Kapitel 4.3.2 der "Spezifikation Sektoraler Identity Provider" der gematik GmbH

Für eine gültige Zwei-Faktor-Authentisierung müssen die beiden Faktoren unterschiedlichen Kategorien (Wissen, Besitz und Inhärenz) angehören.

Quelle:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03161/TR-03161-FAQ/FAQ-TR-03161_node.html

2. Bei welchen konkreten Anwendungen sind diese Vorgaben [Logout nach 30 Minuten] nicht sinnvoll und nicht umsetzbar, und warum nicht?

- In einer verbandsinternen Umfrage wurde festgestellt, dass 58% der befragten Hersteller bei ihrer DiGA auf eine alltägliche, integrierte Nutzung ausgelegt sind, um den in Studien nachgewiesenen Therapieeffekt zu entfalten. Beispiele sind Anwendungen zur Behandlung von kognitiven Einschränkungen, Sprachstörungen, Diabetes, Migräne, Angststörung, chronischen Schmerzen, ADHS und vielen mehr. Die einzelnen Nutzungen sind häufig über den Tag verteilt und erfordern daher jedesmal eine Authentifizierung. An konkreten Beispielen wie bei Oviva wird deutlich, dass alleine hier 15-20% der Nutzer:innen durch diese Pflicht ein sehr hohes technisches Hindernis überwinden müssen, weil sie nicht mit Biometrie arbeiten können oder wollen.
- Im Falle einer Therapie-Anwendung für Sprechtraining ist neben der täglichen Nutzung auch eine Nutzung bei schlechter Internetverbindung im stationären Setting gewünscht. Bei der Überprüfung des Passworts muss man dann aber online sein. Besonders hinderlich ist dies, wenn es sich um eine Web-App handelt. Diese läuft auf dem Desktop oder Tablet und diese Geräte haben oft keine biometrischen Sensoren und wenn, dann müssen diese aufwändig eingerichtet werden. Das bedeutet also, dass jedes Mal das Passwort eingegeben werden muss.

Zitat aus der Umfrage zum Zwangslogout nach 30 Minuten:

> *"Die Zweckbestimmung unseres Medizinprodukts sieht vor, dass man 30-40 min an einem Tag trainiert (kognitives Training, d.h. Hirnleistungstraining).*
> *Unsere Patienten sind Patienten mit kognitiven Störungen, d.h. sie sind gelegentlich überfordert und müssen teils längere Pausen machen, sodass sie sich sammeln können und dann mit dem Training fortfahren können.*
> *Diese Patienten haben aufgrund ihrer kognitiven Störungen auch erhebliche Probleme mit dem automatischen Logout. Da es sich bei kognitiven Störungen auch um*

Gedächtnisstörungen handelt, d.h. um erhöhte Vergesslichkeit, haben sie dann auch ihr Passwort vergessen sowie vergessen, wo es abgelegt ist. Sie werden dann also noch einmal zusätzlich belastet, sich mit dem Problem des Passworts zu befassen, während bereits das kognitive Training schon Herausforderung genug ist.
Der medizinische Nutzen, das Tagestraining über eine längere Zeit inkl. Pausen abschließen zu können, ohne sich mit dem Problem des Passworts mehr als einmal pro Tag befassen zu müssen, überwiegt eindeutig gegenüber dem hypothetischen Schutz etwa vor physischen Hackern."

- Weitere Zahlen und Fakten dazu sind unter Frage 4 zu finden.

3. Lässt das BSI individuelle Spielräume je nach Anwendungsfällen / Produkten / Indikationen zu?

- Grundsätzlich gibt es die Möglichkeit, mit dem BSI zu einzelnen Lösungen zu sprechen. Leider sieht das in der Praxis schwieriger aus als in der Theorie. In einer verbandsweiten Umfrage unter DiGA-Herstellern konnte zum jetzigen Zeitpunkt kein Hersteller berichten, dass im Austausch mit dem BSI eine Anforderung an die Gegebenheiten des Produkts angepasst werden konnte (laufende Umfrage, n=12)

4. Bei wieviel Prozent der mobilen Endgeräte am Markt ist nach BSI/TR Vorgaben keine Biometrie zulässig, so dass unvermeidlich Passwörter eingegeben werden müssen?

- Geräte, die keine Biometrie-Funktionen erlauben (Fingerabdruck oder Gesichtserkennung), sind mittlerweile rar. Bei nativen Apps wie Oviva Direkt betrifft dies 2% der Geräte, die bei Nutzern im Einsatz sind.

- Von den 56 zugelassenen DiGA sind 28 als Webanwendung verfügbar, 14 DiGA sind ausschließlich im Browser und nicht als native App nutzbar. Für diese Anwendungen kann Biometrie nicht einfach verwendet werden, sondern setzt einen Einrichtungsprozess voraus, bei dem auch ein Passkey eingerichtet werden muss. Laut BSI nutzen ca. 18% der Menschen bereits Passkeys. In der DiGA-nutzenden Population wird dieser Wert viel niedriger sein aufgrund der demographischen Verschiebung hin zu älteren und wenig technisch affinen Menschen. Das bedeutet, bei diesen DiGA sind schätzungsweise 82% der Patienten nicht in der Lage, diese zu nutzen, eventuell sogar mehr.

- Bei nativen Apps hingegen ist die Herausforderung, dass ein größerer Anteil der Nutzer die Funktionen gar nicht benutzen will und sie deshalb nicht aktiviert hat. Dies aus verschiedenen Gründen (Datenschutz/Vertrauen, Sicherheitsbedenken, Einfachheit der Smartphone Nutzung). Bei Oviva z.B. betrifft das aktuell:

    - 16% der Android Nutzer

    - 8% der iPhone Nutzer

- Tests von Oviva haben ergeben, dass nur ein verschwindend kleiner Teil dieser Nutzer, ohne aktivierter Biometrie, sich von einer einzelnen App davon überzeugen lässt, diese Funktionen auf Ebene des Betriebssystems zu aktivieren.

- Es ist davon auszugehen, dass die Zahlen von Oviva mit denen anderer DiGA, die ähnliche Technologien verwenden, vergleichbar sind.

5. Wie ist die Lage bei den Browsern, wie viel Prozent der DiGA-Nutzer können (dürfen) wegen Nutzung veralteter Browser nach BSI-Vorgaben keine Passwortmanagerfunktion nutzen und müssen daher jeweils erneut ein Passwort eingeben?

- Es geht bei dieser Problematik nicht um die Browserversion, sondern um die Vorgabe O.Data_11, die die Verwendung der Zwischenablage für sensible Daten regelt. Diese Vorgabe hat in der Konsequenz dazu geführt, dass Hersteller keine copy/paste-Funktion integriert haben, da die Prüfstellen dies sonst als fail werteten. Insgesamt gaben 44% der Hersteller an, dass ihre Prüfstelle dies gefordert hat.

- Viele gängige Passwortmanager nutzen die Zwischenablage, um das Passwort verfügbar zu machen. Diese können bei dieser Implementierung nicht genutzt werden.

- Dies ist eins von vielen Beispielen, wo unklare Anforderungen in der TR durch die Prüfstellen unterschiedlich interpretiert werden können, weil sie nicht eindeutig formuliert sind. Dies führt zu hohen Entwicklungsaufwänden und wiederholten teuren Prüfungen und zu komplizierter Benutzung, die Patient:innen abschreckt.

- Bereits in unserer ersten Kommentierung der TR-03161 im Januar 2024 haben wir das BSI auf diese Unklarheiten hingewiesen und um Klärung gebeten.

Zitat eines DiGA-Herstellers:

> *"Nein, [Passwortmanager] geht wegen dieser Einschränkung nicht. Zudem ist die Verbreitung und Kompetenz bei der Benutzung von PW Managern in unserer Zielgruppe kaum vorhanden."*

6. Ist dies durch Installation aktuellerer Browser einfach lösbar, oder wie sind die Hindernisse einzuschätzen?

- Nein, eine Installation aktuellerer Browser löst das Problem nicht. Eine Klärung oder Streichung der Anforderung würde zumindest für die Zukunft eine Verbesserung bewirken.

7. Bei welchen Geräten und in welchen Fallkonstellationen werden Passwort-Manager nicht anerkannt?

- Siehe Frage 5.

8. Handelt es sich um Vorgaben des BSI oder eine Interpretation der Prüfstellen?

- Siehe Frage 5.

9. Ist der Einsatz von Passwort-Managern im Scope des Prüfverfahrens?

- Indirekt über O.Data_11, siehe Frage 5.

10. Inwiefern sind die Vorgaben für Banking-Apps geringer anzusehen?

- Im Bankingwesen werden die Apps der Banken auditiert hinsichtlich der Umsetzung von Standards und Sicherheitsmaßnahmen. Beispielsweise gibt die BSI TR-03174 Anforderungen an Anwendungen im Finanzwesen vor. Diese wird allerdings nicht mit einem Zertifikat überprüft, sondern dient im Audit als Grundlage für eine Einschätzung des Auditors über die Sicherheit der Apps. Auch hier gibt es einen Prozess, Restrisiken in einer Risikobetrachtung zu evaluieren und somit Anwendungsbezogen vorzugehen. Durch die Konstellation mit dem BSI-Zertifikat für DiGA gibt es diese Hoheit bei den Prüfstellen nicht. Das BSI hat das letzte Wort und die Auslegung der Kriterien ist teils unvorhersehbar und selbst für die Prüfstellen nicht verständlich geschweige denn vorhersehbar. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03174/TR-03174_node.html

- In gängigen Banking Apps sind die untenstehenden Funktionen frei nutzbar, anders als bei DiGA gemäß BSI TR-03161. Die Liste ist nicht abschließend.

	DiGA	Banking Apps
Screenshots aufnehmen	verboten	i.d.R. erlaubt
Eingeloggt bleiben	nicht erlaubt	Bei Aktivität bleibt die Sitzung erhalten, wenn Nutzer:innen dem zustimmen
Gerätebindung länger als 6 Monate ohne Zustimmung auf ein niedriges Sicherheitsniveau	verboten	erlaubt
Gerätebindung kann von einem Gerät an ein anderes übertragen werden	verboten	Bei allen uns bekannten Banking-Apps erlaubt

11. Welche 2FA- bzw. allgemein IT-Sicherheits-Ausgestaltungen bei Mitbewerbern im Gesundheitswesen werden konkret als weniger hoch angesehen?

- Die BSI TR-03161 wird aktuell nur für DiGA verpflichtend eingeführt. Von den Krankenkassen angebotene Gesundheits-Apps brauchen diese “Anforderungen an Anwendungen im Gesundheitswesen” aktuell nicht umzusetzen. Auch die Apps für die Nutzung der ePA oder GesundheitsID müssen dies nicht tun. Dies führt zu einer Ungleichbehandlung im Markt.
- Viele von Krankenkassen eigenständig vermarktete und andere Gesundheits-Apps bieten überhaupt keine 2FA an.
- Zu den wichtigsten Unterschieden gehören auch hier die strengen Anforderungen im Bereich Authentifizierung, Gerätebindung, Geräteverlust, Gerätewechsel, Kontakt zum Support und viele mehr.

12. Lässt sich dies etwas konkreter darstellen (welche Anforderungen sind (nach wie vor) unklar, Anzahl der Anwendungen, Zahl der Rückverweisungen, Anzahl der einmaligen oder mehrmaligen Rückverweisungen, etc.)?

- Die unklaren Anforderungen gehen aus den 22 Fragen (siehe Anhang) hervor. Bisher kamen aber regelmäßig überraschend strenge Auslegungen auch anderer Anforderungen des BSI zutage. Beispiele siehe Frage 13.

- Ein ergänzender Artikel von fbeta zu dem Thema ist gerade erschienen: https://fbeta.de/bsi-astrologie/

13. Können Beispiele für die Ablehnung angegeben werden? Aus welchen Gründen bzw. welche Gestaltungen wurden konkret abgelehnt?

- Hier sind Auszüge aus diesen Ablehnungen. Insgesamt berichten fast 60% der Hersteller von solchen Fällen. Die Prüfstellen sind oft überfordert mit den unklaren Formulierungen und Auslegungen durch das BSI und verweisen die Hersteller dann direkt ans BSI.

O.Auth_1

- **Prüfstelle:** Konzept mit Benutzername, Passwort und OTP per E-Mail wurde als „angemessen" bewertet und als PASS markiert.
- **BSI:** Lehnte dieselbe Lösung ab mit Hinweis auf fehlende 2-Faktor-Authentifizierung und unzureichende Sicherheit.

O.Auth_3

- **Prüfstelle (Mai 2025):** Passkeys mit Biometrie oder Gerätecode gelten als 2FA und wurden positiv bewertet.
- **BSI:** Erkennt Passkeys (inkl. Biometrie/Gerätecode) nicht als ausreichende Zwei-Faktor-Authentifizierung an.

O.Auth_4

- **Prüfstelle (März–Mai 2025):** Uneinheitliche Bewertung, je nach Kommunikation mit dem BSI. Erst akzeptiert, dann Einschränkungen:
    - OTP per Mail nicht mehr zulässig, auch nicht mit Einwilligung.
    - TOTP oder Passkeys nur mit expliziter Einwilligung (§139e SGB V) erlaubt.
    - Gesundheits-ID, eGK+PIN oder Perso+PIN bleiben die einzigen Verfahren ohne Einwilligung mit hohem Vertrauensniveau.
    - Prüfstelle erkennt an, dass die Situation unklar und die Anforderungen volatil sind.

Authentifizierung (Wiederherstellung von 2FA)

- **TÜV:** Recovery-Code als optional speicherbarer dritter Faktor wurde als DSGVO-konform und angemessen bewertet.
- **BSI:** Lehnt dieselbe Lösung ab, fordert FIDO2-Hardwaretoken. Diese sind aus Datenschutzgründen und aufgrund der Zielgruppe (ältere Nutzer) nicht praktikabel.

O.Resi_5 / O.Resi_9

- **Prüfstelle:** Mindestversionen Android 8 und iOS 15 als PASS gewertet.
- **BSI:** Akzeptiert nur neueste Betriebssystemversionen.

14. Welche konkreten Punkte zu den zulässigen Umsetzungen der 2FA sind nach wie vor offen, auch nach Veröffentlichung der FAQ des BSI? Könnten Sie die Liste mit den 22 Fragen einmal übersenden?

- Das Dokument ist als Anlage beigefügt

15. Wurden seitens des SVDGV strukturierte Gespräche mit dem BSI geführt?

- Es gab 4 Schreiben vom SVDGV an das BSI, zuletzt mit der konkreten Bitte um gemeinsame Überarbeitung unter Einbezug von Experten für UX, Medizinprodukte und Barrierefreiheit

Januar 2024	Kommentierung des Spitzenverbands Digitale Gesundheitsversorgung e.V. (SVDGV) zur technische Richtliniengruppe TR-03161
Dezember 2024	Herausforderungen beim Datensicherheitszertifikat für digitale Gesundheitsanwendungen (DiGA)
April 2025	Dringender Handlungsbedarf: Umsetzung der BSI TR-03161 für Digitale Gesundheitsanwendungen (DiGA)
Mai 2025	Zusammenarbeit zur Überarbeitung der TR-03161 - Vorschlag für praxisgerechte Weiterentwicklung bis 31.12.2025

- Bei Anfragen zu Änderungen im Prozess wird auf die geltenden Gesetze verwiesen. Bei Anfragen zur gemeinsamen Überarbeitung wurde bislang auf die unterjährige Überarbeitung verwiesen.
- Neben dem Schriftverkehr wurden Telefonate geführt zwischen dem Vorstand und den Erstellern der Richtlinie und Hersteller sprechen 1:1 um unklare Anforderungen zu klären (es sind hier noch etliche Fragen offen (siehe Anhang). Das Ziel all dieser Anfragen und Gespräche war es stets, die aufgezeigten Probleme zu lösen und einen Weg für die Patient:innen zu finden.

16. Welche gewählten Gestaltungen wurden nach Ihrer Ansicht durch das FAQ als unzulässig erklärt?

- smsTAN-Verfahren nicht erlaubt, obwohl es das Niveau substantiell erfüllt
- OTP per Email nicht erlaubt
- Recovery Codes werden nicht erwähnt, obwohl dieser Fall häufig zu finden ist, werden aber nicht anerkannt

17. Welches sind die wichtigsten jetzt noch offenen Fragen neben dem Umgang mit "Passwort vergessen" und "Gerät verloren" sowie der Frage des Einsatzes von Passwortmanagern?

- Es gibt die offenen Fragen an die FAQ (siehe Anhang). Dort sind die wichtigsten unklaren Szenarien aufgeführt.
- Daneben gibt es die Themen
    - Authentifizierungsmethoden
    - Passwort vergessen
    - Geräte verloren
    - Gerätewechsel
    - Logout-Zeiten bei Aktivität
    - Umgang mit Geräten, die nicht brandaktuell sind
    - Unklare Anforderungen an zahlreichen Stellen
        - Daraus folgend mehrfach das “Go” von der Prüfstelle, aber ein “No” vom BSI

- Prüfung der Updates nach erhaltenem Zertifikat
- und weitere technische Themen, die auch wichtig und drängend sind aber im Vergleich zu den brennenden Themen aktuell nicht so sehr im Fokus stehen

18. Warum führt die Gesundheits-ID zu konkreten Hindernissen für DiGA-Hersteller und DiGA-Nutzer? § 139e Abs. 10 SGB V enthält ein Wahlrecht für ein geringeres Sicherheitsniveau.

- Die genannte Wahlfreiheit löst das Problem in keiner Weise. Die GesundheitsID ist Teil des Problems. Wie im letzten Schreiben ausgeführt ist die Benutzung komplex und die Bewertungen der Nutzer:innen zeigen das Ausmaß der Probleme (siehe unten).
- Zudem ist die Gesundheits-ID bislang kaum verbreitet, technisch komplex und in vielen praktischen Nutzungsszenarien (z. B. Gerätewechsel, Multidevice-Nutzung) kaum umsetzbar. Für viele DiGA-Zielgruppen ist sie faktisch eine Zugangshürde.
- Die TR müsste daher gezielt die Wahlfreiheit für alle Vertrauensniveaus anbieten. Aus Nutzerfeedback der Hersteller geht hervor, dass Nutzer:innen, die zum Beispiel personalisierte physiotherapeutische Begleitung durch eine DiGA brauchen oder Sprechübungen keinen Nutzen in einem hohen Schutzniveau sehen, im Gegenteil. Für diese Nutzergruppen sollte es als selbstbestimmte Bürger:innen die Möglichkeit geben, auch ein niedriges Vertrauensniveau zu wählen. Umgekehrt ist bei psychischen Erkrankungen der Wunsch nach starkem Schutz häufiger zu hören und daher halten wir es für sinnvoll, dass diese Möglichkeit von DiGA verpflichtend angeboten werden muss. Diese Entscheidung sollte aber jede:r mündige Bürger:in selbst treffen dürfen und nicht das BSI oder der Gesetzgeber.
- Vor Inkrafttreten der TR waren im Rahmen der Anlage 1 der DiGAV die "Anforderungen Datensicherheit – Zusatzanforderungen bei digitalen Gesundheitsanwendungen mit sehr hohem Schutzbedarf" (z.B. Verschlüsselung gespeicherter Daten, Authentisierung mit 2FA) nur von DiGA zu erfüllen, für die im Rahmen der geforderten Schutzbedarfsanalyse ein sehr hoher Schutzbedarf festgestellt wurde. Diese Zusatzanforderungen gelten demnach nicht generell für alle DiGA. Das BSI verlangt die Erfüllung entsprechender Anforderungen aber nun flächendeckend bei allen DiGA - unabhängig vom Ergebnis einer Schutzbedarfsanalyse i.S.e. sehr hohen Schutzbedarfs. Diese generelle Pflicht ist insbesondere bei DiGA mit geringem oder normalen Schutzbedarf unangemessen und unverhältnismäßig und führt bei den DiGA-Herstellern zu unnötig hohem Aufwand und hohen Kosten. Sinnvoll wäre - wie bisher in Anlage 1 der DiGAV angelegt - weiterhin ein abgestufter risikobasierter Ansatz, so dass nur solche DiGA, bei denen ein hoher Schutzbedarf besteht, entsprechende Zusatzanforderungen zu erfüllen haben.

  Die Apps, die bereits zur Nutzung der GesundheitsID verfügbar sind, haben sehr schlechte Bewertungen in den App Stores, wobei dies fast ausschließlich auf die komplizierte Benutzung

zurückzuführen ist (siehe Tabelle). Die Bewertungen von DiGA liegen (noch) im oberen Bereich der Skala, i.d.R. über 4 Sterne (maximal sind 5 Sterne möglich).

Bewertungen der GesundheitsID-Apps (Stand 27.Juni 2025):

Krankenkasse	Mitglieder (ca.)	Art	Rating iOS	Anzahl	Rating Android	Anzahl
Techniker Krankenkasse (TK-Ident)	11,5 Millionen	Standalone	1,4	2171	1,6	1560
AOK Ident – gesamt	24 Millionen	Standalone	1,4	471	2,0	588
Barmer Ident	9 Millionen	ePA-App	1,8	868	1,7	1740
DAK-Gesundheit Ident	5,7 Millionen	ePA-App	1,8	308	2,1	428
IKK classic Ident	1,4 Millionen	ePA-App	1,5	200	2,1	385
KKH Kaufmännische Krankenkasse	1,6 Millionen	ePA-App	1,8	124	1,7	157
hkk	0,7 Millionen	ePA-App	1,5	226	1,4	257
VIACTIV BKK	0,5 Millionen	ePA-App	1,7	84	2,0	105

Auszug aus dem Benutzer-Feedback:

TK Ident App

> *"[...] Allerdings ist es mir ein Rätsel, wie kompliziert es sein kann. Gesundheitsdaten hin oder her...jede moderne Banking-App ist intuitiver und bedarf keiner Zwei-App-Strategie. Neuerdings brauche ich zur Anmeldung in TK-Safe diese TK-Ident-App. Warum? Warum muss ich zig Verschlüsselungsmechanismen in der TK-Hauptapp und zusätzlich in TK-Ident durchlaufen? Es braucht so viele unterschiedliche Kennwörter, ID's, Freischaltcodes, Kartennummern, Identifizierungspasswörter. Genau eines für alles und ggf. Face-ID würden doch ausreichen. Ich als mündiger Kunde entscheide doch, ob und wie die Sicherheit meiner Gesundheitsdaten aussehen soll. Ich habe das Gefühl, dass es viel zu kompliziert gedacht ist. UX ist hier auf der Strecke geblieben [...]*

DAK Ident App

> *"Für diese App gibt es keinen Stern. ständig verlangt die App eine neue Identifikation mit Karte und Pin obwohl Biometrie aktiviert ist [...] es nervt einfach. die App ist sehr unübersichtlich. Bei weitere Möglichkeiten zur Ident. erscheint die Meldung erfolgreich angemeldet und Zack schon wieder bei der Id. mit Karte und Pin. Es hat mit Datenschutz nichts zu tun wenn ich in der Apotheke erst Karte u. Pin rauskrosen muss."*

IKK classic Ident App

> *"Eine Bewertung von 2.1 hier im Store scheint die Entwickler nicht zu interessieren. Beide Apps der IKK im Anmeldeprozess total verkompliziert und nutzerunfreundlich. Jedes Mal zur Post, um Post-Ident zu praktizieren, wenn man deinstalliert hatte. Nein, keine Lust. Wenn es die IKK nicht geregelt bekommt eine unkomplizierte Login-Aufgabe zu gewährleisten, dann*

werden die Apps eben nicht benutzt. Lieber fünf-fach absichern und die Nutzer vergraulen, als etwas unbürokratisches zu liefern…"

19. Wieviel Prozent der DiGA-Nutzer haben Geräte mit Betriebssystemen, die vom BSI nicht zugelassen werden, und werden damit durch Umsetzung der TR von der Nutzung ausgeschlossen?

- Gemäß den Aussagen des BSI gegenüber einzelnen Herstellern werden immer die neuesten Betriebssystemversionen mit den aktuellsten Sicherheitspatches gefordert.
- Die folgende Tabelle zeigt die allgemeinen Marktanteile mobiler Betriebssysteme gemäß der Erhebung von Statcounter im Juni 2025 für Deutschland. Die Darstellung differenziert zwischen Android-Geräten mit Version 13 oder höher sowie 12 oder niedriger und iOS-Geräten mit iOS 18 oder höher gegenüber iOS 17 oder niedriger. Die Gegenüberstellung basiert auf einer DiGA-Anwendung mit mehr als 10.000 aktiven Nutzenden und zeigt vergleichbare Aufteilung.

	Allg. Marktanteil mobile OS Juni 2025 (Quelle Statcounter siehe Frage 20.)	**Anteil mobile OS bei Benutzerkontenerstellung einer DiGA (>10.000 aktive Nutzende Dezember 2024 - Juni 2025)**
Android 13 oder höher	69.3%	75.6%
Android 12 oder kleiner	30.7%	24.4%
iOS 18 oder höher	84.4%	76.4%
iOS 17 oder niedriger	15.6%	23.6%

- Insgesamt zeigt sich, dass über Android und iOS hinweg über 24% der Nutzenden betroffen sind und ein Systemupdate oder ein Geräteaustausch vorzunehmen ist, um die Therapie sicher nutzen zu können. Aus den Erfahrungen in der Begleitung von Nutzenden, zeigten sich ca. 31% der Geräte updatefähig auf Android 13. Mit der möglichen Abkündigung im Frühjahr 2026 wird die Zahl der potentiell ausgeschlossenen Android-Nutzenden auf deutlich über 33% angestiegen. Bei iOS können viele der 23.6% betroffenen eine Aktualisierung auf das derzeit aktuelle iOS 18 durchführen. In der Praxis zeigt sich, dass dies nicht von jedem Nutzenden durchgeführt wird, da für das Update nicht ausreichend Systemspeicher zur Verfügung steht, von Nutzenden als zu aufwändig empfunden wird oder auch Angst, dass etwa andere Apps danach nicht mehr funktionieren.
- Wir schlagen vor, dass Patient:innen selbstbestimmt über die Nutzung der DiGA auf einem potenziell nicht mehr vollständig unterstützten Betriebssystem entscheiden. Eine entsprechender Hinweis, etwa beim Download, bei der ersten Aktivierung oder im Rahmen

regelmäßiger Sicherheitsprüfungen innerhalb der App, könnte transparent über Risiken informieren. Somit ließe sich der Ausschluss ganzer Geräteklassen vermeiden, ohne das Sicherheitsbewusstsein zu vernachlässigen. Die Verantwortung wird damit in begrenztem Rahmen an die Nutzenden übergeben, die selbst einschätzen können, ob das verbleibende Risiko in ihrer individuellen Situation vertretbar ist. Eine solche Handhabung muss bereits in der Technischen Richtlinie (TR) Berücksichtigung finden und dort als ergänzende Empfehlung für App-Hersteller bzw. Prüforganisationen aufgenommen werden, um eine ausgewogene Balance zwischen Sicherheit und Nutzbarkeit zu schaffen. Aktuell ist der Prozess über eine Restrisikobetrachtung der Hersteller und Einbezug des BfDI vorgesehen, was angesichts der Menge an Herstellern und des immer gleichen Falls aus unserer Sicht zentral gelöst werden muss.

20. Wie hoch ist der Verbreitungsgrad entsprechender Geräte/Betriebssysteme am Markt, wie viel Prozent der Nutzer mobiler Endgeräte betrifft das?

- Die folgenden zwei Tabellen zeigen die breit gefächerte Verteilung der genutzten Unterversionen von Android und iOS (z. B. Android 13.0, 13.1, iOS 17.3, 18.0 etc.) zum Stand Juni 2025. Die Daten spiegeln die Vielfalt der im Einsatz befindlichen Betriebssystemversionen wider ohne detaillierte Angabe des Patch-Levels.

Android Version	**Allg. Marktanteil Android** Juni 2025 (Quelle Statcounter Link, abgerufen am 01.07.2025)
16	0.4%
15	25.5%
14	27.0%
13	16.4%
12	9.5%
11	8.5%
10	5.6%
9.0 Pie	2.6%
8.1 Oreo	0.2%
8.0 Oreo	1.8%
7.1 Nougat	0.2%
7.0 Nougat	0.6%
6.0 Marshmallow	0.7%
Other	1.0%

iOS Version	**Allg. Marktanteil iOS** Juni 2025 (Quelle Statcounter Link, abgerufen am 01.07.2025)
iOS 19.0	0.5%
iOS 18.6	0.2%
iOS 18.5	69.5%
iOS 18.4	5.7%
iOS 18.3	4.7%
iOS 18.2	1.0%
iOS 18.1	1.9%
iOS 18.0	1.0%
IOS 17.x	5.9%
IOS 16.x	5.5%
IOS 15.x	2.3%
IOS 14.x	0.2%
IOS 13.x	0.0%
IOS 12.x	0.4%
IOS 11.x	0.7%
IOS 10.x	0.3%
IOS 9.x	0.2%
Other	0.1%

21. Wie kann die Informationssicherheit denn gewährleistet werden, wenn die Plattformbetreiber keine Sicherheitsupdates mehr zur Verfügung stellen?

- Es gibt verschiedene Level von Support bei Betriebssystemen:
    - Die aktuellsten Versionen bekommen aktiv alle Sicherheitspatches für alle gefundenen Schwachstellen (im Falle von iOS die Version 18)
    - Die Versionen davor bekommen in der Regel noch die wichtigen, kritischen Sicherheitsupdates (bei iOS aktuell die Versionen 15 und 16, letzte Updates im März 2025).
    - Ganz alte Versionen bekommen gar keine Updates mehr (End of life, EOL). Dies sind bei iOS alle Versionen ab 14 und älter.

- Quelle: https://en.wikipedia.org/wiki/IOS_version_history#Overview
- Das BSI fordert Versionen 16+, was sich mit Erscheinen von iOS 26 verschieben wird. Ausgehend vom Schutzbedarf von DiGA ist es aus Sicht der Informationssicherheit vertretbar, die ersten beiden oben genannten Kategorien zuzulassen.

  Hier wird vom BSI allerdings ausschließlich die erste Kategorie gefordert und für alles Weitere sollen Hersteller eine Risikoabschätzung machen und mit dem BfDI besprechen. Bei über 50 DiGA ist es nicht zielführend, wenn jeder einzeln diesen Sachverhalt klären muss. Es verfehlt den Zweck einer Technischen Richtlinie. Hier muss nachgebessert werden.

22. Können auf Apple Geräten neue Betriebssystemversionen eingespielt werden, wird das gemacht, in welchem Umfang?

- Schätzungen zufolge nutzen etwa 20–30 % der deutschen Bevölkerung Apple-Produkte; bei Menschen mit geringerem Einkommen dürfte dieser Anteil tendenziell noch niedriger sein. Die iPhones 8 und neuer lassen sich noch auf iOS 18 updaten, das neue iOS 26 (Versionssprung bei Apple) lässt sich voraussichtlich nur noch ab iPhone 11 und neuer installieren. Diese können dann nur noch mit einer Einzelfallentscheidung nach Klärung mit dem BfDI und einem Warnhinweis genutzt werden. Es muss dann auf das Risiko verwiesen werden, was in diesem Beispiel aber defacto noch unrelevant ist. Das verunsichert die Nutzer:innen und führt häufig dazu, dass die Anwendung nicht mehr genutzt wird. Rückmeldungen aus dem Kundenfeedback bestätigen dies.

23. Wie lief das denn bisher, also vor Umsetzung der TR [in Bezug auf die Supportprozesse]?

Hier einige Beispiele für Supportprozesse, die es in DiGA gab:

- Wenn der Login noch funktioniert:
  - Am Telefon Identifikation über Abfrage eines Support-Codes aus der App
  - via Anfrage über die App
  - Fernwartungs-Option in der App (mit vorheriger Zustimmung durch Nutzer:in und zeitlich begrenzt)
- Wenn der Login nicht funktioniert (ausgesperrt):
  - via E-Mail
  - Passwort zurücksetzen via E-Mail-Link
  - Abgleich der E-Mail-Adresse oder ggf. anderer Merkmale

24. Welche Verfahren sind erlaubt nach BSI? Welche wären alternativ sinnvoll, d.h. sicher und zugleich nutzerfreundlich?

- Jede Verarbeitung von Daten muss auf dem gleichen Sicherheitsniveau erfolgen wie die Authentifizierung an der App selbst. Uns ist kein Verfahren bekannt, sich auf diesem Niveau telefonisch oder per Mail zu authentifizieren. Dabei kommt erschwerend hinzu, dass DiGA anonym nutzbar sein sollen.

25. Das ist nicht gut verständlich. Der dritte Faktor muss immer egK plus PIN oder nPA plus PIN sein? Oder nur dann, wenn der Nutzer nicht in ein niedrigeres Sicherheitsniveau eingewilligt hat?

- Die Thematik ist komplex und gehört zu den Fragen, die bislang nicht abschließend beantwortet wurden vom BSI. Wir haben das angefragt und warten auf eine Lösung. Die Problematik wird auch gut erläutert in diesem Artikel: https://fbeta.de/bsi-astrologie/. Wir können hier ohne weitere, verbindliche Äußerungen des BSI nur die Herausforderungen schildern:

- Das Szenario „Gerät verloren" ist derzeit faktisch unlösbar, wenn der Nutzer nicht zu Beginn ein alternatives Verfahren mit hohem Vertrauensniveau eingerichtet hat – z. B. eGK + PIN oder nPA + PIN.

- Zwar sieht § 139e Abs. 10 SGB V eine Einwilligung in ein niedrigeres Sicherheitsniveau vor, das BSI lässt aber für Wiederherstellungsfälle nur sehr eingeschränkte Verfahren zu. Gängige Optionen wie Einmalcodes per E-Mail, Wiederherstellung per Post oder biometrische Rückverifikation auf einem neuen Gerät sind entweder ausgeschlossen oder technisch unzulässig, da sie laut BSI nicht als ausreichend sicher gelten.

- Als einzig verbleibende zulässige Lösung nennt das BSI die Kombination aus Benutzername + Passwort und einem Cloud-synchronisierten Passkey. Diese Variante ist jedoch technisch anspruchsvoll, setzt moderne Betriebssysteme voraus (z. B. iOS 16+) und wird laut BSI selbst nur von einer kleinen Nutzergruppe aktiv verwendet (~18 %). Für viele DiGA-Zielgruppen ist sie nicht praktikabel.

- Kritisch ist: Das Schutzziel Verfügbarkeit gemäß Informationssicherheit ISO 27001 ist im Geräteverlustfall nicht mehr erfüllt – obwohl genau das Szenario Geräteverlust/Gerätewechsel im Alltag häufig vorkommt. Außerdem können in diesem Fall die Betroffenenrechte gemäß DSGVO nicht erfüllt werden, es liegt also auch hier ein Verstoß gegen gesetzliche Vorschriften vor. Es braucht deshalb sichere und gleichzeitig nutzerfreundliche Alternativen zur Wiederherstellung, die auch bei pseudonymer Nutzung und älteren Zielgruppen funktionieren.

26. Wenn er aber eingewilligt hat, wie werden laut BSI die Szenarien "Passwort vergessen" und "Gerät verloren" denn gelöst? Welche Verfahren sind erlaubt gemäß BSI? Welche wären alternativ sinnvoll, d.h. sicher und zugleich nutzerfreundlich?

- Auch diese Thematik ist komplex und gehört zu den Fragen, die bislang nicht abschließend beantwortet wurden vom BSI.
- Zum Thema Geräteverlust/Gerätewechsel siehe Frage 25.
- Das Thema Passwort vergessen würde normalerweise über einen Wiederherstellungslink in einer E-Mail in einer klassischen “Passwort vergessen”-Funktion realisiert werden. Da E-Mail aber nicht das Vertrauensniveau substantiell erreicht, fällt dieser Weg nach der BSI TR-03161 weg.

27. Verbot von Screenshots: Vorgabe des BSI oder der Prüfstellen?

- Das Verbot von Screenshots kommt aus der BSI TR-03161, Teil 1, O.Data_13
- Die Prüfstellen geben das nicht vor, sondern versuchen den Anforderungen des BSI Folge zu leisten und diese korrekt anzuwenden. Hier liegt eine der großen Herausforderungen, die dazu führte, dass eine FAQ notwendig war und es danach immer noch viele Unklarheiten gibt.

28. Welchen Einfluss hat die medizinprodukterechtliche Risikoklassifizierung auf die Anforderungen an die Informationssicherheit? Welcher rechtliche Konnex besteht hier?

- Unabhängig ihrer Klassifizierung müssen Software-Medizinprodukte oder Medizinprodukte, die Software enthalten, so entwickelt werden, dass Aspekte der Informationssicherheit berücksichtigt werden (siehe MDR 2017/745, Annex I, 17.2). Konkretisiert wird dies z.B. in der zuletzt 2015 aktualisierten Version der EN 62304 ("Medical device software - Software life-cycle processes"), Kap. 5.2.2 e. Diese fordert, dass im Rahmen der Softwareentwicklung auch IT-Sicherheitsbezogene Aspekte berücksichtigt werden, z.B. hinsichtlich Authentisierung und Datenschutz. Je nach Klassifizierung des Medizinprodukts überprüft eine externe Benannte Stelle die Einhaltung der Anforderungen der MDR. Das heißt im für DiGA-Hersteller ungünstigsten Fall, dass IT-Sicherheitsaspekte durch mehrere externe Stellen geprüft werden.
- Das heißt, dass mit der Einführung der BSI TR-03161 ein Zustand der Überregulierung geschaffen wurde, der für DiGA-Hersteller eine teilweise existenzbedrohende finanzielle Belastung darstellen kann.

- Über die Anforderungen aus der Medizinprodukte-Regulatorik hinaus mussten DiGAs auch vor der Einführung der BSI TR-03161 die Anforderungen der DiGAV erfüllen. Dazu gehörten von Anfang an z.B. die Pflicht zum Durchführen von Penetrationstests (siehe DiGAV, Anhang 1, Datensicherheit, Nr. 32a) sowie seit 01.04.2021 die Pflicht, als Hersteller ein zertifiziertes Informationssicherheitsmanagementsystem (ISMS) gemäß ISO 27001 vorzuweisen (siehe DiGAV, Anhang 1, Datensicherheit, Nr. 1). Letztere fordert bereits die Entwicklung sicherer Anwendungen (siehe ISO/IEC 27001:2023, Annex A, Nr. 8.25 sowie 8.27+8.28).

- Unabhängig des Zusammenhangs zwischen Medizinprodukteklassifizierung und Informationsicherheit handelt es sich hier also um eine Überregulierung und Verkomplizierung der ohnehin schon zahlreich vorhandenen Anforderungen bzgl. IT-Sicherheit.

29. Ist bei PVS-Systemen eine andere rechtliche Bewertung erforderlich, weil die datenschutzrechtlich Verantwortlichen Leistungserbringenden Berufsgeheimnisträger sind und die Krankenkassen über das Sozialdatenschutzrecht besonderen Bindungen unterliegen?

- Die DSGVO unterscheidet hinsichtlich der technischen und organisatorischen Maßnahmen in Bezug auf die Datensicherheit nicht danach, ob ein Datenverantwortlicher dem Berufsgeheimnis unterliegt oder nicht. Ausschlaggebend ist nach Art. 32 Abs. 1 DSGVO u.a. der Umfang der Datenverarbeitung, die Schwere des Risikos für die betroffenen Personen, wenn die Daten öffentlich werden und deshalb die Sensitivität der zu verarbeitenden Daten. Betreiber von PVS-Systemen verarbeiten in großem Umfang hochsensible Gesundheitsdaten von Patient:innen. Deshalb sollte hier das Schutzniveau entsprechend hoch sein, während es für DiGA-Hersteller auf angemessen niedrigerem Niveau gehalten werden kann (siehe oben).

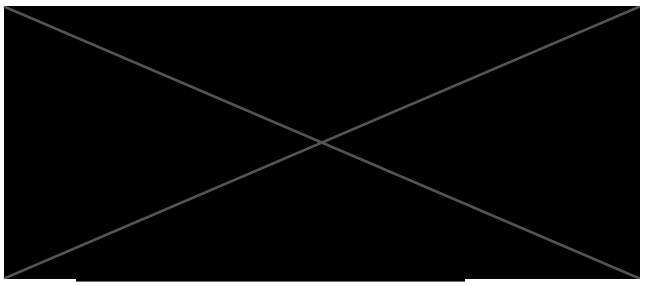
30. Ist der Kostenaufwand für die bisherigen Testverfahren tatsächlich geringer und wenn ja, in welchem Umfang?

- Kosten der bisherigen Verfahren werden bleiben, die Kosten für die TR kommen noch oben drauf. Auch der Pentest entfällt nur im ersten Jahr nach BSI-Zertifizierung und wird danach wieder jährlich gefordert.

31. Wie viele Anforderungen sind im Rahmen der nicht standardisierten Penetrationstests einschließlich des White Box Tests nachzuweisen?

- Die Anforderungen an Penetrationstests bei DiGA wurden mit dem DVPMG verschärft und es gibt Stand heute eine weitreichende Vereinheitlichung. Die aktuellen Anforderungen sind im DiGA-Leitfaden Version 3.5 nachzulesen:

    - Es muss nach dem Durchführungskonzept des BSI für Penetrationstests vorgegangen werden, welches 5 Phasen der Prüfung vorsieht und das Vorgehen bei Pentests vereinheitlicht
    - Es müssen die OWASP-10 Sicherheitsrisiken geprüft werden
    - Der Code der DiGA muss komplett offengelegt werden (white box test)
    - Es müssen Code Reviews durchgeführt werden
    - Es wird empfohlen, eine BSI-zertifizierte Prüfstelle zu wählen, was viele auch getan haben
- Die Anzahl der Anforderungen bezieht sich hier auf bereits bestehende Prüfungen durch das BfArM und akkreditierte Zertifizierungsstellen im Rahmen des Fast Track Verfahrens und der ISO 27001 Zertifizierung sowie MDR für Medizinprodukte:
    - BfArM Antragsverfahren mit inhaltlicher Prüfung gemäß DiGAV
    - MDR I oder MDR IIa mit zahlreichen Anforderungen
    - ISO 27001
    - Anforderungen aus Penetrationstest-Ergebnissen, die implementiert werden müssen (sonst keine Zulassung)
    - zukünftig kommt hier noch die Datenschutzzertifizierung, NIS-2, EU AI Act usw. hinzu



Dr. Christoph Twesten

Vorstandsmitglied des SVDGV