Workshop „Sicherheitsüberprüfung ePA-FdV“

Berlin, 07.07.2020

Agenda

- Historie des Zulassungsverfahrens ePA-FdV
- Überblick Sicherheitsnachweise im Zulassungsverfahren ePA-FdV
- Sicherheitsgutachten ePA-FdV
- Produktgutachten ePA-FdV
- Integration eines ePA-Moduls
- Neubegutachtung ePA-FdV
- BSI-Prüfvorschrift für das ePA-FdV

Historie des Zulassungsverfahrens

elektronische Patientenakte (ePA)

Frontend des Versicherten – Historie des Zulassungsverfahrens

1. Version

- Zulassungsverfahren CC-Evaluierung ePA-Modul FdV
- Bestätigungsverfahren des Herstellers und seiner Entwicklungsprozesse (Sicherheitsgutachten)
- Keine Sicherheitsbegutachtung der Zusatzfunktionen des ePA-FdV

2. Version

- Ein Zulassungsverfahren für das gesamte ePA-FdV
  - Produktgutachten für das **gesamte** ePA-FdV inklusive Zusatzfunktionen
    - kein explizites ePA-Modul FdV mehr (bei R3.1.3 noch in Spezifikationen, aber siehe Disclaimer)
  - Sicherheitsgutachten für die Entwicklungsprozesse des Herstellers

3. Version

- Ein Zulassungsverfahren für das gesamte ePA-FdV **und BSI-Prüfvorschrift**
  - Produktgutachten für das gesamte ePA-FdV inklusive Zusatzfunktionen
    - Berücksichtigung der BSI-Prüfvorschrift *Anforderungen an „Frontend des Versicherten – ePA*“ (basierend auf TR-03161 Sicherheitsanforderungen an digitale Gesundheitsanwendungen)
  - Sicherheitsgutachten für die Entwicklungsprozesse des Herstellers

elektronische Patientenakte (ePA)
BSI-Prüfvorschrift für das ePA-FdV

- Das BSI hat basierend auf der technischen Richtlinie TR 03161 „Sicherheitsanforderungen an digitale Gesundheitsanwendungen“ eine Prüfvorschrift für das ePA-FdV (Anforderungen an „Frontend des Versicherten – ePA“) erstellt.
- Die gematik wird die Anforderungen der Prüfvorschrift für die **ePA-Stufe 2 im Release 4**, Umsetzung bis zum **1.1.2022**, in den Anforderungshaushalt übernehmen und dort die Umsetzung und den Nachweis verpflichtend fordern.
- Für die **ePA-Stufe 1** wird die Umsetzung der Prüfvorschrift zwar gefordert, ein entsprechender Nachweis der Umsetzung ist jedoch erst bis zum **01.01.2022** erforderlich.
  - Eine Änderung der Zulassungskriterien durch verbindliche Forderung der Nachweise zur Umsetzung der Prüfvorschrift zum 01.01.2021 erfolgt nicht.

Überblick Sicherheitsnachweise im Zulassungsverfahren ePA-FdV

elektronische Patientenakte (ePA)
Frontend des Versicherten – Gutachten

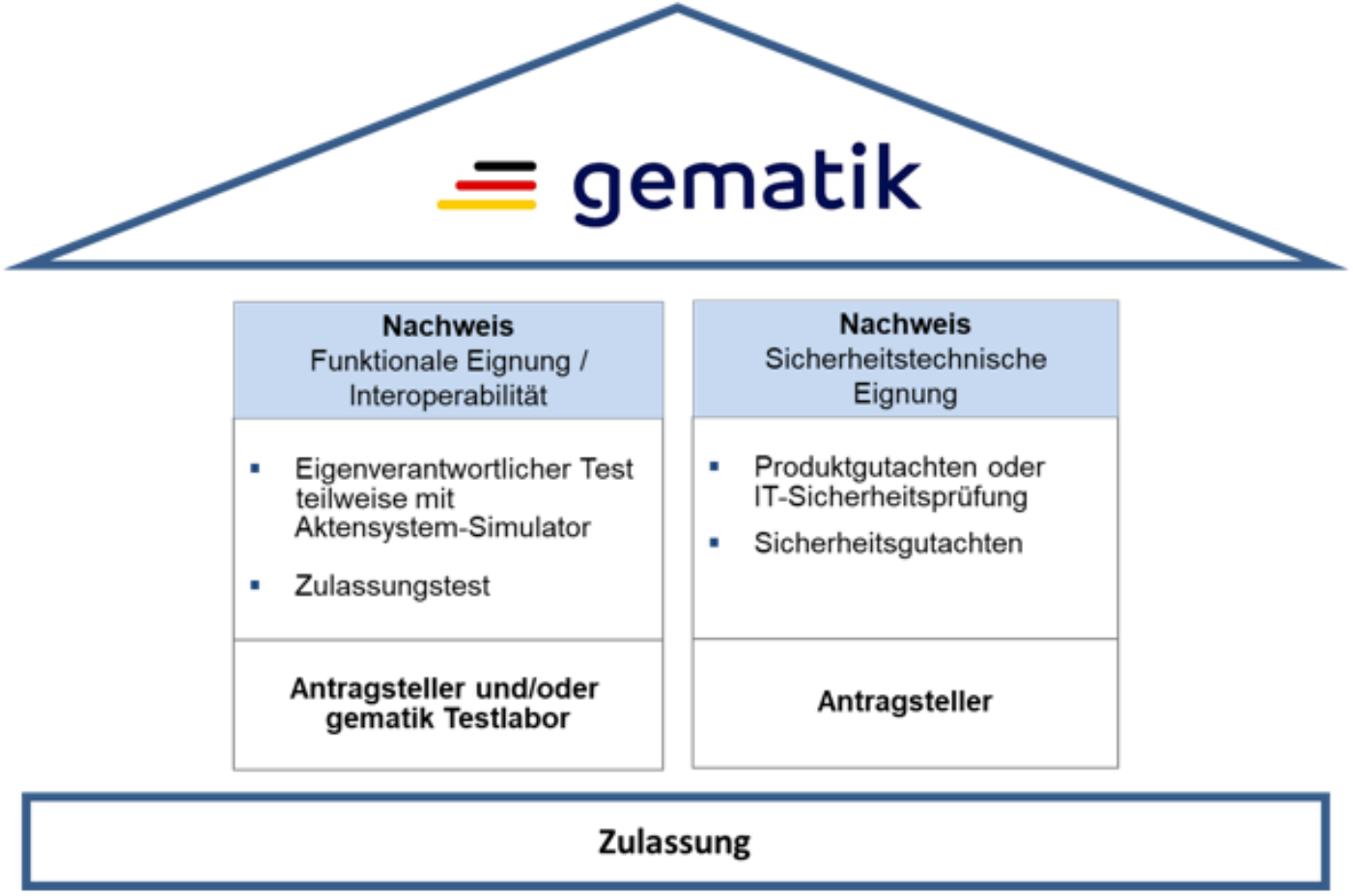

Abbildung 1: Prüfbereiche

Bundesamt für Sicherheit in der Informationstechnik

Produktgutachten
(**oder** CC-Zertifizierung)
des ePA-FdV
plus
Sicherheitsgutachten
über sichere Software-Entwicklungsprozesse

gematik leitet Produktgut-achten an das BSI weiter

Sicherheits- und Produktgutachten
Prüfmethoden

Sicherheitsgutachten

- Aktenanalyse
- Inaugenscheinnahme und Beobachtung
- Technische Prüfung ohne Zugriff auf das System
- Datenanalyse
- Verwendung bestehender Nachweise
- Befragung

- vor-Ort-Audit bei vollständigem Gutachten unverzichtbar
- Technische Prüfung besitzt höchste Aussagekraft; daher einzusetzen, wann immer möglich

Produktgutachten

- Penetrationstest
- Technische Prüfung mit Zugriff auf das System
- Quellcode-Analyse

- Andere Prüfmethoden zusätzlich anwendbar (insbesondere ist Aktenanalyse notwendig, um Verständnis zu erhalten)
- Für Anforderungen mit Prüfverfahren „Produktgutachten“ aber zwingend obige Prüfmethoden (Ausnahmen müssen detailliert begründet werden)

Sicherheitsgutachten ePA-FdV

elektronische Patientenakte (ePA)
Frontend des Versicherten - Sicherheitsgutachten

Ziel: Sicherstellen, dass der Hersteller des ePA-FdV sichere Produkte entwickeln kann

Prüfung der sicheren Software-Entwicklungsprozesse (Software Development Lifecycle)

- Prüfung von Prozessen und Methoden
- Prüfung, ob die Prozesse und Methoden umgesetzt sind
- Fokus auf Sicherheitsaktivitäten in den verschiedenen Entwicklungsphasen (z.B. Architektur, Implementierung, Test)

Orientierungshilfe

(https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/informative-beistellung-fuer-gutachter/)

- Für Entwickler und Sicherheitsgutachter
- Circa 80 Punkte
- OWASP Standards und Empfehlungen
- Es muss nicht alles erfüllt werden => Einschätzung des Gutachters

Produktgutachten ePA-FdV

elektronische Patientenakte (ePA)
Frontend des Versicherten - Produktgutachten

Zu prüfen sind alle Anforderungen des Produkttypsteckbriefs gemProdT_ePA_FdV des Abschnitts „3.2.1 CC-Evaluierung oder Produktgutachten“

- Anforderungen gelten für das gesamte ePA-FdV, d.h.
  - für die von der gematik spezifizierten ePA-Anteile und
  - grundsätzlich auch für die ggf. ebenfalls vorhandenen Zusatzfunktionen
- Pro eingesetzter Plattform (z.B. iOS, Android) wird ein eigenständiges Produktgutachten benötigt.

Die gematik stellt dem Produktgutachter begleitende Informationen bereit

(https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/informative-beistellung-fuer-gutachter/)

- Informationsblatt Gutachter ePA-FdV
  - Informationsblatt ePA-FdV Gutachter Zusatzfunktion
  - Impact Assessment Report ePA-FdV

elektronische Patientenakte (ePA)
Informationsblatt ePA-FdV Gutachter Zusatzfunktion

Begriffsdefinitionen

- Das ePA-FdV besteht aus **ePA-Funktionen** und ggf. **Zusatzfunktionen**

  - **ePA-Funktionen des ePA-FdV** umfassen alle Funktionen des ePA-FdV, die Teil des von der gematik in ihren Spezifikationen normierten Funktionsumfangs sind.
  - **Zusatzfunktionen des ePA-FdV** sind alle Funktionen des ePA-FdV außerhalb des von der gematik normierten Funktionsumfangs. Sie werden nicht von der gematik spezifiziert.

- **ePA-Modul**: ePA-Funktionen des FdV können in einem ePA-Modul gekapselt werden. Der Hersteller eines ePA-FdV kann einen anderen Hersteller mit der Entwicklung eines ePA-Moduls beauftragen und dessen ePA-Modul in sein ePA-FdV integrieren.
  Durch die gematik wird immer nur das gesamte ePA-FdV zugelassen, jedoch nicht das ePA-Modul. Für ePA-Module gibt es kein Zulassungs- oder Bestätigungsverfahren.

elektronische Patientenakte (ePA)
Informationsblatt ePA-FdV Gutachter Zusatzfunktion

gemInfo_ePA-FdV_Gutachter_Zusatzfunktionen#Spalte E zur Prüfung von Zusatzfunktionen

- **Produktgutachter**: die Anforderung muss auch für die Zusatzfunktionen gemäß dem Wortlaut der Anforderung umgesetzt werden

- **Produktgutachter (x)**:
  - Die Anforderung kann abweichend vom Wortlaut der Anforderung alternativ umgesetzt werden.
  - Der Produktgutachter prüft, ob durch die abweichende Umsetzung dennoch ein ausreichendes Sicherheitsniveau für das ePA-FdV erreicht wird.
  - Der Produktgutachter muss im Produktgutachten explizit beschreiben, warum durch die alternative Umsetzung dennoch ein ausreichendes Sicherheitsniveau erreicht wird

- **Für Zusatzfunktionen irrelevant**:
  - Der Hersteller des ePA-FdV kann bei diesen Anforderungen den Produktgutachter darüber begründet informieren, dass diese Anforderungen für die Zusatzfunktionen seines ePA-FdV nicht relevant sind.
  - Es liegt in der Verantwortung des Gutachters, inwieweit er dies nachprüft.

elektronische Patientenakte (ePA)
Integration mit dem Signaturdienst

Im ePA-FdV wird für al.vi eine Komponente integriert, mit der sich Versicherte am Signaturdienst authentisieren können.

- Im Produktgutachten für das ePA-FdV wird begutachtet, dass die Komponente für die al.vi-Authentisierung sicher implementiert wurde und
  - alle Anforderungen des Steckbriefs für das ePA-FdV erfüllt,
  - alle Voraussetzungen im ePA-FdV erfüllt sind, die die Komponente für die al.vi-Authentisierung erwartet.

- Im Produktgutachten für das ePA-FdV wird nicht begutachtet, ob das implementierte Authentisierungsverfahren für al.vi die Anforderungen des Steckbriefs des Signaturdienstes erfüllt. Dies erfolgt im Sicherheitsgutachten des Signaturdienstes.

Integration eines ePA-Moduls

elektronische Patientenakte (ePA)
Integration eines ePA-Moduls eines anderen Hersteller

Szenario: das ePA-FdV integriert ein ePA-Modul eines anderen Herstellers, das die ePA-Funktionen implementiert.

- Die Gutachter geben immer eine Sicherheitsaussage über das **gesamte ePA-FdV**, einschließlich eines ggf. integrierten ePA-Moduls. Das Votum im Sicherheits- und Produktgutachten gilt immer für das gesamte ePA-FdV.

- Die Gutachter des ePA-FdV müssen sich daher davon überzeugen, dass
  - das integrierte ePA-Modul alle Anforderungen an das Produkt erfüllt **und**
  - der Hersteller des ePA-Moduls alle Anforderungen an den sicheren Softwareentwicklungsprozess umsetzt.

elektronische Patientenakte (ePA)
Integration eines ePA-Moduls eines anderen Hersteller

Szenario: das ePA-FdV integriert ein ePA-Modul eines anderen Herstellers, das die ePA-Funktionen implementiert.

- Wurde das ePA-Modul bereits durch einen (anderen) Gutachter geprüft, können die ePA-FdV-Gutachter entscheiden, ob und inwieweit sie die Prüfergebnisse für die Prüfung des ePA-FdV heranziehen und nachnutzen.

- Der Produktgutachter muss insbesondere prüfen, ob ein geprüftes ePA-Modul tatsächlich auch im ePA-FdV integriert und im ePA-FdV korrekt genutzt wird.

- Der Sicherheitsgutachter muss sich davon überzeugen, dass auch die Entwicklungsprozesse des Herstellers des integrierten ePA-Moduls die Anforderungen erfüllen.

- Die Gutachter müssen im Produkt- und Sicherheitsgutachten für das ePA-FdV beschreiben, falls bereits vorhandenen Prüfungen herangezogen wurden.

Neubegutachtung

elektronische Patientenakte (ePA)
Neubegutachtung

Sicherheitsgutachten

- Es gelten die allgemeinen Regeln gemäß „Verfahrensbeschreibung Bestätigung Sicherheitsgutachten“ [gemZul_Best_SiGu]
- **Periodische Wiederholung** nach 3 Jahren
- **Wiederholung aufgrund wesentlicher** technischer oder organisatorischer **Änderungen**, welche die Erfüllung der Anforderungen des Produkttyps betreffen.

Produktgutachten

- Es gelten die speziellen Regeln gemäß „Verfahrensbeschreibung Zulassung Produkte der Telematikinfrastruktur: ePA-Frontend des Versicherten [gemZul_Prod_ePA_FdV]
- **Periodische Wiederholung** nach 3 Jahren
- **Wiederholung aufgrund wesentlicher Änderungen**
  - Der Hersteller entscheidet auf Grundlage eines **Impact-Assessment-Reports** auf Grundlage der in [gemZul_Prod_ePA_FdV] vorgegebenen Kriterien, ob eine erneute Produktbegutachtung erforderlich ist.
  - Ist eines der Kriterien erfüllt, muss der Hersteller eine Neubegutachtung veranlassen.
- Stichprobenartige Überprüfung der Impact-Assessment-Reports bei Folgebegutachtungen

elektronische Patientenakte (ePA)
Neubegutachtung bei wesentlichen Änderungen - Produktgutachten

Eine Änderung ist **wesentlich**, wenn eines der folgenden Kriterien erfüllt ist (vgl. gemZul_Prod_ePA_FdV):

- Änderungen der Sicherheitsfunktionen zur sicheren Datenspeicherung auf dem Endgerät des Versicherten
- Änderungen der Sicherheitsfunktionen zur Kryptographie (z. B. TLS-Cypher Suite, Schlüsselmanagement)
- Änderung der Sicherheitsfunktionen zur Authentifizierung mit Auswirkungen auf das ePA-FdV
- Änderung der Sicherheitsfunktionen der Kommunikation mit Diensten
- Änderung der Sicherheitsfunktionen zur Interaktion mit anderen Apps und der mobilen Plattform.
- Änderung der Sicherheitsfunktionen zur Manipulationssicherheit/Resilienz des ePA-FdV
- Änderung der Sicherheitsfunktionen zur Autorisierung mit Auswirkungen auf das ePA-FdV
- Änderung von Funktionen, die den Anforderungen des Steckbriefs [gem-ProdT_ePA_FdV], sicherheitstechnische Eignung – Produktgutachten unterliegen.

BSI-Prüfvorschrift für das ePA-FdV

Disclaimer & Quellen

Das enthaltene Bildmaterial ist urheberrechtlich geschützt. Diese Unterlage dient der Information des Empfängers. Eine Nutzung dieser Unterlage inklusive des Bildmaterials zu anderen Zwecken ist daher nicht gestattet.