Elektronische Gesundheitskarte und Telematikinfrastruktur

Informationsblatt Sicherheits- und Produktgutachten ePA-FdV

Version: 1.0.0
Stand: 04.05.2020

Informationsblatt für Gutachter des ePA-FdV

Dieses Informationsblatt enthält Informationen an Sicherheits- und Produktgutachter eines ePA-FdV.

1.1 Begriffsdefinitionen

Folgende Begriffe werden im Dokument verwendet.

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-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.

Hinweis: Die Gutachter geben immer eine *Sicherheitsaussage über das gesamte ePA-FdV, einschließlich eines ggf. integrierten ePA-Moduls*.

1.2 Produktgutachten: Sicherheitsnachweis bei Zusatzfunktionen

Grundlage für die folgenden Ausführungen ist die Tabelle „Infoblatt_ePA-FdV_Gutachter_Zusatzfunktionen". Alle Anforderungen dieser Liste sind im Produkttypsteckbrief des ePA-FdV dem sicherheitstechnischen Nachweis „Produktgutachten" zugeordnet.

Bei den in Spalte E mit „für Zusatzfunktionen irrelevant" markierten Anforderungen kann der Hersteller des ePA-FdV den Produktgutachter darüber informieren, dass diese Anforderungen für die **Zusatzfunktionen** seines ePA-FdV nicht relevant sind. Die Anforderungen sind für Zusatzfunktionen nicht relevant, falls die Zusatzfunktionen die in den Anforderungen adressierten Funktionen nicht enthalten. In diesem Fall ist dies vom Hersteller gegenüber dem Produktgutachter zu begründen.

Es obliegt dem Produktgutachter, inwieweit er diese Information des Herstellers bei der Prüfung des ePA-FdV berücksichtigt und in sein Produktgutachten einfließen lässt. Dies liegt in der Verantwortung des Produktgutachters. Der Produktgutachter kann, wenn es aus seiner Sicht erforderlich ist, nachprüfen, ob Anforderungen tatsächlich nicht für Zusatzfunktionen des ePA-FdV relevant sind. Mit dem Produktgutachten gibt der Produktgutachter eine Sicherheitsaussage über das gesamte ePA-FdV, einschließlich der Zusatzfunktionen.

Die in Spalte E mit „Produktgutachter (x)" markierten Anforderungen können für die **Zusatzfunktionen des ePA-FdV** vom Hersteller abweichend vom Wortlaut der Anforderung umgesetzt werden. Es ist in diesem Fall vom Produktgutachter zu prüfen, ob durch die abweichende Umsetzung dennoch ein ausreichendes Sicherheitsniveau für das ePA-FdV erreicht wird. Der Produktgutachter muss im Produktgutachten explizit

beschreiben, wenn eine abweichende Umsetzung der Anforderung für die Zusatzfunktion vom Hersteller gewählt wurde und begründen, warum dennoch ein auseichendes Sicherheitsniveau erreicht wird.

Die in Spalte E mit „Produktgutachter" markierten Anforderungen müssen auch für die Zusatzfunktionen gemäß dem Wortlaut der Anforderung umgesetzt werden. Die Umsetzung muss durch den Produktgutachter geprüft werden. Eine abweichende Umsetzung ist für diese Anforderungen nicht erlaubt.

Für die **ePA-Funktionen des ePA-FdV** müssen alle Anforderungen ausnahmslos gemäß ihrem Wortlaut umgesetzt und durch den Produktgutachter geprüft werden (Spalte D). Eine abweichende Umsetzung ist für ePA-Funktionen des ePA-FdV nicht erlaubt.

1.3 Produktgutachten: Prüfung der Impact-Assessment Reports

Der Hersteller des ePA-FdV ist verpflichtet, für jede Änderung am ePA-FdV in einem Impact-Assessment-Report darzustellen, ob die Änderung oder Abweichung wesentlich im Sinne der in der Zulassungsverfahrensbeschreibung aufgeführten Kriterien ist. Der Hersteller muss auf dieser Grundlage entscheiden, ob eine erneute Produktbegutachtung erforderlich ist.

Der Produktgutachter muss im Rahmen einer Wiederholung der Prüfung (insbesondere bei einem Folgeproduktgutachten) die während der letzten Prüfung erstellten Impact-Assessment-Reports des Herstellers stichprobenartig dahingehend prüfen, ob die vom Hersteller getroffenen Einschätzungen zur Notwendigkeit einer erneuten Produktbegutachtung nachvollziehbar sind. Der Produktgutachter hat das Ergebnis der Prüfung der Impact-Assessment-Reports im Produktgutachten zu dokumentieren.

1.4 Sicherheitsgutachten: Orientierungshilfe für Sicheren Softwareentwicklungsprozess

Grundlage für die folgenden Ausführungen ist die Tabelle „Orientierungshilfe SDL".

Die Orientierungshilfe unterstützt den Sicherheitsgutachter bei der Prüfung und Bewertung des sicheren Softwareentwicklungsprozesses des Herstellers des ePA-FdV. Gleichzeitig kann sie als Orientierung für den Hersteller des ePA-FdV dienen.

Die Orientierungshilfe enthält keine normativen Anforderungen, sondern beschreibt die grundsätzlichen Erwartungen der gematik an einen sicheren Softwareentwicklungsprozess. Der sichere Softwareentwicklungsprozess des ePA-FdV-Herstellers kann von dieser Orientierungshilfe abweichen. Es obliegt der Einschätzung des Sicherheitsgutachters, ob dennoch die Entwicklung von sicheren ePA-FdV durch den Hersteller gewährleistet wird.

1.5 Prüfung bei Nutzung eines ePA-Moduls

Integriert der Hersteller des ePA-FdVs ein ePA-Modul eines anderen Herstellers, müssen sich die Gutachter des ePA-FdV davon überzeugen, dass

- das integrierte ePA-Modul alle Anforderungen an das Produkt und
- der Hersteller des ePA-Moduls alle Anforderungen an den sicheren Softwareentwicklungsprozess

umsetzen. Das Sicherheits- und das Produktgutachten gilt immer für das gesamte ePA-FdV inklusive eines ggf. integrierten ePA-Moduls.

Der Produkt- bzw. Sicherheitsgutachter kann bei der Prüfung des ePA-FdV die bei einem integrierten ePA-Modul bereits durchgeführten Prüfungen nachnutzen. Es obliegt dabei den Gutachtern, inwieweit diese die bereits beim ePA-Modul durchgeführten Prüfungen sowie die bereits beim Hersteller durchgeführten Prüfungen des sicheren Softwareentwicklungsprozesses in ihre Gutachten einfließen lassen und inwieweit sie selbst die Umsetzung nochmals prüfen. Dies liegt in der Verantwortung des Produkt- bzw. Sicherheitsgutachters. Mit dem Produkt- und Sicherheitsgutachten geben die Gutachter eine Sicherheitsaussage über das gesamte ePA-FdV, einschließlich des ePA-Moduls.

Im Gutachten ist explizit zu dokumentieren, ob ein ePA-Modul eines anderen Herstellers eingesetzt wird und ob für dieses bereits eine Prüfung durch Gutachter erfolgte. Es ist zu dokumentieren, welche Anforderungen des ePA-FdV im Kontext des ePA-Moduls bereits geprüft wurden und inwieweit der Gutachter des ePA-FdV die Prüfung des ePA-Moduls bei der Prüfung des ePA-FdV berücksichtigt und warum die Prüfung ausreichend war.

Der Produktgutachter muss prüfen, ob das geprüfte ePA-Modul tatsächlich auch im ePA-FdV integriert und im ePA-FdV korrekt genutzt wird.

1.6 Sicherheitsgutachten: Prüfung der Entwicklungsprozesse bei Nutzung von Komponenten anderer Hersteller

Wenn der Hersteller des ePA-FdV Komponenten für sein ePA-FdV beauftragt und nicht selbst entwickelt, muss der Sicherheitsgutachter dies im Sicherheitsgutachten dokumentieren und begründen, warum die Anforderungen an den sicheren Entwicklungsprozess auch bei den beauftragten Herstellern umgesetzt werden. Es obliegt dem Sicherheitsgutachter, durch welche Prüfmethoden er sich davon überzeugt.

Die Prozesse bei Herstellern gängiger und etablierter Standardsoftwarekomponenten (z.B. Bibliotheken und Frameworks) muss der Sicherheitsgutachter nicht prüfen. Die Prüfung bezieht sich insbesondere auf Hersteller von Softwarekomponenten, die speziell fürs ePA-FdV beauftragt und vom beauftragten Hersteller speziell für das ePA-FdV entwickelt werden.

1.7 Anlagen

- Tabelle „Infoblatt_ePA-FdV_Gutachter_Zusatzfunktionen“
- Orientierungshilfe SDL
- Muster „Impact-Assesment-Report“ (ePA-FdV-IAR)