Elektronische Gesundheitskarte und Telematikinfrastruktur

Feature: ePA-Frontend des Versicherten in der Ausprägung als stationärer Desktop-Client

Version:	1.0.0 CC
Revision:	352134
Stand:	30.03.2021
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemF_ePA_Stat_FdV

Dokumentinformationen

Beim vorliegenden Dokument handelt es sich um einen Entwurf in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik versendet diesen Entwurf mit dem Ziel, dass sich Interessierte vorab einen Überblick zur möglichen Weiterentwicklung der Anwendung elektronische Patientenakte verschaffen können.

Die gematik übernimmt keine Gewähr für Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfs. Die gematik behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt oder teilweise Abstand zu nehmen.

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.1.0	18.02.21		initiale Erstellung	gematik
1.0.0 CC	30.03.21		zur Abstimmung freigegeben	gematik

Inhaltsverzeichnis

1 Motivation des Features

Gemäß § 338 Abs. 1 DVPMG haben zur Wahrung der Versichertenrechte die Krankenkassen bis spätestens zum 1. Januar 2022 ihren Versicherten eine Komponente für stationäre Endgeräte zur Verfügung zu stellen. Damit ergeben sich für Versicherte ohne Smartphone die folgenden äquivalenten Nutzungsszenarien:

- Zugriff auf Zugriffsprotokolle der ePA (Verwaltungs- und § 291a-Protokoll)
- Erteilung von Berechtigungen zum Zugriff der Daten durch Leistungserbringer

Dieses Feature-Dokument beschreibt das ePA-Frontend des Versicherten (ePA-FdV) in der Ausprägung als Desktop-Client (ePA-FdV *für Desktop-Plattformen*) für die Ausführung auf einem PC des Versicherten. Der Desktop-Client umfasst eine analoge Funktionalität wie in [gemSpec_ePA_FdV] beschrieben. Ein wesentliches Unterscheidungsmerkmal ist, dass im Gegensatz zu Smartphones am PC angebundene Kartenleser üblich sind.

In diesem Feature-Dokument werden technisches Konzept sowie Anforderungen beschrieben, die zusätzlich zu den Anforderungen in [gemSpec_ePA_FdV] gelten. Nach erfolgter Abstimmung mit allen beteiligten Partnern werden diese nach [gemSpec_ePA_FdV] übertragen. Der Produkttypsteckbrief [gemProdT_ePA_FdV] umfasst zukünftig somit Anforderungen einer Ausprägung des ePA-FdV auf Smartphones als auch PCs mit gleichen Zulassungsprozessen.

1.1 Zielsetzung

Die Beschreibungen in diesem Dokument erleichterten das Verständnis zum Funktionsumfang und lassen Unterschiede hinsichtlich des ePA-FdV für Smartphones nachvollziehen.

1.2 Zielgruppe

Das Dokument richtet sich an Krankenkassen sowie Hersteller und Anbieter eines Desktop-Clients.

1.3 Abgrenzungen

Nicht Bestandteil dieses Feature-Dokuments sind die bereits in der [gemSpec_ePA_FdV] enthaltenen Anforderungen, die bei der Entwicklung des Desktop-Clients ebenfalls zu berücksichtigen sind – sie gelten additiv. Weiterhin ist das Feature "Patienten-Kurzakte", wofür Krankenkassen ihren Versicherten ab dem 1. Januar 2023 ebenfalls eine Interaktionskomponente bereitzustellen haben, nicht Bestandteil dieses Dokuments.

1.4 Methodik

1.4.1 User Story

User Stories werden durch eine eindeutige ID gekennzeichnet und werden im Dokument wie folgt dargestellt:
<USt-ID> - <Zusammenfassung der User Story>
Text / Beschreibung
[<=]

Dabei umfasst die User Story sämtliche zwischen USt-ID und der Textmarke [<=] angeführten Inhalte.

1.4.2 Anforderungen

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen." die Phrase „DARF NICHT" semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird in diesem Dokument stattdessen „Eine leere Liste DARF KEIN Element besitzen." verwendet. Die Schlüsselworte werden außerdem um Pronomen in Großbuchstaben ergänzt, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

Anforderungen werden im Dokument wie folgt dargestellt:
<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und Textmarke [<=] angeführten Inhalte.

2 Epic und User Stories

Ein Versicherter hat seine Krankenkasse beauftragt, ihm eine elektronische Patientenakte bereitzustellen (Kontoinitialisierung). Dabei wurde die Einwilligung des Versicherten zur Datenverarbeitung gegenüber dem Anbieter sowie in die Nutzung der ePA gegenüber dem Anbieter eingeholt und dokumentiert. Die Krankenkasse hat dem Versicherten weiterhin Hinweise für den Bezug und die Installation eines ePA-FdV als Smartphone App sowie als Desktop-Client gegeben. Der Versicherte entscheidet sich für die spätere Nutzung der ePA mittels Desktop-Client. Ein handelsübliches Kartenlesegerät für das Auslesen seiner eGK hat sich der Versicherte im Internet bestellt.

Nach der erfolgreichen Installation möchte der Versicherte seine Akte nun aktivieren und alle Geschäftsprozesse ausführen (Dokumente hoch- und herunterladen; Berechtigungen für Leistungserbringer, Vertreter, Krankenkassen sowie DiGAs vergeben; Protokolle einsehen etc.).

2.1 User Stories

Im folgenden Abschnitt werden nur diejenigen User Stories berücksichtigt, welche noch nicht oder in veränderter Weise über bereits in [gemSpec_ePA_FdV] avisierte Use Cases adressiert sind.

USt-1 - Mehrbenutzerfähigkeit des Desktop Clients

Als Versicherter möchte ich, dass meine Familienmitglieder den Desktop-Client am selben PC gleichermaßen für ihre ePA nutzen. [<=]

3 Technisches Konzept

Wie auch die Ausprägung des ePA-FdV auf einem Smartphone ordnet sich der Desktop-Client auf dem Gerät des Versicherten ein. Ein Desktop-Client nutzt dieselben Schnittstellen und implementiert dasselbe Verhalten wie auch die Smartphone-Variante. Das ePA-FdV kann Kartenleser der Sicherheitsklassen 1, 2 oder 3 benutzen. Die in [gemSpec_ePA_FdV#6.3.1] festgelegten Vorgaben gelten in vollem Umfang auch für die an das GdV angeschlossenen Kartenleser, unabhängig von der Art, wie der Kartenleser an das GdV angeschlossen wurde. Neben proprietären Schnittstellentreibern von Kartenleserherstellern existieren eine Reihe standardisierter Schnittstellen, die auch von verschiedenen Betriebssystemen zur Anbindung handelsüblicher Kartenleser unterstützt werden. Aber auch eine optionale, alternative Anmeldung per al.vi-Identität ist weiterhin möglich.

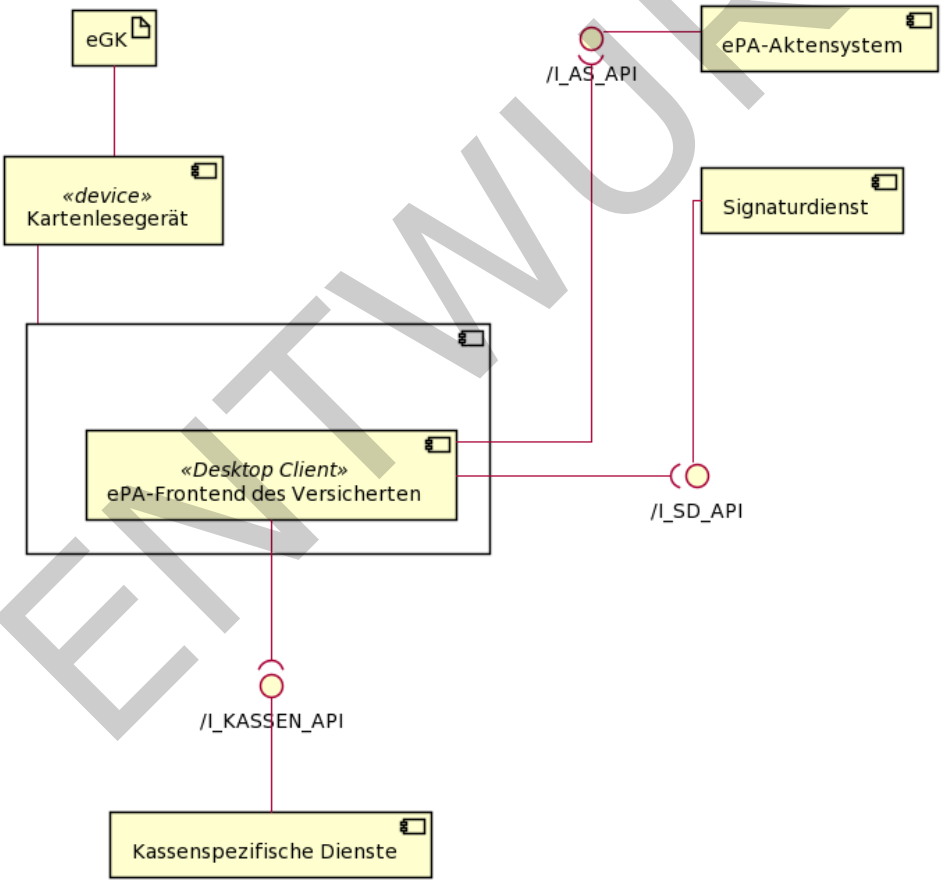

Abbildung 1 UML-Komponentendiagramm ePA-FdV für Desktop-Plattformen

4 Spezifikation

Als Delta zur den Spezifikationsanforderungen aus [gemSpec_ePA_FdV] werden in diesem Kapitel die folgenden, weiteren Anforderungen an den Funktionsumfang eines ePA-FdV *für Desktop-Plattformen* gestellt.

4.1 Funktionale Anforderungen

A_21358 - ePA-FdV für Desktop-Plattformen: Mehrbenutzerfähigkeit des Desktop-Clients
Das ePA-FdV MUSS die Ausführung der Aktensteuerung über verschiedene, lokale Benutzerkonten des Betriebssystems oder alternativ eine FdV-interne Benutzer-Kontensteuerung ermöglichen.**[<=]**

A_21301 - ePA-FdV: Kein Ausführen von aktiven Inhalten bei der Anzeige
Das ePA-FdV DARF bei der Anzeige von Dokumenten aktive Elemente NICHT ausführen. **[<=]**

4.2 Datenschutz und Sicherheit

Unter den unterstützten Plattformen, auf denen das ePA-FdV lauffähig ist, kann es stationäre Nutzer-Endgeräte (PC, Laptop) geben, die eine Desktop-Nutzeroberfläche aufweisen. Der Produktgutachter muss schildern, auf welchen Betriebssystem-Plattformen das ePA-FdV lauffähig ist.

A_21342 - ePA-FdV: Anzeige eines Hinweistextes zum Betrieb auf Hardware, die nicht unter der Kontrolle des Versicherten steht
Das ePA-FdV MUSS den Versicherten in einem Hinweistext darauf hinweisen, dass der Betrieb des ePA-FdV auf Hardware, die nicht unter der Kontrolle des Versicherten steht, verboten ist.**[<=]**

Hinweis: Im Gegensatz zu Betriebssystem für Smartphones und Tablets wie etwa Android und iOS sind Betriebssysteme für stationäre Geräte wie etwa PCs durchaus im öffentlichen Raum verfügbar. So läuft etwa auf den meisten Geräten in Internet-Cafes Windows. Würde hier das ePA-FdV ausgeführt werden und der Versicherte sich Dokumente aus seiner Akte herunterladen, dann muss der Versicherte dafür sorgen, dass keine Daten von ihm auf der Hardware verbleiben, wenn er den Zugriff auf die Hardware beendet. Das ePA-FdV ist in der derzeitigen Version für einen Betrieb auf öffentlich zugänglicher Hardware nicht vorgesehen

A_21343 - ePA-FdV: Ausführen von begutachtetem Code
Der Hersteller des ePA-FdV MUSS technisch sicherstellen, dass nur im Rahmen eines Produktgutachtens begutachteter Code ausgeführt wird oder Code-Änderungen nach Vorgaben der gematik durch den Hersteller des ePA-FdV als nicht zulassungsrelevant bewertet wurden.**[<=]**

Hinweis: Die Anforderung soll das Einschleusen von Schadcode verhindern. Dies kann beispielsweise durch Signieren des ePA-FdV durch den Hersteller erfolgen, um Manipulationen am ePA-FdV vor der Ausführung erkennen zu können. Das Verbot des dynamischen Nachladens von ungeprüftem Code soll insbesondere auch sicherstellen, dass zum Zeitpunkt der Prüfung des ePA-FdV durch den Produktgutachter der gesamte

Anwendungscode vorliegt und dieser nicht später durch ungeprüften Code ersetzt bzw. ergänzt werden kann.

Im Zulassungsverfahren für das ePA-FdV ist festgelegt, wann Änderungen durch die gematik als zulassungsrelevant betrachtet werden. Zulassungsrelevante Änderungen sind z.B. Änderungen von Sicherheitsfunktionen oder deren Implementierung (z.B. Wechsel der TLS-Implementierung). Nicht-zulassungsrelevante Änderungen sind z.B. Sicherheitsupdates für von anderen Herstellern bezogenen Software-Komponenten der Plattform (z.B. Bibliotheken), die aus einer vertrauenswürdigen Quelle bezogen werden.

A_21344 - ePA-FdV: Code von Drittanbietern aus vertrauenswürdigen Quellen
Der Hersteller des ePA-FdV MUSS die Software-Komponenten des ePA-FdV, die nicht vom Hersteller des ePA-FdV selbst entwickelt oder zur Entwicklung beauftragt werden (z.B. TLS-Bibliotheken), aus bekannten und vertrauenswürdigen Quellen beziehen. **[<=]**

A_21346 - ePA-FdV: Lokale Ausführung von Code
Das ePA-FdV MUSS sicherstellen, dass der Code für alle ePA-Funktionen des ePA-FdV ausschließlich lokal auf dem Gerät des Versicherten ausgeführt wird.**[<=]**

Hinweis: Der auszuführende Code für die ePA-Funktionen des ePA-FdV muss lokal vorliegen und ausgeführt werden, so dass insbesondere alle ePA-Daten (medizinische Daten, sicherheitskritische Daten wie Schlüssel) ausschließlich lokal verarbeitet werden. Zudem erschwert es Administratoren von Servern, auf denen der Code liegen könnte, den Code zu manipulieren.

Dies bedeutet insbesondere, dass eine Auslagerung von ePA-Funktionen auf Webserver nicht erlaubt ist. Dies verhindert jedoch nicht, das ePA-FdV mithilfe von Webtechnologien umzusetzen, um eine Plattformunabhängigkeit zu erreichen. Mithilfe des Frameworks *Electron* können beispielsweise in HTML, CSS und JavaScript entwickelte Anwendungen lokal unabhängig vom verwendeten Betriebssystem (Windows, MacOS, Linux) ausgeführt werden. *Electron* bietet auch die Möglichkeit der Nutzung von *WebAssembly*.

A_21354 - ePA-FdV: für Desktop-Plattformen: Schutz von gespeicherten Authentisierungsmerkmalen
Das ePA-FdV für Desktop-Plattformen MUSS sicherstellen, dass Authentisierungsmerkmale ausschließlich unter folgenden Bedingungen gespeichert werden:

- der Versicherte entscheidet sich hierfür bewusst (Opt-in),
- die Speicherung des Authentisierungsmerkmals auf dem Endgerät des Versicherten erfolgt ausschließlich verschlüsselt,
- auf das verschlüsselte gespeicherte Authentisierungsmerkmal kann ausschließlich nach erfolgreicher Authentifizierung des Versicherten über ein Passwort bzw. eine Passphrase zugegriffen werden.

[<=]

Hinweis: Dies ist die analoge Anforderung zu A_20211-01 bei mobilen Endgeräten.

A_21355 - ePA-FdV: Zugriff auf den Geräteidentifikator durch Zusatzfunktionen
Das ePA-FdV DARF Zusatzfunktionen des FdV (d.h. kassenspezifische Dienste) NICHT auf den Geräteidentifikator (die von der Autorisierung übermittelte Zufallszahl bei der Gerätebindung) zugreifen lassen.**[<=]**

A_21356 - ePA-FdV: Speicherung des Geräteidentifikators
Das ePA-FdV MUSS sicherstellen, dass die Speicherung des Geräteidentifikators (die von der Autorisierung übermittelte Zufallszahl bei der Gerätebindung) ausschließlich verschlüsselt erfolgt.**[<=]**

A_21357 - ePA-FdV: Zugriff auf den Geräteidentifikator
Das ePA-FdV MUSS sicherstellen, dass auf den verschlüsselten gespeicherten Geräteidentifikator ausschließlich nach erfolgreicher Authentifizierung des Versicherten beim Start des ePA-FdV zugegriffen werden darf.**[<=]**

Hinweis: Nach A_20746 muss sich der Nutzer beim Starten des ePA-FdV am ePA-FdV authentisieren.

A_21350 - ePA-FdV: Informieren des Versicherten über sichere Bezugsquellen für die Verteilung des FdV
Der Hersteller des ePA-FdV MUSS Versicherte über die vertrauenswürdigen Quellen informieren, von denen Versicherte das ePA-FdV beziehen können und wie sie die Vertrauenswürdigkeit der Quelle erkennen können.**[<=]**

Hinweis: Krankenkassen (als Anbieter eines ePA-Aktensystems) können zur Umsetzung dieser Anforderung z.B. den Versicherten hierzu entsprechendes Informationsmaterial zur Verfügung stellen, wo die Download-Punkte aufgelistet sind.

A_21351 - ePA-FdV: Sicherstellung der Authentifizierung der Bezugsquelle bei Erstbezug
Der Hersteller des ePA-FdV MUSS sicherstellen, dass der Versicherte bei Erstbezug eines ePA-FdV die Authentizität der vertrauenswürdigen Bezugsquelle verifizieren kann.**[<=]**

Hinweis: Beim Erstbezug des ePA-FdV kann die Prüfung der Authentizität der Quelle noch nicht durch das ePA-FdV selbst erfolgen. Dies kann z.B. über eine TLS-Server-Authentifizierung der Bezugsquelle erreicht werden. Bei ePA-FdVs in den Stores der mobilen Plattformen kann der Versicherte die Vertrauenswürdigkeit daran erkennen, dass er den offiziellen Store nutzt. Auch unter Windows und Mac OS und Linux/Debian gibt es einen offiziellen Store.

A_21352 - ePA-FdV: Technische Authentifizierung der Update-Bezugsquellen für die sichere Verteilung der ePA-FdV-Anwendung
Das ePA-FdV MUSS sicherstellen, dass Updates nur von bekannten und vertrauenswürdigen Quellen bezogen werden, nach dem die Authentizität der Quelle technisch erfolgreich verifiziert wurde.**[<=]**

4.3 Betrieb

Es werden keine gesonderten Anforderungen an den Betrieb des ePA-FdV als Desktop-Client erhoben.

4.4 Test

An die Testtreiberschnittstelle werden keine zusätzlichen Anforderungen gestellt. Weitere Unterstützungsleistungen für den Test sind nicht erforderlich.

5 Änderungen an Produkt- und Anbietertyp-Steckbriefen

Es sind keine Änderungen an vorhandenen Produkt- und Anbietertyp-Steckbriefen zur Fachanwendung ePA vorgesehen. Für die oben genannten neuen Anforderungen werden die nachstehenden Prüfverfahren im Produkttypt-Steckbrief [gemProdT_ePA_FdV] definiert.

Afo-ID	Afo Titel	Prüfverfahren
A_21358	ePA-FdV für Desktop-Plattformen: Mehrbenutzerfähigkeit des Desktop-Clients	funkt. Eignung: Herstellererklärung, funkt. Eignung: Test Produkt/FA
A_21356	ePA-FdV: Speicherung des Geräteidentifikators	Sich.techn. Eignung: Produktgutachten
A_21355	ePA-FdV: Zugriff auf den Geräteidentifikator durch Zusatzfunktionen	Sich.techn. Eignung: Produktgutachten
A_21357	ePA-FdV: Zugriff auf den Geräteidentifikator	Sich.techn. Eignung: Produktgutachten
A_21352	ePA-FdV: Technische Authentifizierung der Update-Bezugsquellen für die sichere Verteilung der ePA-FdV-Anwendung	funkt. Eignung: Herstellererklärung, Sich.techn. Eignung: Produktgutachten
A_21354	ePA-FdV: für Desktop-Plattformen: Schutz von gespeicherten Authentisierungsmerkmalen	Sich.techn. Eignung: Produktgutachten
A_21350	ePA-FdV: Informieren des Versicherten über sichere Bezugsquellen für die Verteilung des FdV	funkt. Eignung: Herstellererklärung
A_21351	ePA-FdV: Sicherstellung der Authentifizierung der Bezugsquelle bei Erstbezug	funkt. Eignung: Herstellererklärung, Sich.techn. Eignung: Produktgutachten
A_21346	ePA-FdV: Lokale Ausführung von Code	Sich.techn. Eignung: Produktgutachten
A_21344	ePA-FdV: Code von Drittanbietern aus vertrauenswürdigen Quellen	Sich.techn. Eignung: Produktgutachten
A_21343	ePA-FdV: Ausführen von begutachtetem Code	Sich.techn. Eignung: Produktgutachten
A_21342	ePA-FdV: Anzeige eines Hinweistextes zum Betrieb auf Hardware, die nicht unter der Kontrolle des Versicherten steht	funkt. Eignung: Herstellererklärung, funkt. Eignung: Test Produkt/FA
A_21301	ePA-FdV: Kein Ausführen von aktiven Inhalten bei der Anzeige	Sich.techn. Eignung: Produktgutachten

6 Beispiele und Referenzimplementierungen

Diesem Feature sind keine Beispiele oder Referenzimplementierungen beigefügt.

7 Anhang A – Verzeichnisse

7.1 Abkürzungen

Kürzel	Erläuterung
DVPMG	Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz
ePA-FdV	ePA-Frontend des Versicherten
GdV	Geräte des Versicherten
OWASP	Open Web Application Security Project
TLS	Transport Layer Security

7.2 Referenzierte Dokumente

7.2.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	**Herausgeber: Titel**
[gemProdT_ePA_FdV]	gematik: Produkttypsteckbrief ePA-Frontend des Versicherten
[gemSpec_ePA_FdV]	gematik: Spezifikation ePA-Frontend des Versicherten

7.2.2 Weitere Dokumente

[Quelle]	**Herausgeber (Erscheinungsdatum): Titel**

[RFC2119]	IETF (1997): Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, http://tools.ietf.org/html/rfc2119
[OWASPTop10]	OWASP Foundation (2017): OWASP Top 10 Web Application Security Risks, https://owasp.org/www-project-top-ten/

298