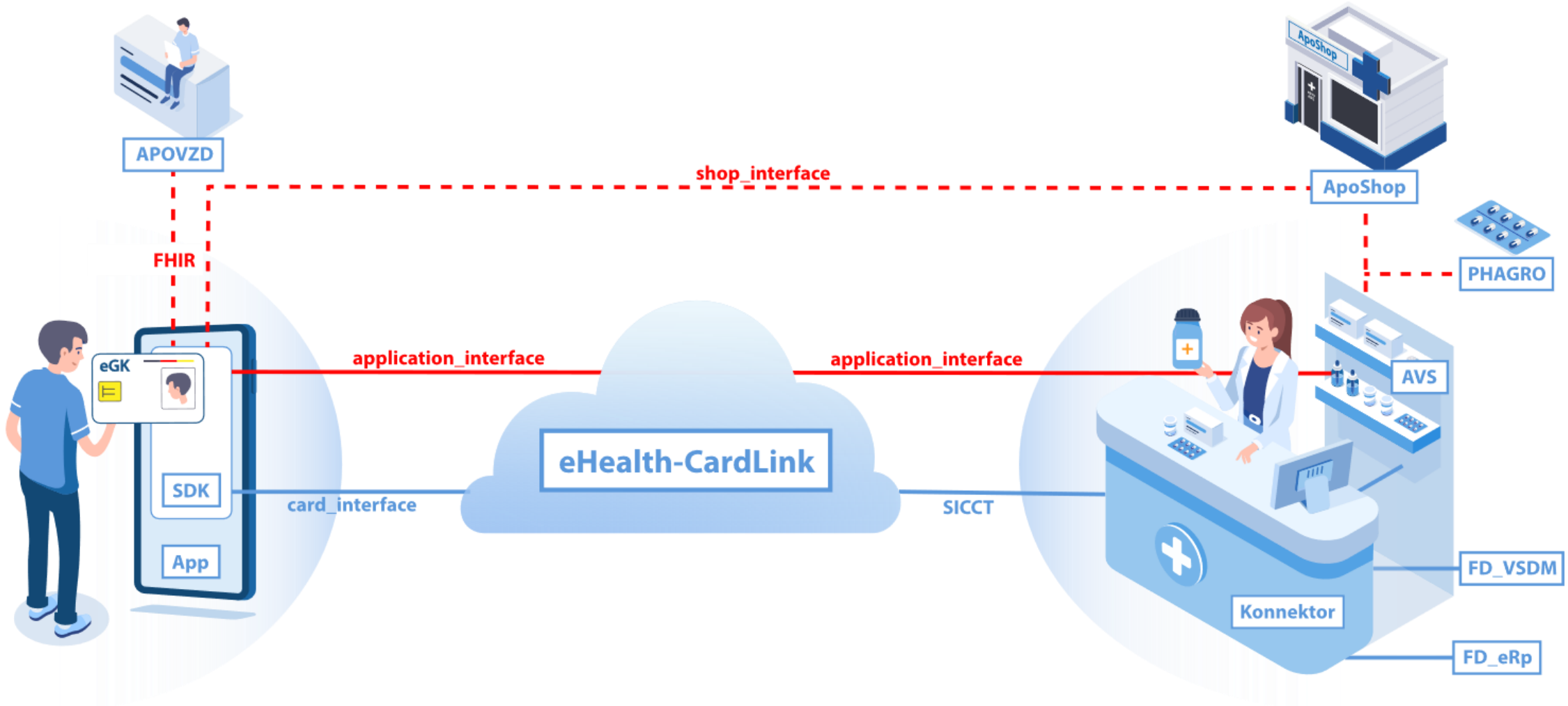
eHealth-CardLink – mit einem konstruktiven Vorschlag zur klugen Förderung der GesundheitsID

04. September 2024

Agenda

- **eHealth-CardLink**
- Problemstellung
- Vorschlag zur Förderung der GesundheitsID

eHealth-CardLink im Überblick



eHealth-CardLink - Generische Basisspezifikation

▼ **Inhaltsverzeichnis**

Über dieses Dokument
Versionierung
1. - **Einleitung**
    1.1 - Zielsetzung
    1.2 - Methodik
2. - **Generische Basisspezifikation**
    2.1 - Überblick
    2.2 - Grundlegende Abläufe beim eHealth-CardLink-Verfahren
    2.2.1 - Phase 0 - Vorbereitende Schritte und SMS-TAN-Verfahren
    2.2.2 - Phase 1 - eGK mit App kontaktieren und Daten auslesen
    2.2.3 - Phase 2 - Übermittlung der für den Prüfablauf relevanten Daten
    2.2.4 - Phase 3 - Das Primärsystem ruft ReadVSD am Konnektor auf
    2.2.5 - Phase 4 - Das Fachmodul VSDM startet die Onlineprüfung der eGK
    2.2.6 - Phase 5 - Das Fachmodul VSDM im Konnektor führt Onlineprüfung der eGK durch
    2.2.7 - Phase 6 - Das Fachmodul VSDM im Konnektor erstellt den Prüfungsnachweis
    2.2.8 - Phase 7 - Der Konnektor liefert den Prüfungsnachweis in ReadVSDResponse zurück
    2.3 - Nachrichten jenseits der gematik-Spezifikation
3. - **Anwendungsfallspezifische Ergänzungsmodule**
    3.1 - Generelle Anforderungen an das application_interface
    3.2 - Existierende und geplante anwendungsspezifische Ergänzungsmodule

Existierende und geplante anwendungsspezifische Ergänzungsmodule

Anhang	Version	Datum	Beschreibung des anwendungsspezifischen Ergänzungsmoduls
Anhang A	1.0.0 (RC)	01.07.2024	Einlösen von E-Rezepten in einer Apotheke
geplant			Zugriff auf ePA-Aktensystem für Arzneimittelinteraktionsprüfung
geplant			Anforderung eines Folgerezeptes
geplant			Entfernter Versicherungsnachweis
geplant			Ambulante Pflege
geplant			Stationäre Pflege
geplant			Videosprechstunde
geplant			Mobile Szenarien für Leistungserbringer (Notarzt, Rettungssanitäter etc.)

Anhang A - Einlösen von E-Rezepten

▼ **Inhaltsverzeichnis**

Über dieses Dokument
Versionierung
1. **A.1 Ablauf beim Einlösen von E-Rezepten**
    - A.1.0 - eHealth-CardLink-Basisablauf
    - A.1.1 - Phase 1 - Aufbau der Verbindung zum FD_eRp
    - A.1.2 - Phase 2 - Auslesen der verfügbaren E-Rezepte aus FD_eRp
    - A.1.3 - Phase 3 - Bereitstellen der E-Rezept-Informationen und Auswahl der zu dispensierenden Exemplare
    - A.1.4 - Phase 4 - Verbindliche Zuweisung der zu dispensierenden E-Rezepte an Apotheke
    - A.1.5 - Phase 5 - Signaturvalidierung, Dispensierung der E-Rezepte und Abschluss der Transaktion
2. **A.2 - Nachrichten jenseits der gematik-Spezifikationen**
    - A.2.1 - requestPrescriptionList
    - A.2.2 - availablePrescriptionLists
    - A.2.3 - selectedPrescriptionList
    - A.2.4 - selectedPrescriptionListResponse
3. **A.3 - In den Nachrichten enthaltene Datenelemente**
    - A.3.1 - coverage
    - A.3.2 - medication
    - A.3.2.1 - medicationPZN (KBV_PR_ERP_Medication_PZN)
    - A.3.2.2 - medicationIngredient (KBV_PR_ERP_Medication_Ingredient)
    - A.3.3.3 - medicationCompounding (KBV_PR_ERP_Medication_Compounding)
    - A.3.3.4 - medicationFreeText (KBV_PR_ERP_Medication_FreeText)
    - A.3.3 - organisation
    - A.3.4 - patient
    - A.3.5 - pobAddress
    - A.3.6 - person
    - A.3.7 - practiceSupply
    - A.3.8 - practitioner
    - A.3.9 - prescription
    - A.3.10 - prescriptionBundle
    - A.3.11 - prescriptionIndexList
    - A.3.12 - streetAddress

Agenda

- eHealth-CardLink
- **Problemstellung**
- Vorschlag zur Förderung der GesundheitsID

Bewusste Einschränkung des Anwendungsbereichs sinnvoll?

Anlage 2 zum Vertrag über die Zulassung als Anbieter eHealth-CardLink
Zusätzliche Regelungen

gematik

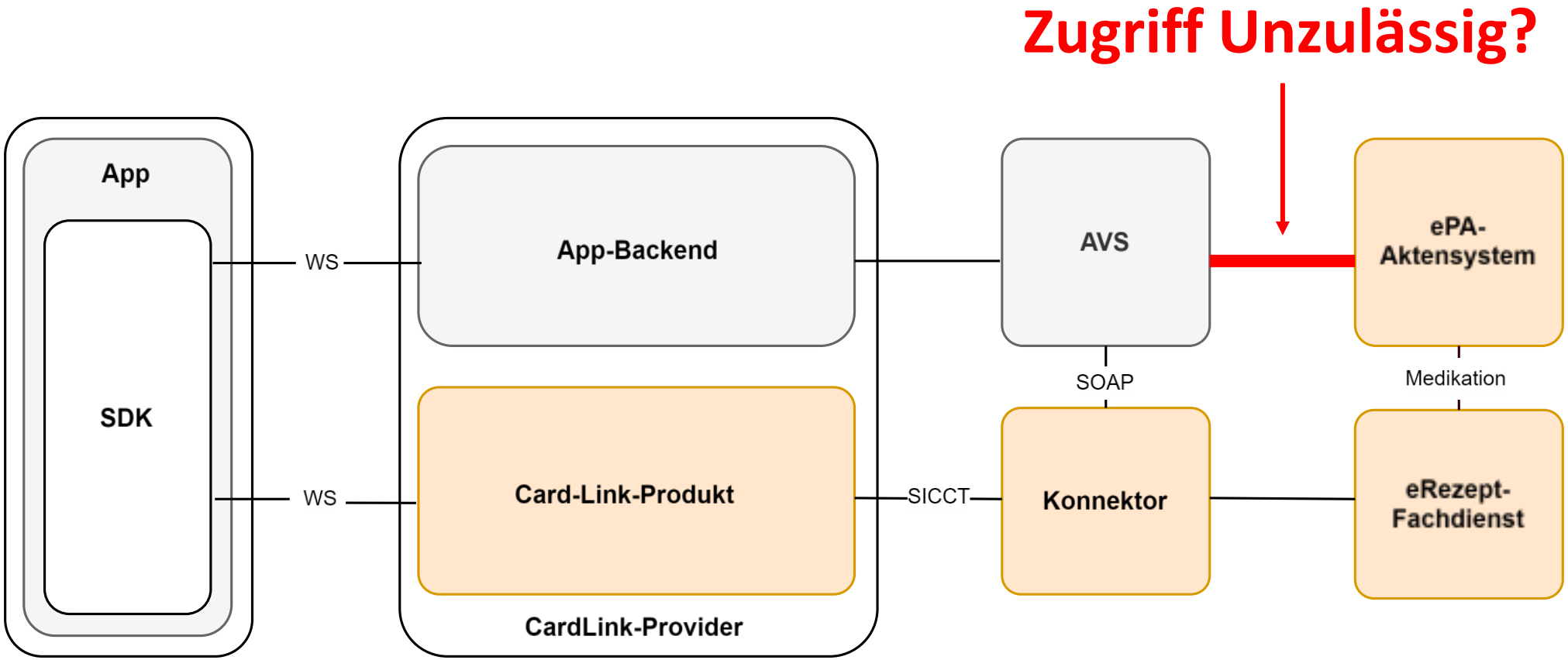
2 Anwendungsbereich eHealth-CardLink

Ziffer 1.1 (1) wird für die Anbieter eHealth-CardLink ergänzt durch folgende Regelungen:

a) Der Zulassungsnehmer darf den eHealth-CardLink ausschließlich im Anwendungsszenario gem. Ziffer 2.1 der gemSpec_eHealth-CardLink_V1.0.0 - Mobiles Erstellen eines VSDM-Prüfungsnachweises mit eGK ohne PIN verwenden, um E-Rezepte des Patienten vom Fachdienst abzurufen.

b) Der Zulassungsnehmer muss der Zulassungsstelle der gematik alle mit seinem eHealth-CardLink angebundenen Applikationen, deren Einsatzumgebungen (z.B. Smartphone) sowie den jeweiligen Zweck der Nutzung während der Vertragslaufzeit unverzüglich per eMail an Zulassung@gematik.de melden.

Kein Zugriff für Apotheke auf Medikation in ePA bei CardLink?!



Sicherheits- und Vertrauensniveaus gemäß eIDAS-Verordnung

- Art. 8 (EU) No 910/2014 (aka „eIDAS-Verordnung“)
- Durchführungsrechtsakt DFV (EU) 2015/1502 (Anhang)
- BSI TR-03107-1 („Elektronische Identitäten und Vertrauensdienste im E-Government“)

2.1 Anmeldung	2.2 Verwaltung elektronischer Identifizierungsmittel	2.3 Authentifizierung	2.4 Management und Organisation	
	Schutz gegen Duplizierung, **Fälschung** und gegen Angreifer mit „**hohem Angriffspotenzial**“ (2.2.1)	Sicherheit gegen Angreifer mit „**hohem Angriffspotenzial**“ (2.3.1)		**Hoch**
Verlässliche Quelle und Ausgabeprozesse bzw. entsprechend notifizierte Identifizierungsmittel	Mindestens **zwei Faktoren**, Nutzung nur unter Kontrolle des Besitzers (2.2.1)	**Dynamische Authentifizierung** und Sicherheit gegen Angreifer mit „**mäßigem Angriffspotenzial**“ (2.3.1)	ca. ISO/IEC 27001	**Substanziell**
		Sicher gegen Angreifer mit „**erhöhtem grundlegenden Angriffspotenzial**“ (2.3.1)		**Niedrig**

gematik-ehealth-loa-high

CardLink wäre
gematik-ehealth-loa-substantial!

Festlegung der gematik bzgl. der Zulässigkeit von Identifikations-verfahren für das Level of Assurance (LoA) gematik-ehealth-loa-high

Hintergrund

Die gematik legt im Rahmen ihrer Aufgabe nach § 311 Absatz 1 Nummer 9 SGB V und in Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nachstehende Identifikationsverfahren als geeignet zur Identifikation von natürlichen Personen im Sinne des Vertrauensniveaus/LoA „gematik-ehealth-loa-high" fest. Diese Festlegung wird bei Bedarf erweitert oder reduziert.

Die gematik weist ausdrücklich darauf hin, dass Identifikationsverfahren bei Bekanntwerden von Schwachstellen entfernt werden können. Gleichzeitig können weitere Verfahren bei Nachweis der Eignung für das Vertrauensniveau gematik-ehealth-loa-high hinzugefügt werden.

Version: 1.0

Stand: 19.06.2023

Aktuell geeignete Verfahren

- [oaf] Online-Ausweisfunktion des neuen Personalausweises, des elektronischen Aufenthaltstitels oder der EU-Bürgerkarte
- [egk] Identifikation mittels eGK und PIN
- [pif] POSTIDENT Filiale
- [kkg] Persönliche Identifikation in der Geschäftsstelle der Krankenkasse
- [bot] Identifikation in einer Botschaft (Botschafts-Ident)
- [not] Identifikation bei einem Notar (Notar-Ident)

Verfahren, welche zur Festlegung vorgemerkt sind

- [apo] Apotheken-Ident

https://www.bvitg.de/wp-content/uploads/2024-07-10-bvitg-Positionspapier-eHealth-CardLink.pdf

§ 291 (8) SGB V (Digitale Identität aka „GesundheitsID“)

- (8) Spätestens ab dem 1. Januar 2024 stellen die Krankenkassen den Versicherten ergänzend zur elektronischen Gesundheitskarte auf Verlangen eine sichere digitale Identität für das Gesundheitswesen barrierefrei zur Verfügung, die die Vorgaben nach Absatz 2 Nummer 1 und 2 erfüllt und die Bereitstellung von Daten nach § 291a Absatz 2 und 3 durch die Krankenkassen ermöglicht. Ab dem 1. Januar 2026 dient die digitale Identität nach Satz 1 in gleicher Weise wie die elektronische Gesundheitskarte zur Authentisierung des Versicherten im Gesundheitswesen und als Versicherungsnachweis nach § 291a Absatz 1. Die Gesellschaft für Telematik legt die Anforderungen an die Sicherheit und Interoperabilität der digitalen Identitäten fest. Die Festlegung der Anforderungen an die Sicherheit und den Datenschutz erfolgt dabei im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragen für den Datenschutz und die Informationsfreiheit auf Basis der jeweils gültigen Technischen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik und unter Berücksichtigung der notwendigen Vertrauensniveaus der unterstützten Anwendungen.

Eine digitale Identität kann über verschiedene Ausprägungen mit verschiedenen Sicherheits- und Vertrauensniveaus verfügen.

Das Sicherheits- und Vertrauensniveau der Ausprägung einer digitalen Identität muss mindestens dem Schutzbedarf der Anwendung entsprechen, bei der diese eingesetzt wird. Abweichend von Satz 6 kann der Versicherte nach umfassender Information durch die Krankenkasse über die Besonderheiten des Verfahrens in die Nutzung einer digitalen Identität einwilligen, die einem anderen angemessenen Sicherheitsniveau entspricht.

Die Anforderungen an die Sicherheit und Interoperabilität dieses Nutzungsweges der digitalen Identität werden von der Gesellschaft für Telematik festgelegt. Die Festlegung erfolgt hinsichtlich der Anforderungen an die Sicherheit und den Datenschutz im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

Krankenkassen sind verpflichtet, spätestens ab dem 1. Oktober 2024 berechtigten Dritten die Nutzung der digitalen Identitäten nach Satz 1 zum Zwecke der Authentifizierung von Versicherten zu ermöglichen. Berechtigte Dritte nach Satz 10 sind Anbieter von Anwendungen nach § 306 Absatz 4 oder Anbieter, für die aufgrund eines Gesetzes oder einer Rechtsverordnung die Nutzung der digitalen Identität nach Satz 1 vorgeschrieben ist. Darüber hinaus kann die Gesellschaft für Telematik durch verbindlichen Beschluss nach § 315 Absatz 1 Satz 1 Anbieter weiterer Dienste oder Anwendungen nach § 306 Absatz 1 Nummer 2 Buchstabe a als berechtigte Dritte diskriminierungsfrei festlegen. Berechtigte Dritte dürfen zum Zweck der Authentifizierung von Versicherten mittels der digitalen Identitäten personenbezogene Daten des Versicherten verarbeiten, sofern diese für die Nutzung der digitalen Identität erforderlich sind und der Versicherte in die Nutzung der digitalen Identität durch die jeweilige Anwendung eingewilligt hat. Bei der Verarbeitung sind die Anforderungen des Datenschutzes einzuhalten. Spätestens ab dem 1. Juli 2023 stellen die Krankenkassen zur Nutzung berechtigten Dritten Verfahren zur Erprobung der Integration der sicheren digitalen Identität nach Satz 1 zur Verfügung.

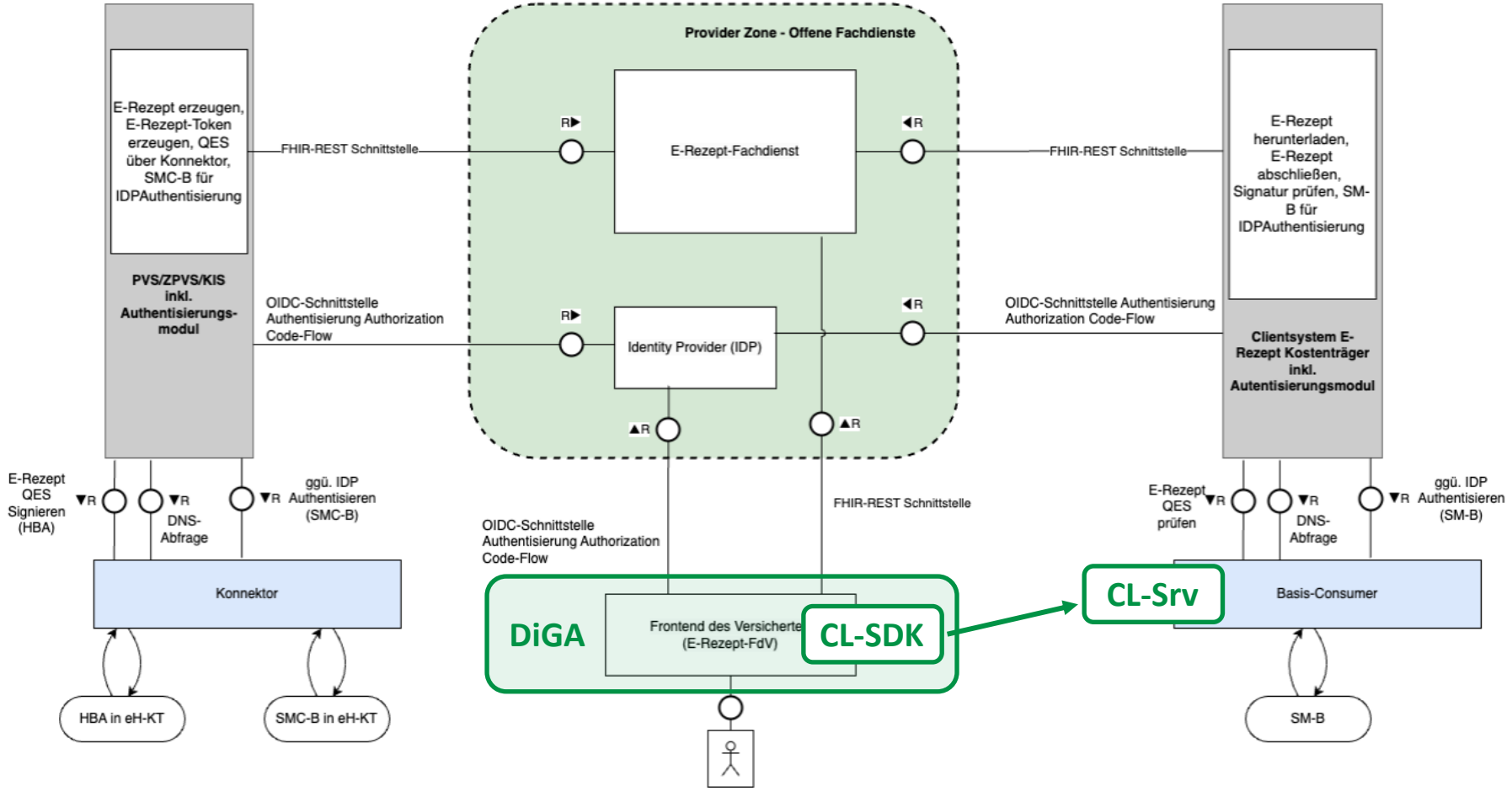
§ 336 (2) SGB V (Zugriffsrechte der Versicherten)

(2) Jeder Versicherte ist berechtigt, auf Daten in einer Anwendung nach § 334 Absatz 1 Satz 2 Nummer 1 und 6 auch ohne den Einsatz seiner elektronischen Gesundheitskarte mittels eines geeigneten sicheren technischen Verfahrens zuzugreifen, wenn

1. der Versicherte nach umfassender Information durch den für die jeweilige Anwendung datenschutzrechtlich Verantwortlichen über die Besonderheiten eines Zugriffs ohne den Einsatz der elektronischen Gesundheitskarte gegenüber dem datenschutzrechtlich Verantwortlichen schriftlich oder elektronisch erklärt hat, dieses Zugriffsverfahren auf Daten in einer Anwendung nach § 334 Absatz 1 Satz 2 Nummer 1 und 6 nutzen zu wollen, und
2. der Versicherte sich für diesen Zugriff auf Daten in einer Anwendung nach § 334 Absatz 1 Satz 2 Nummer 1 und 6 jeweils durch ein geeignetes sicheres technisches Verfahren, das einen hohen Sicherheitsstandard gewährleistet, authentifiziert hat.

Abweichend von Satz 1 kann der Versicherte nach umfassender Information durch den für die jeweilige Anwendung datenschutzrechtlich Verantwortlichen über die Besonderheiten des Verfahrens in die Nutzung eines Authentifizierungsverfahrens einwilligen, das einem anderen angemessenen Sicherheitsniveau entspricht. Die Anforderungen an die Sicherheit und Interoperabilität solcher alternativer Authentifizierungsverfahren werden von der Gesellschaft für Telematik festgelegt. Die Festlegung erfolgt hinsichtlich der Anforderungen an die Sicherheit und den Datenschutz im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Die für ein geeignetes sicheres technisches Verfahren nach Satz 1 erforderliche Identifizierung der Versicherten kann auch in einer Apotheke durchgeführt werden.

Spitzenverband Digitale Gesundheitsversorgung e.V. (SVDGV) fordert CardLink für DiGA-Verordnung per E-Rezept



Vgl. https://gemspec.gematik.de/downloads/prereleases/Draft_eRp_DiGA/gemF_eRp_DiGA_V1.0.0_CC.pdf und https://digitalversorgt.de/wp-content/uploads/2024/07/Stellungnahme_DiGA-Verordnung-E-Rezept.pdf

Agenda

- eHealth-CardLink
- Problemstellung
- **Vorschlag zur Förderung der GesundheitsID**

Konstruktiver Vorschlag zur Förderung der GesundheitsID im Zuge der potenziellen CardLink-Nutzung

Anlage 2 zum Vertrag über die Zulassung als Anbieter eHealth-CardLink
Zusätzliche Regelungen

gematik

2 Anwendungsbereich eHealth-CardLink

Ziffer 1.1 (1) wird für die Anbieter eHealth-CardLink ergänzt durch folgende Regelungen:

a) Der Zulassungsnehmer darf den eHealth-CardLink ausschließlich im Anwendungsszenario gem. Ziffer 2.1 der gemSpec_eHealth-CardLink_V1.0.0 - Mobiles Erstellen eines VSDM-Prüfungsnachweises mit eGK ohne PIN verwenden, ~~um E-Rezepte des Patienten vom Fachdienst abzurufen~~.

b) Der Zulassungsnehmer muss der Zulassungsstelle der gematik alle mit seinem eHealth-CardLink angebundenen Applikationen, deren Einsatzumgebungen (z.B. Smartphone) sowie den jeweiligen Zweck der Nutzung während der Vertragslaufzeit unverzüglich per eMail an Zulassung@gematik.de melden.

sofern vom Zulassungsnehmer sichergestellt wird, dass die betreffende Applikation alternativ auch mit der GesundheitsID genutzt werden kann.

Vielen Dank für Ihre Aufmerksamkeit!

Sind noch Fragen offen?

Kontakt