eHealth-CardLink-Taskforce

06.06.2024

Agenda

- **Begrüßung**
- Bericht E-REZEPT-SUMMIT
- Antworten von gematik und BMG auf unsere Fragen
- Kommentare zur API-Spec der gematik
- Finale Abstimmung der Spezifikation für E-Rezept
- CardLink für gematik-ehealth-loa-substantial
- Sonstiges

Agenda

- Begrüßung
- **Bericht E-REZEPT-SUMMIT**
- Antworten von gematik und BMG auf unsere Fragen
- Kommentare zur API-Spec der gematik
- Finale Abstimmung der Spezifikation für E-Rezept
- CardLink für gematik-ehealth-loa-substantial
- Sonstiges

Bericht E-REZEPT-SUMMIT (Eindrücke Bruno)

- Sebastian Zilch (BMG)
  - eHealth-CardLink ist eine Übergangstechnologie
  - Ausweitung auf andere Bereiche als E-Rezept wird es nicht geben
  - Ziel ist es, die GesundheitsID zu pushen
    - Diese wird als strategisch angesehen – das eHealth-CardLink-Verfahren würde das konterkarieren
  - Meine persönliche Erklärung der Entstehung des Verfahrens
    - Man musste das „Problem“ mit den Europäischen Versandapotheken dringend lösen
- Dr. Paul Blankenhagel, Hauke Langhoff (gematik)
  - Sehen aufgrund der rechtlichen Rahmenbedingungen keine Notwendigkeit für eine weitergehende Spezifikation
  - Haben absolute Gesprächsbereitschaft signalisiert, aber eher nicht im Taskforce-Format
- …

Agenda

- Begrüßung
- Bericht E-REZEPT-SUMMIT
- **Antworten von gematik und BMG auf unsere Fragen**
- Kommentare zur API-Spec der gematik
- Finale Abstimmung der Spezifikation für E-Rezept
- CardLink für gematik-ehealth-loa-substantial
- Sonstiges

Antworten von gematik und BMG auf unsere Fragen

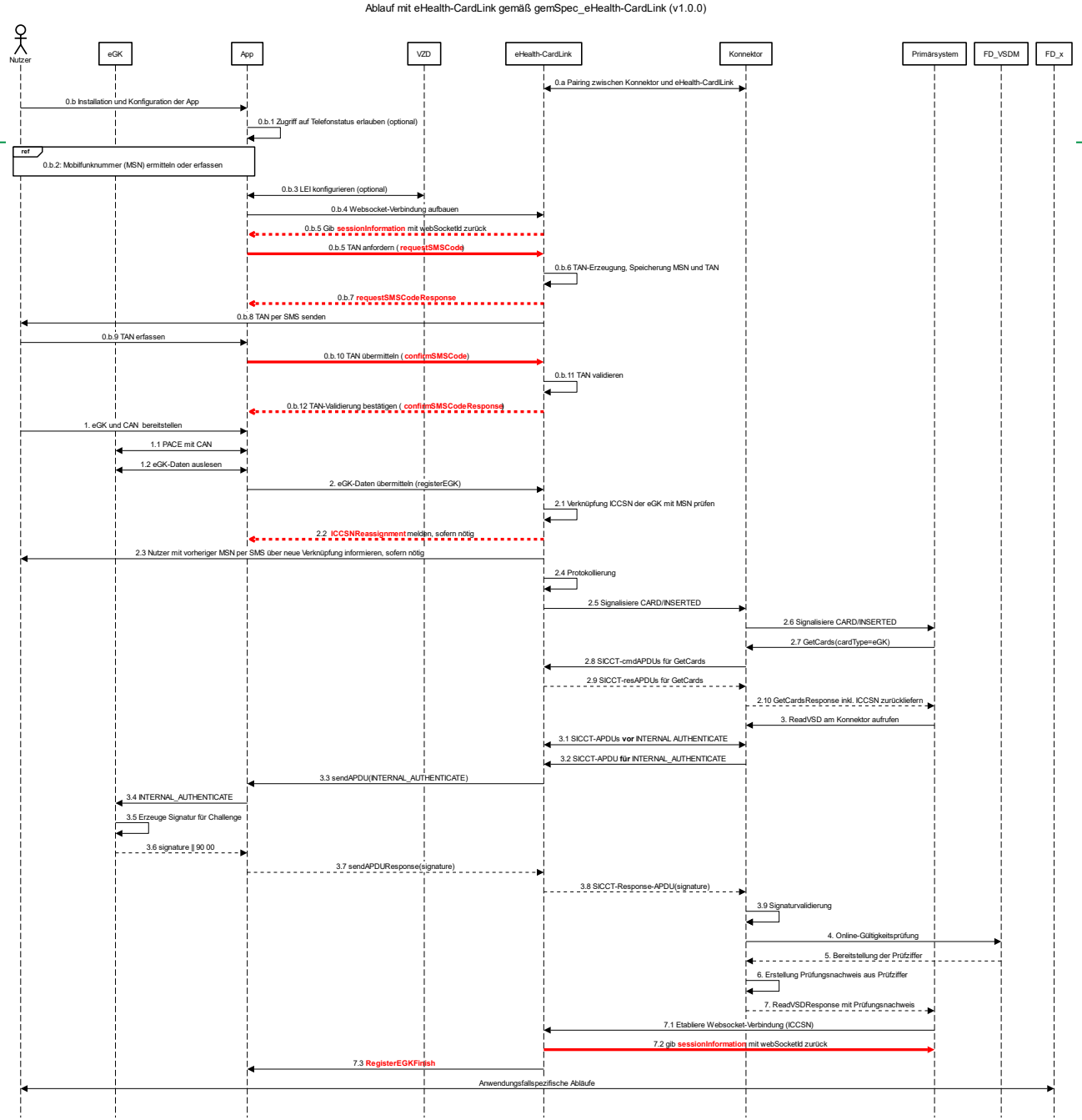
- In der TI ist, was durch Produktsteckbriefe und Afos definiert ist.
- Mit „Zugangsdaten“ sind in § 360 (16) SGB V die E-Rezept-Token gemeint. Prüfungsnachweise sind keine „Zugangsdaten“ in diesem Sinne.
- Auftragsverarbeitung ist für § 360 (16) Satz 2 Nr. 3 SGB V erlaubt.
- Es wird keine Implementierungsleitfäden für CardLink von der gematik geben.
- Für die Umsetzung von § 360 (16) Satz 2 Nr. 4 SGB V muss der Verzeichnisdienst der gematik genutzt werden.
- Spezifikation soll bzgl. der Zulässigkeit von EU-Telefonnummern auf Grund der befristeten Nutzung nicht geändert werden.
- Es soll kein zusätzliches Authentisierungsverfahren für professionelle Nutzer geben.
- Eine Erhöhung der Anzahl der gültigen eGKs pro Session ist nicht geplant.

Agenda

- Begrüßung
- Bericht E-REZEPT-SUMMIT
- Antworten von gematik und BMG auf unsere Fragen
- **Kommentare zur API-Spec der gematik**
- Finale Abstimmung der Spezifikation für E-Rezept
- CardLink für gematik-ehealth-loa-substantial
- Sonstiges

Aktueller Stand

https://github.com/eHealthCardLink



Fehlende Nachrichten

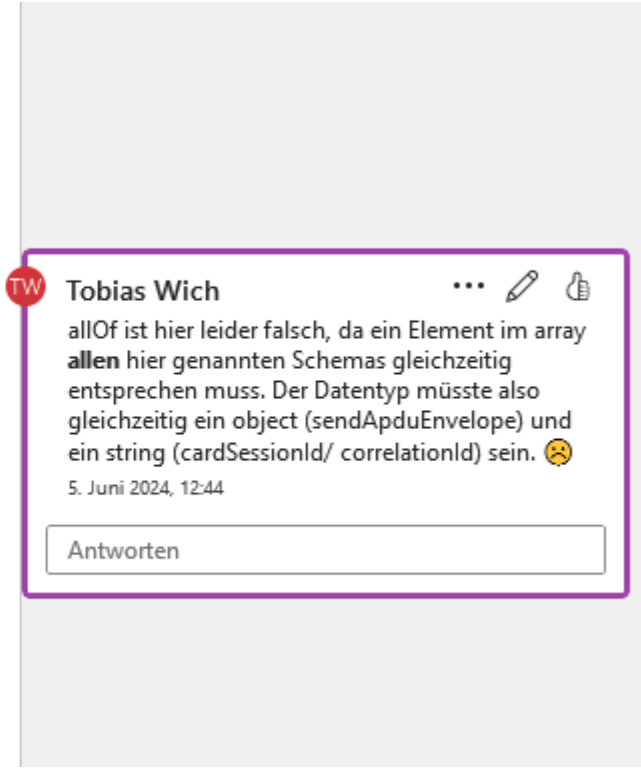
sessionInformation
requestSMSCode
requestSMSCodeResponse
confirmSMSCode
confirmSMSCodeResponse

ICCSNReassignment

sessionInformation
RegisterEGKFinish

Warum die API-Spec der gematik kaputt ist?

```
····sendApduMessage:¶
·····name:·receive¶
·····title:·receive¶
·····summary:·Token·to·be·signed¶
·····contentType:·application/json¶
·····payload:¶
·····type:·array¶
·····items:¶
·····allOf:¶
·····$ref:·'#/components/schemas/sendApduEnvelope'¶
·····$ref:·'#/components/schemas/cardSessionId'¶
·····$ref:·'#/components/schemas/correlationId'¶
·····minItems:·3¶
·····maxItems:·3¶
·····examples:¶
·····-name:·sendAPDU¶
·····summary:·sendAPDU·message¶
·····payload:¶
·····type:·sendAPDU¶
·····payload:·>-¶
·····
eyJjYXJkU2Vzc2lvbklkIjoiMzUwOTU4NGEtMDRlNy00NzU2LWJhYjAtMGRhNGE4NGQwYzEyIiwiYXBk
dSI6IkFJZ0FBQmlBSjJpQkdabVpsb05wRDdiRDI3RWgweTFrbVV0RDN0a0EifQ==¶
·····3509584a-04e7-4756-bab0-0da4a84d0c12¶
·····38a5fb1b-f8e4-4132-8ec6-00fcd07bc5cc¶
```



https://json-schema.org/draft/2020-12/json-schema-core#name-allof

… und warum das ein ernstes Problem ist …

A_25159 - eHealth-CardLink - Card Communication Interface, Websocket-Verbindungen
Der eHealth-CardLink (eH-CL) MUSS eine Webschnittstelle "Card Communication Interface" anbieten, die

1. mindestens Verbindungen per Websocket unterstützt und

Spezifikation eHealth-CardLink gematik

2. auf Applikationsebene Nachrichten gemäß dem Schema in folgendem Projekt austauscht:
   https://github.com/gematik/api-ehcl

[<=]

A_25160 - eHealth-CardLink - Card Communication Interface, API-Dokumentation
Falls eHealth-CardLink (eH-CL) für die Kartenkommunikation Schnittstellen anbietet, die nicht gemäß A_25159 arbeiten, dann MUSS der Hersteller des eH-CL zusätzlich eine Referenzimplementierung bereitstellen, der das Interface aus A_25159* unterstützt und die Nachrichten in die herstellerspezifische Kommunikation zu eH-CL und zum nutzenden System weiterleitet.
[<=]

, das sich vielleicht nur durch Magie lösen lässt?

3 Ergebnisse

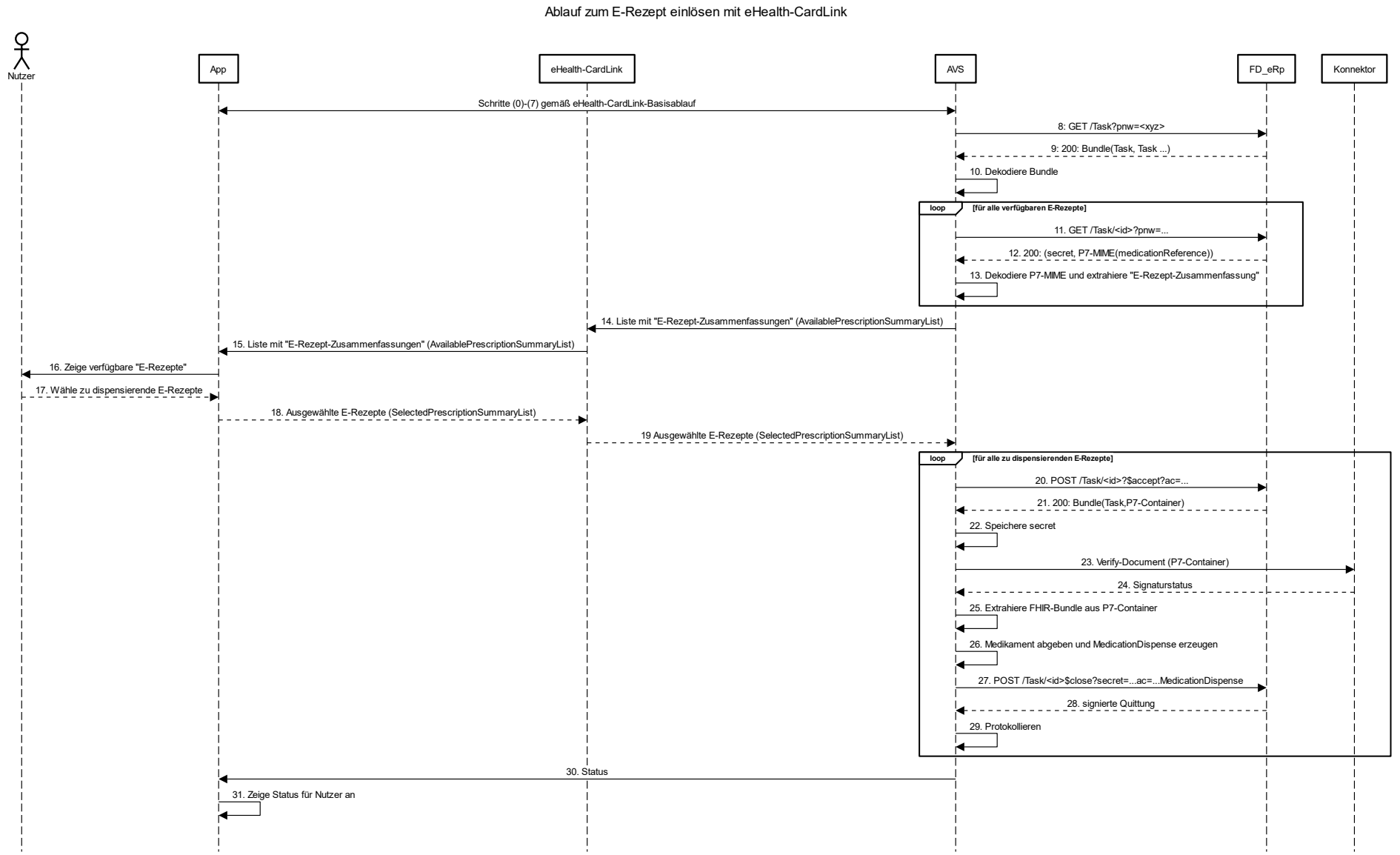
Produkttyp	Herstellername / Institution	Produktname	Produktversion	Produkttypversion	Zulassungsdc
eHealth-CardLink Zugelassen	eHealth Experts GmbH	ehex cardlink	1.0.3	1.0.0	23.04.2024
eHealth-CardLink Zugelassen	DocMorris N.V.	DocMorris eHealth-CardLink	1.0.4	1.0.0	03.06.2024
eHealth-CardLink Zugelassen	DocMorris N.V.	DocMorris eHealth-CardLink	1.0.3	1.0.0	09.04.2024

https://tinyurl.com/eH-CL-Zulassung

Agenda

- Begrüßung
- Bericht E-REZEPT-SUMMIT
- Antworten von gematik und BMG auf unsere Fragen
- Kommentare zur API-Spec der gematik
- **Finale Abstimmung der Spezifikation für E-Rezept**
- CardLink für gematik-ehealth-loa-substantial
- Sonstiges

Ablauf für Einlösen eines E-Rezepts



Agenda

- Begrüßung
- Bericht E-REZEPT-SUMMIT
- Antworten von gematik und BMG auf unsere Fragen
- Kommentare zur API-Spec der gematik
- Finale Abstimmung der Spezifikation für E-Rezept
- **CardLink für gematik-ehealth-loa-substantial**
- Sonstiges

§ 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 Bundesbeauftragten 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.

Sicherheits- und Vertrauensniveaus

- 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

Was und wo genau ist nochmal dieses „Europa“?

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

Art. 6 (EU) No 910/2014

Artikel 6 - Gegenseitige Anerkennung

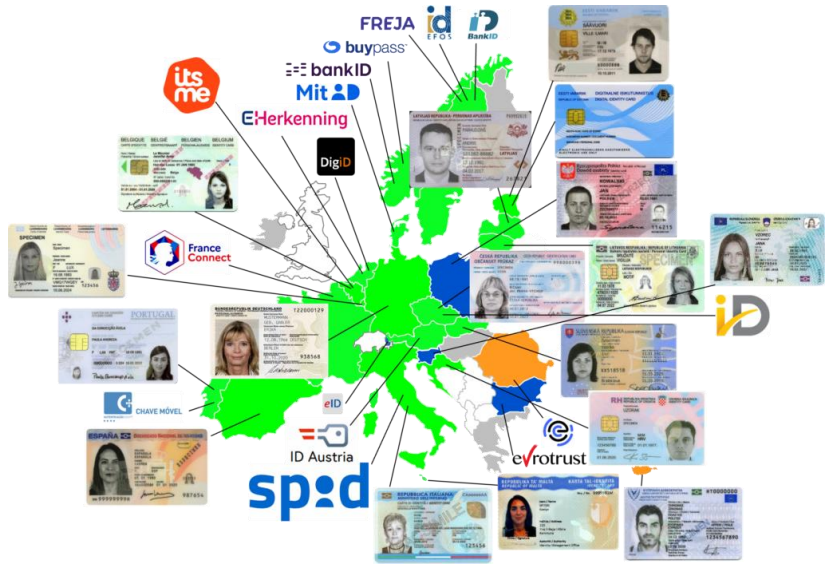
(1) Ist für den Zugang zu einem von einer öffentlichen Stelle in einem Mitgliedstaat erbrachten Online-Dienst nach nationalem Recht oder aufgrund der Verwaltungspraxis eine elektronische Identifizierung mit einem elektronischen Identifizierungsmittel und mit einer Authentifizierung erforderlich, so wird ein in einem anderen Mitgliedstaat ausgestelltes elektronisches Identifizierungsmittel im ersten Mitgliedstaat für die Zwecke der grenzüberschreitenden Authentifizierung für diesen Online-Dienst anerkannt, sofern folgende Bedingungen erfüllt sind:

(a) Das betreffende elektronische Identifizierungsmittel wird im Rahmen eines elektronischen Identifizierungssystems ausgestellt, das in der von der Kommission gemäß Artikel 9 veröffentlichten Liste aufgeführt ist.

(b) Das Sicherheitsniveau des betreffenden elektronischen Identifizierungsmittels entspricht einem Sicherheitsniveau, das so hoch wie oder höher als das von der einschlägigen öffentlichen Stelle für den Zugang zu diesem Online-Dienst geforderte Sicherheitsniveau ist, sofern das Sicherheitsniveau dieses elektronischen Identifizierungsmittels dem Sicherheitsniveau „substanziell“ oder „hoch“ entspricht.

(c) Die betreffende öffentliche Stelle verwendet für den Zugang zu diesem Online-Dienst das Sicherheitsniveau „substanziell“ oder „hoch“.

Diese Anerkennung muss spätestens 12 Monate nach Veröffentlichung der in Unterabsatz 1 Buchstabe a genannten Liste durch die Kommission erfolgen.



seit 29.09.2018 Pflicht!

https://tinyurl.com/eIDAS-Schemes

Agenda

- Begrüßung
- Bericht E-REZEPT-SUMMIT
- Antworten von gematik und BMG auf unsere Fragen
- Kommentare zur API-Spec der gematik
- Finale Abstimmung der Spezifikation für E-Rezept
- CardLink für gematik-ehealth-loa-substantial
- **Sonstiges**

Vielen Dank für Ihre Aufmerksamkeit!

Sind noch Fragen offen?

Kontakt

esec ... bring secure made easy

ecsec GmbH
Sudetenstr. 16
96247 Michelau
Telefon + 49 9571 948 1020
Mobil + 49 171 9754980
detlef.huehnlein@ecsec.de
https://www.ecsec.de

Dipl.-Inform. (FH)
Dr. Detlef Hühnlein
Geschäftsführer

C&S managing care.

C&S Computer und Software GmbH
Wolfsgäßchen 1
86153 Augsburg
Telefon +49 821 2582 0
Mobil +163 4258 200
BrunoRistok@cs-ag.de
https://www.managingcare.de

Bruno Ristok
Geschäftsführer