2024-04-29 CardLink Taskforce Anfrage

gematik
Nationale Agentur für Digitale Medizin

Nr.	Frage	Antwortvorschlag
1	In § 360 (16) SGB V wird ein Verbot der "Übermittlung von elektronischen Verordnungen oder elektronischen Zugangsdaten zu elektronischen Verordnungen [...] außerhalb der Telematikinfrastruktur" (TI) definiert. Leider scheint weder im SGB V noch in den Spezifikationen der gematik präzise definiert zu sein, was genau innerhalb und außerhalb der TI ist. Zur Abgrenzung der TI gibt es historisch betrachtet verschiedene Ansätze, die hier leider allesamt nicht zu einer widerspruchsfreien und tragfähigen Interpretation der Rechtslage bezüglich des eHealth-CardLink-Verfahrens zu führen scheinen. Vor diesem Hintergrund möchten wir freundlich bitten, eine klare Definition zu schaffen, was genau innerhalb und außerhalb der Telematikinfrastruktur ist. Es wäre nett, wenn Sie kurz darauf eingehen könnten, ob die folgenden Komponenten in diesem Sinne innerhalb oder außerhalb der TI sind: die Primärsysteme der Leistungserbringer (Apothekenverwaltungssystem (AVS), Praxisverwaltungssystem (PVS) etc.) • eHealth-Kartenterminal gemäß gemSpec_KT • eHealth-CardLink-Dienst gemäß gemSpec_eHealth-CardLink • Client des Nutzers ("App") gemäß gemSpec_eHealth-CardLink (Abschnitt 3) • E-Rezept-App der gematik gemäß gemSpec_eRp_FdV • Frontends der Versicherten gemäß gemSpec_ePA_FdV Abschließend wäre es nett, wenn auch geklärt werden könnte, ob ein bei einer dieser Komponenten endender TLS-Kanal in diesem Sinne innerhalb oder außerhalb der TI ist.	Von den aufgelisteten Produktiven sind alle mit Produkttypsteckbrief und normativen Anforderungen, die für einen Einsatz ein Zulassungsverfahren oder ähnlichen benötigen, als TI-Produkte einzustufen. Dazu gehören das eHealth-Kartenterminal, der eHealth-CardLink und die FdV-Apps zu E-Rezept und ePA. "Innerhalb der TI" meint dabei den Umfang der über die Produkttypsteckbriefe definierten Anforderungen, nicht aber die etwaig darüber hinaus zulässigen Funktionalitäten, die nicht explizit untersagt sind. Ein innerhalb eines TI-Produktes endender TLS-Kanal ist damit nicht als "innerhalb der TI" zu verstehen, sofern Schnittstelle und Payload dieses Kanals nicht explizit als Anforderungen im Produkttypsteckbriefes dargelegt wurden und im Rahmen von Zulassungsverfahren nachgewiesen sind.

2	Der in § 360 (16) SGB V genutzte Begriff der "Zugangsdaten" zu elektronischen Verordnungen ist leider nicht gesetzlich bestimmt, so dass hier vielfältige Interpretationen dieses Begriffes existieren, die davon abhängen, wie breit die wörtliche Auslegung des Begriffes bei den vier von der gematik spezifizierten Möglichkeiten zur Einreichung von elektronischen Verordnungen erfolgt. Gestützt auf das in der Informatik übliche Verständnis des Begriffs "Zugangsdaten" könnte man bei den unterschiedlichen Einreichungsvarianten für elektronische Verordnungen zu folgenden Interpretationen gelangen: Einlösung von Verordnungen mit ... • eGK und PIN in der E-Rezept-App der gematik: Hier könnten die "Zugangsdaten" aus dem kryptographischen Schlüsselmaterial der eGK und der PIN bestehen. • ausgedrucktem E-Rezept-Token: Hier könnten die "Zugangsdaten" schlicht aus dem ggf. als QR-Code codierten E-Rezept-Token gemäß gemSpec_DM_eRp (§ 2.3.1) bestehen. • gesteckter eGK ohne PIN in der Apotheke: Hier könnten die "Zugangsdaten" aus dem Schlüsselmaterial der physikalisch in der Apotheke befindlichen eGK samt der optisch sichtbaren Merkmale bestehen. • dem eHealth-CardLink-Verfahren und eGK ohne PIN: Hier könnten die "Zugangsdaten" aus dem Schlüsselmaterial der per App gekoppelten eGK und der per SMS verschickten TAN bestehen. Könnten Sie bitte präzise klären, was in § 360 (16) SGB V genau unter dem Begriff "Zugangsdaten" zu elektronischen Verordnungen zu verstehen ist?	Zugangsdaten im Sinne des §360 Abs. 16 sind die E-Rezept-Token bzw. Einlöseinformationen gemäß gemSpec_DM_eRp (Kap 2.3.1). Dies geht aus der Gesetzesbegründung des DigiG hervor, siehe Seite 146 "Zu Buchstabe l" in https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/D/Kabinettvorlage_Digital-Gesetz-DigiG.pdf Da es im § 360 Absatz 16 um die Übermittlung von elektronischen Verordnungen oder deren elektronischen Zugangsdaten durch IT-Systeme außerhalb der TI geht, passen Interpretationen wie das Stecken der eGK in der Apotheke in diesem Kontext nicht, auch wenn die offene Formulierung durch das Wort „Zugangsdaten“ prinzipiell größeren Interpretationsspielraum zulassen würde. Der Zugang zu TI-Fachdiensten ist nur über eine 2-Faktor-Authentisierung möglich. Der Zugriff via Punkte 3+4 erfolgt durch den angebundenen LE mittels SMC-B und PIN. Der VSDM-Prüfungsnachweis berechtigt alleinig nicht zum Zugriff auf den Fachdienst und stellt lediglich zusätzliche Informationen zum Kontext des bereits durch die SMC-B authentisierten Zugriffs bereit. Der durch die Punkte 3+4 erzeugte VSDM-Prüfungsnachweis sind demnach nicht als klassische Zugangsdaten zu betrachten.

3	In § 360 (16) Satz 2 Nr. 3 SGB V ist eine Ausnahme vom generellen Übermittlungsverbot definiert für informationstechnischen Systeme, "die eine Apotheke betreibt". Ist mit dem gewählten Wort "betreibt", statt beispielsweise "verantwortet" im Sinne von Art. 4 (7) DSGVO bzw. "anbietet" im Sinne der Regularien der gematik und auch im Vergleich zur Wahl des Begriffes "Anbieter" in § 360 (16) Satz 2 Nr. 3 SGB V - tatsächlich gemeint, dass die Apotheke selbst das System in einem eigenen Rechenzentrum "betreiben" muss, ohne dass hier Auftragsverarbeiter gemäß Art. 28 DSGVO eingesetzt werden dürften, oder ist für diesen Fall auch der rechtskonforme Einsatz von Auftragsverarbeitern zulässig?	Die Frage wurde bereits durch das BMG beantwortet. BMG: „Die Nutzung einer Standard-App als App für eine individuelle Apotheke ist möglich. Durch die Ausnahme werden Anwendungen einzelner Apotheken zur Einlösung von E-Rezepten durch einen Versicherten bei der jeweiligen Apotheke ermöglicht. Die App darf daher nur die Einlösung für die eine Apotheke ermöglichen. Der Betrieb der App muss durch die Apotheke erfolgen oder von dieser beauftragt werden." Quelle: https://www.deutsche-apotheker-zeitung.de/news/artikel/2024/05/03/bmg-diskriminierungsfrei-bedeutet-auch-kostenlos
4	Wie soll nach Ihren Vorstellungen bzw. nach den Vorstellungen der gematik für den in § 360 (16) Satz 2 Nr. 4 SGB V beschriebenen Fall der "diskriminierungsfreien Anbindung" die Erfüllung des "Standes der Technik gemäß den Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik" nachgewiesen werden, so lange die gemSpec_eHealth-CardLink nur einen Teil des hierfür notwendigen Systems adressiert? Ist seitens der gematik geplant, einen entsprechenden Implementierungsleitfaden mit einschlägigen Sicherheitsanforderungen und -empfehlungen zu erarbeiten? Falls ja, wann ist mit der Bereitstellung einer ersten Version zur Kommentierung und mit einer finalisierten Version zu rechnen?	Das eHealth-CardLink vermittelt einen VSDM-Prüfungsnachweis in der, an das CardLink angebundenen LEI. Seitens gematik ist nicht geplant entsprechende weitere Implementierungsleitfäden als Ergänzung zur eHealth-CardLink-Spezifikation zu erstellen. Für den in § 360 (16) Satz 2 Nr. 4 SGB V beschriebenen Fall ist der Verzeichnisdienst der gematik zu nutzen. Dieser Dienst stellt ein Zertifikat und einen Endpunkt pro Apotheke bereit. Diese Informationen können für die Einlösung von E-Rezept-Token bei der jeweiligen Apotheke genutzt werden.

5	Wie kann nach Ihren Vorstellungen bzw. nach den Vorstellungen der gematik für den in § 360 (16) Satz 2 Nr. 4 SGB V beschriebenen Fall der "diskriminierungsfreien Anbindung" die Nutzung "normierter Schnittstellen der Gesellschaft für Telematik" nachgewiesen werden, so lange die gemSpec_eHealth-CardLink nur einen Teil der hierfür notwendigen Schnittstellen spezifiziert? Sind offene Schnittstellen, die in der eHealth-CardLink-Taskforce unter Mitwirkung von zahlreichen Experten erarbeitet und abgestimmt wurden, als "normierte Schnittstellen" in diesem Sinne zu betrachten?	Für den in § 360 (16) Satz 2 Nr. 4 SGB V beschriebenen Fall ist der Verzeichnisdienst der gematik zu nutzen. Dieser Dienst wird durch normierte Schnittstellen in der Verwendung angesprochen (siehe Dokumentation in github). "normierter Schnittstellen der Gesellschaft für Telematik" werden laut Gesetzesbegründung wie folgt beschrieben "Um diese Diskriminierungsfreiheit zu erreichen, sind dafür der Verzeichnisdienst der Gesellschaft für Telematik und normierte Schnittstellen zu den Apothekenverwaltungssystemen zu nutzen." Neben den Schnittstellen zum VZD gibt noch die Schnittstellen zum Konnektor in der Apotheke.
6	Es zeichnet sich ab, dass es mehrere zugelassene Produkte und Angebote im Markt für den eHealth-CardLink-Dienst und auch mehrere Apps geben wird, die diese für die Kommunikation mit den verschiedenen Apotheken nutzen werden. Vor diesem Hintergrund erscheint es für die Realisierung der "diskriminierungsfreien Anbindung" gemäß § 360 (16) Satz 2 Nr. 4 SGB V naheliegend, die entsprechenden Adressinformationen (u.a. welcher eHealth-CardLink-Dienst für eine bestimmte Apotheke aktuell zuständig ist) im Apothekenverzeichnis gemSpec_eRp_APOVZD, bzw. mit Blick auf den Einsatz des eHealth-CardLink-Verfahrens bei anderen Leistungserbringern, im Verzeichnisdienst gemSpec_VZD_FHIR_Directory der gematik zu pflegen. Ab wann werden seitens der gematik geeignete Verzeichnisdienste für die diskriminierungsfreie Anbindung zur Verfügung stehen?	Der Verzeichnisdienst der gematik ist bereits verfügbar und kann nach Antrag bei der gematik genutzt werden. Es ist nicht geplant, Informationen über die eHealth-CardLink Nutzung der Apotheken dort zu hinterlegen. Die diskriminierungsfreie Anbindung bezieht sich auf die Nutzung des Verzeichnisdienstes der gematik über den die Informationen zum Einlösen des E-Rezeptes bei den Apotheken bezogen werden können.

7	Gemäß gemSpec_eHealth-CardLink (A_25478 - eHealth-CardLink - Anwendung nur mit deutscher Telefonnummer) wird die Nutzung des eHealth-CardLink-Verfahrens auf Telefonnummern deutscher Anbieter eingeschränkt. Dies ist beim Einsatz des Verfahrens in grenznahen Gebieten äußerst unglücklich, da gesetzlich Versicherte bisweilen Mobilfunkverträge mit teilweise günstigeren Telekommunikationsanbietern aus dem angrenzenden Ausland haben, mit denen das eHealth-CardLink-Verfahren folglich nicht genutzt werden könnte. Ist es vorstellbar, diese Anforderung zukünftig zu lockern, so dass zumindest Telefonnummern aus unmittelbar angrenzenden Ländern akzeptiert werden könnten? Vor dem Hintergrund des Europäischen Binnenmarktes wäre die Zulässigkeit der Nutzung von Telefonnummer aus dem Europäischen Wirtschaftsraum sicherlich zu bevorzugen.	Eine Anpassung der eHealth-CardLink-Spezifikation ist derzeit, auch in Hinblick auf die befristete Nutzung bis zum Abschalten der heutigen VSDM-Fachdienste, nicht geplant.
8	Gemäß gemSpec_eHealth-CardLink (A_25168 - eHealth-CardLink - SMS-Code Gültigkeit) ist die Etablierung einer 15-minütigen Session zulässig. Leider ist diese hier definierte maximale Länge der Session für professionelle Nutzerinnen und Nutzer (z.B. in Pflegeheimen) regelmäßig zu kurz. Ist es denkbar, dass diese Anforderung für professionelle Anwender des eHealth-CardLink-Verfahrens, die möglicherweise mit einem zusätzlichen und sicherheitstechnisch geeigneten Authentisierungsverfahren angemeldet sein könnten, entsprechend gelockert wird?	Eine Erweiterung der der eHealth-CardLink-Spezifikation um ein zusätzliches Authentisierungsverfahren von professionellen Anwendern ist nicht geplant.
9	Gemäß gemSpec_eHealth-CardLink (A_25212 - eHealth-CardLink - Maximale Anzahl eGKs pro Session) ist die Nutzung von höchstens zehn (10) eGKs in einer Session erlaubt. Leider führt dies für professionelle Nutzerinnen und Nutzer (z.B. in Pflegeheimen) regelmäßig zu Einschränkungen. Ist es denkbar, dass diese Anforderung für professionelle Anwender des eHealth-CardLink-Verfahrens, die möglicherweise mit einem zusätzlichen und sicherheitstechnisch geeigneten Authentisierungsverfahren angemeldet sein könnten, entsprechend gelockert wird?	Eine Erhöhung der gültigen eGKs pro Session ist nicht geplant. Die Verknüpfung der eGKs kann wieder aufgehoben werden, um in einer neuen Session 10 weitere eGKs einzulesen. Aus Sicht eines professionellen Nutzers ist dieser UseCase also durchführbar.