Schlechte Karten
Schlechte Karten
Schlechte Karten
Schlechte Karten
Schlechte Karten
Schlechte Karten
Schlechte Karten
Schlechte Karten
Schlechte Karten
Schlechte Karten
Schlechte Karten

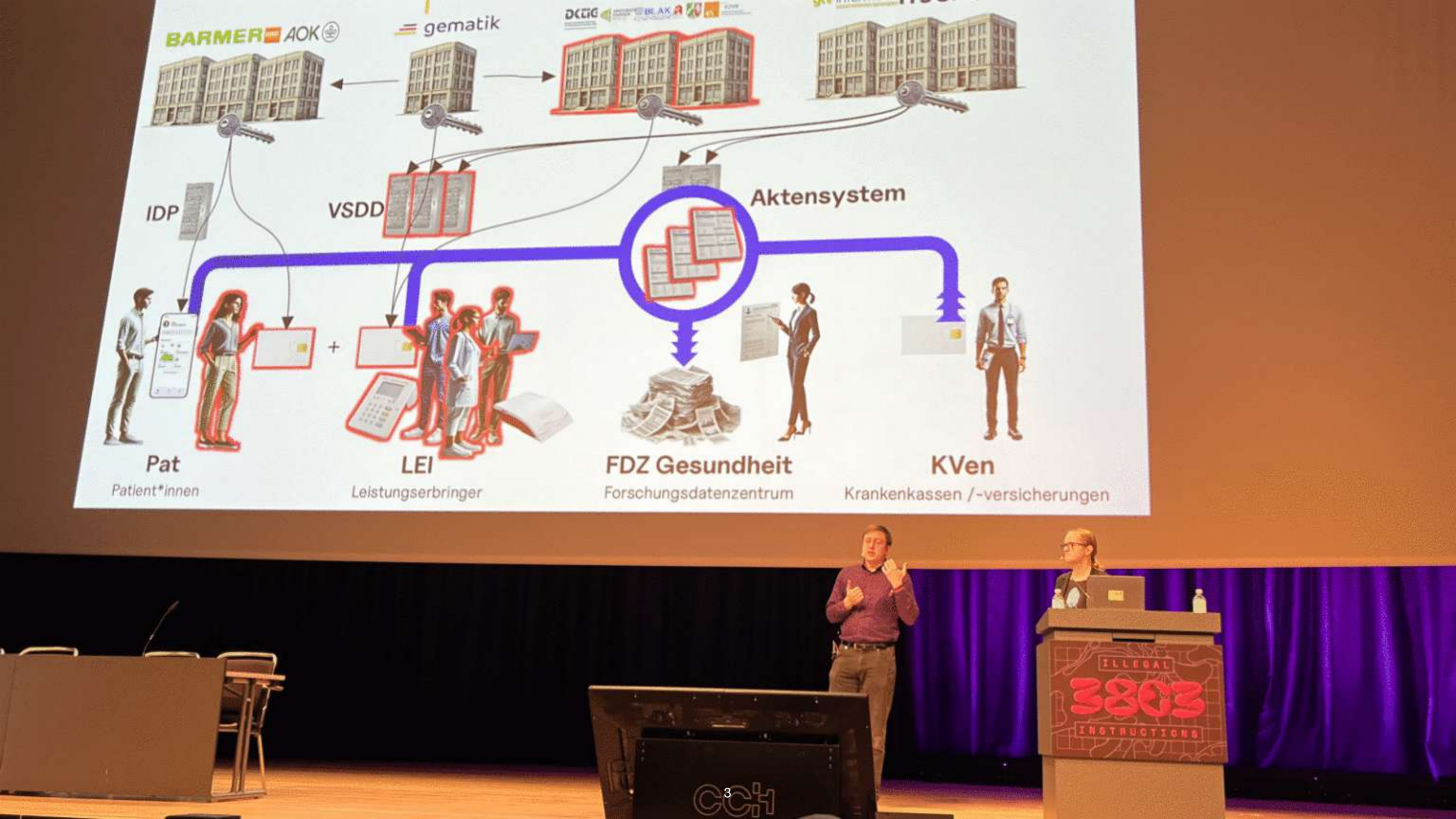
IT-Sicherheit im Jahr null der ePA für alle

Bianca Kastl – 39C3 – 29.12.25

Über

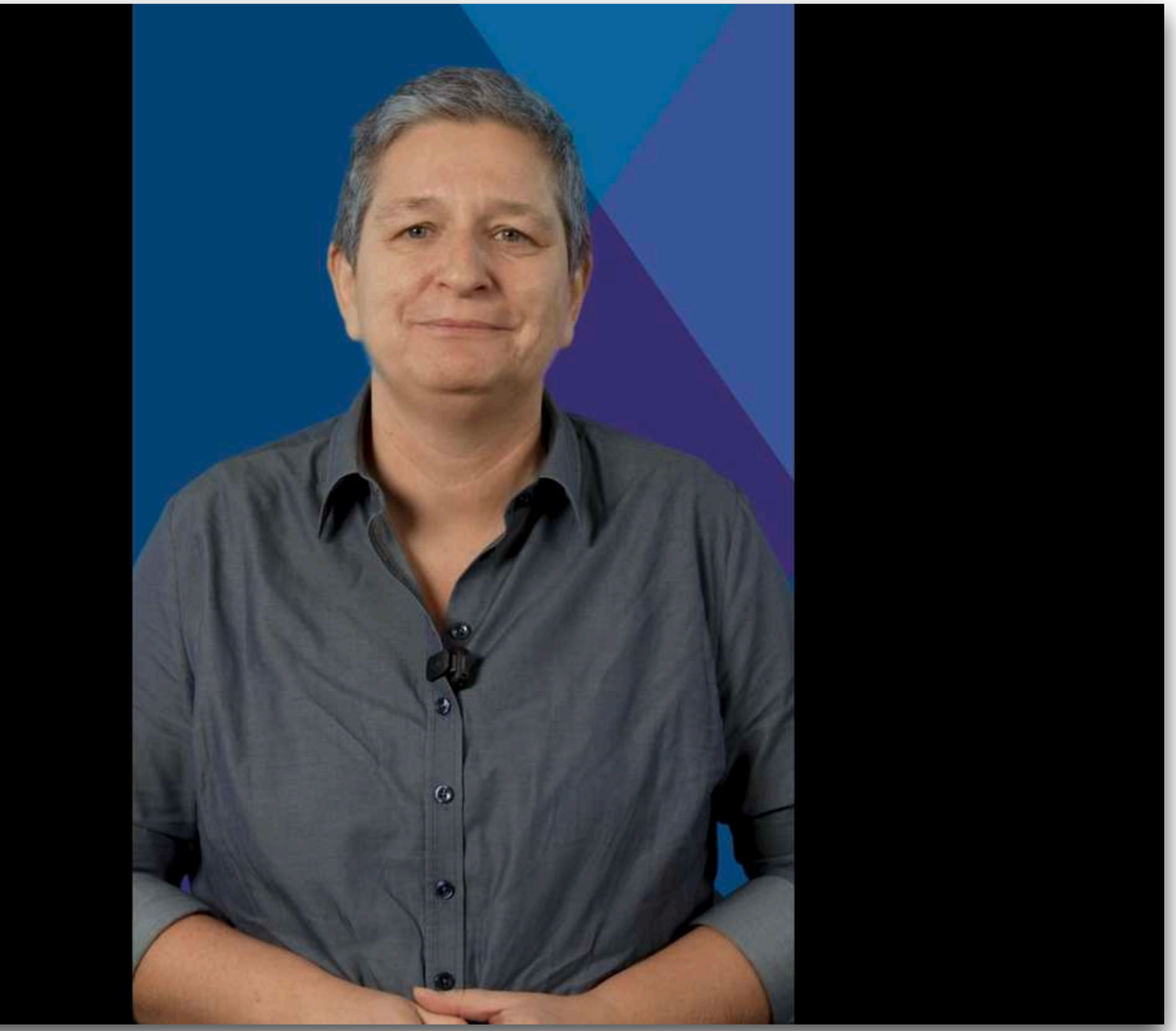
Bianca Kastl

- Ethische Hackerin aus dem Umfeld des Chaos Computer Club
- Vorsitzende Innovationsverbund Öffentliche Gesundheit (InÖG)
- Technische Projektleitung für Softwarelösungen im Öffentlichen Gesundheitsdienst
- Sachverständige zu diversen Themen der Digitalisierung von Verwaltung und Gesundheitswesen in diversen Bundestagsausschüssen (2021, 2021, 2023, 2023, 2024)
- Kolumnistin netzpolitik.org & t3n


BARMER
AOK
gematik
IDP
VSDD
Aktensystem
Pat
Patient*innen
LEI
Leistungserbringer
FDZ Gesundheit
Forschungsdatenzentrum
KVen
Krankenkassen /-versicherungen
ILLEGAL
3803
INSTRUCTIONS

„…gerade das, **was der CCC macht**, ist wahnsinnig wichtig, um am Ende […] diese **Vertrauenskomponente** mit dem System zu haben.“

BfDI Prof. Dr. Louisa Specht-Riemenschneider, 16.01.2025



„Ich weiß, dass ihr [einen Beitrag für digitalen Erfolg] leistet, tagtäglich durch eure Expertise, durch die Tatsache, dass **ihr die Technik versteht**.“

Claudia Plattner, Präsidentin BSI, 26.12.25

Die selbstverantwortliche Nutzung digitaler Tools bedarf der Abwägung von Risiken. Oftmals werden Informationen zur Abwägung der Risiken aber nicht transparent gemacht.

Widersprüchliche Risikodarstellung

Datensicherheit

Sind meine Daten in der ePA sicher?

Ja. Eine sichere Nutzung von Gesundheitsdaten ist die Grundvoraussetzung für die Nutzung der ePA. Die Umsetzung der ePA für alle erfolgt datenschutzkonform. Die Daten werden auf sicheren Servern innerhalb der Telematikinfrastruktur (TI) gespeichert und in der ePA verschlüsselt abgelegt. Die Kommunikation zwischen den Komponenten der ePA ist Ende-zu-Ende verschlüsselt. Niemand außer der oder dem Versicherten oder seiner Vertreterin bzw. seinem Vertreter und denjenigen, die zugriffsberechtigt sind, können die Inhalte lesen. Die Krankenkasse darf und kann beispielsweise nicht auf die Inhalte zugreifen.

Wo sind die Server, auf denen die ePA-Daten gespeichert werden?

Die Server, auf denen die Daten der elektronischen Patientenakten der Versicherten gespeichert werden, stehen in Rechenzentren in Deutschland. Die umfangreich sicherheitsgeprüften Rechenzentren werden im Auftrag der Krankenkassen durch zwei Anbieter betrieben.

mit Datum vom 12.02.2025 haben Sie über www.fragdenstaat.de die Ü
Datenschutzfolgenabschätzung (im Weiteren: DFSA) für das Aktensy
Versicherten-Frontend zur Nutzung der „ePA für alle" beantragt.

Ihren Antrag auf Informationszugang weisen wir hiermit zurück.

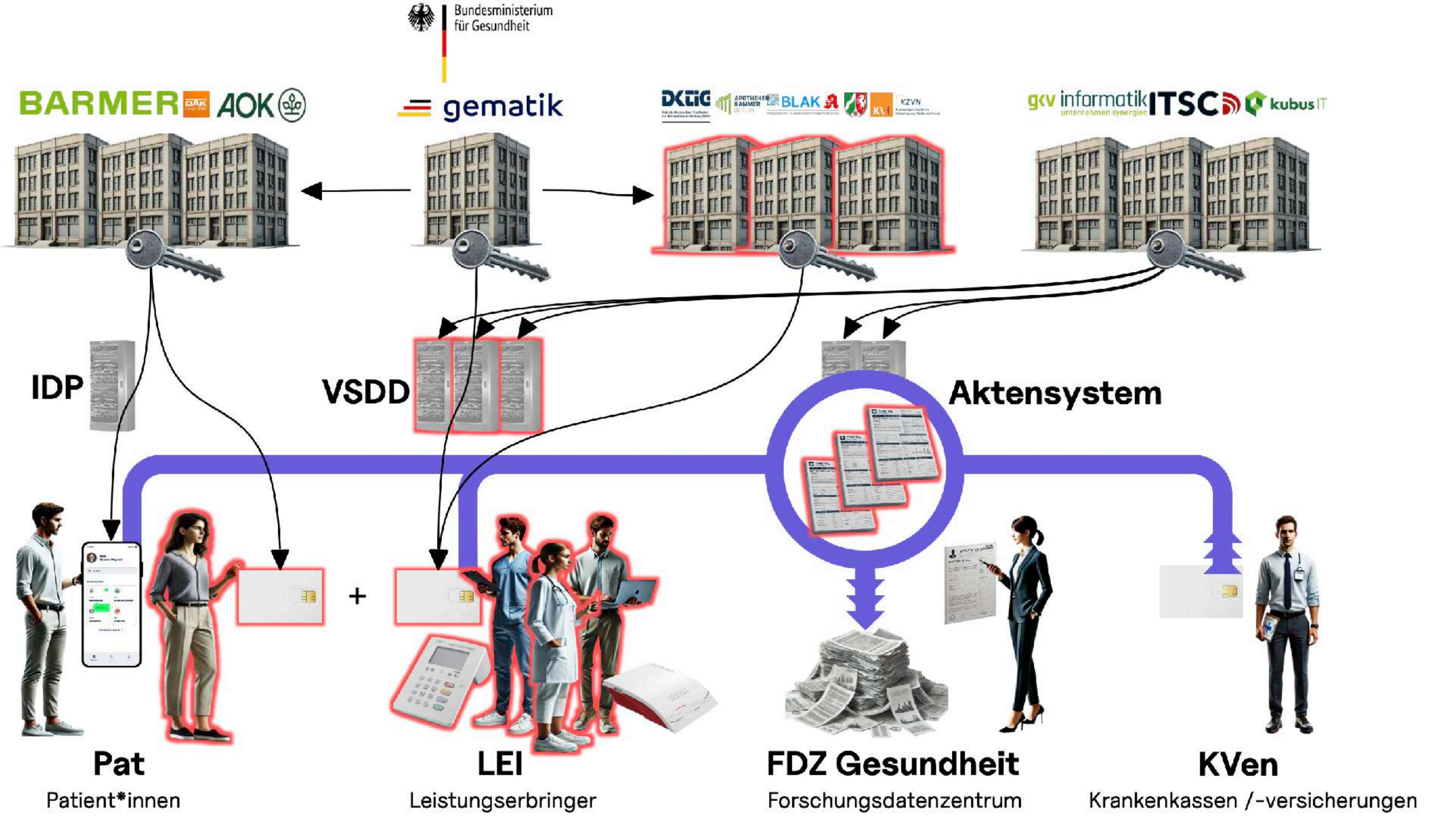
Gebühren oder Auslagen werden für diese Entscheidung nicht erhoben.

Begründung:

I.

Gemäß § 1 Absatz 1 Satz 1 IFG hat jeder nach Maßgabe dieses Gesetzes
Behörden des Bundes einen Anspruch auf Zugang zu amtlichen Information
Information im Sinne des IFG ist dabei jede amtlichen Zwecken dienend
unabhängig von der Art ihrer Speicherung (§ 2 Nr. 2 IFG). Ein solcher Ans
grds. auch gegen die SBK als bundesunmittelbare Körperschaft des öffe
richten.

Ein Anspruch auf Informationszugang besteht allerdings nicht, sofern das
der begehrten Informationen die öffentliche Sicherheit gefährden könnte, §


Bundesministerium
für Gesundheit
BARMER
DAK
AOK
gematik
DKTIG
APOTHEKER KAMMER BERLIN
BLAK
KZVN
gkv informatik
unternehmen synergien
ITSC
kubus IT
IDP
VSDD
Aktensystem
+
Pat
Patient*innen
LEI
Leistungserbringer
FDZ Gesundheit
Forschungsdatenzentrum
KVen
Krankenkassen /-versicherungen

Zugriff für Patient*innen
Zugriff für Patient*innen
Zugriff für Patient*innen
Zugriff für Patient*innen
Zugriff für Patient*innen
Zugriff für Patient*innen
Zugriff für Patient*innen
Zugriff für Patient*innen
Zugriff für Patient*innen
Zugriff für Patient*innen
Zugriff für Patient*innen

eGKs, PINs und Löschungen

Erlangung einer eGK (einer fremden Person)

Update

- Erlangung eGK seit 2014 in Folge möglich (2015, 2016, 2017, 2017, 2019, 2024)
- Zusendung PIN zur beantragten eGK erfolgreich (Januar 2025)

Krankenkassen

Whistleblower legt unbefugt Widerspruch gegen ePA ein

Ein Brief mit willkürlicher Unterschrift reichte aus, um unbefugt einen Widerspruch gegen die elektronische Patientenakte einzureichen. Es ist nicht das erste Sicherheitsproblem mit der ePA.

Britta Rybicki
05.05.2025 - 10:13 Uhr

Zugangsmittel für LEI
Zugangsmittel für LEI
Zugangsmittel für LEI
Zugangsmittel für LEI
Zugangsmittel für LEI
Zugangsmittel für LEI
Zugangsmittel für LEI
Zugangsmittel für LEI
Zugangsmittel für LEI
Zugangsmittel für LEI
Zugangsmittel für LEI

Kleinanzeigen, eHBAs und d(on't)-trust

News

Updates: Datenschutzvorfall 13. Januar 2025

Berlin, 24.01.2025 – Am 23.1.2025 hat die D-Trust ein Schreiben des Chaos Computer Clubs erreicht, in dem der Verein die Verantwortung für den Angriff auf das Antragsportal für Signatur- und Siegelkarten der D-Trust einem "anonymen Sicherheitsforscher" (sic!) zuschreibt. Dieser hat demnach Anfang Januar unzulässigerweise in mehreren Sitzungen Daten aus dem Antragsbearbeitungssystem entwendet (siehe unten).

Laut Aussage des „Sicherheitsforschers" seien die ausgelesenen Daten im Nachgang gelöscht worden, so dass den Betroffenen kein weiterer Schaden entstehe. Die in dem Schreiben gemachten Aussagen werden aktuell ausgewertet. In diesem Zusammenhang arbeitet die D-Trust weiterhin eng mit den involvierten Sicherheitsbehörden und externen Sicherheitsexperten zusammen.

Berlin, 22.01.2025 - Das IT-Sicherheitsteam der D-Trust GmbH arbeitet intensiv an der Aufarbeitung des Angriffs auf das Antragsportal für Signatur- und Siegelkarten. Dabei kooperiert die D-Trust eng mit den zuständigen Aufsichtsbehörden. Auch die Strafermittlungsbehörden sind infolge der Strafanzeige der D-Trust GmbH involviert.

5-Punkte-Plan für d(on't)-trust

24 January, 2025 17:34, linus

Mit bedeutungsschwangerer Cyber-Rhetorik will d-trust von der Verantwortung für ein großes Datenleck ablenken. Der CCC erklärt die Hintergründe und fordert Konsequen-

IT-SICHERHEITSLÜCKE

Datenleck D-Trust: Auch Zahnärzte und Justiz betroffen

10. Februar 2025, 12:17 Uhr

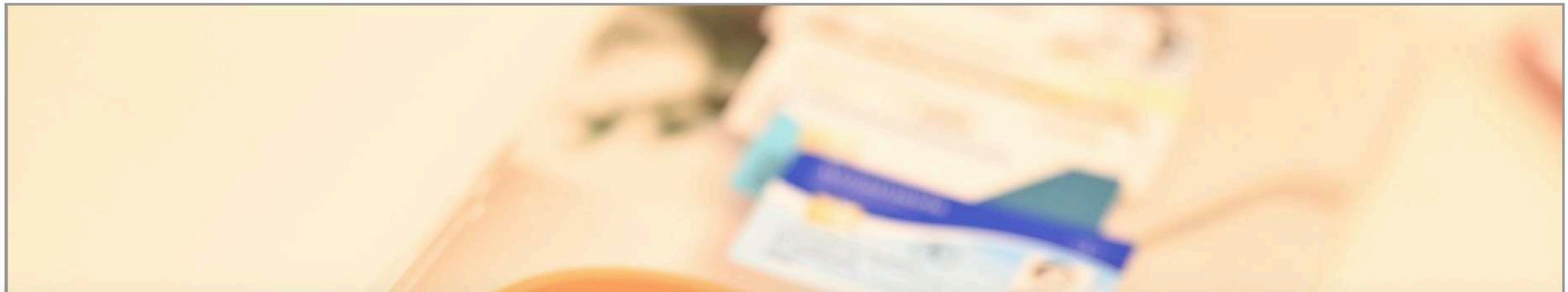
ARTIKEL HÖREN

Von dem IT-Sicherheitsvorfall beim Dienstleister D-Trust sind noch mehr Menschen betroffen als bisher gedacht. Nach Informationen von MDR SACHSEN-ANHALT sind die Daten von 300 Ärztinnen und Ärzten betroffen –

AUCH KAMMER HAT PROBLEME

Chaos bei HBA: Medisign verweist an Konkurrenz

APOTHEKE ADHOC, 21.11.2025 14:13 Uhr



a+ „KEINE HOFFNUNG, DASS ES RECHTZEITIG KLAPPT“

HBA-Chaos bei D-Trust: Karte wohl falsch zugestellt

Katharina Brand, 03.11.2025 10:31 Uhr aktualisiert am 07.11.2025 08:55 Uhr

14.11.2025 | News

Aktuelle Information TI-Verschlüsselungsalgorithmen: Umstellung von RSA auf ECC

Die gematik hat heute folgendes Update zur Umstellung der Verschlüsselungsalgorithmen an die Gesellschafter gegeben:

Die Umstellung der Verschlüsselungsalgorithmen RSA 2048 auf ECC 256 für die Telematikinfrastruktur (TI) läuft aktuell auf Hochtouren. Die gematik ergreift dafür alle erforderlichen Maßnahmen. Dazu gehört, dass die Umstellung mit klar definierten Fristen, verbindlichen Vorgaben und bedarfsabhängiger Eskalationsmechanismen vorangetrieben wird. Begleitend dazu wurden umfassende Leitfäden veröffentlicht, Testmöglichkeiten bereitgestellt und fortlaufend zu den aktuellen Entwicklungen kommuniziert, um alle Beteiligten zielgerichtet zu unterstützen. Ihr Engagement hat dazu beigetragen, dass die Informationen breitflächig geteilt worden sind. Dafür möchten wir uns an dieser Stelle bei Ihnen bedanken.

Zahlreiche Leistungserbringende haben bereits verantwortungsvoll gehandelt und einen Tausch betroffener Komponenten beauftragt bzw. durchgeführt. Dennoch sind insbesondere die Tauschprozesse bei den Heilberufsausweisen (HBA) – zu einem bedeutenden Anteil unabhängig vom Engagement der Leistungserbringenden – noch nicht auf dem Stand, den es für einen reibungslosen Wechsel zum Jahresende 2025 brauchen würde. Aktuell geht die gematik von etwa mehr als 30.000 HBA aus, die derzeit noch getauscht werden müssen.

Vor dem Hintergrund der hohen Anzahl noch zu tauschender HBA haben sich die gematik und ihre Gesellschafter für eine Übergangslösung eingesetzt, um die Gesundheitsversorgung in Deutschland ohne Beeinträchtigungen zum 1. Januar 2026 gewährleisten zu können. Infolgedessen konnte die gematik im intensiven Austausch mit der für den Bereich der Qualifizierten Elektronischen Signatur (QES) zuständigen Bundesnetzagentur und der eIDAS-Zertifizierungsstelle SRC eine Einigung für eine **Übergangslösung für Heilberufsausweise** erzielen.

Das bedeutet im Einzelnen:

- HBA, die ausschließlich RSA-Zertifikate enthalten (HBA G2.0), können noch **bis zum 30. Juni 2026** von betroffenen Leistungserbringenden genutzt werden. Danach können nur noch HBA eingesetzt werden, die auch über ECC-basierte Zertifikate verfügen (HBA G2.1), um beispielsweise E-Rezepte zu signieren.

Was macht eigentlich der Gebrauchtmarkt?

„§ 340a

Sicherer Umgang mit Komponenten zur Authentifizierung von Leistungserbringerinstitutionen

(1) Eine Komponente zur Authentifizierung von Leistungserbringerinstitutionen darf von demjenigen, an den sie ausgegeben wurde, weder entgeltlich noch unentgeltlich unbefugt weitergegeben werden. Bei Aufgabe der Leistungserbringerinstitution hat derjenige, an den eine Komponente zur Authentifizierung von Leistungserbringerinstitutionen ausgegeben wurde, oder dessen Nachfolger deren Sperrung unverzüglich zu veranlassen.

(2) Die Einrichtungsleitung einer ambulanten oder stationären Pflegeeinrichtung nach dem Elften Buch ist für die Einhaltung der Vorgaben nach Absatz 1 verantwortlich. Die Einrichtungsleitung hat darüber hinaus dafür Sorge zu tragen, dass die Pflegedienstleitung oder eine andere beschäftigte Person über einen gültigen elektronischen Heilberufsausweis oder eine digitale Identität für das Gesundheitswesen nach § 340 Absatz 6 verfügt.“

Praxisverwaltungssystem
Praxisverwaltungssystem
Praxisverwaltungssystem
Praxisverwaltungssystem
Praxisverwaltungssystem
Praxisverwaltungssystem
Praxisverwaltungssystem
Praxisverwaltungssystem
Praxisverwaltungssystem
Praxisverwaltungssystem

Die Praxis ist sicher?

Talk

GO BACK

BSI Project SiPra: Security of Doctor's Office Software

SLIDE DOWNLOAD COMING SOON.

VIDEO COMING SOON.

The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik - BSI) is running the project **SiPra** in order to assess the current state of security of management software for doctors' offices (Praxisverwaltungssysteme) in Germany. The goal is to get an overview over the state of the market and derive guidance and recommendations for doctors' offices and their IT environments.

As part of this project, ERNW is conducting a security assessment of four distinct products chosen by the BSI. All chosen vendors were contacted by the BSI and asked for cooperation. The goal was to be assisted during the installation process, with documentation, and if possible access the source code to conduct a white-box assessment to utilize the short time-frame as efficiently as possible.

In this presentation, we will share the results from our market analysis and findings of the technical security assessments. We highlight common vulnerabilities and vulnerability types identified in the different software products. We also discuss their implications for healthcare providers, and provide practical recommendations for potential remediation. Additionally, we address potential regulatory actions that can improve the security

Sicherheitsprobleme von PVS und angebundenen Systemen

Beispiel Authentifizierung eines Onlineportals

- Username numerisch aufsteigend (Enumeration)
- Keinerlei Durchsetzung von Passwort Policies
- Vollständig unwirksame Mehrfaktor-Authentifizierung (TOTP)

PUSH VERFÜGBARKEIT, AX
=> VERFÜGBARKEIT <=
:: VERFÜGBARKEIT ::
@experimental VERFÜGBARKEIT
0b00110011 | VERFÜGBARKEIT
[OK] 39C3 :: VERFÜGBARKEIT
$> netcat --port=VERFÜGBARKEIT
>>> VERFÜGBARKEIT <<<
/* === VERFÜGBARKEIT === */
[39C3VERFÜGBARKEIT] exec()
0xDEFEC8ED >> VERFÜGBARKEIT

Läuft die TI oder nicht?

„Tatsächlich lag die TI-Betriebsstabilität in den ersten gut zwei Monaten der sogenannten Hochlaufphase der ePA (29. April bis 9. Juli) bei 96 Prozent. Das klingt nicht so schlecht, entspricht jedoch hochgerechnet auf ein Jahr einer **Nichtverfügbarkeit von 14,5 Tagen**. Also über zwei Wochen, in denen die ePA für die Praxen nicht verfügbar ist.“

Dr. Sibylle Steiner, KBV, 12.09.25

PROBLEME BEI IBM DEUTSCHLAND

ePA: Störung zum verpflichtenden Start

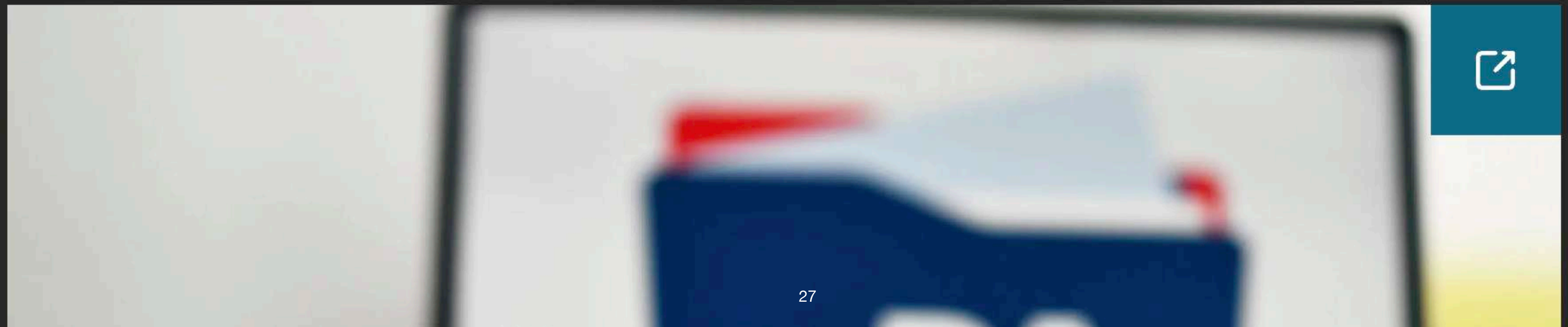
APOTHEKE ADHOC, 01.10.2025 10:35 Uhr aktualisiert am 01.10.2025 17:23 Uhr

Deutsches
Ärzteblatt

Politik

Wegen Betriebsstörungen bei ePA und Co: Stärkung der Gematik geplant

Donnerstag, 9. Oktober 2025



Deutsches
Ärzteblatt

Politik

Gematik räumt Unzufriedenheit mit Telematikinfrastruktur ein

Mittwoch, 3. Dezember 2025

VSDM++ Mitigationen
VSDM++ Mitigationen
VSDM++ Mitigationen
VSDM++ Mitigationen
VSDM++ Mitigationen
VSDM++ Mitigationen
VSDM++ Mitigationen
VSDM++ Mitigationen
VSDM++ Mitigationen
VSDM++ Mitigationen
VSDM++ Mitigationen

Steckt hier wirklich eine eGK?

VSDD

VSDM+

ICCSN

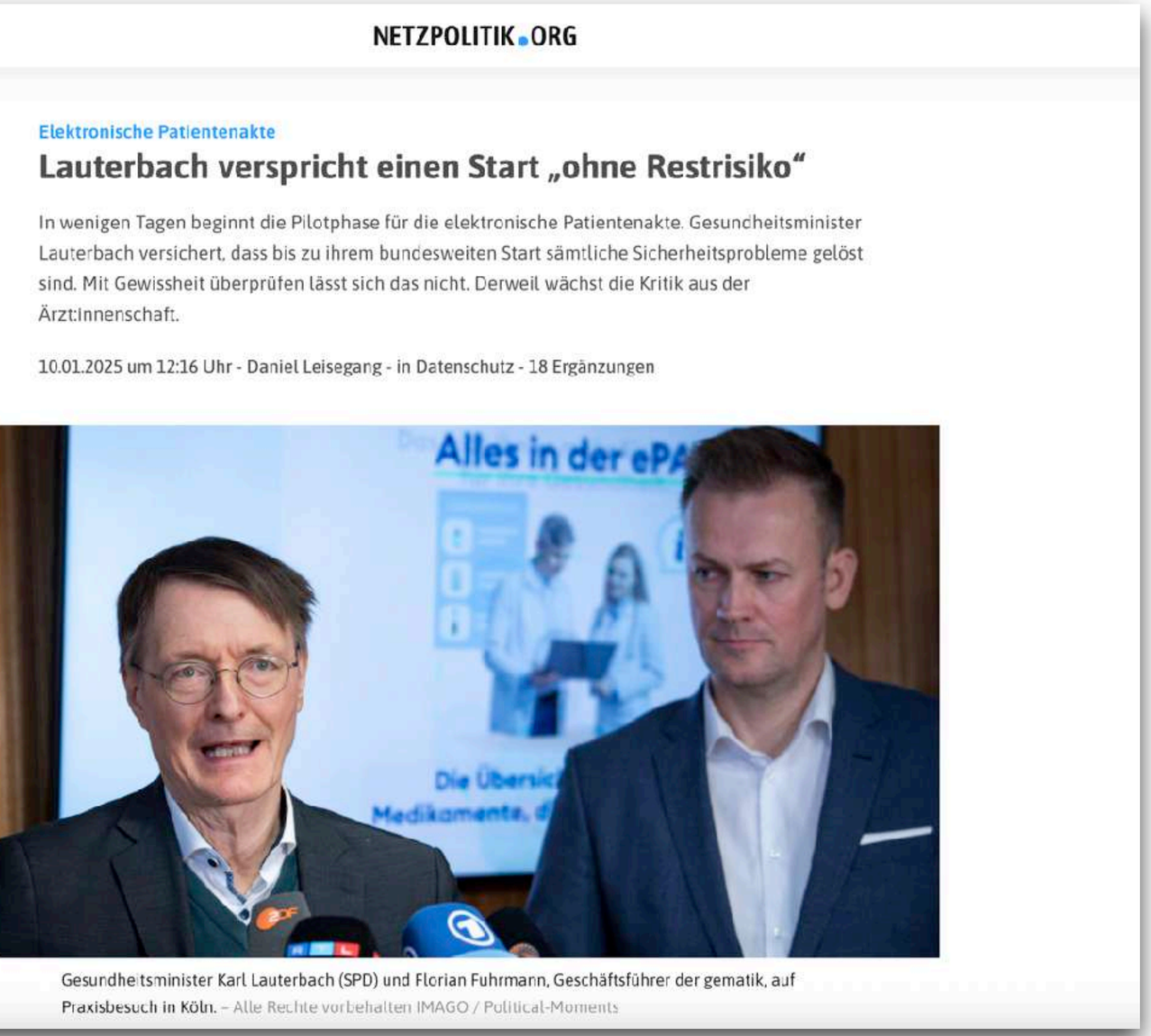
PNW

PNW

Daten

EF.GDO ICCSN

EF.C.eGK.AUT_CVC ICCSN



NETZPOLITIK.ORG

Elektronische Patientenakte

Lauterbach verspricht einen Start „ohne Restrisiko“

In wenigen Tagen beginnt die Pilotphase für die elektronische Patientenakte. Gesuncheitsminister Lauterbach versichert, dass bis zu ihrem bundesweiten Start sämtliche Sicherheitsprobleme gelöst sind. Mit Gewissheit überprüfen lässt sich das nicht. Derweil wächst die Kritik aus der Ärzt:Innenschaft.

10.01.2025 um 12:16 Uhr - Daniel Leisegang - in Datenschutz - 18 Ergänzungen

Gesundheitsminister Karl Lauterbach (SPD) und Florian Fuhrmann, Geschäftsführer der gematik, auf Praxisbesuch in Köln. – Alle Rechte vorbehalten IMAGO / Political-Moments

„Hinzu kommt, dass die von Kastl und Tschirsich genutzte **Sicherheitslücke auch einen anderen Fachdienst der gematik betrifft: das E-Rezept.“**

Daniel Leisegang, netzpolitik.org, 10.01.25

VSDM-Mangel von 2024

Maßnahmen, die das Individuum dagegen ergreifen könnte

- Häufig den Wohnort wechseln
- Häufig die Krankenkasse wechseln

Mitigationsmaßnahmen VSDM-Angriff

Stand der Technik

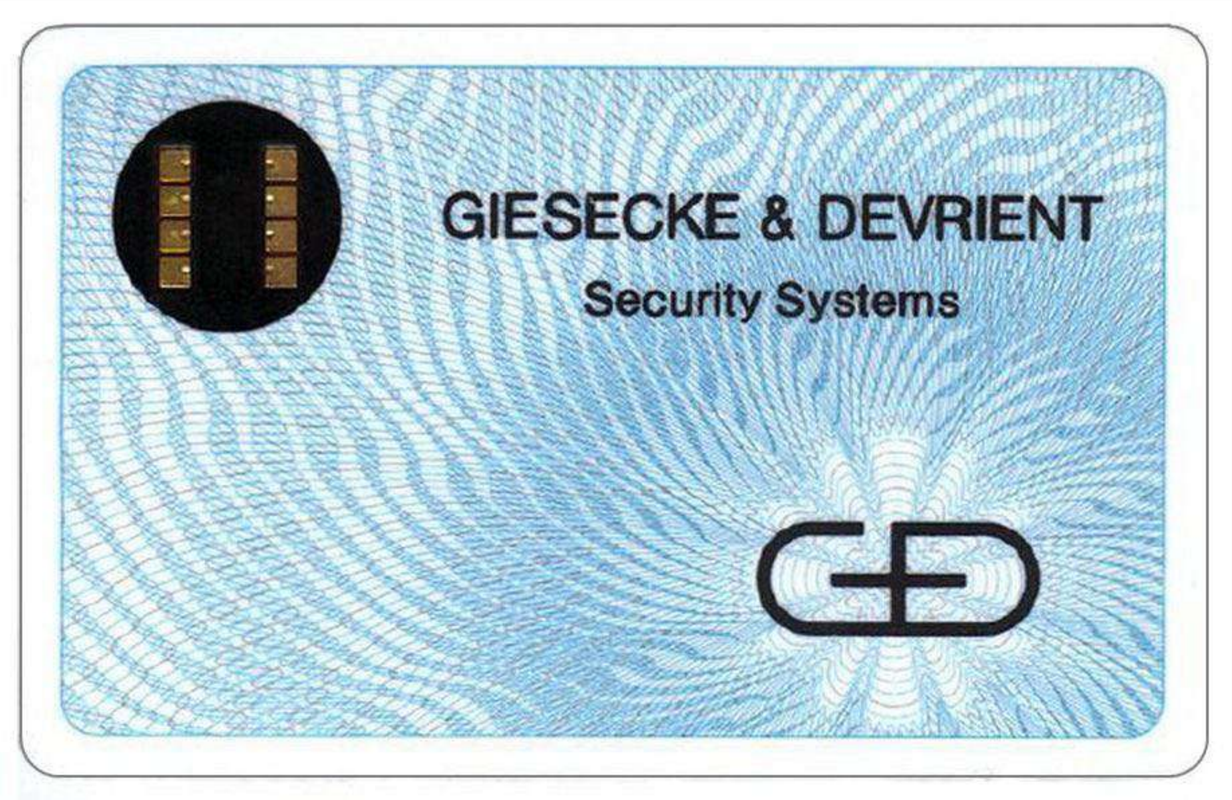
Potentiell unsicher

Zugang TI / SMC-B

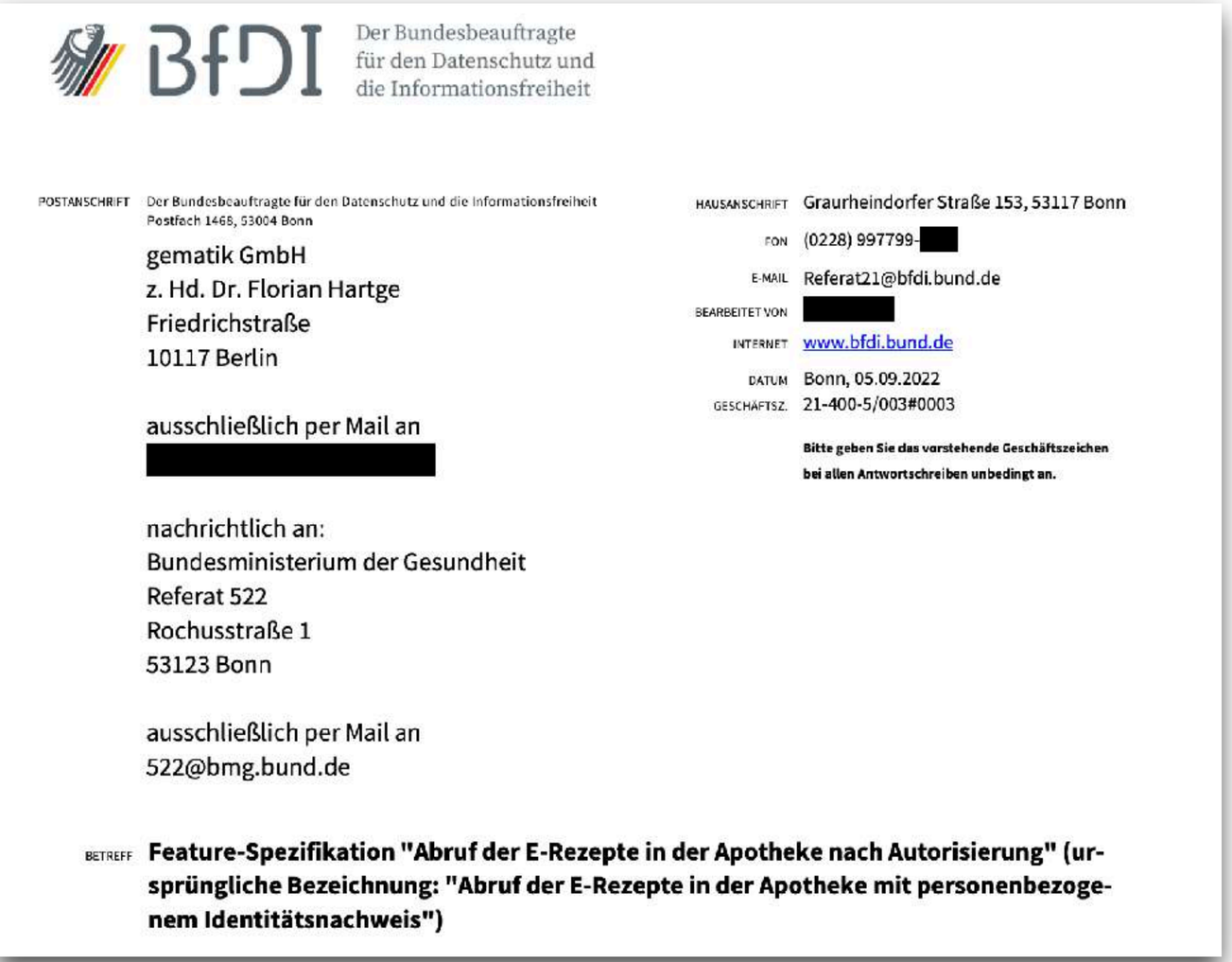
+ Nummern zählen

Sehr unsicher

1979



Erste Chipkarte von Giesecke & Devrient mit intelligentem Speicherchip von Siemens aus dem Jahr 1979. 8 Kontakte in 2 Spalten.



BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

gematik GmbH
z. Hd. Dr. Florian Hartge
Friedrichstraße
10117 Berlin

ausschließlich per Mail an
[redacted]

nachrichtlich an:
Bundesministerium der Gesundheit
Referat 522
Rochusstraße 1
53123 Bonn

ausschließlich per Mail an
522@bmg.bund.de

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-[redacted]
E-MAIL Referat21@bfdi.bund.de
BEARBEITET VON [redacted]
INTERNET www.bfdi.bund.de
DATUM Bonn, 05.09.2022
GESCHÄFTSZ. 21-400-5/003#0003

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Feature-Spezifikation "Abruf der E-Rezepte in der Apotheke nach Autorisierung" (ursprüngliche Bezeichnung: "Abruf der E-Rezepte in der Apotheke mit personenbezogenem Identitätsnachweis")**

„Prüfungsnachweise sind aus Gründen des VSDM-Designs nicht signiert. Der **E-Rezept-Fachdienst kann daher weder die Integrität noch die Authentizität** eines Prüfungsnachweise[s] überprüfen."

Zitat der gematik aus Schreiben von BfDI Prof. Dr. Kelber, 05.09.2022

Erstmaßnahmen Mitigation VSDM Mangel

Was, wenn authentitätsgeprüfte Daten nicht funktionieren?

- Verhinderung, dass Ausweise der Telematikinfrastruktur missbräuchlich verwendet werden können
- Schließung der Sicherheitslücke durch eine zusätzliche Verschlüsselung der Krankenversichertennummer
- Sensibilisierung der Nutzerinnen und Nutzer der Telematikinfrastruktur im Umgang und Schutz der technischen Infrastruktur, Ausweisen und Karten
- Ausweitung der Überwachungsmaßnahmen wie Monitoring und Anomalie-Erkennung

Wie das Rate-Limit umgesetzt wurde...

Intermediär

Vermittler für Versichertenstammdaten

Der Intermediär VSDM in der TI – Das

Der Intermediär für das Versichertenstammdaten-Management ist ein fa
Telematikinfrastruktur. Er unterstützt die Anwendungsfälle der Fachanwe
Fachmodul an die Fachdienste VSDM weiterreicht und die Antworten zus
te der zentralen TI-Plattform, zum Beispiel durch Zugriff auf Zertifikatsva

Der Intermediär muss in hohem Maß verfügbar sein, da die Fachdienste
tem und Versichertenstammdatendienst der Krankenversicherungen nic
ausfällt.

1 - Entitlement Management – RateLimit-oid-List: Maximale Anzahl von Befugnissen für

nent Management MUSS in der *RateLimit-oid-List* sicherstellen, dass eine LEI mit der Rolle

axis_arzt maximal 200 Befugnisse
ankenhaus maximal 1.000 Befugnisse
stitution-vorsorge-reha maximal 1.000 Befugnisse
hnarztpraxis maximal 200 Befugnisse
fentliche_apotheke maximal 200 Befugnisse
axis_psychotherapeut maximal 100 Befugnisse
stitution-pflege maximal 100 Befugnisse
stitution-geburtshilfe maximal 100 Befugnisse
axis-physiotherapeut maximal 100 Befugnisse
axis-ergotherapeut maximal 100 Befugnisse
axis-logopaede maximal 100 Befugnisse
axis-podologe maximal 100 Befugnisse
axis-ernaehrungstherapeut maximal 100 Befugnisse
stitution-oegd maximal 100 Befugnisse
stitution-arbeitsmedizin maximal 100 Befugnisse

iner Stunde durch das Primärsystem im Aktensystem registrieren kann.

Mitigationsmaßnahmen VSDM-Angriff

Stand der Technik

Potentiell unsicher

Zugang TI / SMC-B

\+ Nummern zählen

\+ Rate Limit

Sehr unsicher

Mitigation VSDM Mangel - Identifier

Wie hilfreich sind Identifier?

Identifier	Agilität	Komplexität / Erratbarkeit	Geheimnisfaktor
ICSSN	**Okay (5 Jahre)**	Schlecht	**Gut**
KVNR	Schlecht (lebenslang)	**Gut**	Eher schlecht

ICSSN
802760099900123456 78

KVNR
T026292252

W;Ordnungsbegrifftyp;Ordnungsbegriff;Anzahl Fehllogin;Partner ID;Mandant ID;Salt;Nachname;Vorname;Geburtsdatum;VIP;ICCSN

You must be logged in to see this link.

img + xlsx

d in to see this link.

IRA system You must be logged in to see this link.

Mitigation VSDM Mangel

Schaffung der VSDM-Prüfziffer Version 2

- Für Zugriff auf ePA müssen folgende Informationen abgeglichen werden:
  - Kartennummer (ICSSN)
  - Krankenversicherungsnummer (KVNR)
  - Sowie eine Hash Check Value aus
    - Straße und Hausnummer der Person
    - Datum des Versicherungsbeginns

Mitigationsmaßnahmen VSDM-Angriff

Stand der Technik

Zugang TI / SMC-B

\+ Nummern zählen

\+ Rate Limit

\+ KVNR

\+ Hash Check Value

Potentiell unsicher

Sehr unsicher

ELEKTRONISCHE PATIENTENAKTE

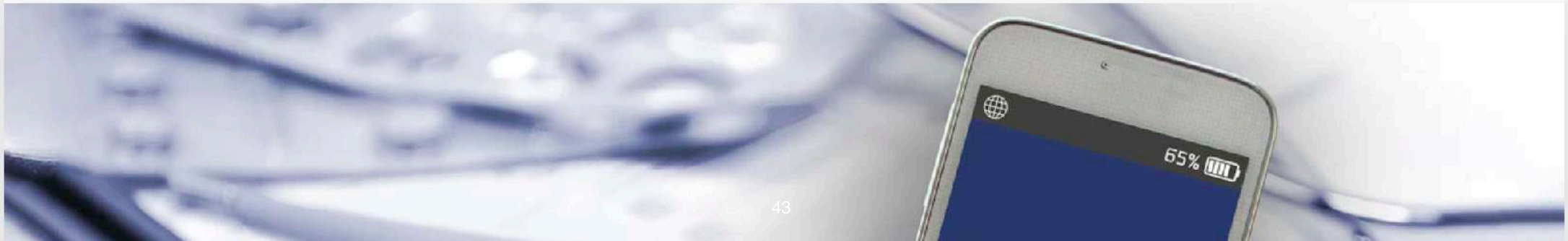
ePA-Hacker warnen vor übereiltem Start der Akte im April

Können Patientinnen und Patienten der elektronischen Patientenakte vertrauen? Die IT-Sicherheitsforscher Bianca Kastl und Martin Tschirsich sind skeptisch.

Von S. Schersch (Medizinredakteurin), A. Vahid Roodsari (Medizinredakteur) • 25.03.2025

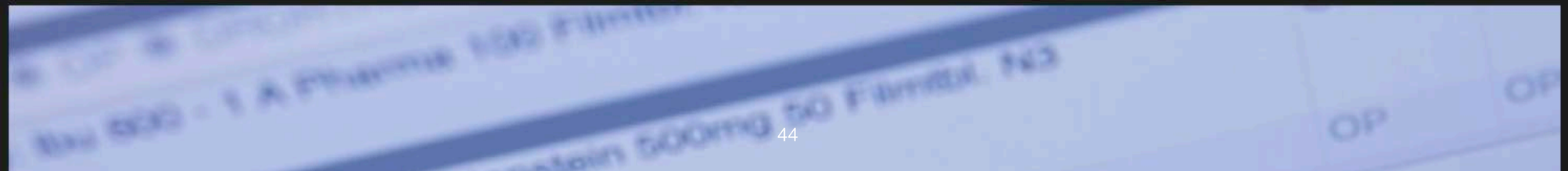
Jetzt hören, statt zu lesen

Diese Audiodatei wurde mit KI erzeugt.



IT-Experten sehen Sicherheitsmängel bei E-Patientenakte nicht beseitigt

16. April 2025 • 15:55 Uhr



BUNDESWEITER START AM 29. APRIL

Lauterbach: „Die sicherste ePA von allen“

dpa/ APOTHEKE ADHOC, 16.04.2025 17:01 Uhr

Die ePA habe viel zu lange für den Start gebraucht, jetzt sei es an der Zeit, damit Menschen zu retten, so Karl Lauterbach (SPD).

Foto: APOTHEKE ADHOC


TK-App
LTE
HD
Sicherheitsmängel bei
E-Patientenakte
tagesschau

EILMELDUNG — Hacker hebeln erweiterten Schutz der elektronischen Patientenakte aus

EILMELDUNG

S+ Digitalisierung in der Medizin: Hacker hebeln erweiterten Schutz der elektronischen Patientenakte aus

»Die ePA bringen wir erst dann, wenn alle Hackerangriffe technisch unmöglich gemacht worden sind«, hat Karl Lauterbach im Januar verkündet. CCC-Experten haben nun bewiesen: Er hat zu viel versprochen. Die Betreiber reagieren mit einer Notfallmaßnahme. Von Patrick Beuth und Marcel Rosenbach

7 Min

Elektronische Ersatzbescheinigung als Versicherungsnachweis ab sofort* nutzbar

Digitalisierung

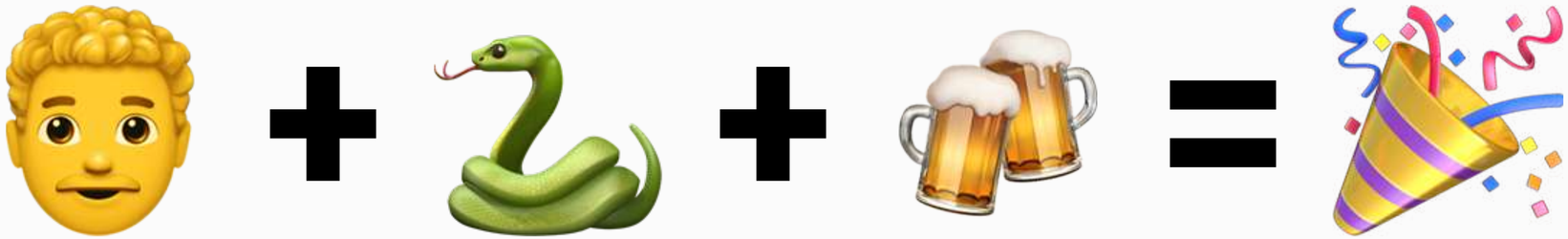
28.10.2024

← Zurück zur Übersicht

Patienten ist es ab sofort möglich die elektronische Ersatzbescheinigung zu nutzen, wenn Ihre elektronische Gesundheitskarte (eGK) in der Praxis nicht eingelesen werden kann oder vergessen wurde. Die Anwendung dieses Verfahrens ist derzeit für Krankenkassen und Arztpraxen noch freiwillig, bevor sie ab Juli 2025 zur Pflicht wird.

Für die Nutzung muss der Kommunikationsdienst KIM im Praxisverwaltungssystem (PVS) vorhanden sein, da die Zustellung der elektronischen Ersatzbescheinigung auf diesem Weg erfolgt. In wenigen Minuten werden die Versichertendaten automatisiert zu Verfügung gestellt und können dann direkt aus dem KIM-Postfach in das PVS übertragen werden. Damit entfällt das händische Einpflegen, was beim papiergebundenen Ersatzverfahren notwendig ist und sorgt damit für eine Entlastung des Praxispersonals.

Die Ersatzbescheinigung wird durch den Patienten über die Applikation der Krankenkasse angefragt und dabei die KIM-Adresse der Praxis an die Krankenkasse übermittelt. Sobald die Anfrage bei der Krankenkasse eingeht wird die Bescheinigung automatisch generiert und per KIM an die Praxis gesendet.



Umgehung VSDM Prüfziffer Version 2

Woher kommen die Informationen?

Identifier	Quelle
ICSSN	**Leaks (z.B. hier)**
KVNR	eEB Profil für KVNR (PLZ, Name, Geburtsdatum, Kasse)
Adresse	eEB Profil für Bescheinigung (KVNR, Kasse)
Datum des Versicherungsbeginns	eEB Profil für Bescheinigung (KVNR, Kasse)

30.04.2025 | ePA

Aktuelles | ePA-Sicherheitslücke geschlossen

Der gematik liegen Informationen vor, dass der Chaos Computer Club ein Szenario für unberechtigte Zugriffe auf die elektronische Patientenakte beschrieben hat. Über elektronische Ersatzbescheinigungen für Versichertenkarten könne man an Informationen gelangen, um auf einzelne elektronische Patientenakten (ePA) zuzugreifen. Die gematik hat die Sicherheitslücke, die für einzelne Versicherte weniger Krankenkassen bestehen könnte, geschlossen. Die potenziell betroffenen Versicherten werden identifiziert und geschützt.

Bundesgesundheitsminister Prof. Karl Lauterbach:

„In der Frühphase des ePA-Starts war mit solchen Angriffsszenarien zu rechnen. Ich bin der gematik dankbar, dass sie auf die ersten Hinweise direkt reagiert und die Sicherheitslücke geschlossen hat. Die elektronische Patientenakte muss sehr gut geschützt bleiben. Massenangriffe auf Patientendaten müssen ausgeschlossen bleiben."

gematik-Geschäftsführer Dr. Florian Fuhrmann:

„Der bundesweite Rollout der ePA wird von unseren Sicherheitsteams gemeinsam mit dem BSI eng begleitet. Hinweise externer Sicherheitsforscher:innen gehen wir in standardisierten Prozessen umgehend nach und leiten bei entsprechender Bewertung passende Maßnahmen ein. Aufgrund der Hinweise haben wir präventiv als erste Sofortmaßnahme das Verfahren vorerst ausgesetzt, das bereits einige Kassen für Ersatzbescheinigungen alternativ zur Versichertenkarte (eGK) nutzen. Wir prüfen und monitoren laufend und mit höchster Priorität. Wir haben bislang keine Hinweise darauf, dass es einen unbefugten Zugriff auf elektronische Patientenakten gegeben hat."

Laut CCC ist es möglich gewesen, über Elektronische Ersatzbescheinigungen von Versichertenkarten den Behandlungskontext einer versicherten Person zu fälschen. In Kombination mit der Versichertennummer, einem Codierungsschlüssel sowohl einem illegal beschafften Praxisausweis (SMC-B) und einem Anschluss an die Telematikinfrastruktur (TI) wäre damit theoretisch der Zugriff auf Patientenakten vereinzelt möglich. Die gematik geht nicht davon aus, dass Versichertendaten tatsächlich abgeflossen sind.

Mitigation VSDM Mangel, Part 2

Anpassung eEB

- Schaffung eines EEBCoverageEgkNoAddressLine Profils (jetzt mit ohne Adresse)
- Teilweise Modifikation von Versicherungsdatum (z. B. Rückgabe von 01.01.1900 als Versicherungsbeginn)
- Rate Limit (wieder mal)

Mitigationsmaßnahmen VSDM-Angriff

Stand der Technik

Zugang TI / SMC-B

\+ Nummern zählen

\+ Rate Limit

\+ KVNR

\+ Hash Check Value

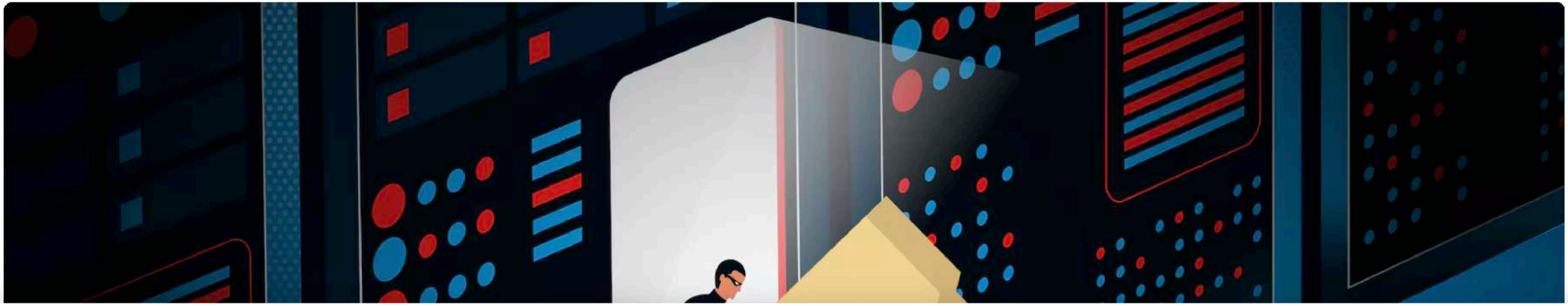
\+ Modifizierte eEB

Potentiell unsicher

Sehr unsicher

Chaos Computer Club warnt

Warum die elektronische Patientenakte noch immer nicht ganz sicher ist



„Die Krankenkasse darf und kann beispielsweise nicht auf die Inhalte [der ePA] zugreifen.“ *

Allerdings liegen bei Krankenkassen aktuell auch alle Daten, um technisch gesehen Karten simulieren zu können.

POSITIONSPAPIER

Digitalstrategie für eine zukunftsgerichtete Gesundheitsversorgung

Beschlossen vom Verwaltungsrat am 5. Dezember 2025

PoPP

Proof of Patient Presence: Nachweis des Versorgungskontextes als kryptografisch gesicherter Token

Hinweise zu Standardkartenlesern →

Zuverlässiger Dienst in der TI 2.0

PoPP (Proof of Patient Presence) ist ein singulärer Plattformdienst der TI 2.0. Er liefert einen kryptografisch gesicherten Token, der Gesundheitseinrichtungen einen ortsunabhängigen Zugriff auf Versichertendaten und damit auf TI-Anwendungen wie die elektronische Patientenakte (ePA) oder das E-Rezept ermöglicht. Der Zugriff wird ausschließlich in einem gemeinsamen Versorgungskontext gewährt, beispielsweise während einer Behandlung oder Beratung.

Im Rahmen der Erzeugung eines PoPP-Token verfolgt der PoPP-Service bei der Kommunikation mit einer Smartcard die folgenden Ziele:

1. Der PoPP-Service überzeugt sich, dass es sich bei der Smartcard um eine echte eGK handelt.
2. Der PoPP-Service überzeugt sich, dass die eGK gültig ist.
3. Der PoPP-Service liest aus der eGK Daten aus, die für die Erstellung des PoPP-Token relevant sind.

Die genannten Ziele werden bei kontaktbehafteter Kartenkommunikation mit einer eGK basierend auf [gemSpec_eGK_ObjSys_G2.1] wie folgt erreicht:

1. Der PoPP-Service baut einen Trusted Channel mit der Identität ID.C.eGK.AUT_CVC.E256 auf. Gelingt dies, dann ist die Echtheit der eGK bestätigt.
2. Der PoPP-Service liest innerhalb des Trusted Channel das X.509-Zertifikat aus der Datei EF.C.CH.AUT.E256 aus und überprüft dieses auf Gültigkeit.
3. Der PoPP-Service konsultiert eine Datenbank, welche die Frage beantwortet: Stammen das CV-Zertifikat der Echtheitsprüfung und das präsentierte X.509-Zertifikat aus ein und derselben eGK? So eine Datenbank wird in [6.1.1.9 eGK-Hash-Datenbank] beschrieben.
4. Der PoPP-Service entnimmt dem ausgelesenen X.509-Zertifikat die für das PoPP-Token notwendigen Informationen.

Die genannten Ziele werden bei kontaktloser Kartenkommunikation mit einer eGK basierend auf [gemSpec_eGK_ObjSys_G2.1](die einen PACE Kanal voraussetzt) wie folgt erreicht:

1. Der PoPP-Service authentisiert die eGK mit der Identität ID.C.eGK.AUT_CVC.E256. Wegen [gemSpec_COS#N107.235)b] ist es nicht möglich dabei einen Trusted Channel zwischen PoPP-Service und eGK zu etablieren.
2. Der PoPP-Service liest aus der eGK das X.509-Zertifikat aus der Datei EF.C.CH.AUT.E256 aus und überprüft dieses auf Gültigkeit. Da der Kommunikationskanal zwischen PoPP-Service und eGK im kontaktlosen Fall nicht Ende-zu-Ende gesichert ist, ist der PoPP-Service nicht ohne weiteres in der Lage zu beurteilen, ob das ihm präsentierte X.509-Zertifikat von derselben eGK stammt, deren Echtheit er mit der Identität ID.C.eGK.AUT_CVC.E256 überprüft hat. Deshalb konsultiert der PoPP-Service im kontaktlosen Fall eine Datenbank, welche die Frage beantwortet: Stammen das CV-Zertifikat der Echtheitsprüfung und das präsentierte X.509-Zertifikat aus ein und derselben eGK? So eine Datenbank wird in [6.1.1.9 eGK-Hash-Datenbank] beschrieben.
3. Der PoPP-Service entnimmt dem präsentierten X.509-Zertifikat die für das PoPP-Token notwendigen Informationen.

OneRoadmap gematik-Produkte Q4-2025

Planung vorbehaltlich der aktuellen Auswirkungsanalyse zu EHDS

2025 (Q1 Q2 Q3 Q4) | 2026 (Q1 Q2 Q3 Q4) | 2027 (Q1 Q2 Q3 Q4)

ART Anwendungen

KIM

KIM 1.5.4 (Kommunikation im Medizinwesen)
- Betriebsdatenerfassung BDE 2

KIM 1.6
- Anbindung FHIR-VZD an KIM

KIM Backlog
- Anwendungskennzeichen
- Nutzererweiterung durch mobile Szenarien
- KIM auf Basis TI 2.0 konnektorlos
- Mailkontoverwaltung durch IMAP

VSDM

VSDM 2.0 - Fachdienste
§ online Leistungspflichtprüfung der KK
§ Versicherungsnachweis durch Nutzung eGK/digit. ID
- Erweiterung FHIR Basis Profil für VSDM 2
- Betrieb VSDM2
- Außerbetriebnahme VSDM1

§ *291a Abs.2 & 291b Abs.1+2 - 1.1.26*

VSDM 2.0 - Clientsysteme
§ online Leistungspflichtprüfung bei VSDM2
§ Versicherungsnachweis durch digit. ID und eGK,
- mit PoPP 1.0 ausschließlich Nutzung der eGK, keine Nutzung der digit. ID
- mit PoPP 2.0 zusätzlich PoPP Nachweis aus dem mobilen Workflow sowie digit. ID nutzbar
- Migration von VSDM1 auf VSDM2
- Migration (Nicht)Nutzung VSDM++ zu PoPP (in Produkten die VSDM++ nutzen, ePA, eRX)

§ *291a Abs.2 & 291b Abs.1+2 - 1.1.26*

Digitale Patienten-rechnung

DiPag1.0 - Digitale Patientenrechnung
MVP
- Rechnungsübermittlung über Fachdienst an den Versicherten
- Verwaltung der Rechnungen durch Versicherten
- Einreichung durch den Versicherten per Frontend an Kostenträger
- Abruf digitalisierter-, per Post eingereichter Rechnungen durch den KTR
- Unterstützung von Rechnungen med. oder sonst. Leistungen (nicht Sachleistungsprinzip)

Ärzte, Zahnärzte, Apotheken, PKV Versicherte, Beihilfeversicherte

- Unterstützung der Gebührenordnungen GOÄ , GOZ (und BEMA)
- Nutzung des Fachdienstes für Versicherte 16+
- Pauschale Berechtigungen für LEI zur Rechnungsübermittlung und Versichertenwiderspruch
- techn. Validierung der Rechnung auf Basis festgelegter Pflichtfelder für eine erfolgreiche Zustellung

DiPag Backlog
- Einreichung per Fachdienst
- Leistungsabrechnung
- Gebührenordnungen
- Weitere Rechnungstypen
- Berechtigungsverwaltung
- Rechnungsarchivierung

Weitere LE-Sektoren (KH, Pflege...)

Art Basic Infrastructure

Identitäts-management

(PT IDM)

VertrReg 1.0 - Vertreterregelung
- Anwendungsübergreifende Vertreterregelung bzw. -funktion

IDM Backlog
- digitaleID für Leistungserbringerinstitutionen (LEI/O)

PAT 1.0
- Bestätigungsverfahren Plattformanwendungen der TI

LISA 1.5 - LE ID Signatur Authentisierung
- TI-Fernsignatur (Q2/2026); Fokus: Krankenhaus

§ *312 Abs.1 S.1 Nr.8b - 1.4.23*
§ Digitale Identität für LE (2027)

LE (HBA, digID, ggfs. Wallet)
- EUdi Wallets bereitgestellt

§ *340 Abs.6 - 1.1.25*

gID 3.0 - GesundheitsID 3.x (Versicherte) - Wallet & eIDAS 2.0

FedMaster 2.0 - Neuaufstellung Federation Master
- Betriebliche Ausrichtung des Federation Master an den sicherheitstechnischen Anforderungen der neuen TI
- Ausrichtung am PAT Prozess
- Automatisierung und Verbesserung des aktuellen Registrierungsprozess durch Überarbeitung und Bereitstellung eines Portals

Verzeichnis-dienst

(PT Directory)

VZD SSP 1.0 (Self Service Portal)
- Authentisierung am SSP
- Lesezugriff auf Daten
- teilw. Schreibzugriff (Mehrwertdaten)

Kartenherausgeber, Leistungserbringer, Kostenträger

VZD FHIR 1.3
- Einf. Prüfmatrix (bis 17.3.25)
- Schwenk APO- zu FHIR VZD
- Systemstabilisierung und Performance

§ *313 Abs.1,3,4*

VZD FHIR 1.4
- Systemstabilisierung und Performance
- Abkündigung APO-VZD
- Verbesserung/Sicherstellung der Datenqualität
- ECC Unterstützung

VZD LDAP 3.3
- Systemstabilisierung und Performance
- ECC Readyness
- Optimierung der Datenqualität
- LDAP-Abkündigungsstrategie entwickeln

VZD Backlog
- Implementierung Zero Trust Policy
- User Discovery zur Identifizierung von VZD Nutzungserwartungen
- Einführung weitere Authentisierungsmöglichkeiten für das Self-Service-Portal
- Abbildung von Organisationsstruktur für u.a. TI-Messenger
- Weitere Optimierung der VZD Suche
- Abkündigung LDAP VZD

TI-Zugang

(PT Edge)

TI-G 2.0
- RSA2ECC
- HSK mit HSM-B
- HSK PTV6-Featurescope
- Zugangsmodul HSM-B-ready

TI-G 3.0
- Optimierung Anbindung CloudPS

TI-G Backlog
- Positionierung / Umbau TI-Service-Hub
- Ggfs. Erweiterung um KIM-Modul

Neue Zugangswege
Neue Zugangswege
Neue Zugangswege
Neue Zugangswege
Neue Zugangswege
Neue Zugangswege
Neue Zugangswege
Neue Zugangswege
Neue Zugangswege
Neue Zugangswege
Neue Zugangswege

Rückkehr einer Brücken-Technologie?

2025-12-27 00:30:00

Wählen Sie die gewünschte Anwendung durch Klicken auf das passende Bild:

Registrierte Gesundheits-IDs (Verlauf)

Registrierte Gesundheits-IDs

4.301.573

PER VIDEO

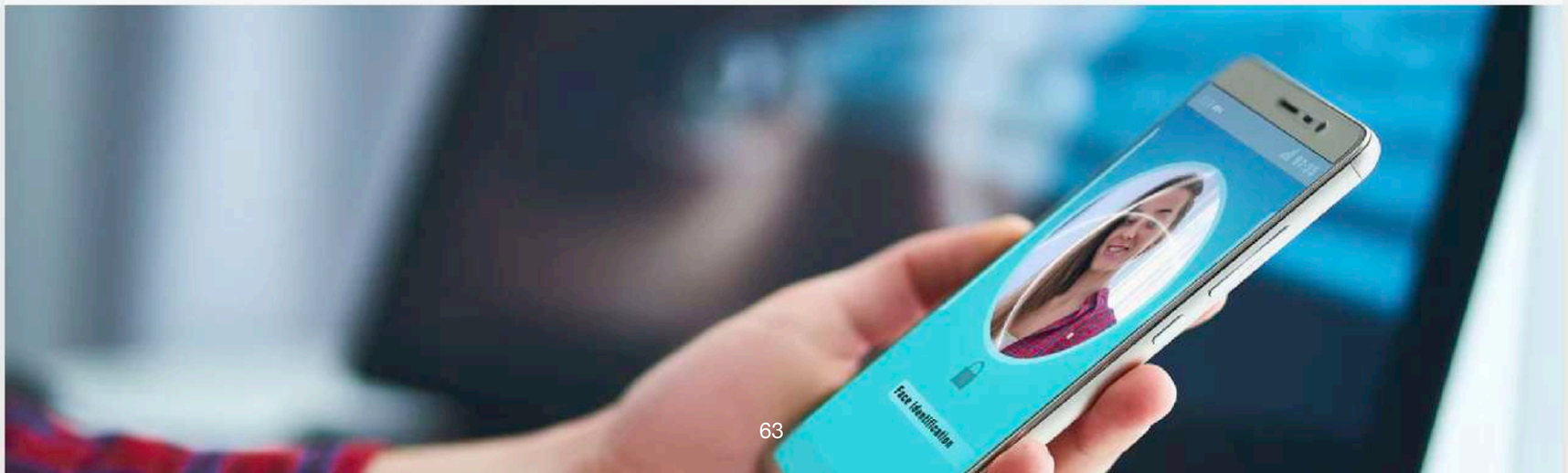
Neues Ident-Verfahren für Krankenkassen-Angebote wie die ePA

Für das Freigeben von Krankenkassen-Diensten wie die elektronische Patientenakte benötigen Versicherte eine PIN. Die kann jetzt auch per Video beantragt werden.

Von Ali Vahid Roodsari (Medizinredakteur) • 15.08.2025

Jetzt hören, statt zu lesen

Diese Audiodatei wurde mit KI erzeugt.



„Im Gesundheitssektor **gelten Vertrauensniveaus als erreicht, wenn ein Sicherheitsgutachten bestätigt**, dass das Identifizierungsmittel entsprechenden Angriffsmöglichkeiten „standhält“.“

Prüfung „Digitale Identitäten“ des Bundesrechnungshofes, 12.09.25

01.12.2025 | News

gematik bestätigt Eignung von VideoIdent-Verfahren für die Einrichtung der GesundheitsID

Die gematik hat gemäß der Prozessprüfung „Level of Assurance (LoA) gematik-ehealth-loa-high" die Eignung des Identifizierungsverfahrens „Nect ePass" von Nect GmbH für die Einrichtung der GesundheitsID bestätigt. Damit steht Versicherten neben der Online-Ausweisfunktion des neuen Personalausweises (nPA) künftig ein weiteres, biometriebasiertes Identifizierungsverfahren zur Verfügung, um Zugang zu digitalen Gesundheitsanwendungen zu erhalten. Die GesundheitsID wird bspw. für die Nutzung der ePA-App benötigt. Das sichere VideoIdent-Verfahren ermöglicht eine ortsungebundene Einrichtung der GesundheitsID ohne PIN, sofern Krankenkassen ihren Mitgliedern diese Möglichkeit anbieten.

Bereits im August 2025 hat die gematik die sicherheitstechnische Eignung des Verfahrens für die digitale Identitätsbestätigung zur PIN-Ausgabe und Freischaltung der elektronischen Gesundheitskarte (eGK) ausgestellt. Mit der nun erfolgten Bestätigung zur Nutzung im Rahmen der GesundheitsID wird der Anwendungsbereich des Verfahrens entsprechend erweitert.

Das Verfahren „Nect ePass" kombiniert ein biometrisches Identifikationsverfahren mit dem elektronischen Auslesen von Ausweisdokumenten (z. B. Personalausweis oder Reisepass). Die Bestätigung beschränkt sich auf die „Stand Alone"-Version der „Nect App". Das bedeutet, dass das Verfahren in Drittanwendungen – beispielsweise Anwendungen der Krankenkassen – nicht integriert werden darf.

zurück

Biometrische Authentifierung

Gematik gibt Nect Ident mit ePass frei

01.12.2025 · Von Stephan Augsten · 2 min Lesedauer ·

Bislang mussten Krankenversicherte eine eID-PIN nutzen, um eine GesundheitsID zu erstellen und auf ePA, E-Rezept und TI-Messenger zugreifen zu können. Mit Nect Ident und einer zugehörigen digitalen Wallet hat die Gematik nun ein biometrisches Verfahren als alternativen Authentifizierungsweg freigegeben.

„Mit Zustimmung des Versicherten **sind die Krankenkassen hierbei befugt, zur Prüfung der Identität des Versicherten Daten** entsprechend den Vorgaben des § 20 Absatz 3a Satz 1 des Personalausweisgesetzes, des § 16a Absatz 3 Satz 1 des Passgesetzes und des § 78 Absatz 7 Satz 3 des Aufenthaltsgesetzes zu den betroffenen Datenkategorien und deren Verarbeitung auszulesen und zu verwenden.“

Beschlussempfehlung und Bericht zum Gesetz zur Befugniserweiterung und Entbürokratisierung in der Pflege

Alte (Un-)Sicherheiten
Alte (Un-)Sicherheiten
Alte (Un-)Sicherheiten
Alte (Un-)Sicherheiten
Alte (Un-)Sicherheiten
Alte (Un-)Sicherheiten
Alte (Un-)Sicherheiten
Alte (Un-)Sicherheiten
Alte (Un-)Sicherheiten
Alte (Un-)Sicherheiten
Alte (Un-)Sicherheiten

Wie wir zu diesem Stand der (Un-)sicherheit gekommen sind

BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

gematik GmbH
z. Hd. Dr. Florian Hartge
Friedrichstraße
10117 Berlin

ausschließlich per Mail an
[redacted]

nachrichtlich an:
Bundesministerium der Gesundheit
Referat 522
Rochusstraße 1
53123 Bonn

ausschließlich per Mail an
522@bmg.bund.de

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-[redacted]
E-MAIL Referat21@bfdi.bund.de
BEARBEITET VON [redacted]
INTERNET www.bfdi.bund.de
DATUM Bonn, 05.09.2022
GESCHAFTSZ. 21-400-5/003#0003

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Feature-Spezifikation "Abruf der E-Rezepte in der Apotheke nach Autorisierung" (ursprüngliche Bezeichnung: "Abruf der E-Rezepte in der Apotheke mit personenbezogenem Identitätsnachweis")**

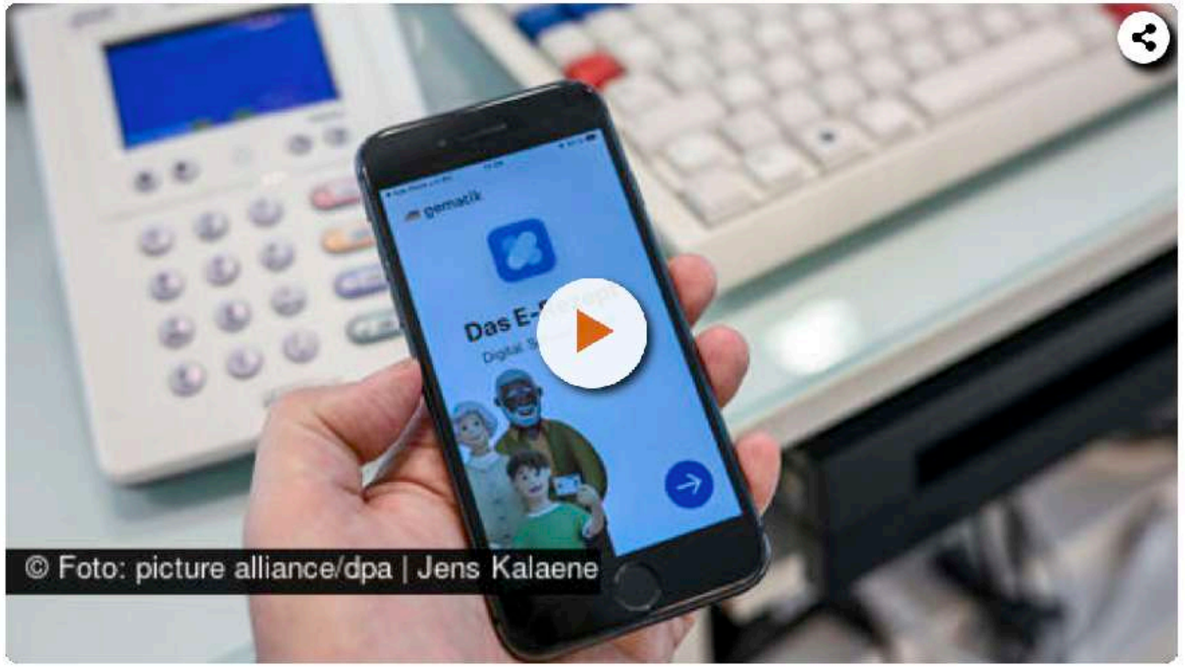
Unter anderem als Reaktion auf die folgende Datenschutz-Debatte verankerte das Bundesministerium für Gesundheit (BMG) im Krankenhauspflege-Entlastungsgesetz (KHPflEG), dass die Gematik künftig alle Anforderungen an Sicherheit und Datenschutz »im Einvernehmen« mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BFDI) abklären muss. Zuvor hatte es für das geplante Ident-Verfahren in der Apotheke keine Einspruchsmöglichkeiten durch Datenschützer gegeben.

Zeitstempel beweist Apothekenbesuch

Jetzt liegen die neuen technischen Spezifikationen der Gematik vor, die die diskutierten Datenschutzprobleme lösen sollen. Allerdings stehen nach PZ-Informationen die entscheidenden Unterschriften von BFDI und BSI noch aus. Darüber hinaus müssen auch alle Gesellschafter der Gematik noch ihr Okay zu der aktualisierten Version geben. Die Gematik ist aber zuversichtlich, dass den Versicherten der EGK-Einlöseweg ab Sommer 2023 in den Apotheken zur Verfügung stehen wird. Das sagte die Gesellschaft auf Nachfrage der PZ.

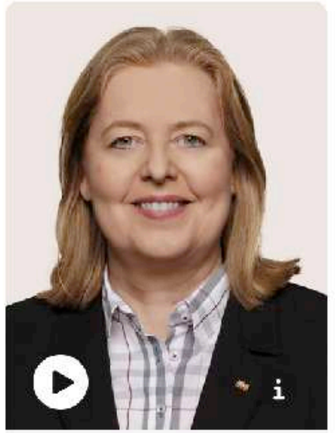
Gesundheit

Mehr Digitalisierung im Gesundheitssystem beschlossen



Der Bundestag hat am **Donnerstag, 14. Dezember 2023,** diverse Neuerungen im Hinblick auf die **elektronische Patientenakte (ePA)** beschlossen. Die Abgeordneten haben einen entsprechenden Gesetzentwurf „zur Beschleunigung der Digitalisierung des Gesundheitswesens“ (Digital-Gesetz – DigiG) (20/9048) in einer vom Gesundheitsausschuss geänderten Fassung mit den Stimmen von SPD, Bündnis 90/Die Grünen und FDP gegen die Stimmen der AfD bei Stimmenthaltung der CDU/CSU angenommen. Darüber hinaus wurde ein zweiter vom Ausschuss geänderter Gesetzentwurf „zur verbesserten Nutzung von Gesundheitsdaten“ (Gesundheitsdatennutzungsgesetz – GDNG) (20/9046) mit der Mehrheit

Reden zu diesem Tagesordnungspunkt

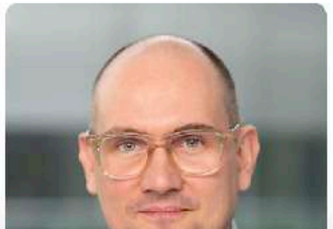


Bas, Bärbel

Bundestagspräsidentin

Lauterbach, Prof. Dr. Karl

Bundesminister für Gesundheit



Politik

Neue Verschlüsselung soll Performance der ePA in der Praxis verbessern

Mittwoch, 13. Dezember 2023

Berlin – Die Änderung der Sicherheitsarchitektur der elektronischen Patientenakte (ePA) soll nicht nur zu einem besseren Datenzugang für die Sekundärnutzung führen, sondern auch ihre Performance in den Praxisverwaltungssystemen (PVS) verbessern. Das werde ihre Akzeptanz in den Praxen erhöhen, erklärte Susanne Ozegowski, Leiterin der Abteilung Digitalisierung und Innovation im Bundesministerium für Gesundheit (BMG), gestern in Berlin.

Mit dem Kabinettsbeschluss zum Gesetz zur Beschleunigung der Digitalisierung im

Ozegowski: Mehr, nicht weniger Tempo.

TRANSFORMERS.health April 15, 2024 OTHER NEWS

Dr. Susanne Ozegowski betont die Notwendigkeit einer beschleunigten Digitalisierung im Gesundheitswesen. Der schnelle Vorstoß in die digitale Transformation, insbesondere durch die Implementierung der EPA, sei unerlässlich ist, um die Gesundheitsversorgung zu verbessern, sagte die Leiterin der Abteilung Digitalisierung und Innovation im Bundesministerium für Gesundheit auf der DMEA in Berlin.

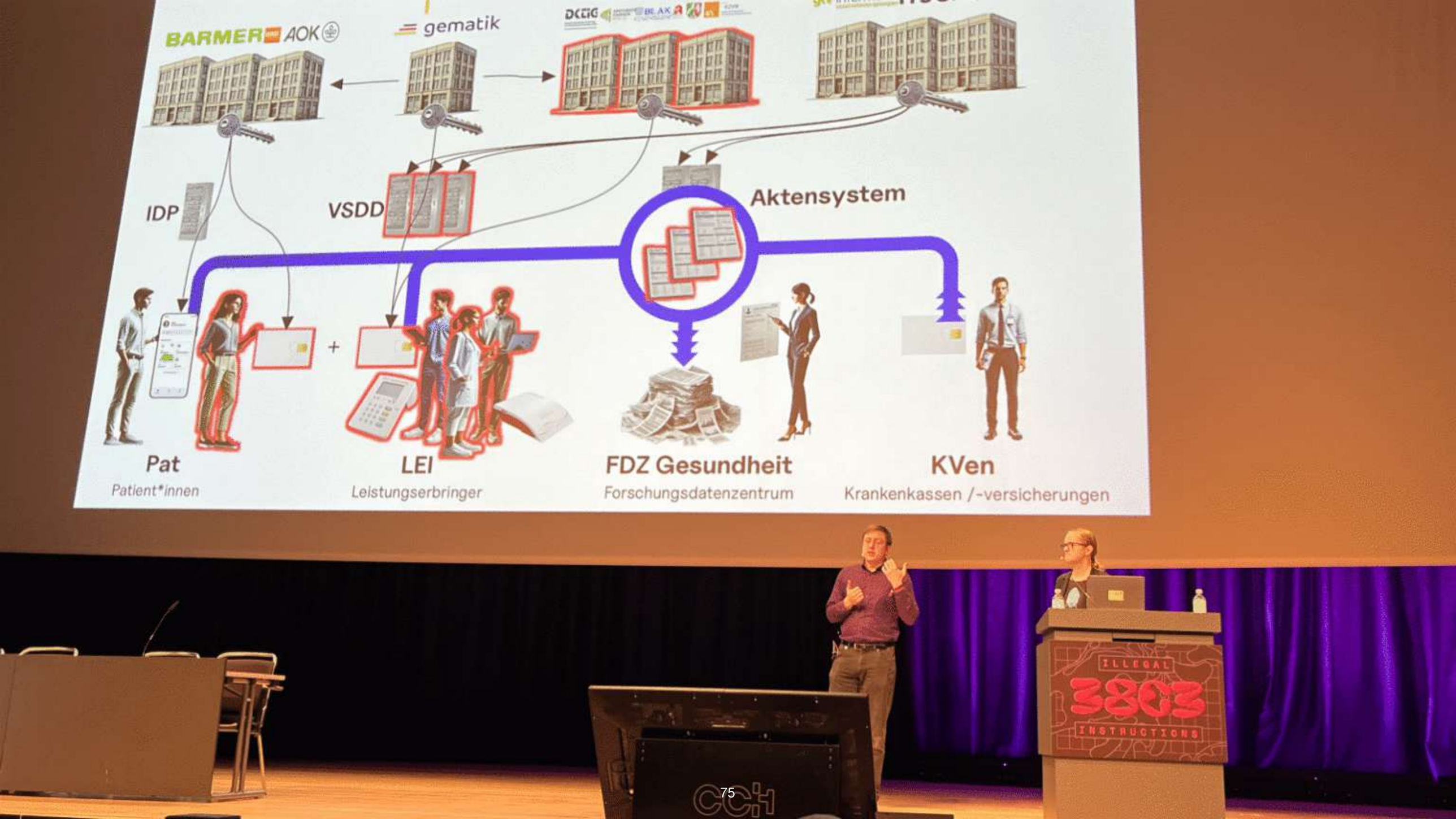
Elektronische Patientenakte

Warnungen von Experten wurden monatelang ignoriert

Die elektronische Patientenakte startet trotz Sicherheitslücke in Teilen Deutschlands. Dokumente, die ZEIT ONLINE vorliegen, zeigen: Das Problem war schon länger bekannt.

Von Eva Wolfangel

15. Januar 2025, 13:17 Uhr


BARMER
AOK
gematik
IDP
VSDD
Aktensystem
Pat
Patient*innen
LEI
Leistungserbringer
FDZ Gesundheit
Forschungsdatenzentrum
KVen
Krankenkassen /-versicherungen
ILLEGAL
3803
INSTRUCTIONS

EILMELDUNG — Hacker hebeln erweiterten Schutz der elektronischen Patientenakte aus

EILMELDUNG

S+ Digitalisierung in der Medizin: Hacker hebeln erweiterten Schutz der elektronischen Patientenakte aus

»Die ePA bringen wir erst dann, wenn alle Hackerangriffe technisch unmöglich gemacht worden sind«, hat Karl Lauterbach im Januar verkündet. CCC-Experten haben nun bewiesen: Er hat zu viel versprochen. Die Betreiber reagieren mit einer Notfallmaßnahme. Von Patrick Beuth und Marcel Rosenbach

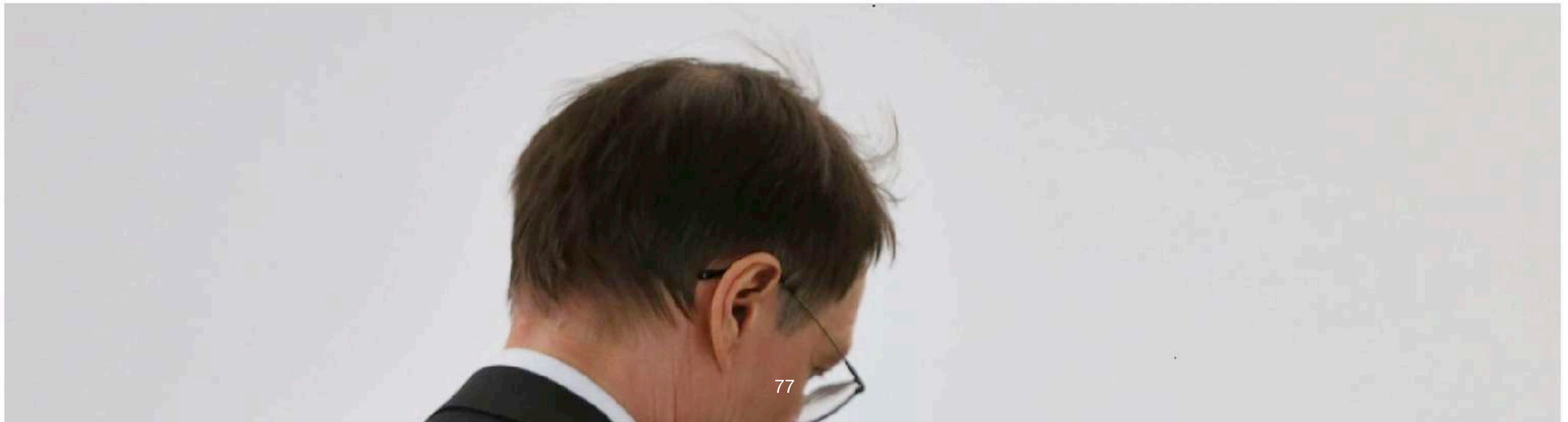
7 Min

Elektronische Patientenakte

Keine Verantwortung, nirgends

Vor einer Woche fanden IT-Fachleute erneut gravierende Sicherheitslücken in der elektronischen Patientenakte. Bislang wollen aber weder das Gesundheitsministerium noch die Gematik dafür die Verantwortung übernehmen. Unklar ist damit auch, wie sich ähnliche Fehler künftig vermeiden lassen.

06.05.2025 um 17:10 Uhr - Daniel Leisegang - in Datenschutz - 18 Ergänzungen



Blick in die **Zukunft**
Blick **in die Zukunft**
Blick **in die Zukunft**
Blick **in die Zukunft**
Blick **in die Zukunft**
Blick **in die Zukunft**
Blick **in die Zukunft**
Blick **in die Zukunft**
Blick in die Zukunft
Blick in die Zukunft
Blick in die Zukunft
Blick in die Zukunft

Wie sieht das bei anderen digitalen Großprojekten aus?

Ein Großteil der Probleme der Gesundheitsdigitalisierung der letzten Jahrzehnte sind Identifikations- und Authentifizierungsprobleme.

Was macht **die EUDI Wallet?**
Was macht **die EUDI Wallet?**
Was macht **die EUDI Wallet?**
Was macht **die EUDI Wallet?**
Was macht **die EUDI Wallet?**
Was macht **die EUDI Wallet?**
Was macht **die EUDI Wallet?**
Was macht **die EUDI Wallet?**
Was macht **die EUDI Wallet?**
Was macht **die EUDI Wallet?**
Was macht **die EUDI Wallet?**

Die Lösung aller Probleme?

„Wir werden sicherlich das Highlight werden irgendwann auf dem CCC Jahrestreffen. Da gehen wir fest von aus.“

Thomas Jarzombek, re:publica, 27.05.25

Beitrag von Markus Richter

Markus Richter
1 Jahr

📱 Gemeinsam für eine sichere und digitale Zukunft mit der staatlichen EUDI-Wallet

💡 Gemeinsam mit der **SPRIND - Bundesagentur für Sprunginnovationen** und mit dem **Federal Office for Information Security (BSI)** haben wir mit der Entwicklung der staatlichen EUDI-Wallet begonnen. Dabei haben wir uns nach intensiver Prüfung und in Abstimmung mit BSI und BfDI für die Umsetzung einer der sechs diskutierten Architektur-Varianten für die Personenidentifizierungsdaten entschieden, die auf einen Hardware-Sicherheitsanker in der Cloud und auf signierte Daten setzt (im Architekturentwurf als Variante C' bezeichnet).

🔍 Warum haben wir diese Variante gewählt?

🇪🇺 Europäischer Weg: Wir setzen damit auf technische Konzepte, die in unseren Nachbarstaaten erfolgreich erprobt sind und zur Verbreitung beigetragen haben. Wir gehen keinen deutschen Sonderweg, sondern setzen voll auf gemeinsame Standards und auf Interoperabilität.

🔐 Sicherheit und Verfügbarkeit: Durch den Rückgriff auf Hardwaresicherheit in der Cloud erreichen wir höchste Sicherheitsanforderungen, gewährleisten durch signierte Daten Unfälschbarkeit bzw. Nutzerbindung und schaffen gleichzeitig eine Lösung, die auf nahezu allen handelsüblichen Smartphones verfügbar sein wird.

„Vermeintlich kleine Architekturentscheidungen haben oft große Auswirkungen.“

Rafael Laguna de la Vera, „Deutschland muss mutig digitalisieren“ , FAZ, 02.09.2024

„In der Folge ist jede Kopie der **Kombination aus Identitätsdaten und Signatur** vergleichbar mit einer **beglaubigten Kopie**. Problematisch ist hierbei, dass jede Person, die in den Besitz der Identitätsdaten mit Signatur gelangt, über nachweislich authentische Daten verfügt und dies auch **beliebig an Dritte weitergeben kann**, ohne dass der Inhaber der Identitätsdaten dies kontrollieren kann.“

Antworten zum Fragenkatalog seitens des BSI, Anhörung Digitale Identitäten, 29.06.22

„**Die Politik geht damit Risiken ein, die am Ende von den Individuen getragen werden müssen**. Sie reichen von Gefahren für die individuelle Privatsphäre, Ausfall von Systemen oder Manipulation von Daten – diese Risiken tragen am Ende die Patient*innen persönlich. Unbedachte Szenarien von Datennutzung und der „Hebung von Datenschätzen“ führen bei Problemen zu massenhaftem, individualisiertem Schaden, wohingegen die Verursacher dieser Probleme kaum langfristige Risiken zu befürchten hätten.“

Offener Brief zur ePA von 2023, Vertrauen lässt sich nicht verordnen

Digitalminister nennt konkretes Zeitziel

Ab 2027 sollen sich Bürger per Smartphone ausweisen können

Beim Alkoholkauf im Supermarkt das Handy statt des Ausweises vorzeigen: Eine neue digitale Brieftasche soll so etwas möglich machen. Für sie gibt es jetzt ein offiziell avisiertes Startdatum.

11.12.2025, 11.49 Uhr

Forderungen aus dem letzten ePA-Talk vom 38C3

Wie sieht es hiermit aus?

- unabhängige und belastbare Bewertung von Sicherheitsrisiken
- transparente Kommunikation von Risiken gegenüber Betroffenen
- offener Entwicklungsprozess über gesamten Lebenszyklus

Unabhängige und belastbare Bewertung von Sicherheitsrisiken?

Missing explicit security requirements per component

Offen Ticket erstellt vor 1 Monat von **Sascha Block**

Title Missing explicit security requirements per component

Submitted for: Mobil Krankenkasse (statutory public body under German law)
Contact: Sascha Block, IT Architect

Summary The current architecture documentation (decomposition, data flows, guidelines) describes the main components of the German National EUDI Wallet, but does not define explicit, verifiable security requirements per component (PAP, MDVMP, WB, RWSCD, etc.). For implementers, evaluators and auditors, it remains unclear which concrete security properties each component must fulfil.

Relation to existing issues This issue is intended to *complement* and operationalize:

- **"Comments on and recommendations for the German EUDI wallet architecture relating to cryptographic security" (Eric Verheul)** – which calls for clear (cryptographic) security objectives and analysis against high attack potential.

Where Eric's issue focuses on *what* type of security assurance is needed at system level, this issue focuses on *where and how* to document concrete per-component security requirements inside the existing architecture documentation.

Background The architecture concept under:

- `Architecture → Decomposition`
- `Data Flows`
- `Guidelines → Establishing app integrity`
- `Guidelines → eID Flow`

Beauftragte(r)
Keine

Labels
Keine

Meilenstein
Keine

Termine
Beginn: Keine
Fällig: Keine

Zeiterfassung
Weder Schätzung noch Zeitaufwand eingetragen

2 Teilnehmer(innen)

Transparente Kommunikation von Risiken gegenüber Betroffenen?

Quelle: anyaberkut - fotolia.com

Datum: 21.02.2025

Digitale Identität: Verbraucher:innen müssen digitalen Brieftaschen vertrauen können

vzbv veröffentlicht Gutachten: Datenmissbrauch bei digitaler Brieftasche muss verhindert werden

„The repudiation requirement and the appropriateness of using authenticated PID is subject of ongoing discussions within the consultation process.“

Ecosystem architecture, Blueprint for the EUDI Wallet Ecosystem in Germany, v2.9.1, 18.12.25

Offener Entwicklungsprozess über gesamten Lebenszyklus?

Will there be reproducible builds?

Offen Ticket erstellt vor 4 Monaten von **Rita Stadtmann**

I have a simple question about the EUDI Wallet.

The EUDI Wallet is intended to be open source. However, to ensure trust, the builds must also be reproducible. It is imperative to ascertain whether the application in question is consistent with the publicly available code. If it is not possible to verify the code is exactly what have been published, the app could contain anything such as surveillance functionality.

Will I personally be able to build the wallet app locally and ensure that it results in exactly the same app?

👍 1 👎 0 👀 1

Um Designs hochzuladen, musst du LFS aktivieren und ein(e) Administrator(in) muss den gehashten Speicher aktivieren. Weitere Informationen

Aktivität

Alle Aktivitäten ⌄ Älteste zuerst ⌄

- **Lucas Licht** added analysing label vor 4 Monaten
- **Sander Dijkhuis** mentioned in issue #1 vor 3 Monaten

Bitte registriere oder melde dich an um zu antworten

Beauftragte(r)
Keine

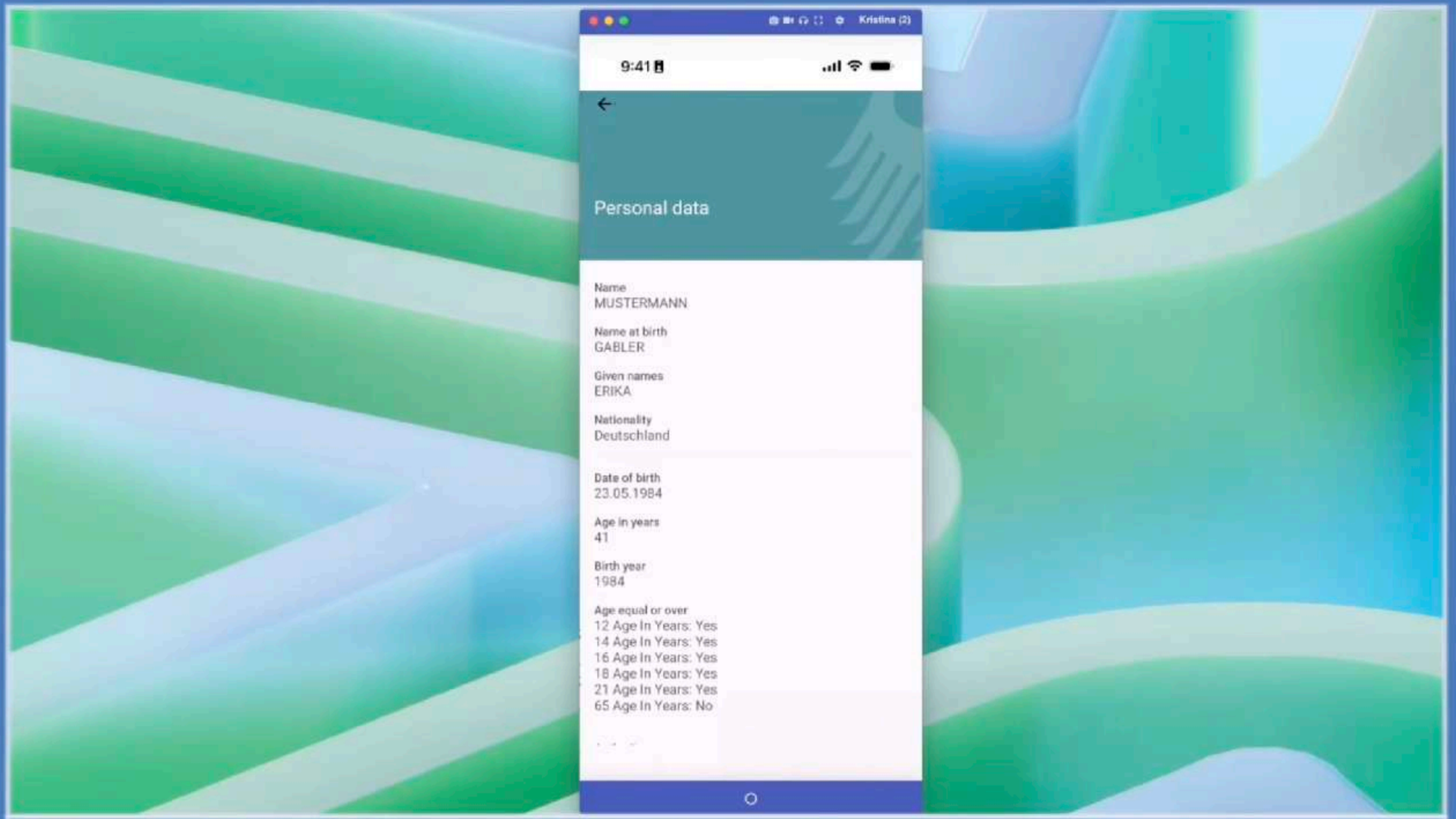
Labels
analysing

Meilenstein
Keine

Termine
Beginn: Keine
Fällig: Keine

Zeiterfassung
Weder Schätzung noch Zeitaufwand eingetragen

3 Teilnehmer(innen)



OK, now I typed the same pin twice and.
Just like that the pin is sat and user gets a digital identity ...

SUMMIT ON
EUROPEAN
DIGITAL
SOVEREIGNTY

Riesiges, komplexes Ökosystem

Umsetzung eines Marktmodells

Zeitdruck

Hoher Blast Radius

Offline als After-Thought

Cloud-Komponenten als Sicherheitsanker

Die Genese der deutschen staatlichen EUDI Wallet befindet sich auf einem ähnlich unguten Weg wie die ePA.

Unbestimmte Risikokommunikation

Unklare Sicherheitsanforderungen

Kein offener Entwicklungsprozess über gesamten Lebenszyklus

„Mutig digitalisieren“

Umfangreiche, komplexe Spezifikationen

Diskussion, **Fragen, Lob**
Diskussion, **Fragen, Lob**
Diskussion, **Fragen, Lob**
Diskussion, **Fragen, Lob**
Diskussion, **Fragen, Lob**
Diskussion, **Fragen, Lob**
Diskussion, **Fragen, Lob**
Diskussion, Fragen, Lob
Diskussion, Fragen, Lob
Diskussion, Fragen, Lob

39c3@inoeg.de

bkastl.de

mastodon.social/@bkastl