HOCHSCHULE MAINZ

Wirtschaft
Business

Daten in der Gesundheitswirtschaft Wie lassen sich diese sicher nutzen und verteilen?

23/04/2025

University of
Applied Sciences

«Eines der größten IT-Projekte der Bundesrepublik»

Florian Fuhrmann, gematik, im Ärzteblatt

«Unsere ePA ist die sicherste in Europa»

Susanne Ozegowski, Bundesgesundheitsministerium, im Ärztenachrichtendienst

ePA – elektronische Patientenakte
Was ist das nochmal?

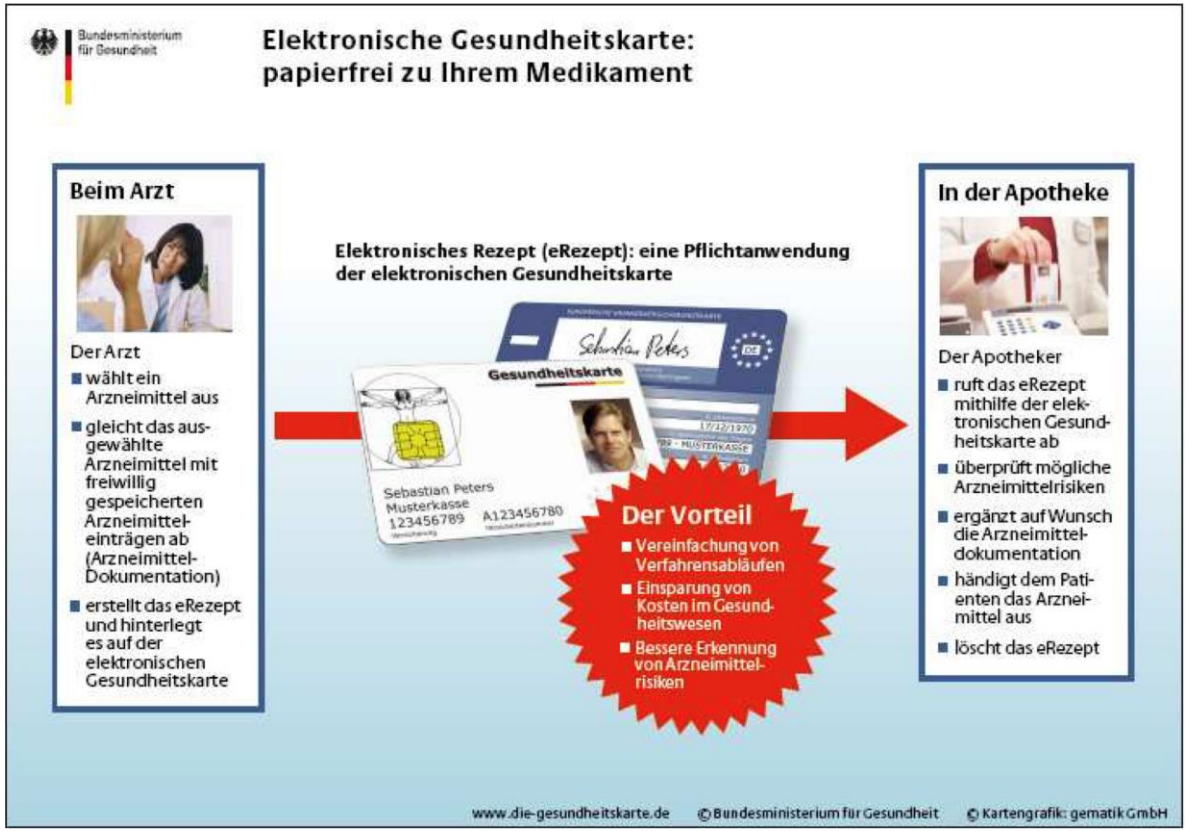
Die **elektronische Gesundheitsakte** (**ELGA** oder **eGA**[1]) oder **elektronische Patientenakte**(**ePA**), englisch *electronic health record* oder *electronic patient record,* ist eine digital angelegte Akte, also eine Form einer Datenbank, in der Gesundheitsdaten von Krankenversicherten (z. B. Anamnese, Behandlungsdaten, Medikamente, Allergien) sektor- und fallübergreifend sowie landesweit einheitlich gespeichert, verändert und abgerufen werden können.

https://de.wikipedia.org/wiki/Elektronische_Gesundheitsakte

https://www.gematik.de/media/erezept/_processed_/4/2/csm_gematik_Piktogramm_Patientenakte_2_Blau_16c8bd9402.png

Exkurs: Das elektronische Rezept
Die Anfänge der Digitalisierung

- Das Rezept sollte auf der Karte gespeichert werden und in der Apotheke ausgelesen.
- Zugriff auf das Rezept war nur in Kombination mit einer Karte der Apotheke möglich
- Keine weiteren Online-Systeme oder Speicher nötig
- Erste Praxistests 2002

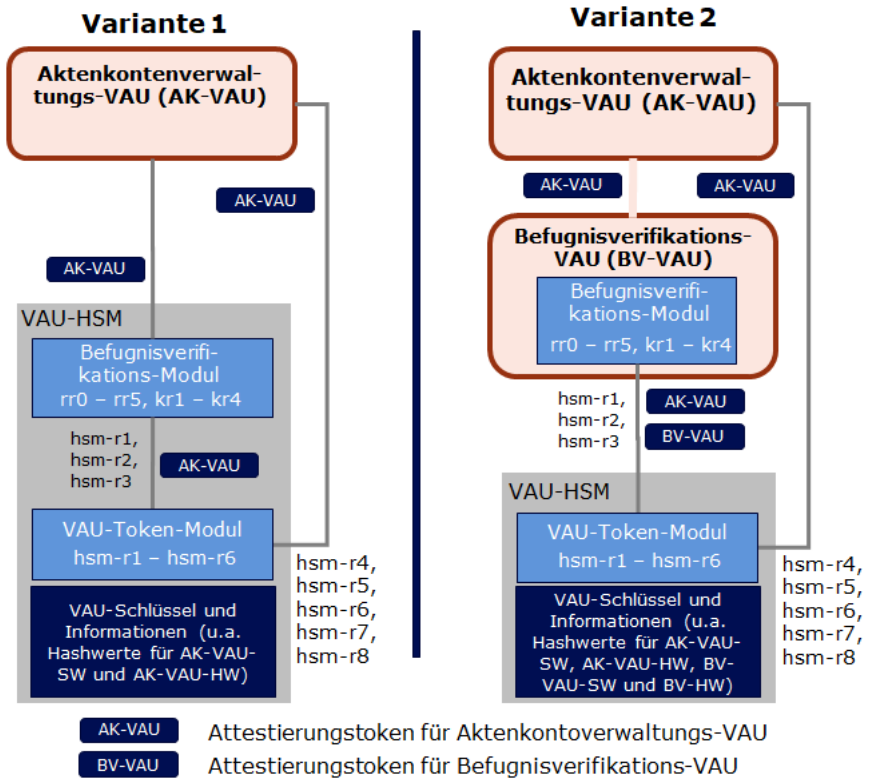


https://lbv.landbw.de/documents/20181/42056/Gesundheitskarte.pdf/be68c2d3-82be-42c9-a7b4-b7966c998375

Kritik am elektronischen Rezept
Definiere Ende-zu-Ende

- „Die E-Rezepte werden von der Arztpraxis verschlüsselt an einen zentralen Dienst übertragen, dort verschlüsselt gespeichert und verarbeitet und wieder verschlüsselt von der Apotheke abgerufen. Damit sind die E-Rezepte vor unbefugtem Zugriff geschützt.“ (Gematik)

- Verarbeitung erfolgt dabei unverschlüsselt, somit besteht keine Ende-zu-Ende-Sicherheit und die Gematik kann die medizinischen Daten der Bürger auswerten
- Schutz erfolgt durch eine „vertrauenswürdigen Ausführungsumgebung“ (VAU), die auf Intel SGX basiert
- Intel SGX gilt als gebrochen und seit 2021 als deprecated



https://x.com/gematik1/status/1566711677076250624
https://www.heise.de/select/ct/2022/21/2225319484122825196
https://gemspec.gematik.de/downloads/gemSpec/gemSpec_Aktensystem_ePAfueralle/gemSpec_Aktensystem_ePAfueralle_V1.3.0.html
https://en.wikipedia.org/wiki/Software_Guard_Extensions
https://www.ccc.de/de/updates/2022/erezept-mangelhaft

Bei Intel-SGX sind die durch die Intel-Hardware erzeugten Signaturen RSA-3072-Bit-Signaturen, bei denen der öffentliche Exponent 3 ist. Dies entspricht nicht den Vorgaben in [gemSpec_Krypt] für allgemeine RSA-Signaturen (also nicht im SGX-Kontext). Deshalb steht in A_24613-* diesbezüglich nur eine SOLL-Formulierung. Im Kontext SGX ist der öffentliche RSA-Exponent 3 zulässig.

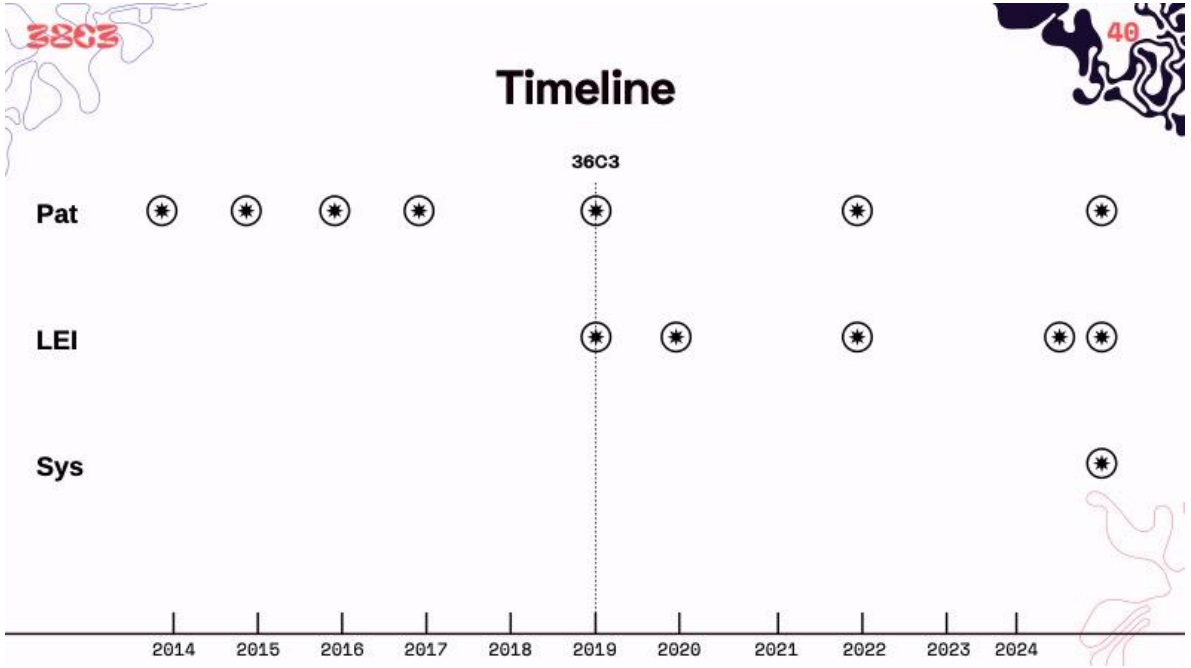
— Spezifikation Aktensystem ePA für alle, Gematik, 24.04.2024

— Warum das kritisch ist:

- Kleine Exponenten machen Krypto anfällig
- https://itsc.uni-wuppertal.de/fileadmin/Abteilung/ITSC/DigitaleSignaturen.pdf

Elektronische Patientenakte
Historie der Schwachstellen

- Bekannte Angriffe auf verschiedene Prozesse und Komponenten
  - Ausgabe der eGK
  - Konnektoren
  - VideoIdent
  - Kartenherausgeberportale
- Stand 2025:
  - Gematikauftrag: Das Fraunhofer SIT benennt insgesamt 21 Schwachstellen, von denen 4 als „hoch“ eingestuft werden.
  - CCC: Die auf dem 38C3 demonstrierten Sicherheitsmängel der elektronischen Patientenakte bestehen fort. Die bisher angekündigten Updates sind grundsätzlich ungeeignet, die aufgedeckten Mängel in der Sicherheitsarchitektur auszugleichen. Bei den versprochenen Updates handelt es sich lediglich um den Versuch der Schadensbegrenzung bei einem der vielen von uns demonstrierten Angriffe



https://fahrplan.events.ccc.de/congress/2024/fahrplan/media/38c3/submissions/SRXRMA/resources/38c3_epa_kastl_tschirsich_fYQhbAq.pdf
https://www.gematik.de/media/gematik/Medien/ePA_fuer_alle/Abschlussbericht_Sicherheitsanalyse_ePA_fuer_alle_Frauenhofer_SIT.pdf
https://www.heise.de/news/Trotz-Sicherheitsbedenken-Sanktionsbewaehrte-Nutzung-der-E-Patientenakte-kommt-10333673.html

Kann man das besser ~~ma~~chen?

Mentalität / Problembewusstsein

1. Enough Is Enough: The Threats Have Changed. (Michael Howard and Steve Lipner, The Security Development Lifecycle, Microsoft, 2006)

2. Akzeptanz und Bewusstsein sind die Basis von jeder Planung

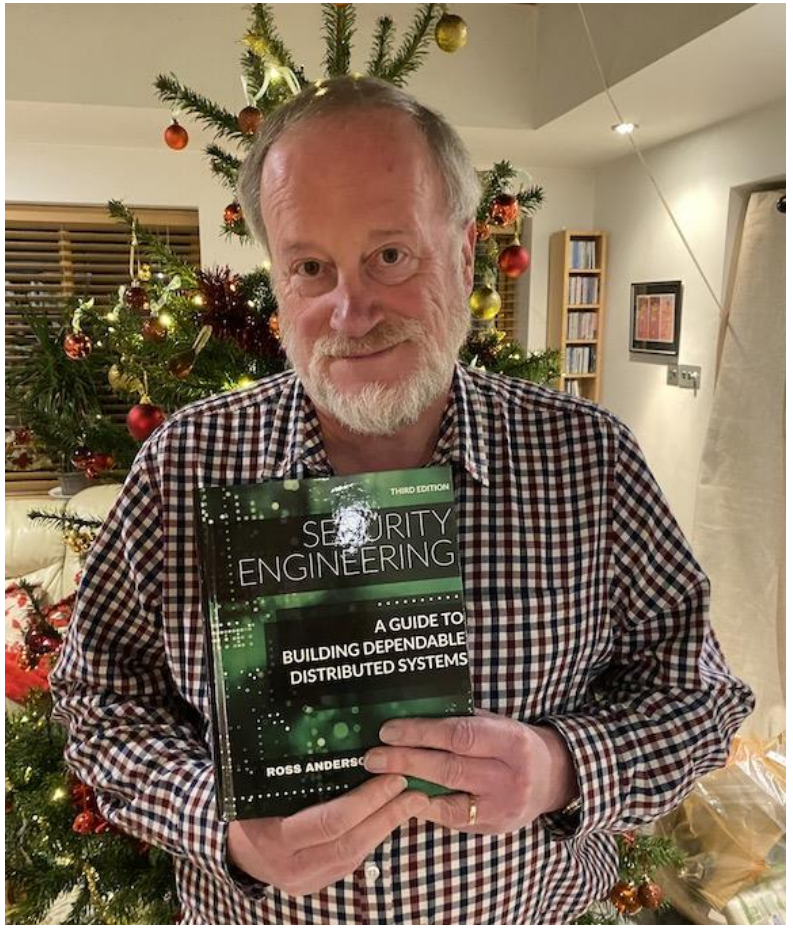
3. Beispiel: „In Bezug auf das ePA-System wurde in Abstimmung mit der gematik festgestellt, dass Angriffe durch staatliche Organisationen nicht relevant sind.“ (Kap. 5.2.2 des SIT Abschlussberichts)

4. Beispiel: „**Die Sicherheit der ePA für alle hat für uns oberste Priorität. Das gilt für alle Sicherheitsprobleme, die wir bisher [...] analysieren konnten, gilt zum Beispiel auch für die Sicherheitsbedenken, die der Chaos Computer Club vorgetragen hat.“**

https://www.kuketz-blog.de/hoffnung-als-strategie-kommentar-zur-unsicheren-elektronischen-patientenakte-epa/

Planung

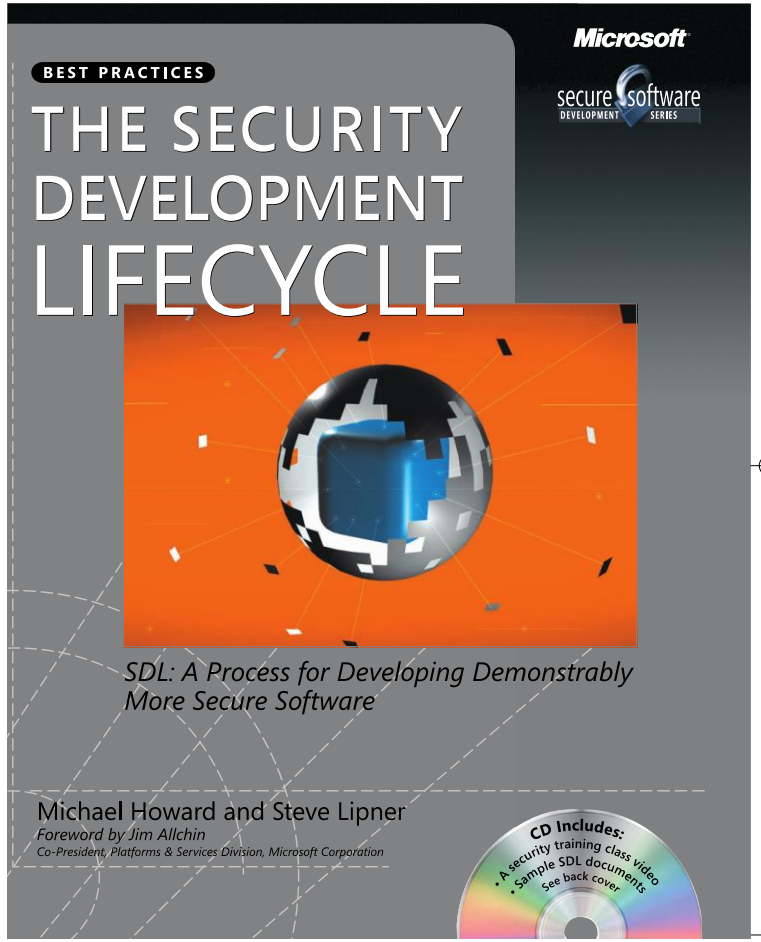
1. Vorbereitung
   - Verantwortlichkeiten (Security Advisor, Security Leadership Team)
   - Ausbildung
   - Buchtip: Security Engineering von Ross Anderson
2. Threat Model
   - Use Cases verstehen und Festhalten
   - Strukturiertes Vorgehen
   - Formalisierte Modelle mit deinierten Risiken
3. Sicherheitskonzept
   - Best Practices nutzen
   - Geeignete Schutzmaßnahmen für den Use Case wählen – TLS löst nicht jedes Problem



https://www.cl.cam.ac.uk/archive/rja14/book.html

Umsetzung

1. It‘s really about quality (Microsoft)
2. Designziele:
   - Datensparsamkeit
   - Privacy Enhancing Technologies (PETS) nutzen
   - Verständliche und strukturierte Spezifikationen
   - Sicherheit von Anfang an einplanen
3. Implementierung
   - Qualität der Implementierung
   - Werkzeuge nutzen
   - Checklisten



https://download.microsoft.com/download/8/1/6/816C597A-5592-4867-A0A6-A0181703CD59/Microsoft_Press_eBook_TheSecurityDevelopmentLifecycle_PDF.pdf

Sicherheit ist «A und O für die ePA und für das Vertrauen der Menschen in die ePA»

Susanne Ozegowski, Bundesgesundheitsministerium

https://www.deutschlandfunkkultur.de/elektronische-patientenakte-durchbruch-ins-digitale-oder-sicherheitsrisiko-dlf-kultur-7de426d7-100.html

HOCHSCHULE MAINZ

Wirtschaft
Business

Vielen Dank für Ihre Aufmerksamkeit.

University of
Applied Sciences

Kontakt

Prof. Dr. Nicolai Kuntze
Professor für Angewandte Informatik
Studiengangsleitung Angewandte Informatik
Informationssicherheitsbeauftragter
Hochschule Mainz
University of Applied Sciences
Lucy-Hillebrand-Str. 2
55128 Mainz, Germany

T +49 6131 628-3218
E nicolai.kuntze@hs-mainz.de
W hs-mainz.de