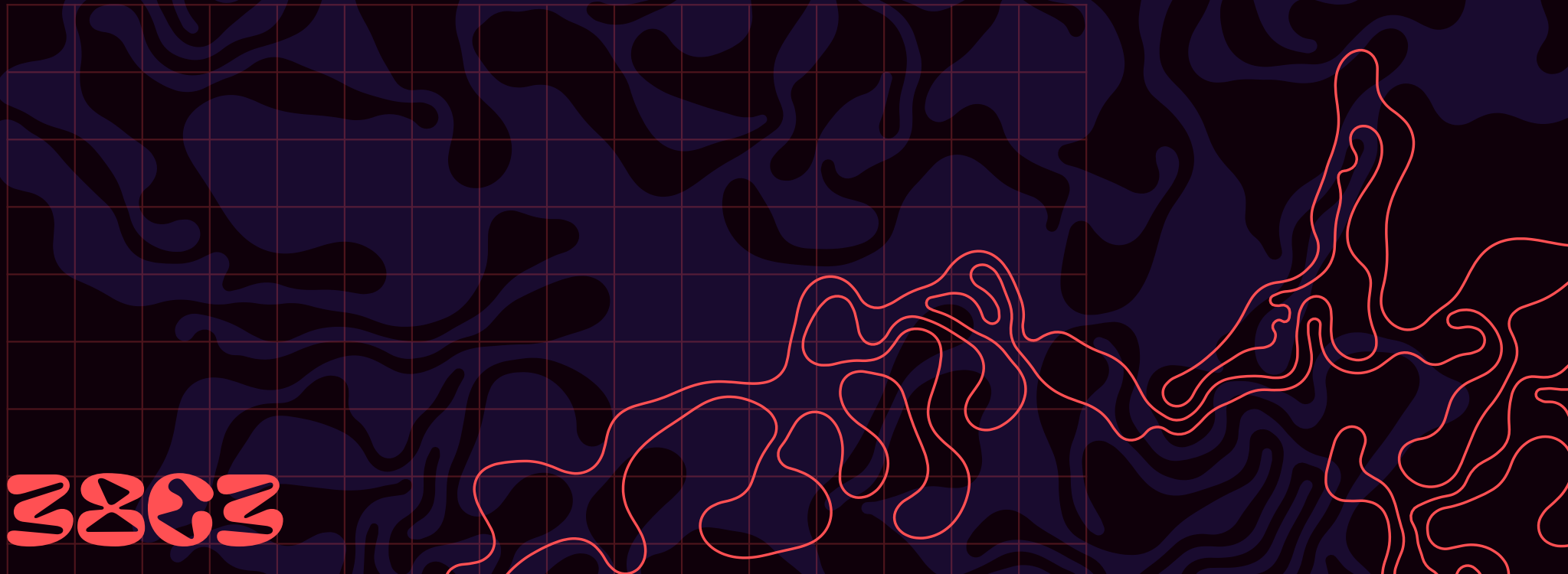
«Konnte bisher noch nie gehackt werden»: Die elektronische Patientenakte kommt – jetzt für alle



Über uns

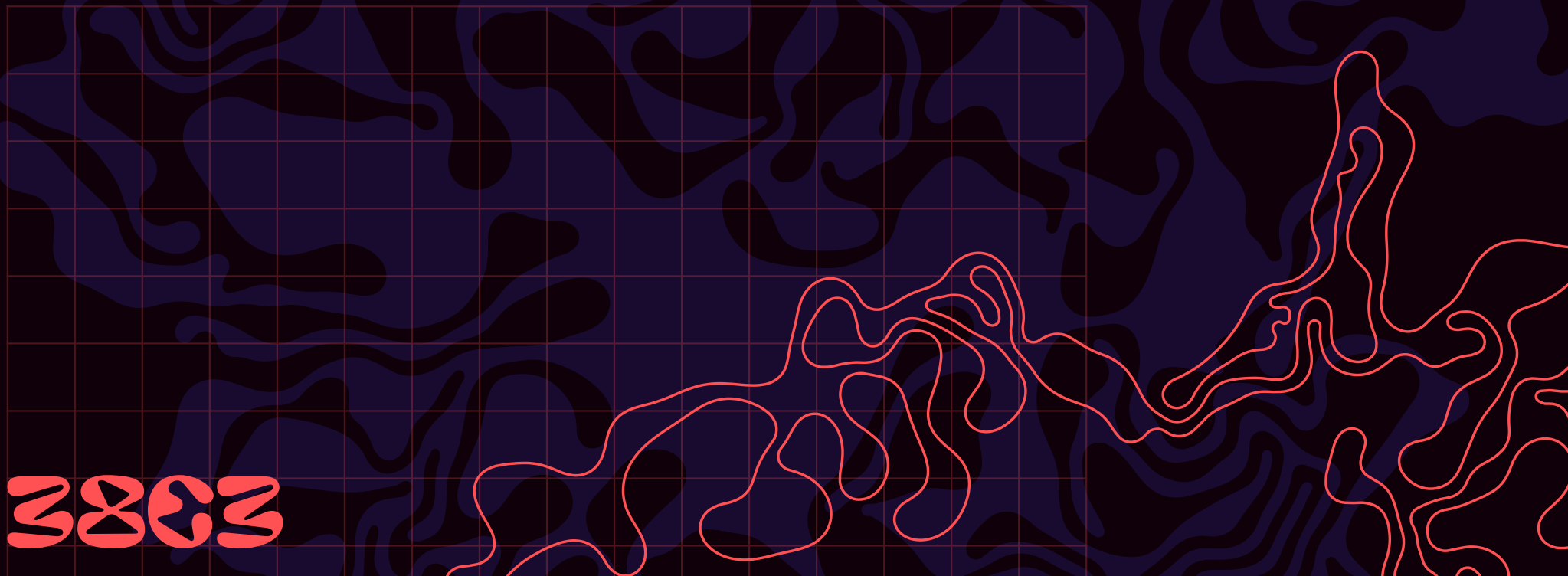
Bianca Kastl

- Congress-Talks: rC3: NOWHERE, 37C3
- Sachverstand Bundestag: 2021, 2021, 2023, 2024

Martin Tschirsich

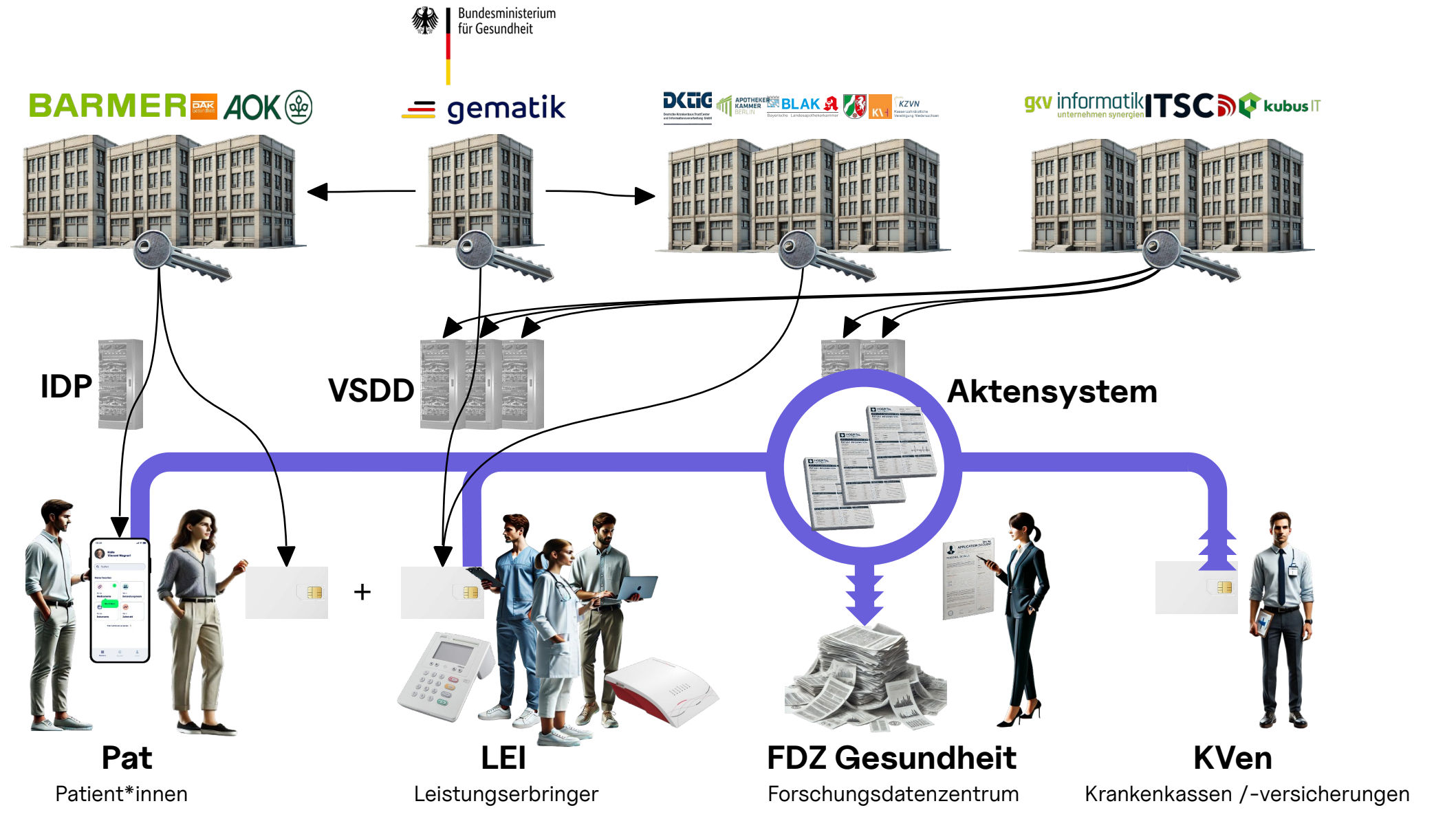
- Congress-Talks: 35C3, 36C3, rC3
- Sachverstand Bundestag: 2019, 2020, 2021, 2021

Die elektronische Patientenakte für alle

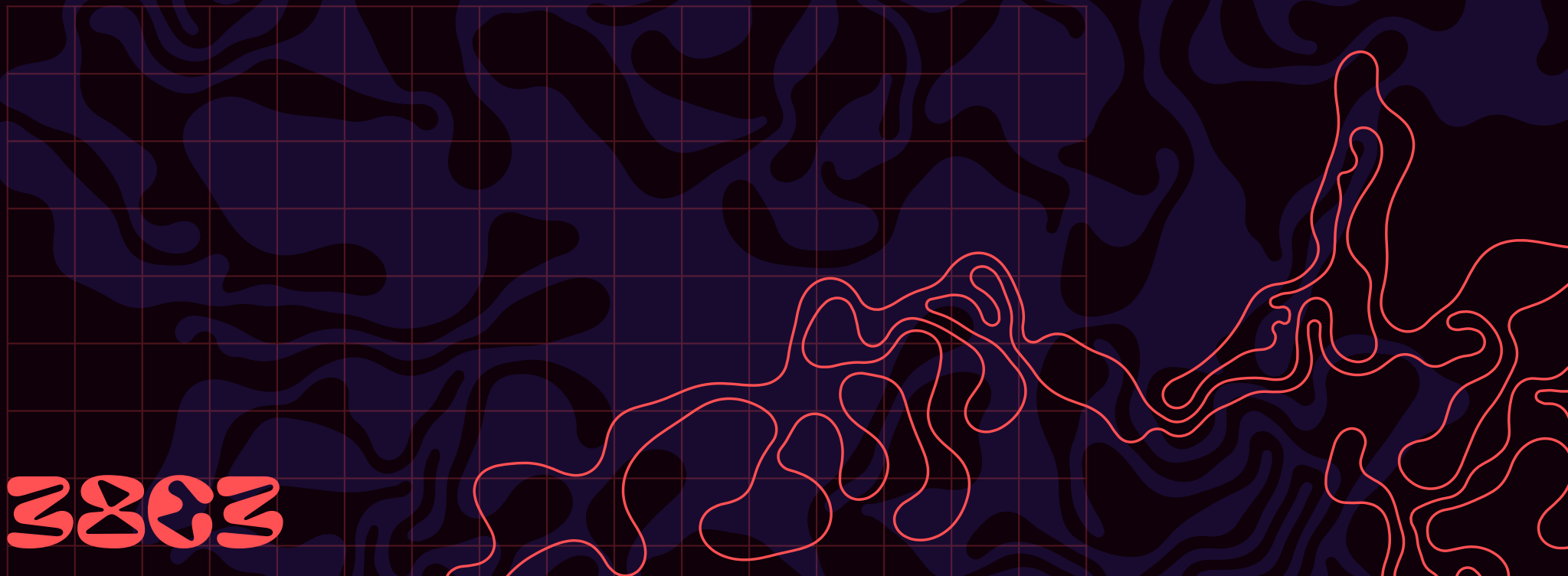


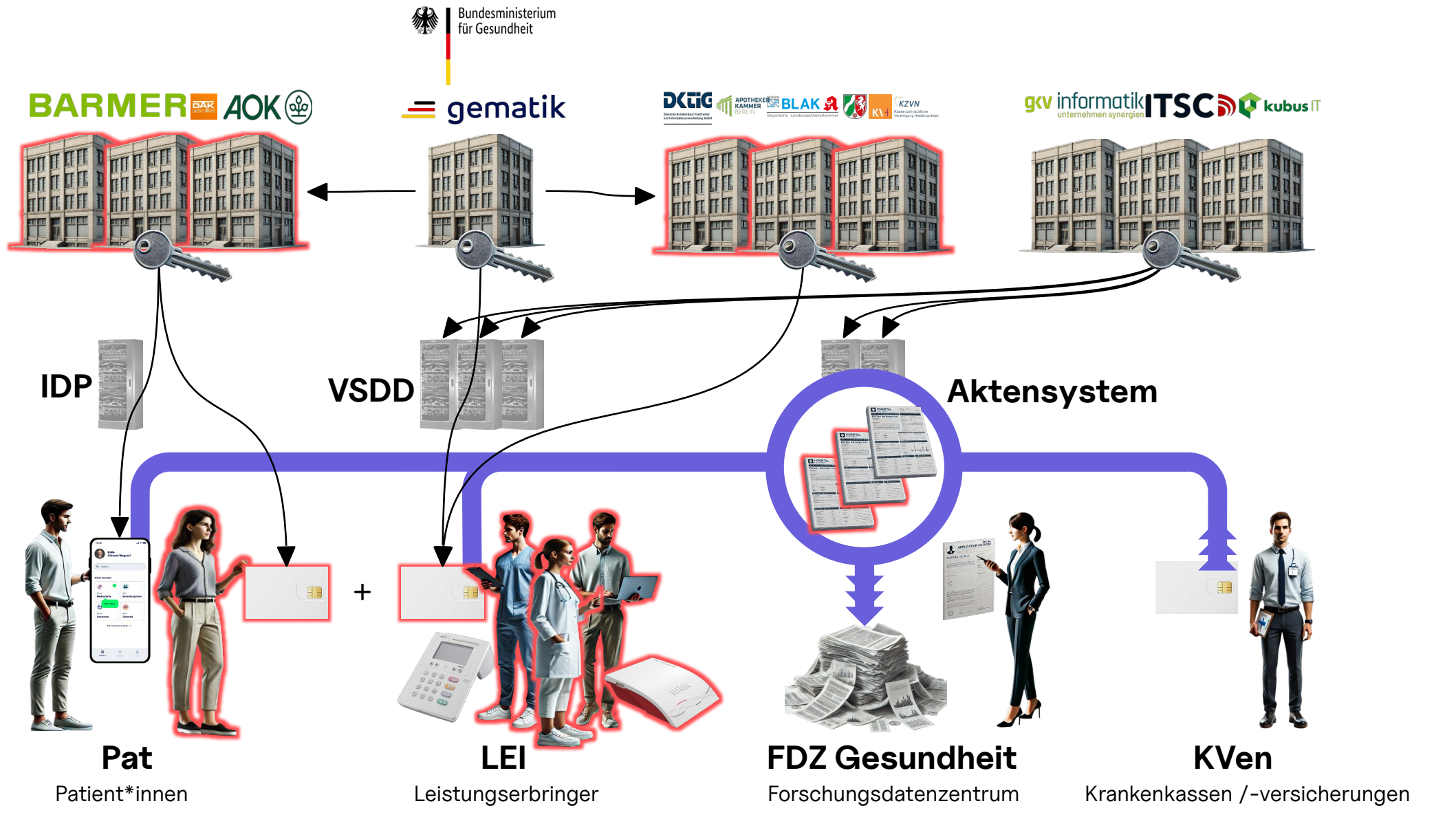
Elektronische Patientenakte für alle

- wesentliche Änderung: **Opt-Out**, Widerspruch auf mehreren Ebenen
- ab 15.01 in Testregionen, ab 15.02 deutschlandweit
- automatische Befüllung

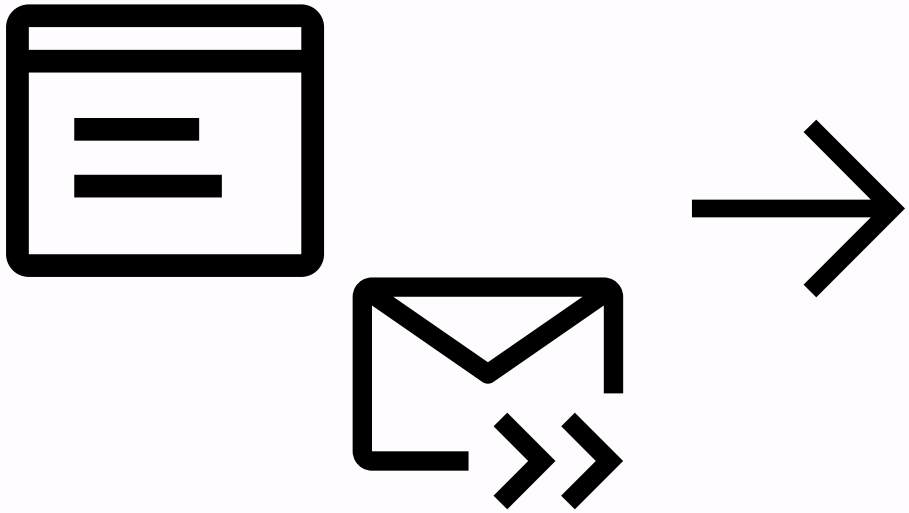

Bundesministerium
für Gesundheit
BARMER
DAK
AOK
gematik
DKTIG
APOTHEKER KAMMER BERLIN
BLAK
KZVN
gkv informatik
ITSC
kubus IT
unternehmen synergien
IDP
VSDD
Aktensystem
+
Pat
Patient*innen
LEI
Leistungserbringer
FDZ Gesundheit
Forschungsdatenzentrum
KVen
Krankenkassen /-versicherungen

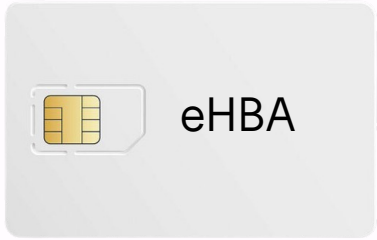
Recap: 36C3 und die Zeit dazwischen

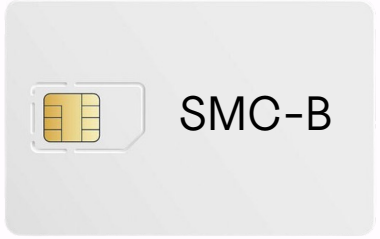



Bundesministerium
für Gesundheit
BARMER
DAK
AOK
gematik
DKTIG
APOTHEKER KAMMER BERLIN
BLAK
KZVN
gkv informatik
unternehmen synergien
ITSC
kubus IT
IDP
VSDD
Aktensystem
+
Pat
Patient*innen
LEI
Leistungserbringer
FDZ Gesundheit
Forschungsdatenzentrum
KVen
Krankenkassen /-versicherungen

Ausgabeprozesse eGK, SMC-B, …







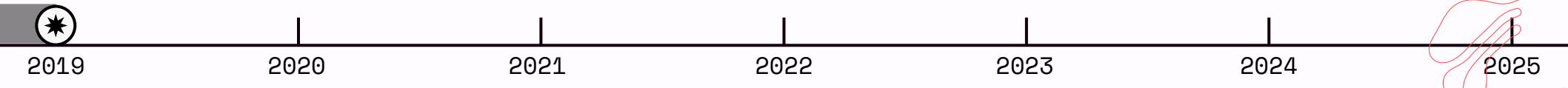
◀ **Bekannt seit 2012**

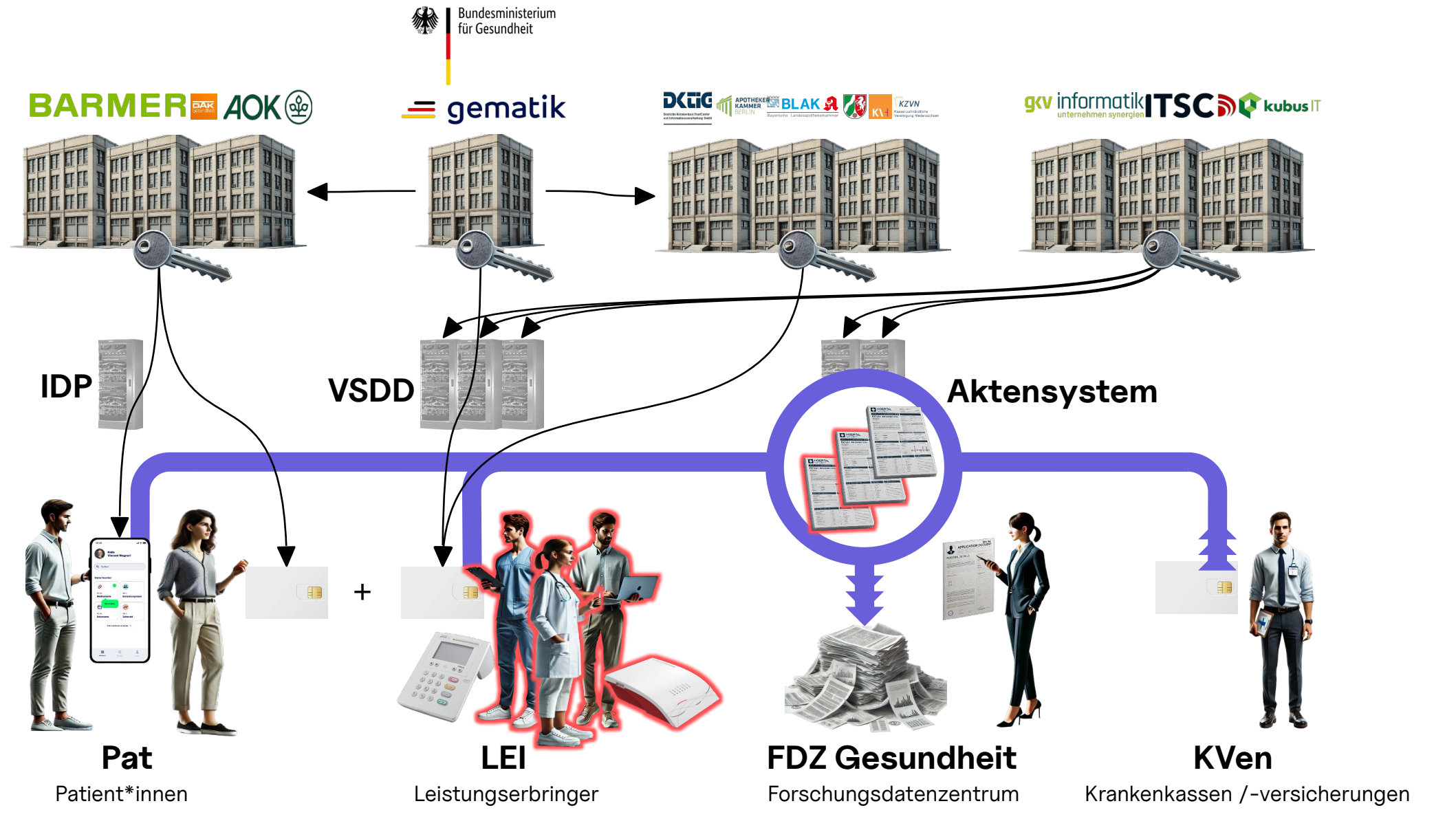
Demonstriert 2019

2019 2020 2021 2022 2023 2024 2025

Ausgabeprozesse eGK, SMC-B, …

Der Angriff
hatte einen Aufwand von etwa **1 Stunde**,
war **remote** durchführbar und
ermöglichte **Vollzugriff** auf **eine ePA** bzw.
alle für diese LEI freigegebene ePAs..




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

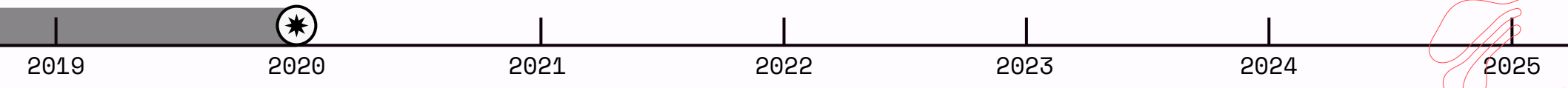
Konnektoren falsch herum

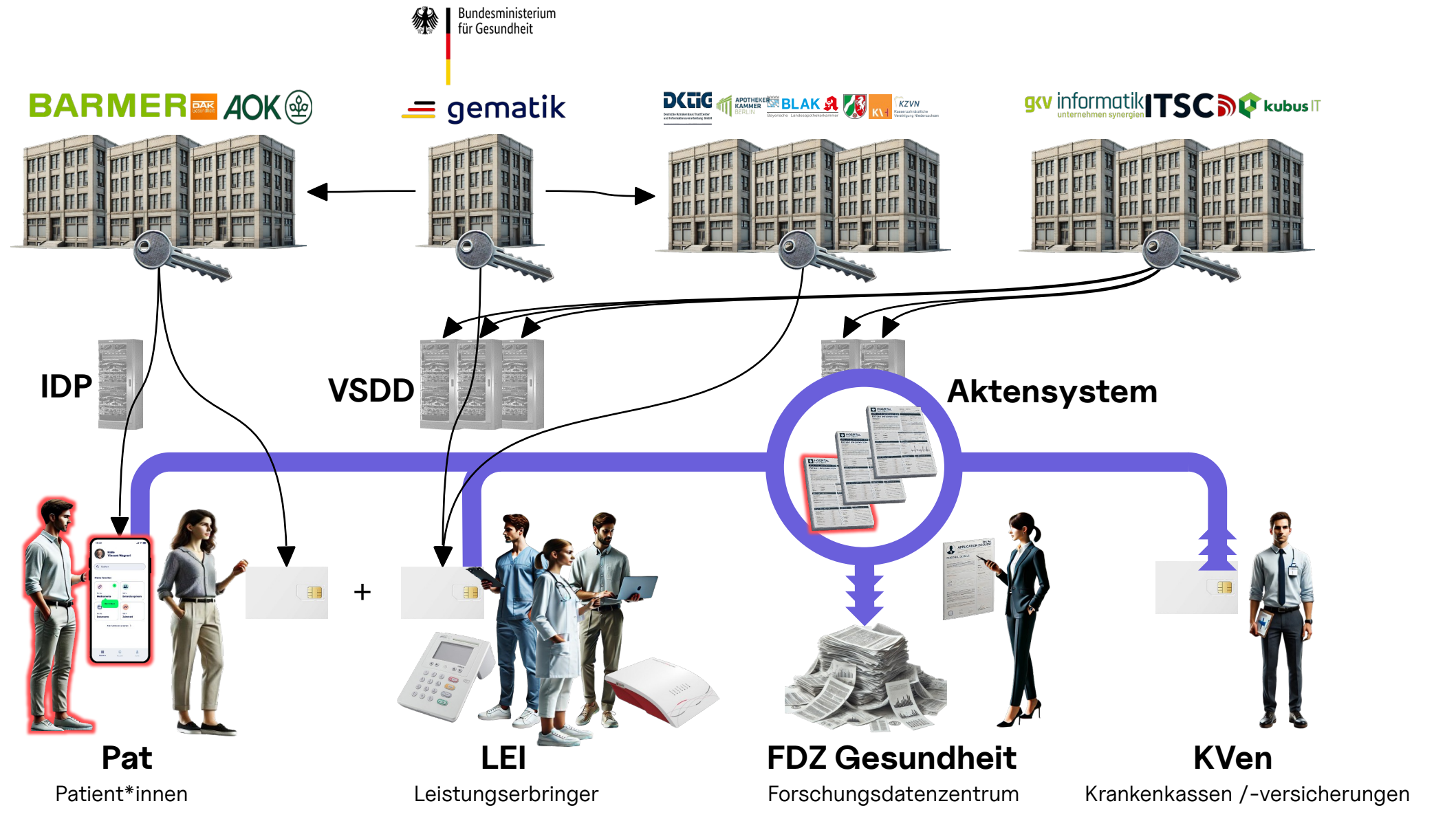
«Wenn die elektronische Patientenakte dagewesen wäre, hätten wir sie lesen können»

Christoph Saatjohann, auf dem rC3 2020

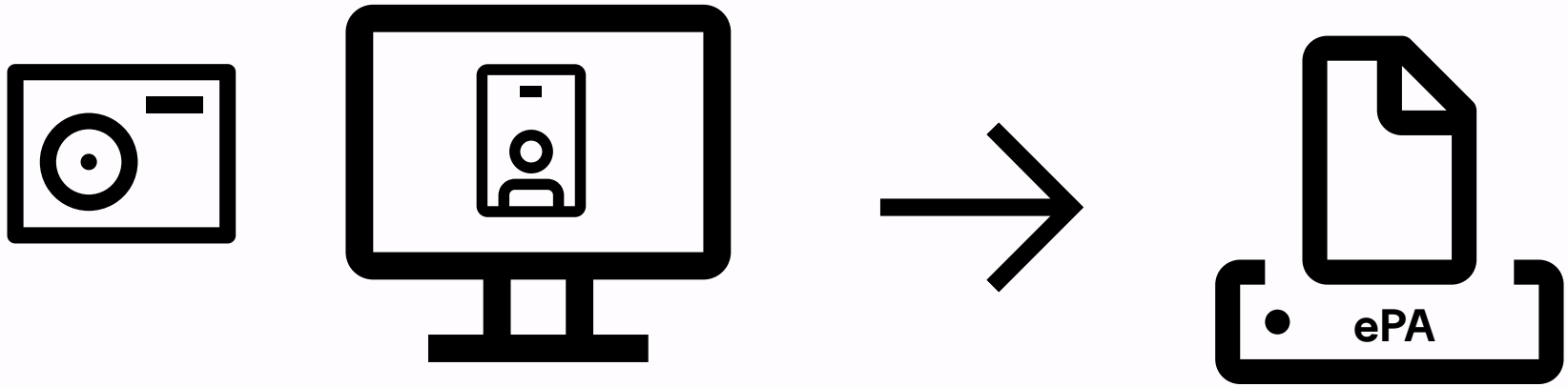
Konnektoren falsch herum

Der Angriff
hatte einen Aufwand von etwa **1 Tag**,
war **remote** durchführbar und
ermöglichte **Vollzugriff** auf **für diese LEI freigegebene ePAs**.




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

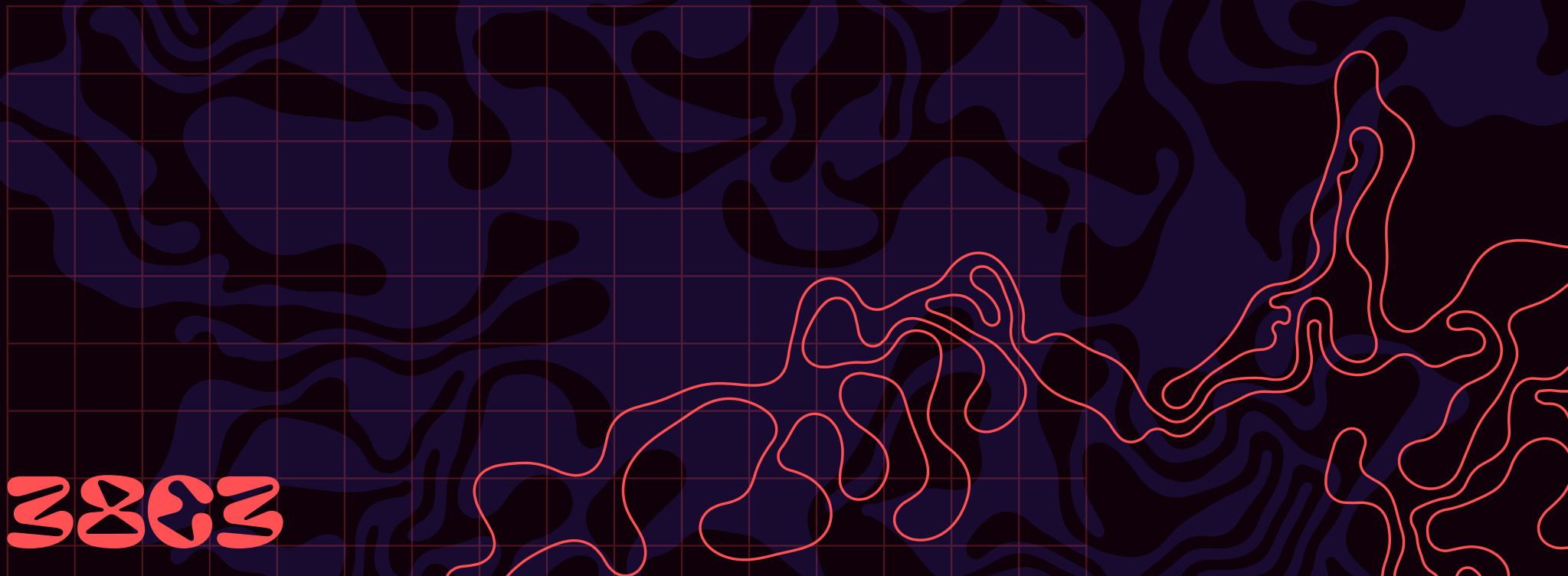
Videoident



Videoident

Der Angriff
hatte einen Aufwand von etwa **1 Woche**,
war **remote** durchführbar und
ermöglichte **Vollzugriff** auf eine **ePA**.

Aktueller Stand Mitte Dezember 2024

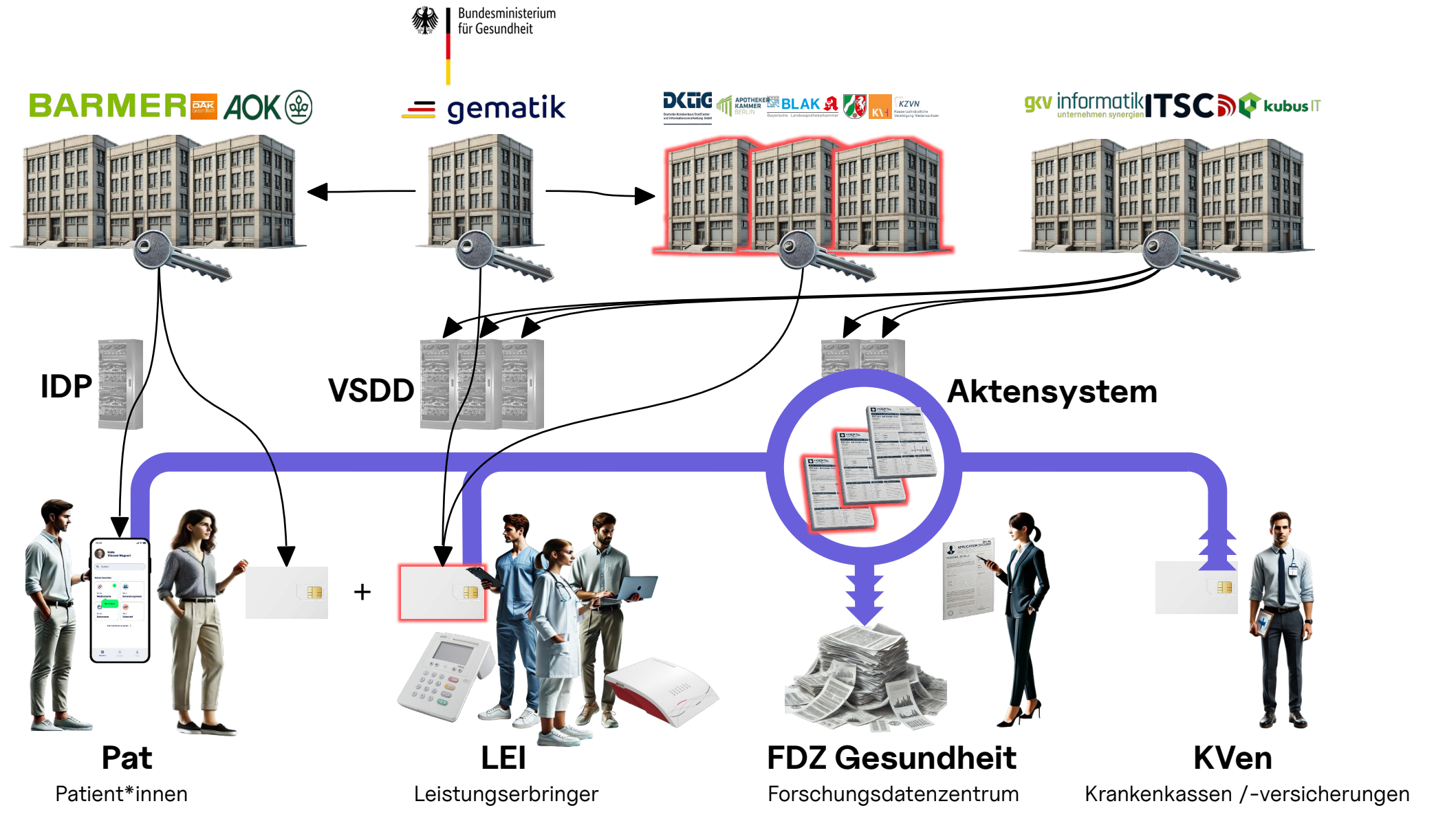


«Eines der größten IT-Projekte der Bundesrepublik»

Florian Fuhrmann, gematik, im Ärzteblatt

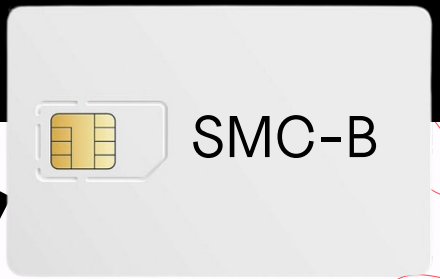
«Unsere ePA ist die sicherste in Europa»

Susanne Ozegowski, Bundesgesundheitsministerium, im Ärztenachrichtendienst


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

Kartenherausgeberportale

```
SELECT *
  FROM mitglieder
 WHERE passwort='f925916e2754e5e03f75dd58a5733251'
   AND mitgliedsnummer='<SQLi>'
```

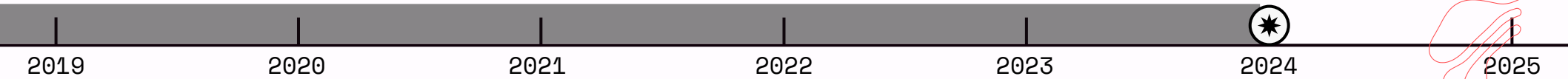


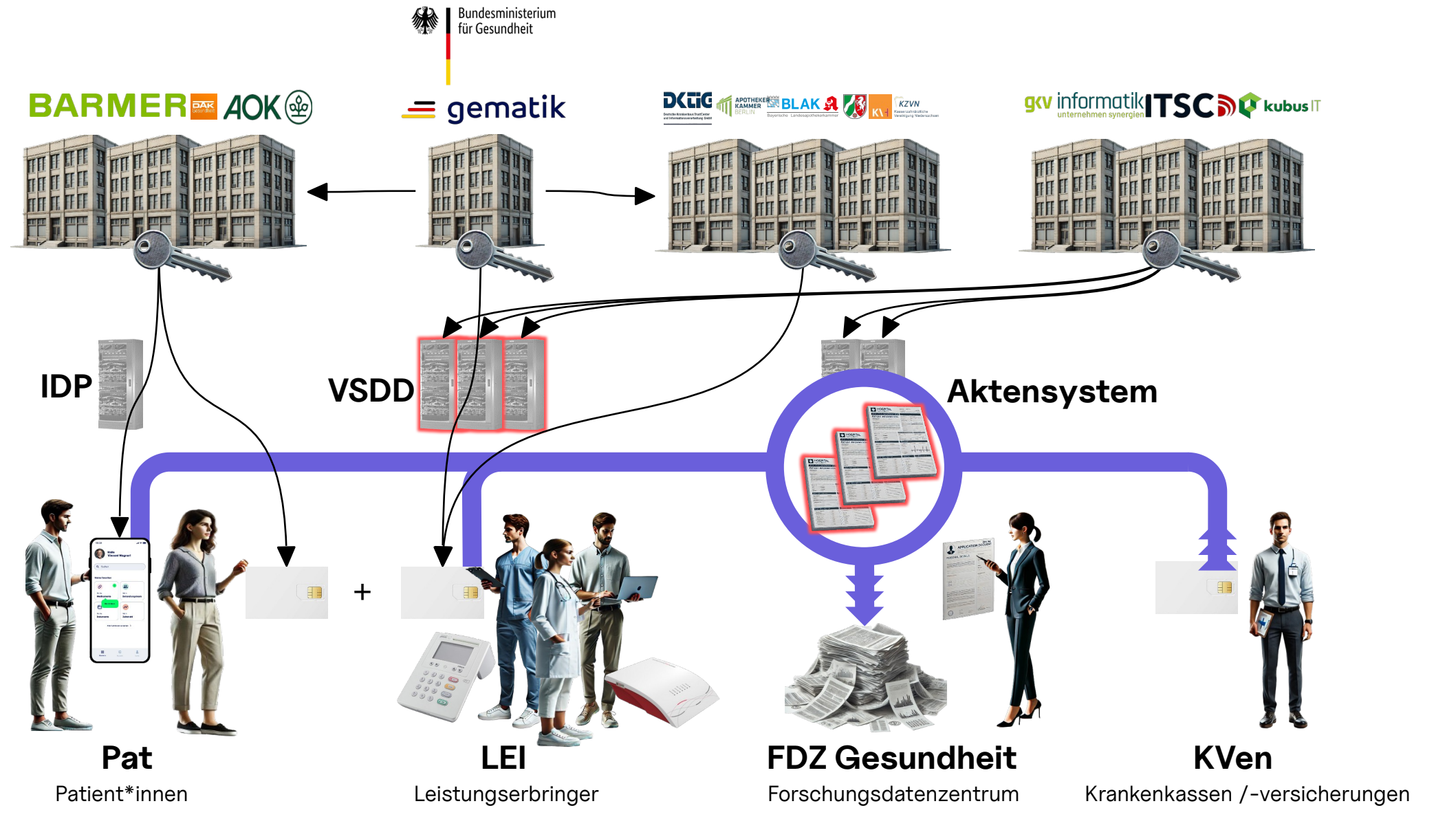
Kartenherausgeberportale

Der Angriff
hat einen Aufwand von etwa **1 Stunde**,
ist **remote** durchführbar und
ermöglicht **Vollzugriff** auf **für diese LEI freigegebene ePAs**.

Bekannt seit 2019

Nachgewiesen 2024




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

VSDD

VSDM+

ICCSN

PNW

PNW

Daten

EF.GDO ICCSN

EF.C.eGK.AUT_CVC ICCSN

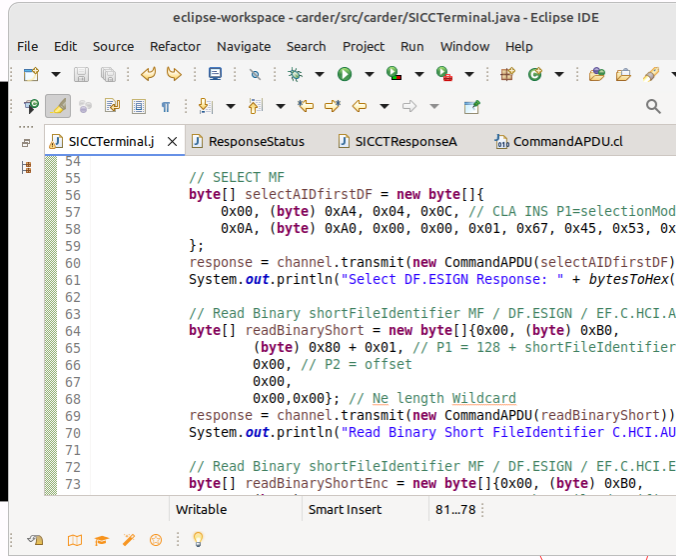
VSDM+

ICSSN

8027600999001234567 6

8027600999001234567 7

8027600999001234567 8



«Eine von der gesteckten eGK abweichende ICCSN deutet auf einen Fehler der dezentralen TI oder einen Angriff hin»

SST Fachdienste (UFS/VSDD/CMS), gematik, in Spezifikation 1.6.0

«Daher kann der Angreifer im Remote-Fall Karten während des Vorgangs tauschen, von der Karte gelesene Daten manipulieren oder selbst erzeugte Daten senden, die gar nicht von einer eGK gelesen wurden.»

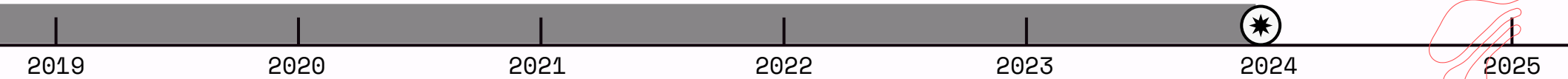
Spezifikation eHealth-CardLink (eH-CL), gematik, in Spezifikation 1.0.0

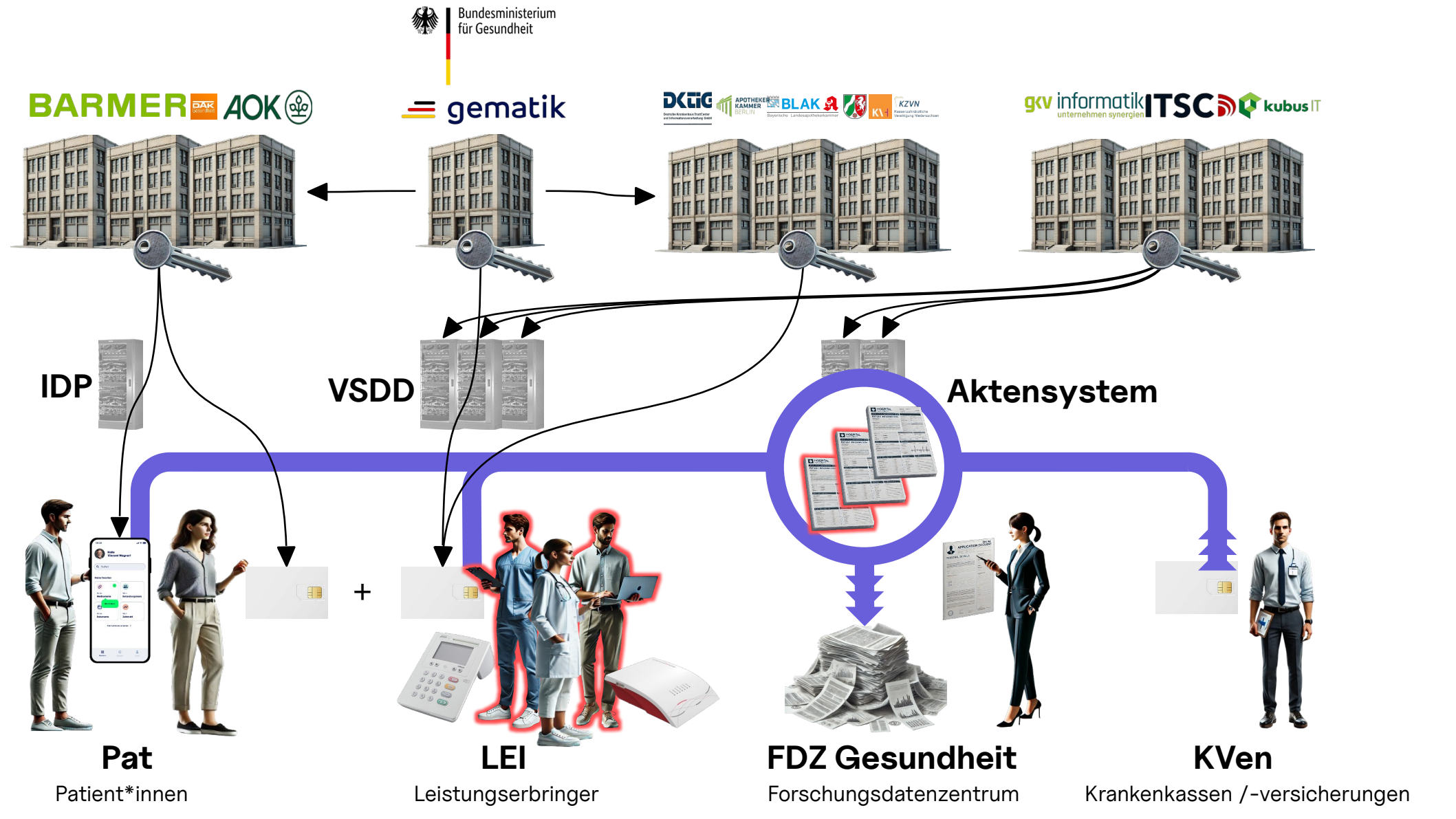
VSDM+

Der Angriff
hat einen Aufwand von etwa **1 Monat**,
ist **remote** durchführbar und
ermöglicht **Vollzugriff auf alle ePAs**.*

* Vorbedingung: Zugang zur TI sowie SMC-B sowie keine spezifische Einschränkung spezifischer LEI in individueller ePA

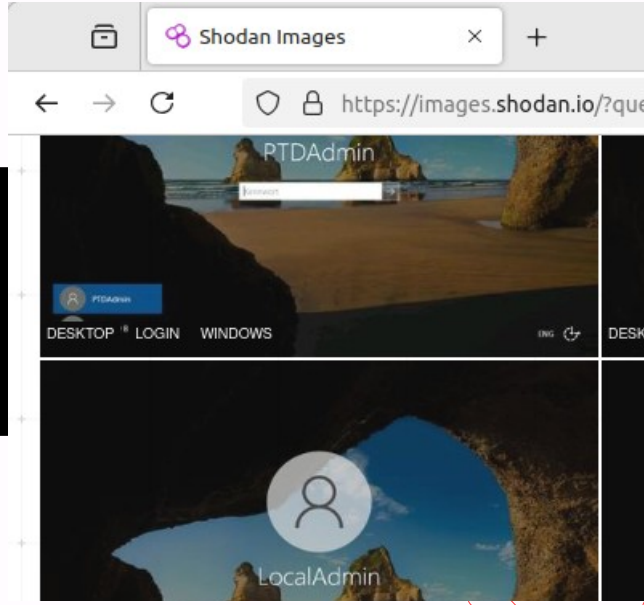
◀ Bekannt seit mindestens 2016 **Gemeldet 08/ 2024**




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

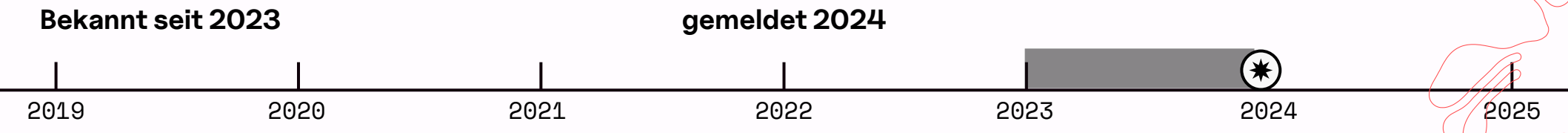
Praxis-IT in großem Stil verwundbar

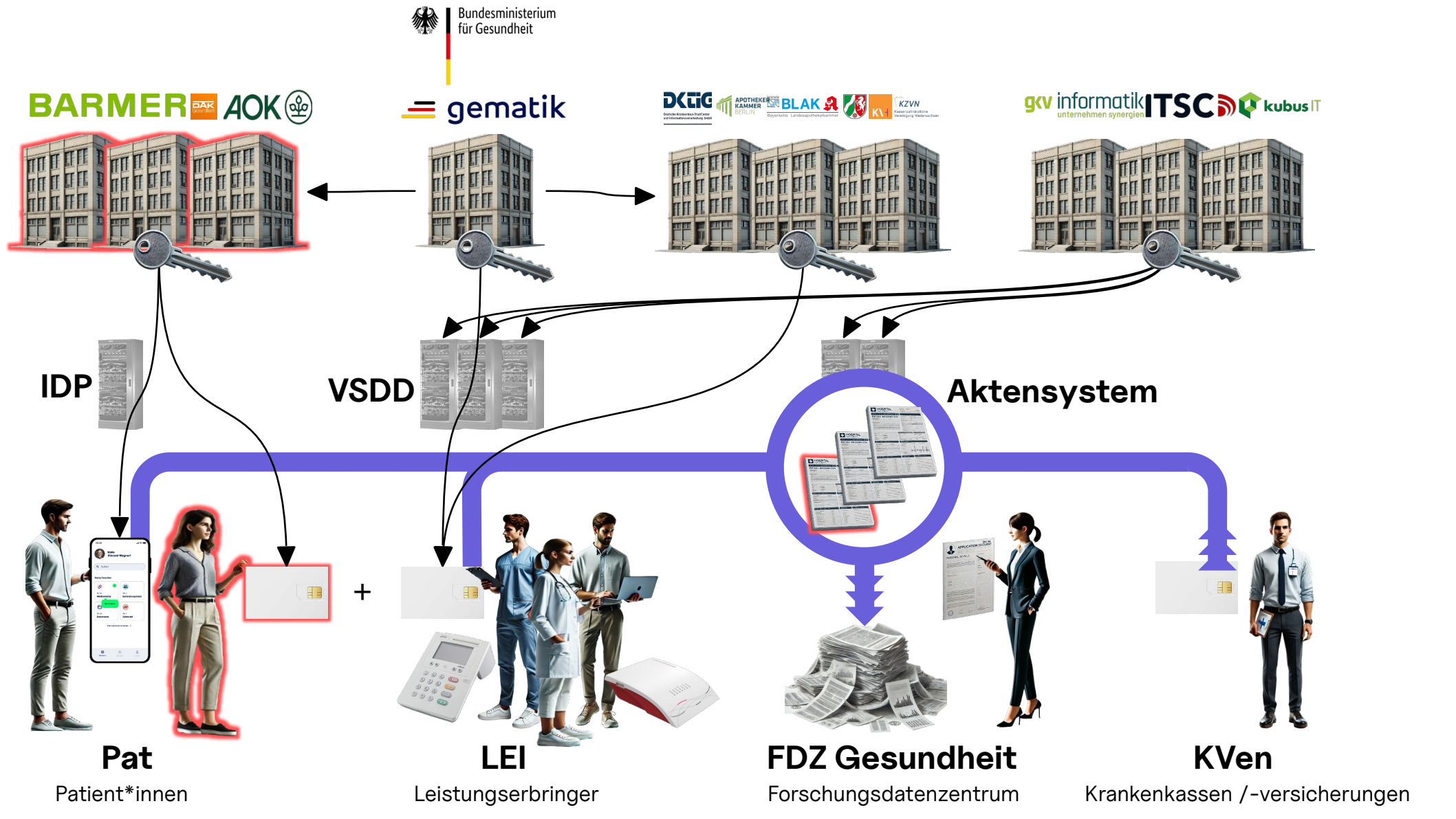
USER	admin
PASSWORD	password



Praxis-IT in großem Stil verwundbar

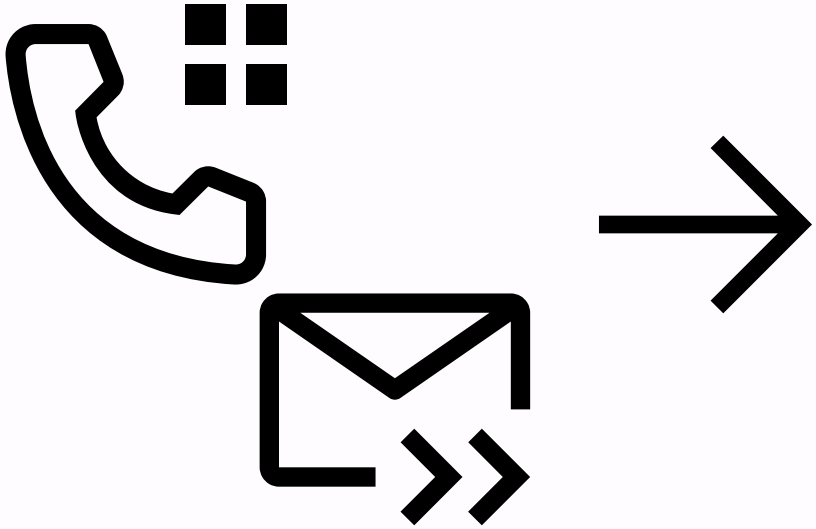
Der Angriff
hat einen Aufwand von etwa **2 Stunden**,
ist **remote** durchführbar und
ermöglicht **Vollzugriff** auf auf **für diese LEI freigegebene ePAs**.

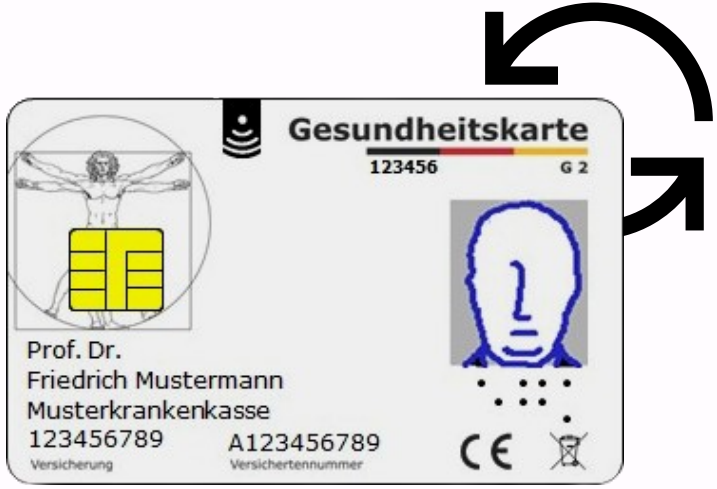



Bundesministerium
für Gesundheit
BARMER
DAK
AOK
gematik
DKTIG
APOTHEKER KAMMER BERLIN
BLAK
KZVN
gkv informatik
ITSC
kubus IT
IDP
VSDD
Aktensystem
+
Pat
Patient*innen
LEI
Leistungserbringer
FDZ Gesundheit
Forschungsdatenzentrum
KVen
Krankenkassen /-versicherungen

Ausgabeprozesse eGK

- 2014
- 2015
- 2016
- 2017
- 2017
- 2019



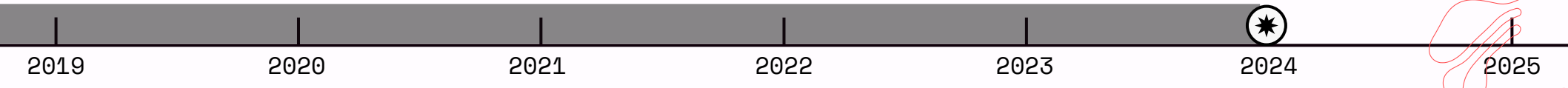


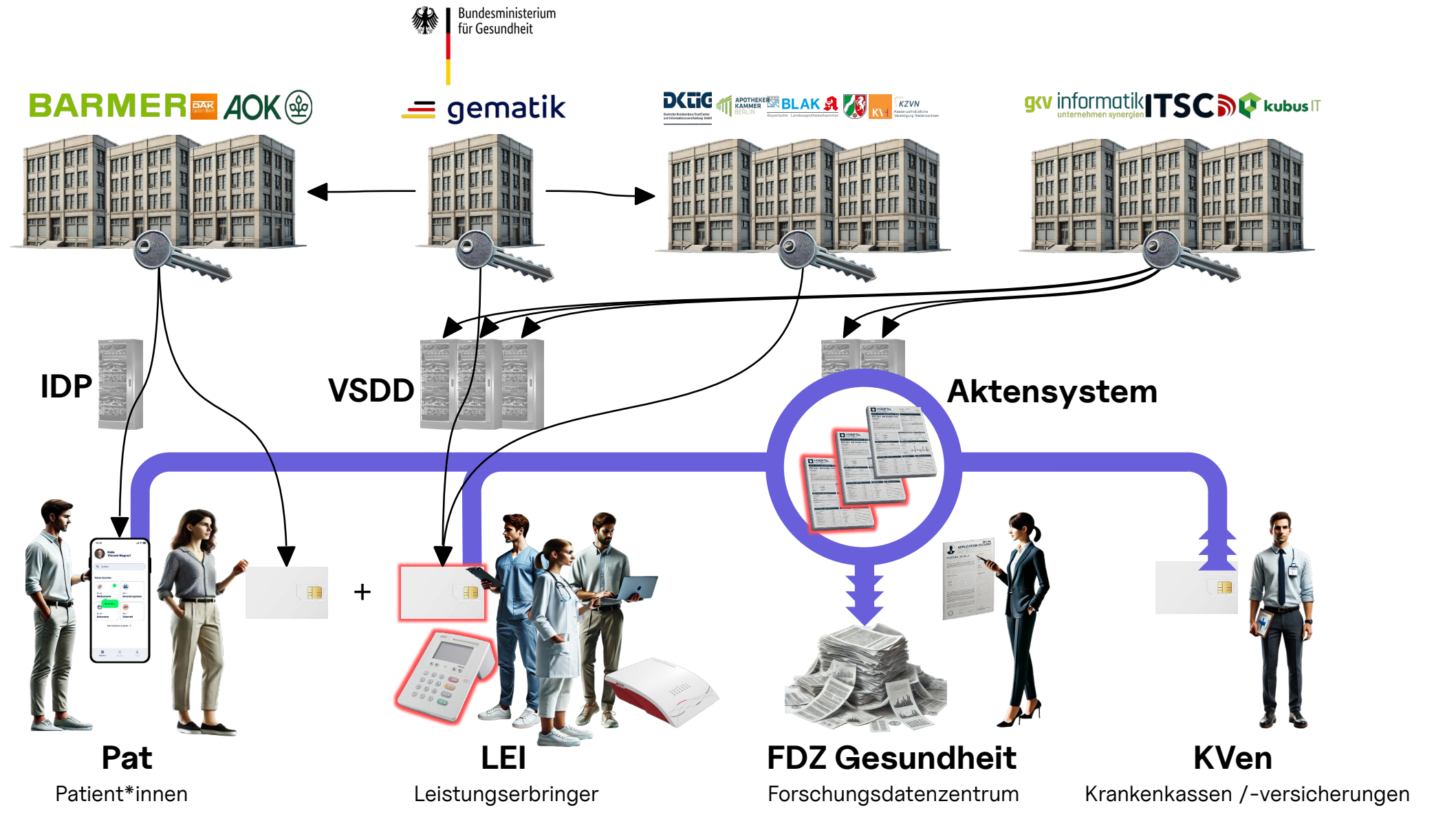
Ausgabeprozesse eGK

Der Angriff
hat einen Aufwand von etwa **20 Minuten**,
ist **remote** durchführbar und
ermöglicht **Lese-Lösch-Zugriff** auf diese eine ePA.

◀ **Bekannt seit 2012**

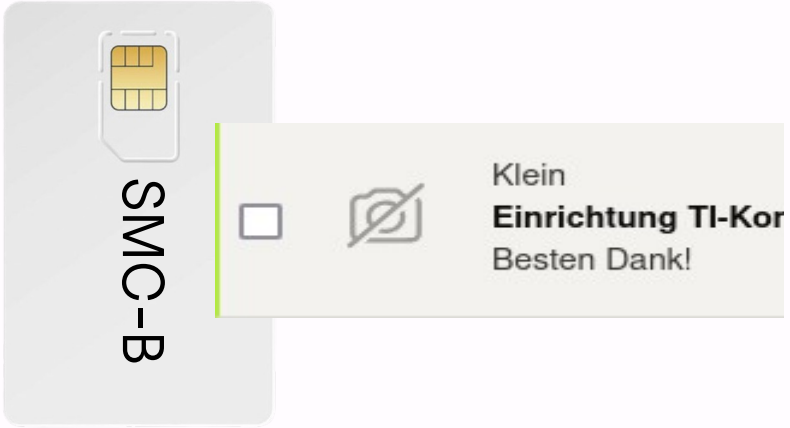
Demonstriert 12/2024




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

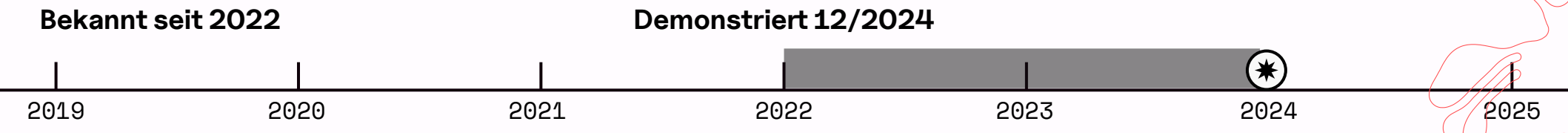
Kompromittierung Telematik-ID

Kleinanzeigen

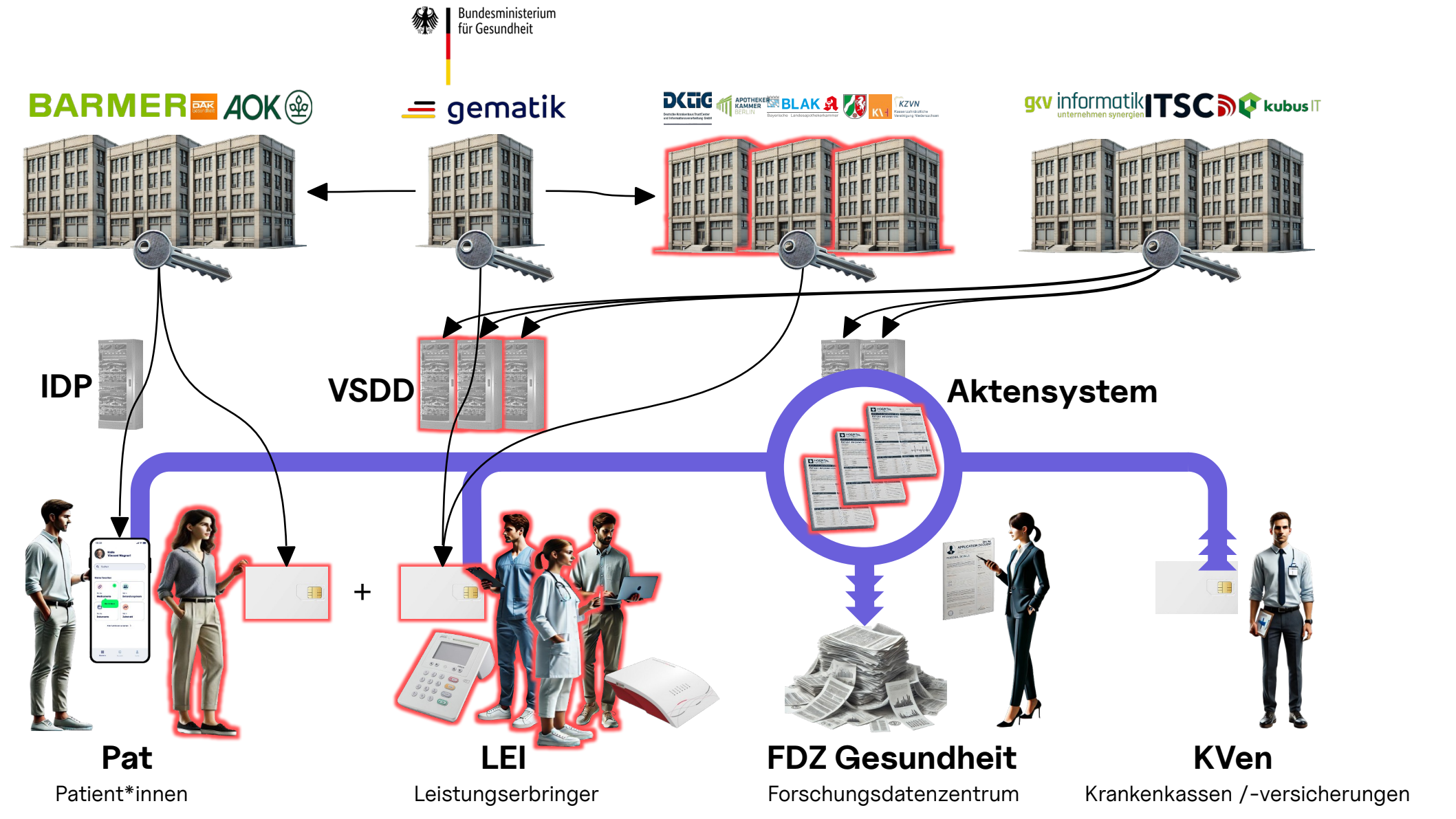


Kompromittierung Telematik-ID

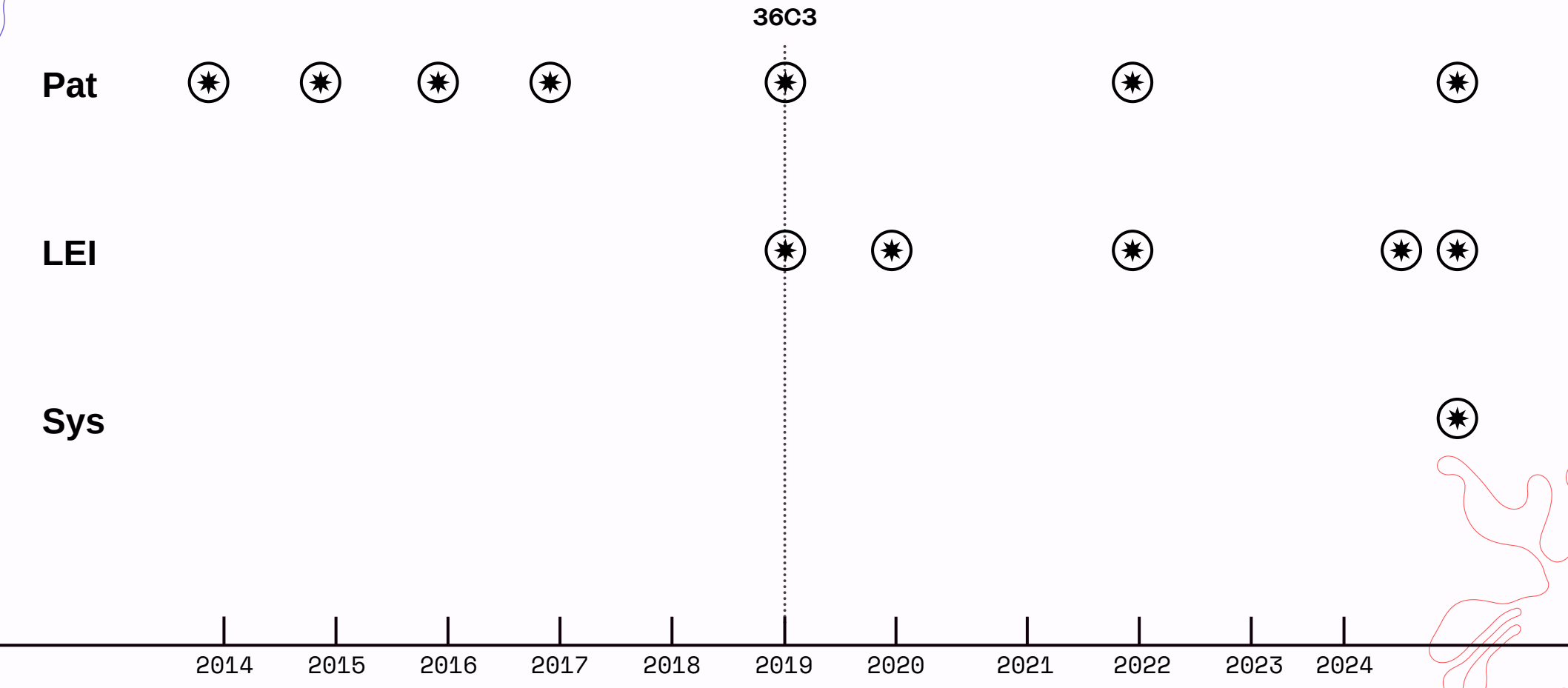
Der Angriff
hat einen Aufwand von etwa **4 Stunden**,
ist **remote** durchführbar und
ermöglicht **Vollzugriff** auf auf **für diese LEI freigegebene ePAs**.



Fazit


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

Timeline


36C3
Pat
LEI
Sys
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024

Opportunitätskosten

- Narrativ von «ePA zu sicher» nicht haltbar aus Historie
- **Schadensausmaß** durch Cyberangriffe durch ePA für alle **gesteigert**
- Kosten eines Vertrauen verlierenden digitalen Gesundheitswesens in Gesamtbetrachtung immens

Gemeinsamkeiten

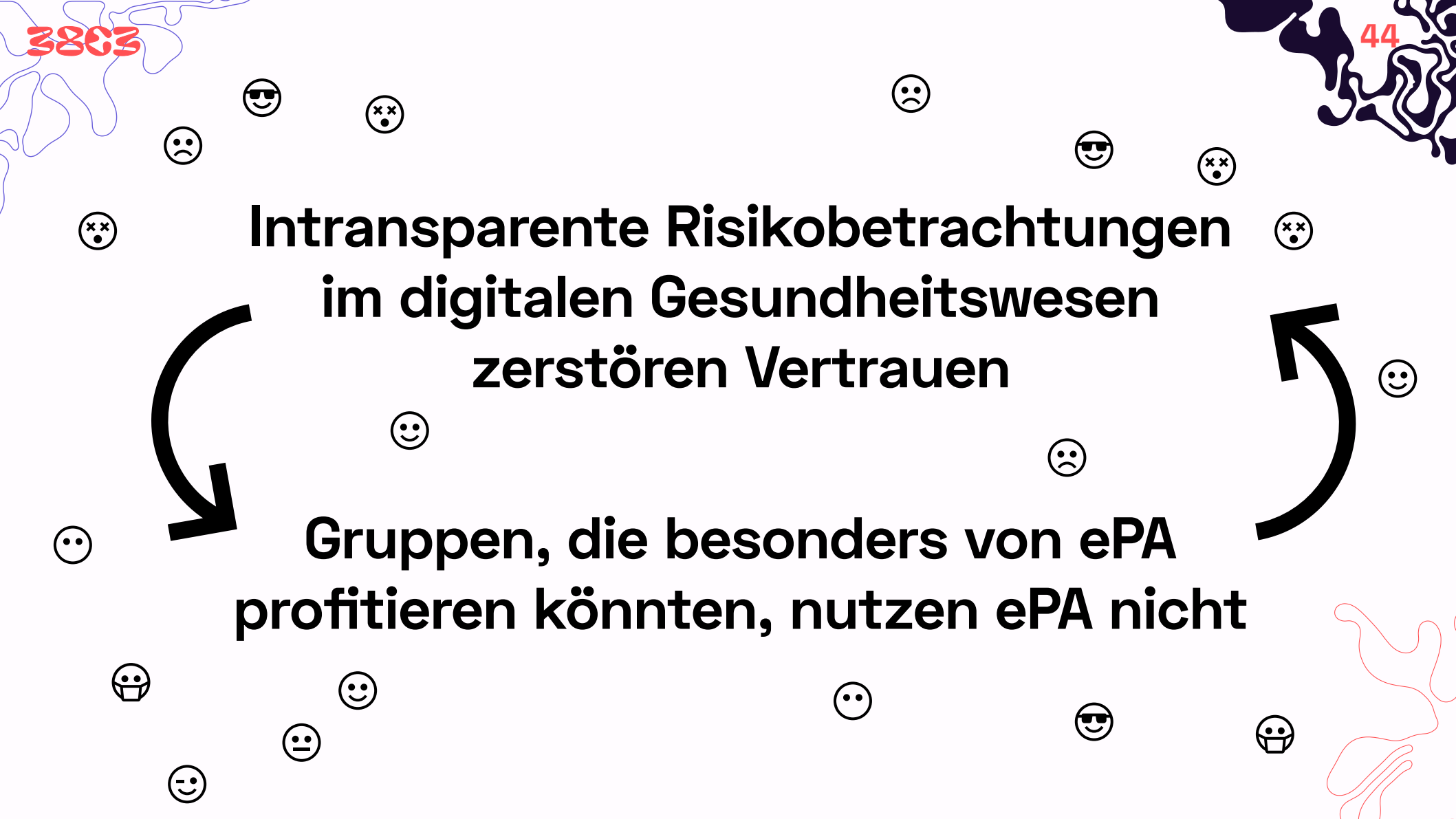
- Komplexität & Obskurität

Das System ist „inzwischen so komplex, dass es kaum noch jemand vollständig durchdringt.“
Randolf-Heiko Skerka, SRC

- Alles Außentäter-Szenarien, keine Innentäterposition

Forderungen

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



Intransparente Risikobetrachtungen im digitalen Gesundheitswesen zerstören Vertrauen

Gruppen, die besonders von ePA profitieren könnten, nutzen ePA nicht

Ziel: vertrauenswürdige Lösung für jeden Sicherheitsbedarf

«Es gilt Lösungen zu finden die es möglich machen, dass alle glücklich sind!»

Alena Buyx, ehemalige Vorsitzende Deutscher Ethikrat, im BR Podcast

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

Susanne Ozegowski, Bundesgesundheitsministerium, im Deutschlandfunk