achelos

OMNISECURE®

Ist das Mobilgerät bereit für die elektronische Patientenakte?

achelos GmbH

Christof Basener | Director eID Solutions

security health mobility public IoT

SecurITy made in Germany

Was beeinflusst die Eignung?

Top 10 Apps & Games by Downloads

Worldwide | 2019F

Rank	Apps	Parent Company	Games	Parent Company
1	Facebook Messenger	Facebook	Free Fire	Sea
2	Facebook	Facebook	PUBG MOBILE	Tencent
3	WhatsApp Messenger	Facebook	Subway Surfers	Kiloo
4	TikTok	ByteDance	Color Bump 3D	Good Job Games
5	Instagram	Facebook	Fun Race 3D	Good Job Games
6	SHAREit	SHAREit	Run Race 3D	Good Job Games
7	Likee	YY Inc	My Talking Tom 2	Outfit7
8	Snapchat	Snap	Homescapes	Playrix
9	Netflix	Netflix	Stack Ball	Azur Interactive Games
10	Spotify	Spotify	Call of Duty: Mobile	Activision Blizzard

Note: iOS and Google Play combined; 2019F based on January to November data

Quelle: https://www.appgemeinde.de

Generelle Aspekte

- Daten sind der Antrieb aller Top-Apps
- Zweitverwerter kaufen Daten und deuten die Kombinatorik
- Gesetzlage zweitrangig

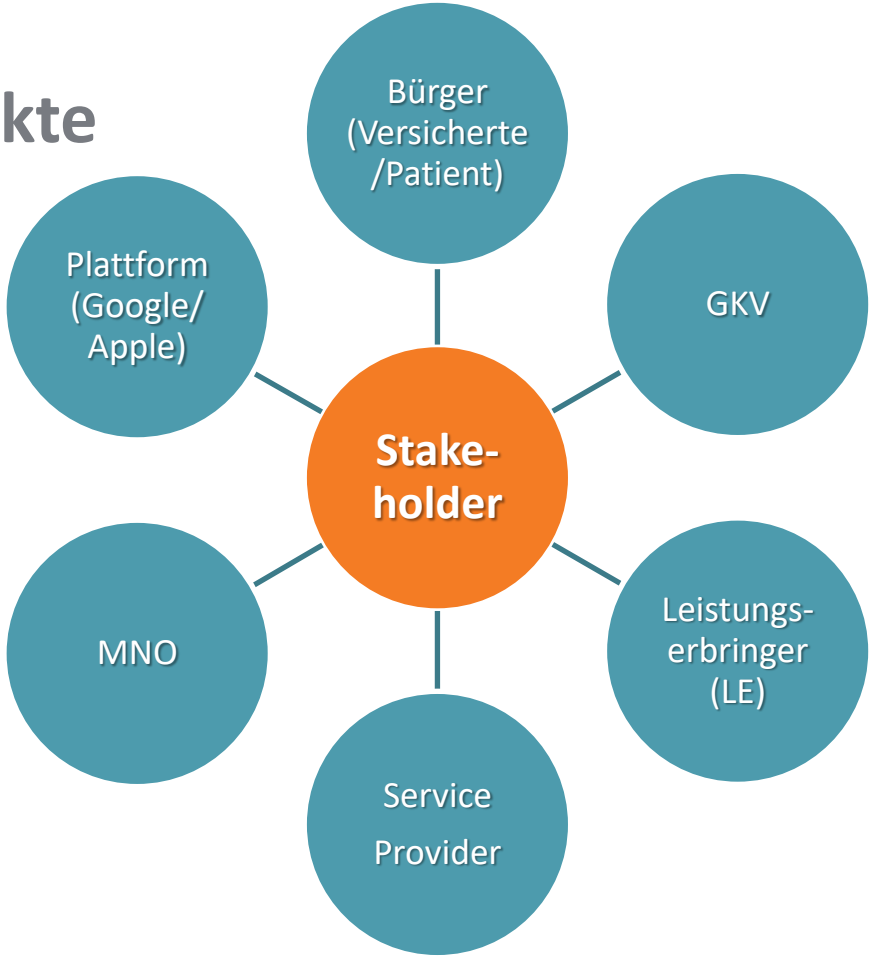
  (siehe: https://www.forbrukerradet.no/side/new-study-the-advertising-industry-is-systematically-breaking-the-law/)
- Ethik/Moral nicht vorhanden oder nachvollziehbar

  (Grindr: Weitergabe der HIV-Status der Teilnehmenden)

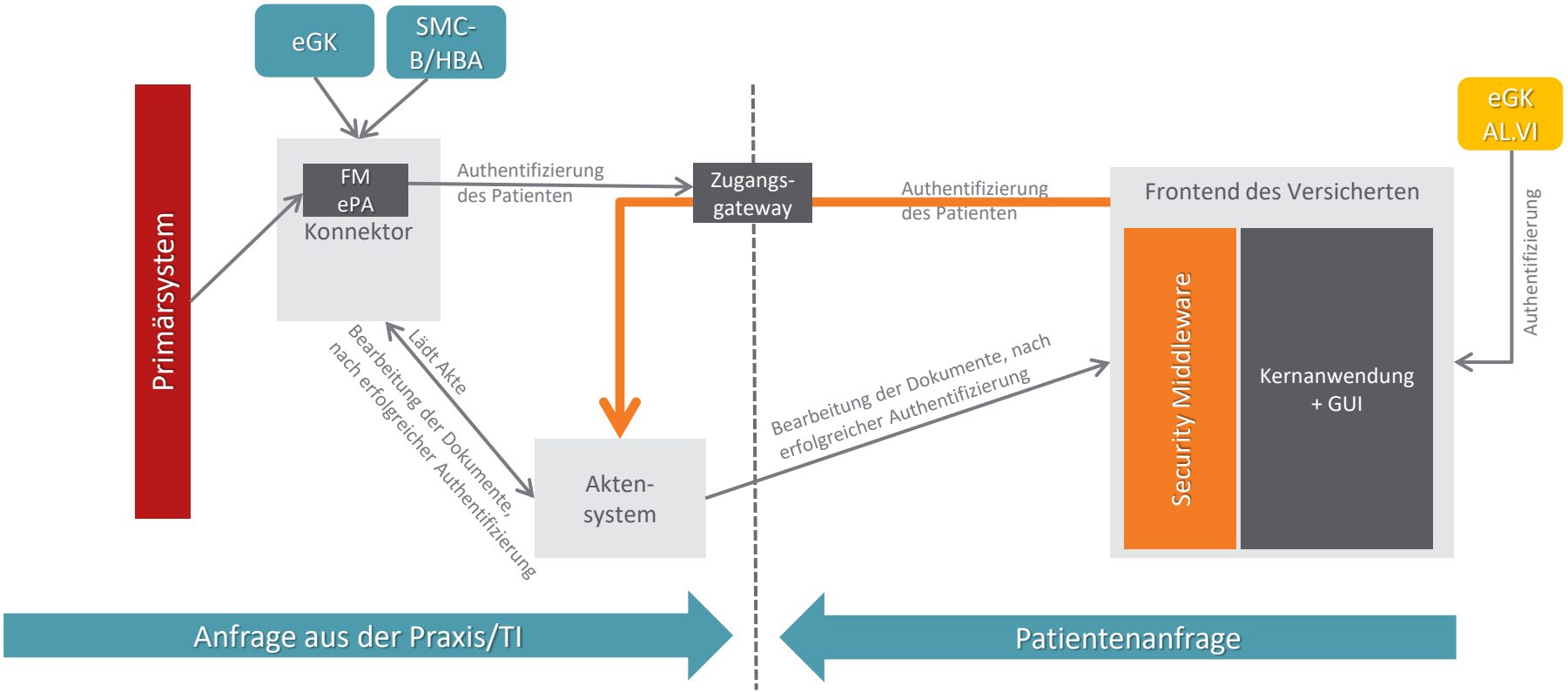
Was beeinflusst die Eignung?

- Organisatorische Aspekte
- Funktionale Eignung
- Technische Aspekte und Leistungsmerkmale
- Gesellschaftlicher Konsens (politischer Wille)
- Historische Erfahrungen
- Geschäftsbedingungen!!

Organisatorische Aspekte



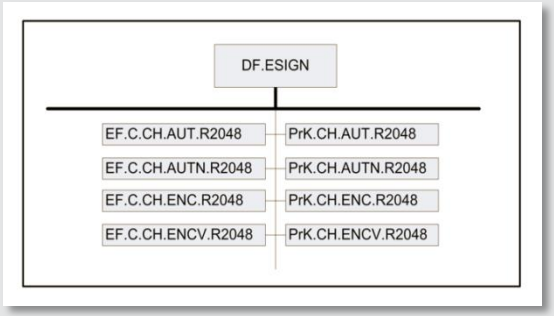
Schematischer Aufbau ePA

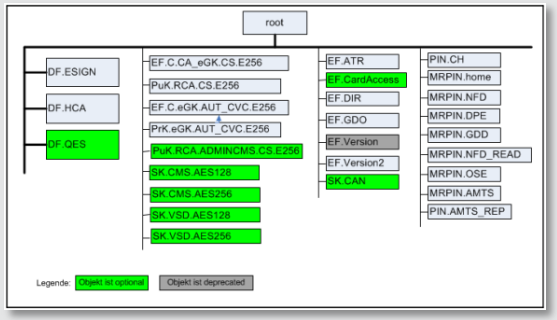


Aufgabe: eGK

Digitalisierte Versichertenidentität der Bürger/Bürgerinnen

- Digitalisierung der „LE“ nach §291a ff
  - TI mit VSDM
  - eIDAS, NFD, AMTS, Kom/LE, (ePA)
- Digitalisierung der Bürger
  - Die Karte hat seit ihrer Einführung ein komplettes Set an x509-Zertifikaten
  - Umrüstung der nächsten Generation von RSA zu ECC
  - Bis 2019: als kontakt – Karte: TR03116! EAL4+
  - Ab 2020: als kontaktlose Karte (NFC): TR03116! EAL4+
  - Ab 2021: „Alternative Authentisierung“ für Smartphones: ~~EAL2~~
  - Ab 2021: als virtuelle „Karte“ (eSE/eUICC)

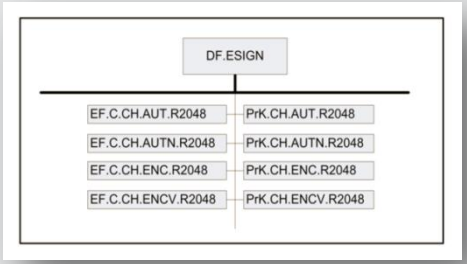




Ziel: Der vernetzte Patient

Digitalisierung für die Bürger/Bürgerinnen

- 2004 begann die Bundesrepublik mit der Digitalisierung der Patienten, indem eine digitale Identität auf Basis kryptographischer Methoden entwickelt wurde:
  die elektronische Gesundheitskarte (eGK)
- Von Beginn an waren Schlüssel und Zertifikate für die Authentisierung an Online-Portalen und die hochwertige
  Ver- und Entschlüsselung im Standardumfang JEDER eGK
- 2021 werden diese Identitäten zur Anmeldung an die elektronische Patientenakte (ePA) verwendet.
- Zu den „mitwachsenden“ Bedingungen gehören die grundsätzlichen Anforderungen an sichere Datenverarbeitung.



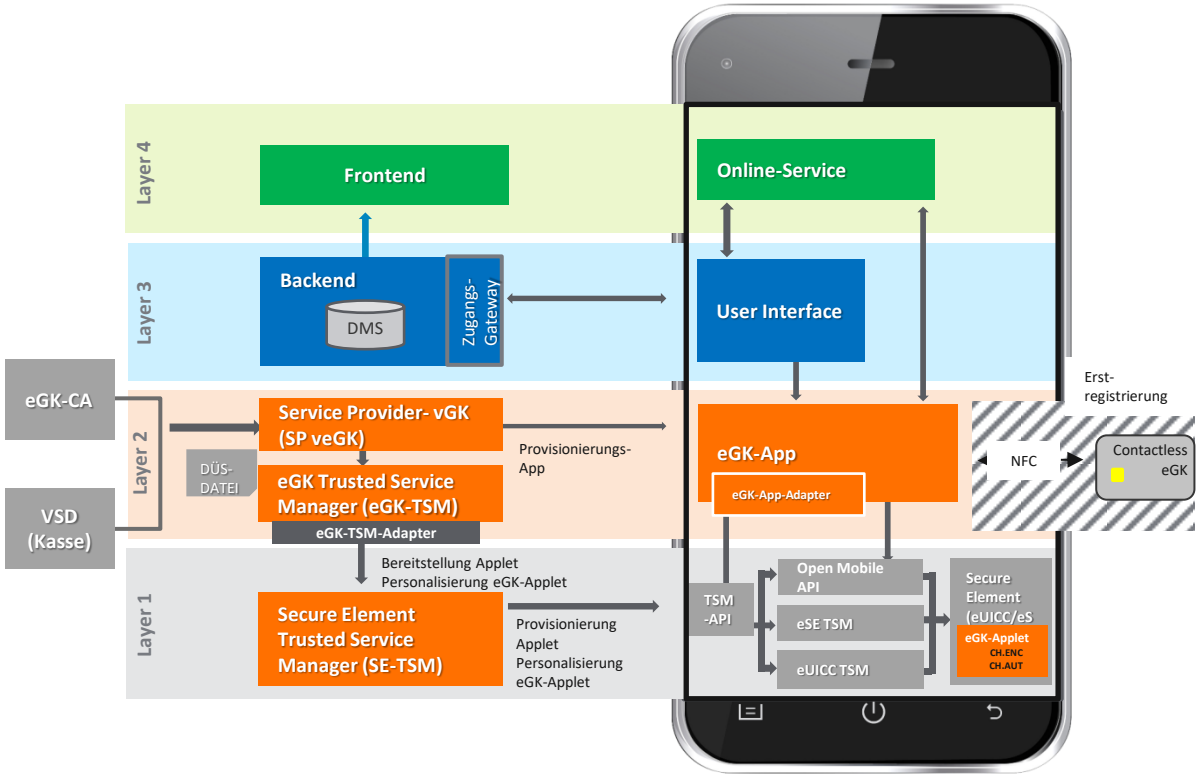
Motivation: es muss extrem sicher sein

Digitalisierung für die Bürger/Bürgerinnen

- Kriterien für sichere Datenverarbeitung:
  - Als Online-Authentisierung haben sich PKI-gestützte Verfahren bewährt.
  - Kritisch ist die Herstellung, Verwahrung und Verwendung der geheimen Schlüssel (PrK)
  - Kernanforderungen:
    - Der Besitzer ist jederzeit und unmittelbar „Herr“ über seinen/ihre Prk
    - Der Besitzer kann jederzeit den Schlüssel vernichten, wenn er/sie es für angemessen hält
    - Aufbewahrung und Verwendung passieren auf einer Plattform, die nach Common Criteria EAL4+ zertifiziert ist.
  - → Die vorgenannten Bedingungen werden von der eGK eingehalten
    - Mindestens die ersten beiden Bedingungen schließen eine Schlüsselverwahrung online aus, weil der Besitzer online sein muss, um sein Besitzrecht zu wahren bzw. zu beenden.
    - Die Sicherheitsmaßnahme beginnt beim Bürger, auf dessen Endgerät. Die Verlagerung der kryptographischen Verfahren ins Netz bedeutet, dass die Verfahren zur Aktivierung und Verwendung der Prks ebenso stark angelegt sein müssen.
  - → Die vorgenannten Bedingungen können auf mobilen Endgeräten eingehalten werden, wenn ein starker Mechanismus direkt am Gerät (eGK per NFC) oder im Gerät (Secure Element, UICC) vorhanden ist.

Virtuelle eGK

Funktionsmodell



Fazit

Eignung ist gegeben, wenn …

- Besitz und Eigentum der Daten klar sind.
- Bewusstsein bei allen Stakeholdern gleich ist, dass Datenverlust nicht geheilt werden kann. (Im Gegensatz zu Bankgeschäften)
- Technik lückenlos ist
- die Verwendung der Daten klar geregelt ist.
  (Ist Datenspende ein Geschäftsmodell oder Forschung?)
- die Plattform sich an Gesetze hält und der Staat diese auch durchsetzt.

achelos auf einen Blick

achelos.de
iot.achelos.com

Firmensitz	achelos GmbH | Vattmannstraße 1 | 33100 Paderborn
Geschäftsführung	Kathrin Asmuth, Thomas Freitag
Unternehmen	Herstellerunabhängiges Softwareentwicklungs- und Beratungshaus in Paderborn, gegründet im Mai 2008
Kompetenz	Expertenwissen in verschiedensten Kompetenzen in Kryptographie und Sicherheitstechnologie
Zielmärkte	Security, Health, Mobility, Public, IoT
Angebot	Produkte, Services (Beratung, Testen), Produktentwicklungspartner für embedded Security
Fokus	Übergreifende IT-Sicherheitsthemen und Industrielösungen für den internationalen Markt
Kunden | Partner	staatliche Institutionen, private Unternehmen und Organisationen mit Bedarf an Lösungen für sicherheitskritische Anwendungsfelder

achelos

Vielen Dank | Thank you

achelos GmbH
Vattmannstraße 1 | 33100 Paderborn | GERMANY
T +49 5251 14212-0 | info@achelos.de
achelos.de | IoT.achelos.com

security | health | mobility | public | IoT

SecurITy made in Germany