DiGA & DiPA:
Technischer Rundum- und Vorausblick

Zertifikate, ePA-Anbindung, MIO und Co.

Webinar SVDGV x _fbeta am 27. Oktober 2022

_fbeta

Agenda des Webinars am 27. Oktober 2022

1	Begrüßung
2	Rundumblick: Technische Anforderungen an DiGA & DiPA
3	Datenschutz
4	Datensicherheit
5	Kassen eID
6	Interoperabilität - ePA-Anbindung für DiGA - Best Practices DiGA MIO
7	Q&A

_fbeta: Unsere Geschäftsbereiche

Gesundheit. Digitalisierung. Transformation.

Healthcare Research & Market Access

- Research & Development
- Market Access
- Lifecycle Management
- Beyond the Pill
- Innovative Versorgungslösungen

Digital Health

- Market Access DiGA & DiPA
- Aufbau und Umsetzung Inkubatoren- und Acceleratoren-Programme
- Bewertung von Digital-Health-Produkten
- Digitales Versorgungs-management

Health Information Exchange

- Digitale Vernetzung von Gesundheitsregionen
- Einführung von Telematikanwendungen
- Strategieberatung für Vernetzungsprojekte

Technology & Architecture

- Technik, IT-Strategie und Architektur
- KI und Automatisierung

Digital Transformation

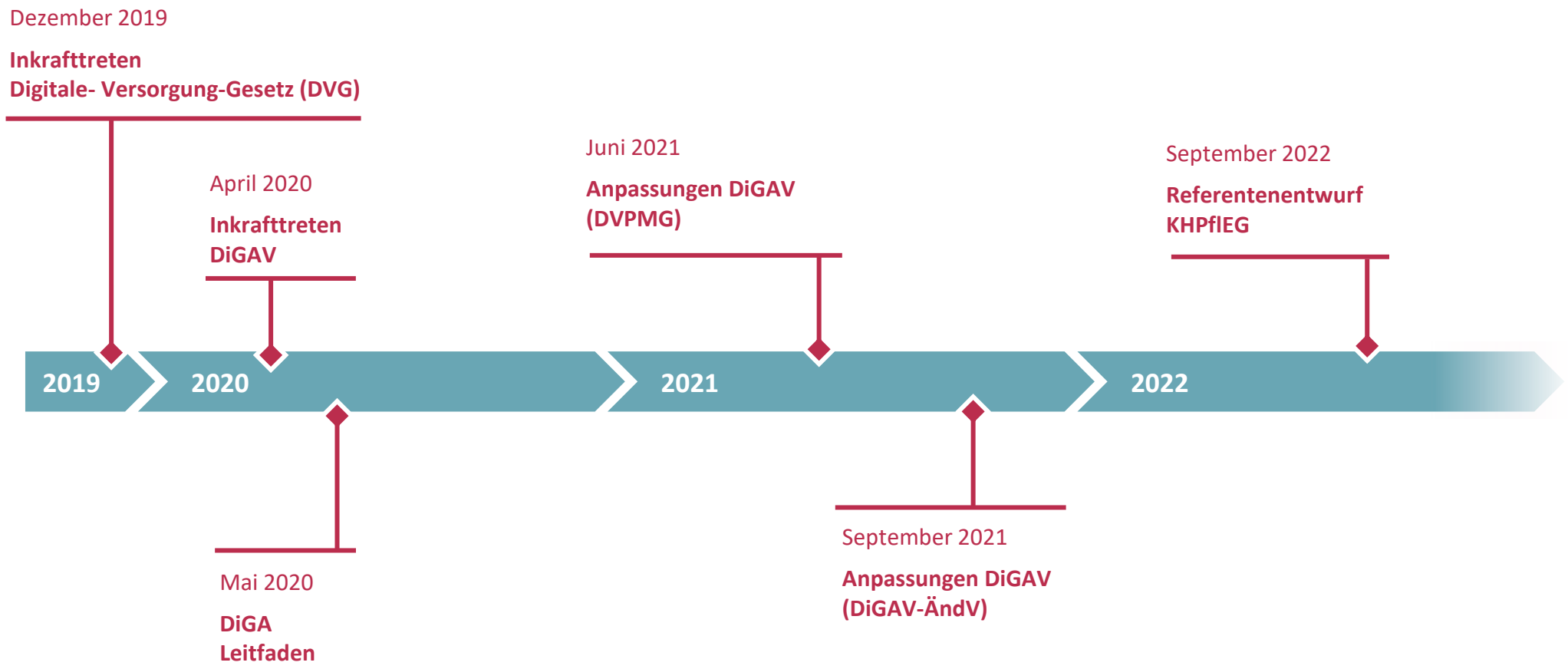
- Digitalisierungsstrategien für Krankenhäuser
- ePA und Telematik-infrastruktur: Chancen erkennen und Veränderungen nutzen
- Prozessoptimierung

Technische Anforderungen an DiGA & DiPA

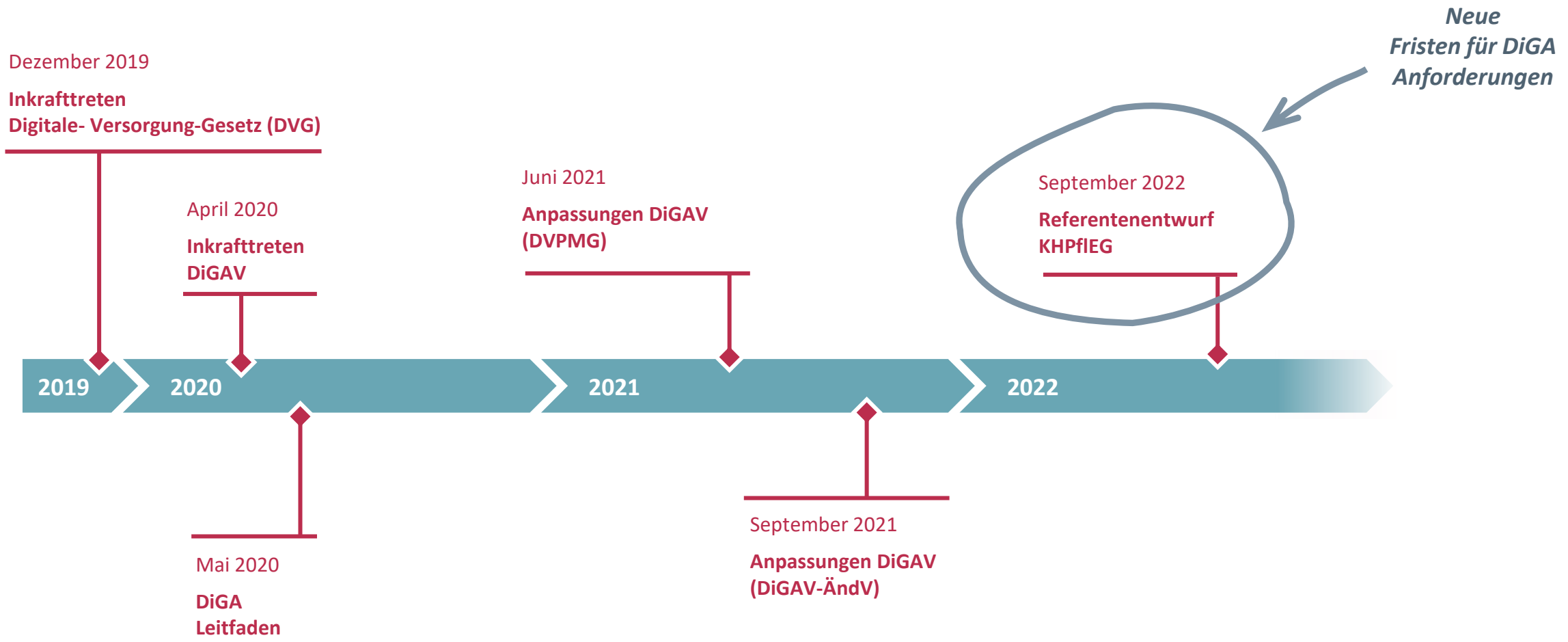
Rundum- und Ausblick auf die bestehenden
und kommenden Anforderungen

_fbeta

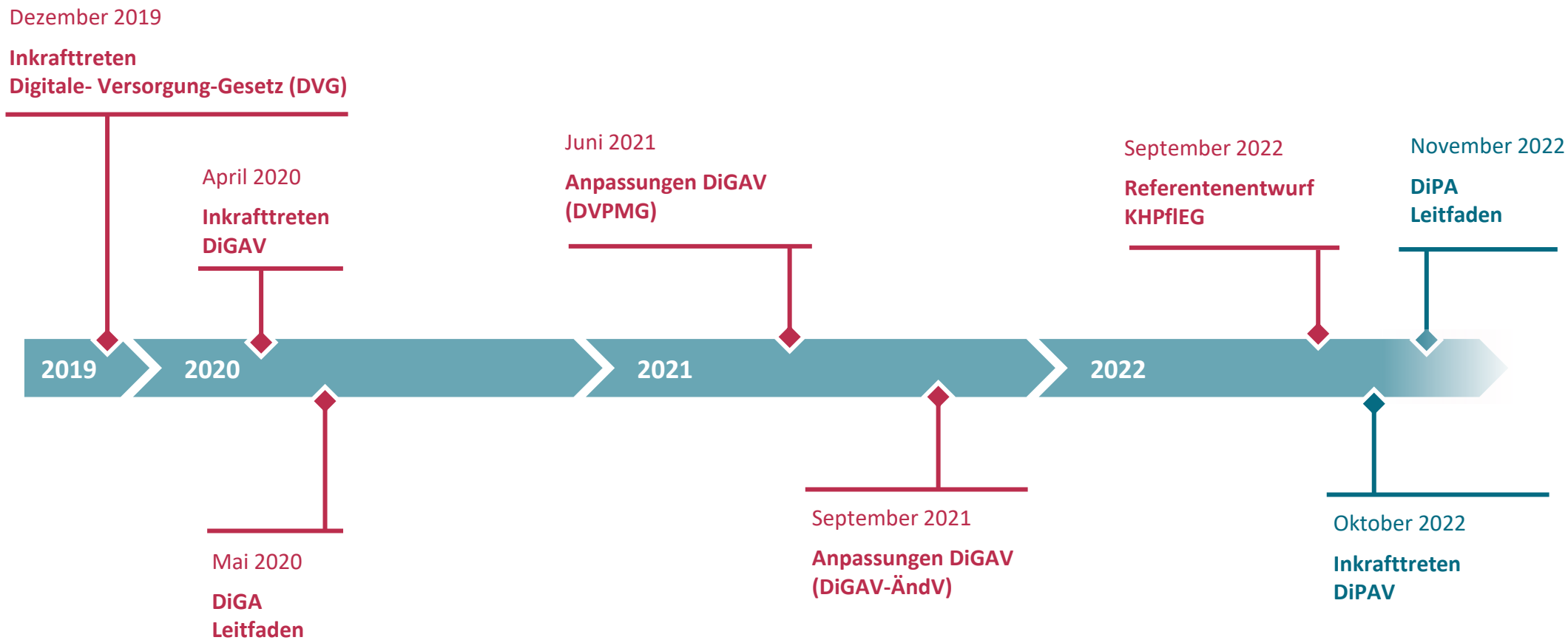
Agile Anpassung der gesetzlichen Anforderungen



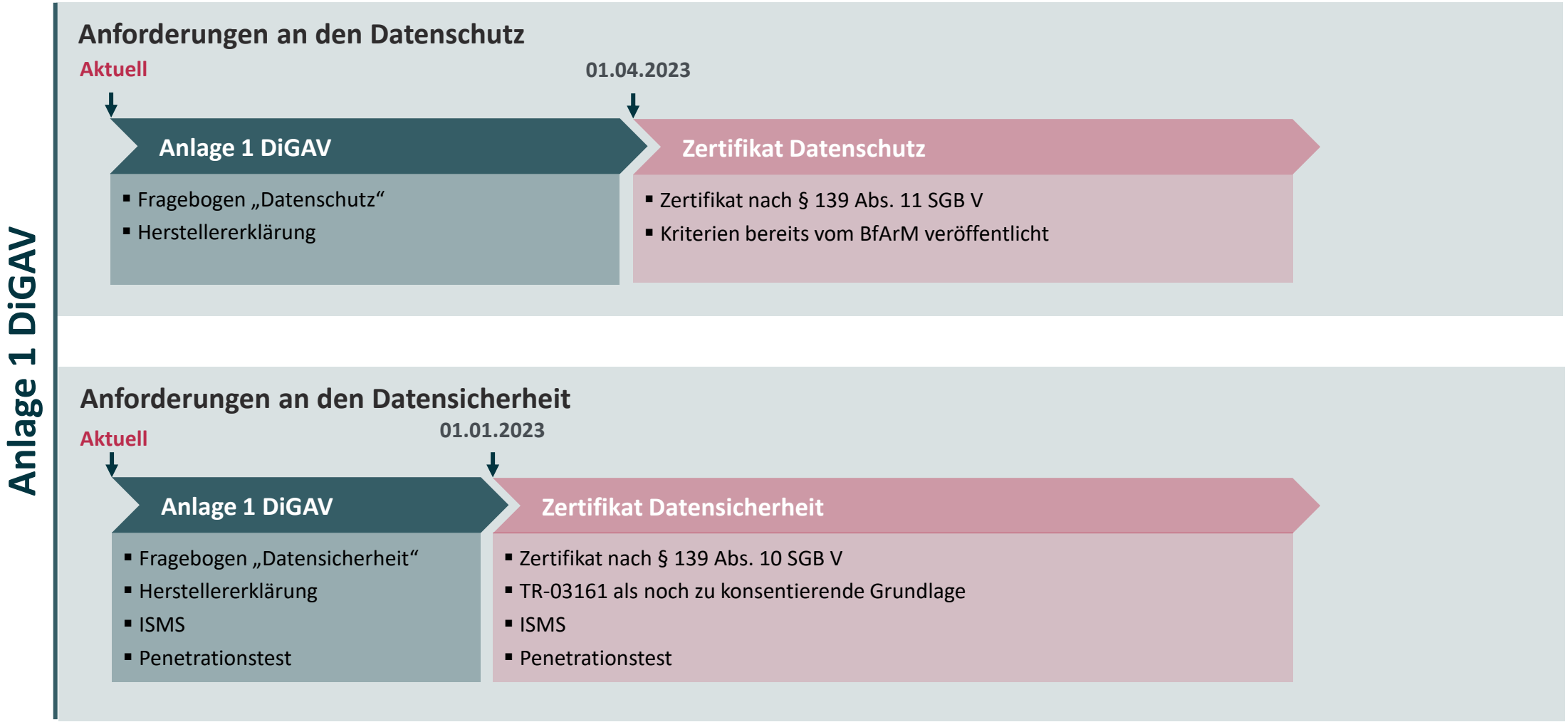
Agile Anpassung der gesetzlichen Anforderungen



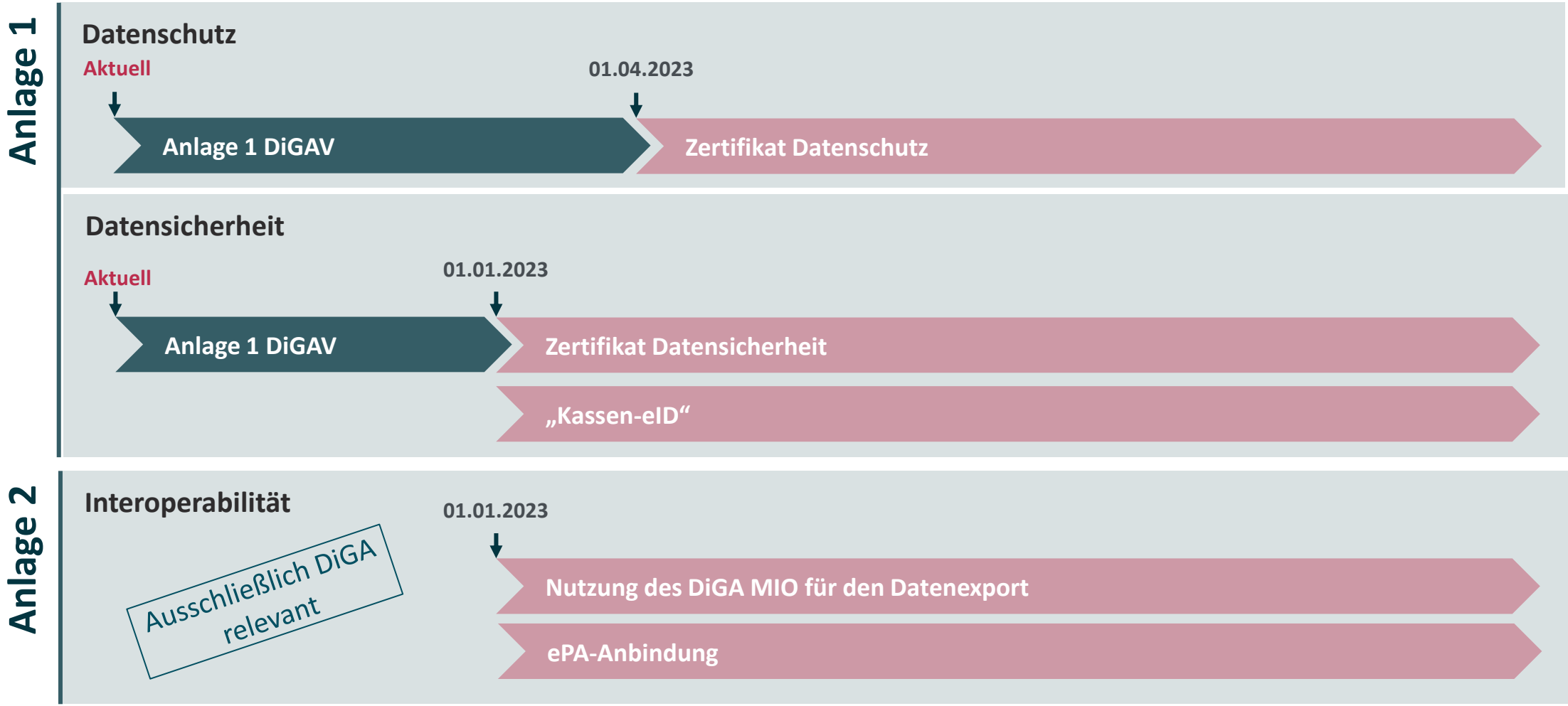
Agile Anpassung der gesetzlichen Anforderungen



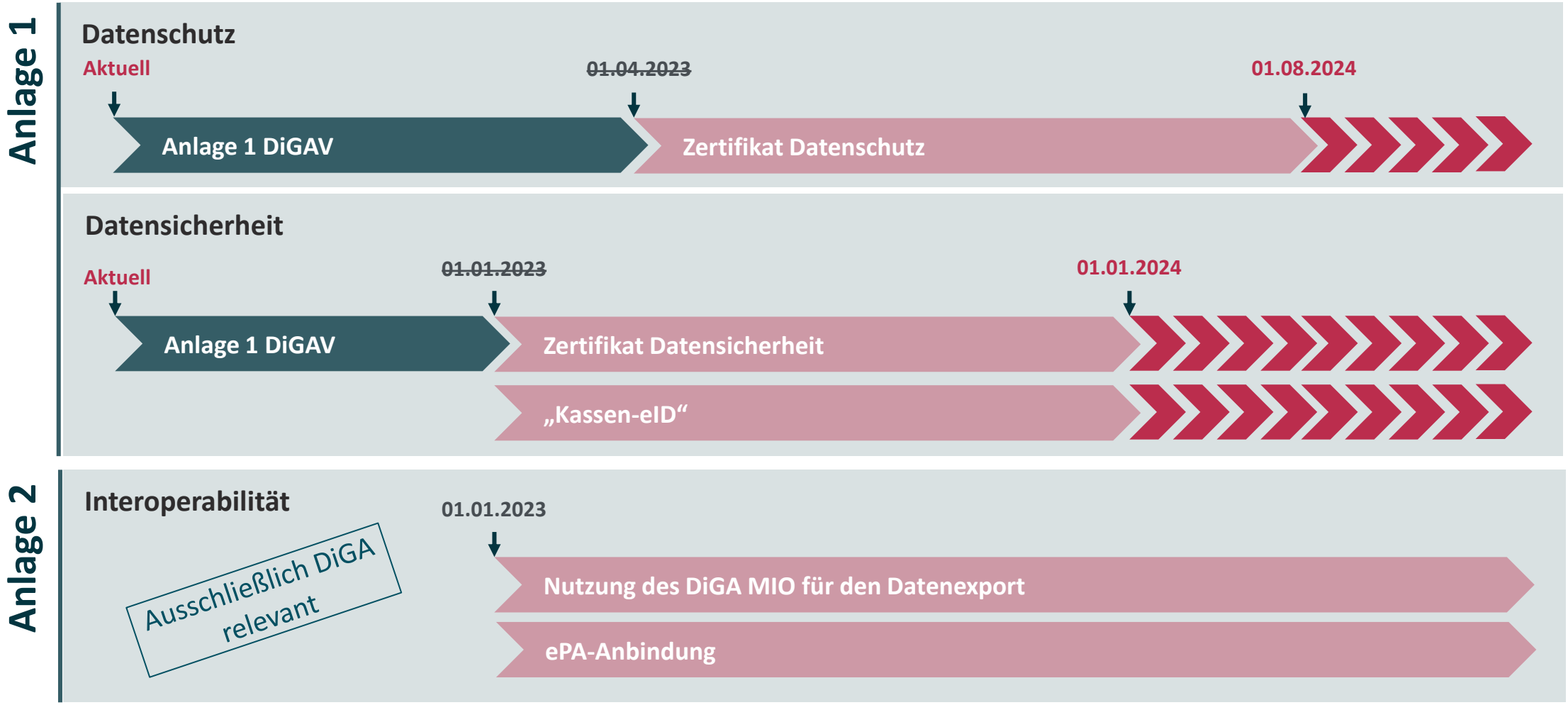
Neue DiGA Zertifikate in 2023



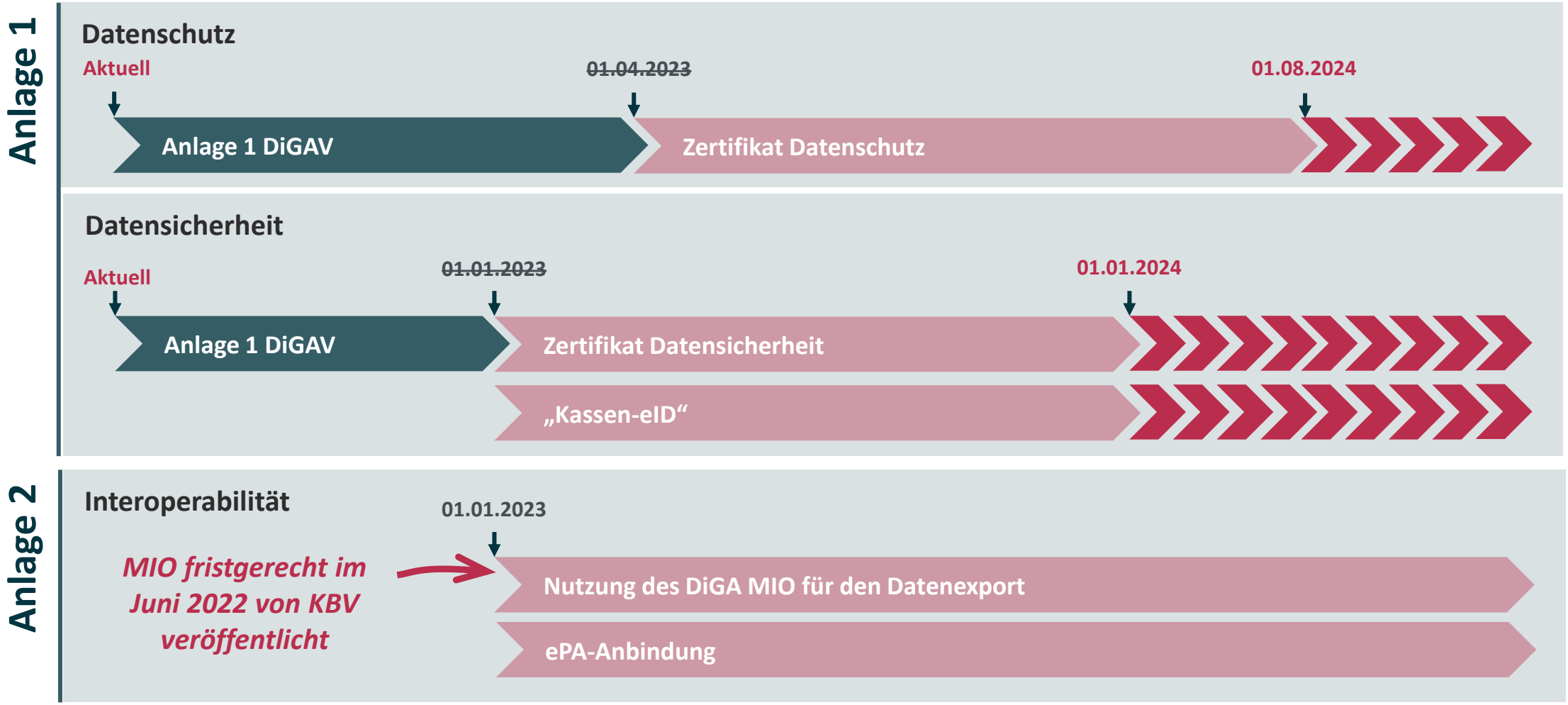
Weitere Anforderungen ab 2023 im Überblick



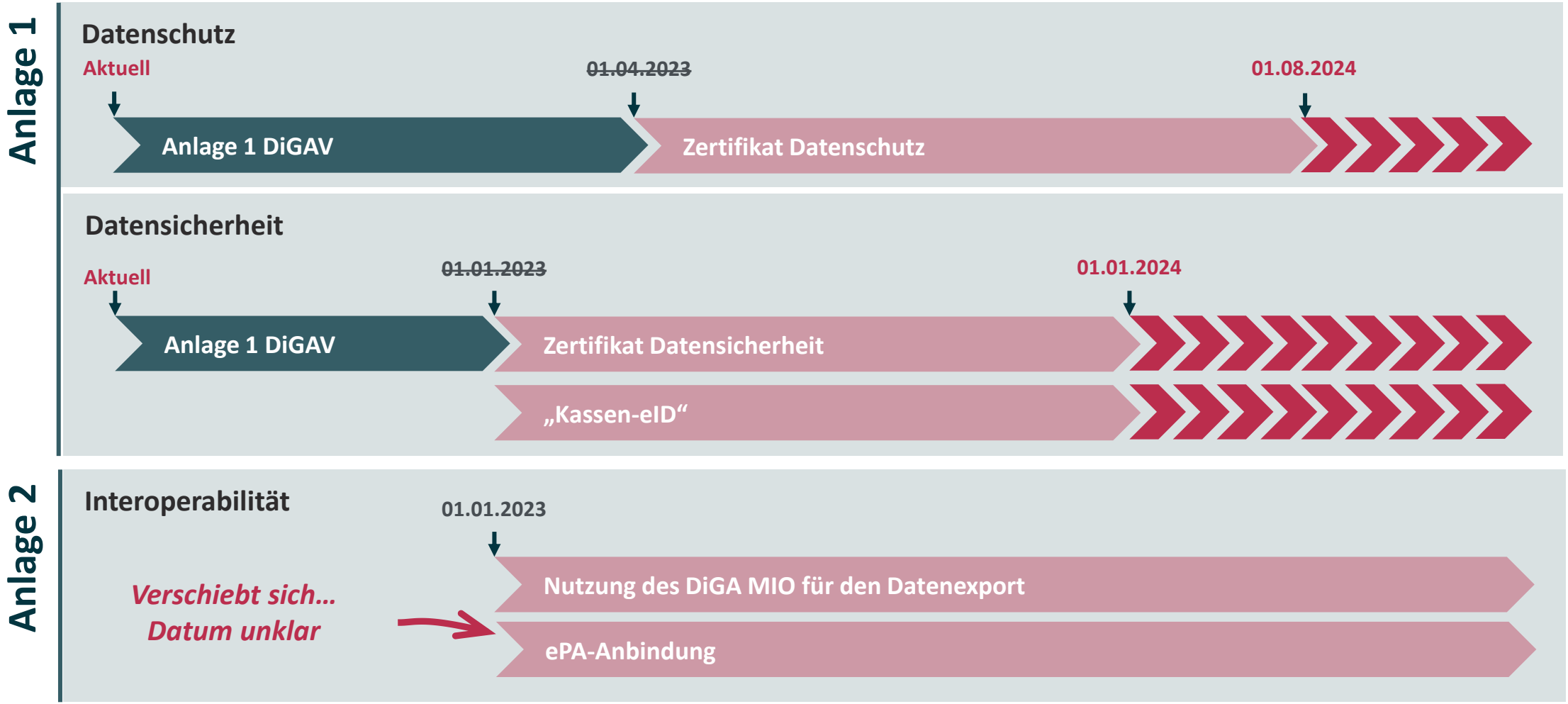
Der Referentenentwurf des KHPflEG verschiebt einige Fristen…



Der Referentenentwurf des KHPflEG verschiebt einige Fristen…



Der Referentenentwurf des KHPflEG verschiebt einige Fristen…



Impuls: Überblick der Anforderungen

Q&A

Anforderungen an den Datenschutz

Zertifikat nach §139e Abs. 11 SGB V

Datenschutz: Faustregel zur Selbsteinschätzung

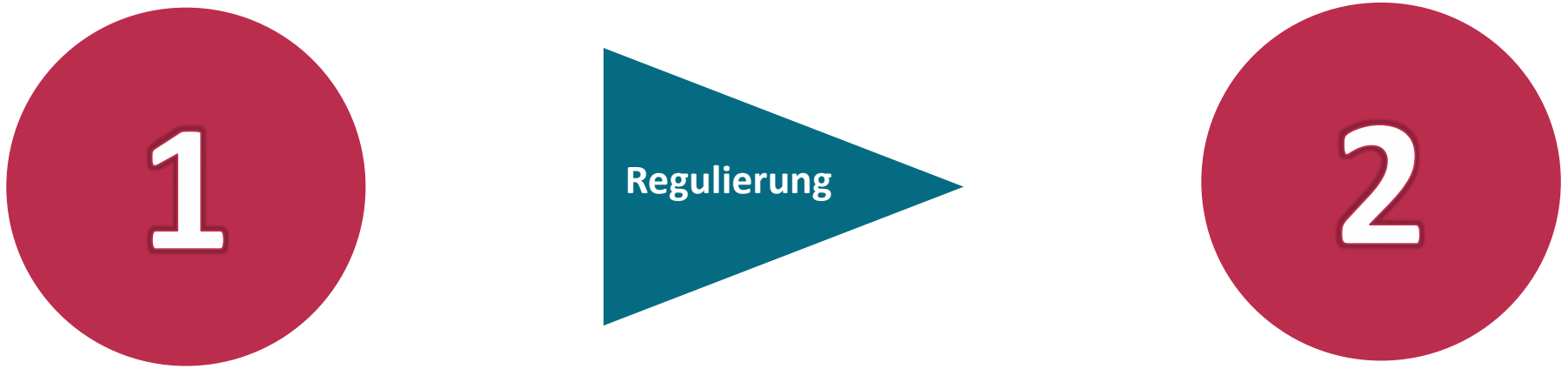
Wenn du denkst, dass du mit deiner App vielleicht ein Datenschutzproblem haben könntest, dann hast du ziemlich sicher ein Datenschutzproblem….

Datenschutzbestimmungen

- Datenschutzgrundverordnung
- Bundesdatenschutzgesetz
- Landesdatenschutzgesetze
- Sozialgesetzbücher
- Spezialgesetze und -verordnungen (z. B. DiGAV)

- DiGAV vor DSGVO
- Je nach Kundengruppe variiert Komplexität der spezifischen Regelungen (wie z.B.: Landeskrankenhausgesetz)

Regulierung des Gesundheitsmarktes



GKV-finanzierte
Leistungen und Produkte

- § 33a SGB V
- § 137f SGB V
- § 140a SGB V
- § 40a SGB XI

…

durch den Patienten selbst bezahlte
Leistungen und Produkte

Regulierung des Gesundheitsmarktes

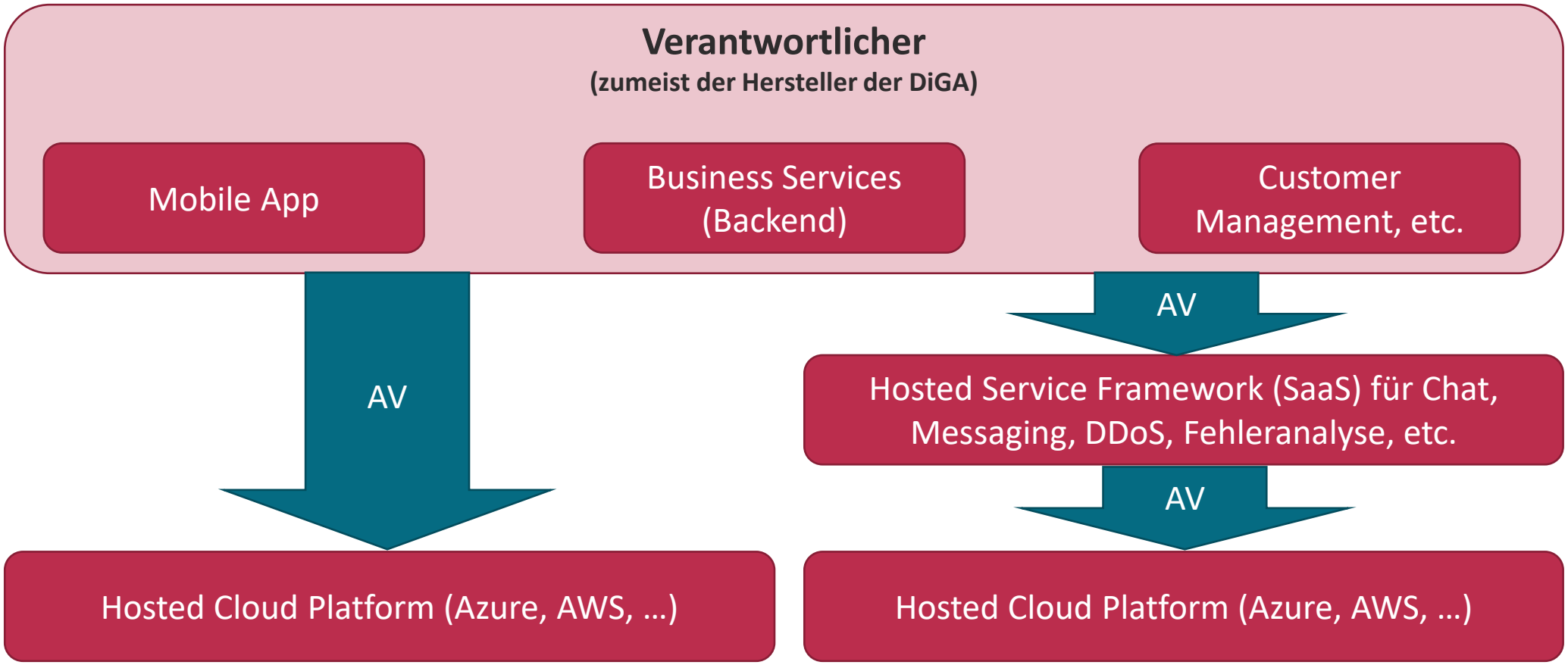
GKV-finanzierte
Leistungen und Produkte

- § 33a SGB V
- § 137f SGB V
- § 140a SGB V
- § 40a SGB XI

…

durch den Patienten selbst bezahlte
Leistungen und Produkte

Auftragsverarbeitung (AV) und AV-Ketten

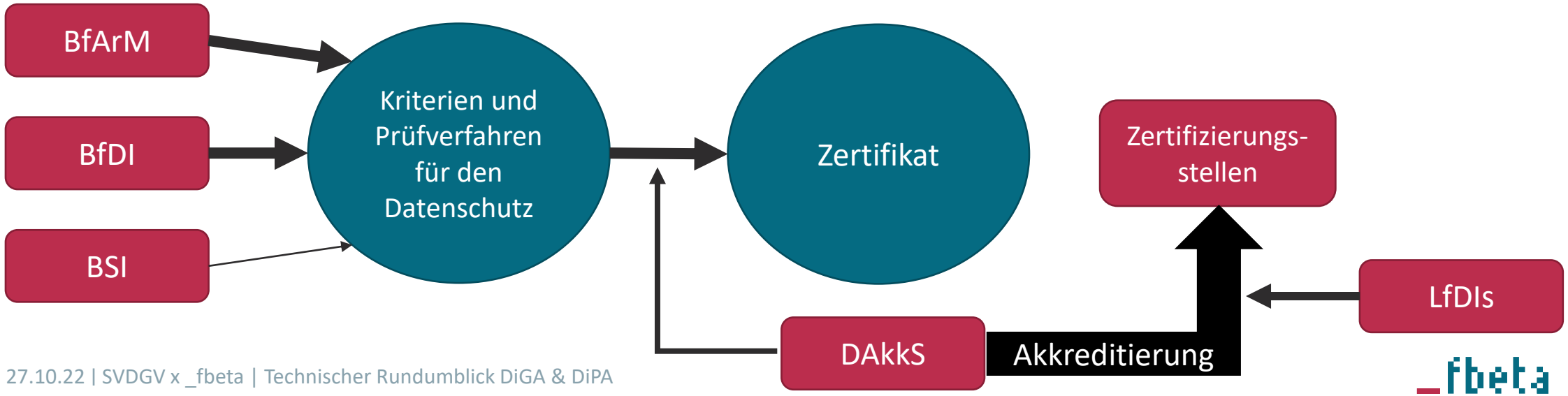


Beispiel: Nutzung von Crisp (SaaS Chatbot)

1. Crisp ist ein europäisches Unternehmen im Rechtsraum der DSGVO. Crisp nutzt DigitalOcean als Hosting Provider. Alle Daten sind in den Niederlanden in einem Rechenzentrum einer europäischen Tochterfirma von DigitalOcean.
   - DigitalOcean ist ein US-Unternehmen. Der AV-Vertrag ist zwischen Crisp und der europäischen Tochter von DigitalOcean geschlossen. Crips muss sicherstellen, dass der AV-Vertragspartner nicht “aufgrund der Rechtsvorschriften des Drittlandes (...) daran gehindert ist, seinen Verpflichtungen nachzukommen“.
   - Aufgrund des US Cloud Act kann die europäische Tochter von DigitalOcean ohne spezifische TOMs ihren Verpflichtungen aus der DSGVO nicht nachkommen. Das Data Processing Agreement (DPA) von DigitalOcean gibt keine Hinweise, dass solche TOMs vorhanden sind.
2. Die Datenschutzerklärung von Crips führt aus, dass Daten ausschließlich in Europa GESPEICHERT werden. Das stimmt. Aber: Crisp und seine AV-Partner VERARBEITEN Daten außerhalb der EU. Insbesondere Vultr und Cloudflare verarbeiten Daten, auch wenn sie diese nicht speichern. Beides sind US-Unternehmen. Relevant ist nicht die Speicherung, sondern die Verarbeitung!
3. Aber: auch der Bundestag nutzt Cloudflare für DDoS-Abwehr und für den Zensus2022 werden ebenfalls Dienste von Cloudflare genutzt.

Datenschutzzertifikat §139e Absatz 11 SGB V

Das Bundesinstitut für Arzneimittel und Medizinprodukte legt im Einvernehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik erstmals bis zum 31. März 2022 und dann in der Regel jährlich die Prüfkriterien für die von digitalen Gesundheitsanwendungen nachzuweisenden Anforderungen an den Datenschutz nach Absatz 2 Satz 2 Nummer 2 fest. Der Nachweis der Erfüllung der Anforderungen an den Datenschutz durch den Hersteller ist ab dem 1. April 2023 durch Vorlage eines anhand der Prüfkriterien nach Satz 1 ausgestellten Zertifikates nach Artikel 42 der Verordnung (EU) 2016/679 zu führen.



Neues Datenschutzzertifikat ab 1.8.2024

Was kann/soll man jetzt schon mal angehen…

- Anforderungen spiegeln DSGVO und DiGAV wider, gehen aber nicht darüber hinaus
- Anforderungen sind sehr prozess- und PDCA-lastig, z. B.
  - Prozesse zur Umfeldbeobachtung
  - PDCA-Zyklus über TOMs
  - Unmittelbare Rückkopplung von App-Änderungen auf den Datenschutz
- Nutzung der DiGA muss grundsätzlich pseudonym erfolgen
- Möglichkeit einer „Grace Periode“ (Zeit bis zur Folgeverordnung)
- Zusätzliche erlaubte Einwilligungen: Grace Periode, Daten für die Forschung
- Dokumentation von Prozessen, Maßnahmen, Entscheidungen, Löschregeln, kryptografischen Verfahren, etc.

Impuls: Zertifikat für Datenschutz

Q&A

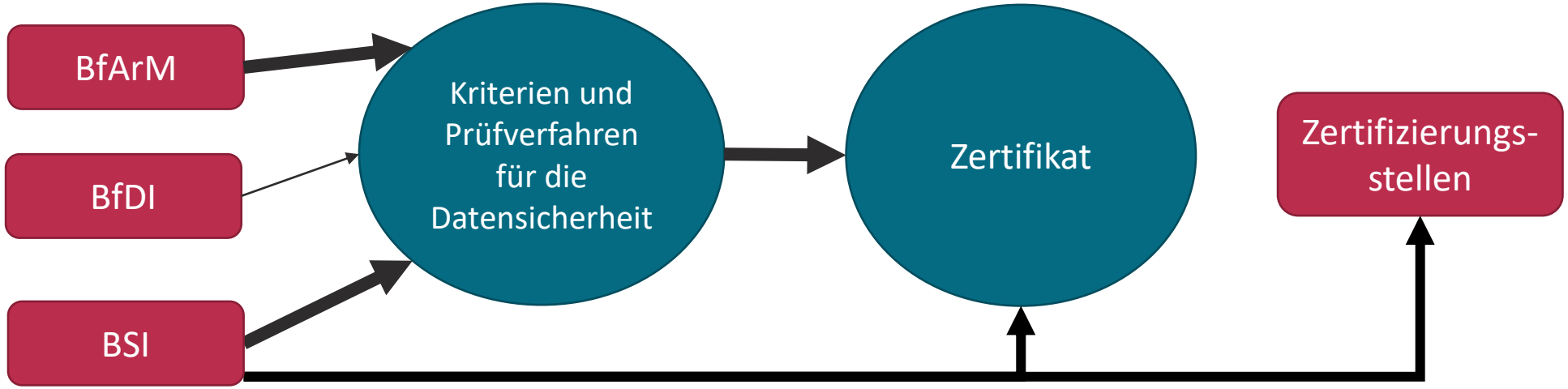
Anforderungen an die Datensicherheit

Zertifikat nach §139e Abs. 10 SGB V

_fbeta

Zertifikat des BSI zur Datensicherheit bei DiGA

Das Bundesamt für Sicherheit in der Informationstechnik legt im Einvernehmen mit dem Bundesinstitut für Arzneimittel und Medizinprodukte und im Benehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erstmals bis zum 31. Dezember 2021 und dann in der Regel jährlich die von digitalen Gesundheitsanwendungen nachzuweisenden Anforderungen an die Datensicherheit nach Absatz 2 Satz 2 Nummer 2 fest. Das Bundesamt für Sicherheit in der Informationstechnik bietet ab dem 1. Juni 2022 Verfahren zur Prüfung der Einhaltung der Anforderungen nach Satz 1 sowie Verfahren zur Bestätigung der Einhaltung der Anforderungen nach Satz 1 durch entsprechende Zertifikate an. Der Nachweis der Erfüllung der Anforderungen an die Datensicherheit durch den Hersteller ist spätestens ab dem 1. Januar 2023 unter Vorlage eines Zertifikates nach Satz 2 zu führen.



BSI TR-03161: Deutlich verschärfte Anforderungen an die Authentisierung

- Grundsätzlich nur noch Zwei-Faktor-Authentisierung
  - Keine Step-Up-Authentisierung oder zweistufige Authentisierung mehr zulässig
  - Biometrie nur noch als Faktor in einer 2FA zulässig; max. 5 ungültige Anmeldeversuche per Biometrie
- Anhang C (und zukünftig TR-03166) wird Nutzbarkeit von Biometrie weiter einschränken; aber: Software als Ergänzung zu biometrischen Sensoren ist jetzt zulässig, um die Vorgaben von Anhang C zu erfüllen
- Neu-Anmeldung nach angemessener Frist (grace period), wenn die App in den Hintergrund gestellt wurde
- Neu-Anmeldung nach angemessener Frist (idle time), wenn die App aktiv ist, aber nicht aktiv genutzt wurde (NEU)
- Neu-Anmeldung nach angemessener Frist (active time), auch wenn die App genutzt wird (NEU)

Impuls: Zertifikat für Datensicherheit

Q&A

Kassen eID

Authentisierung und Umsetzungsempfehlung

Kassen eID

Authentisierung

- Anforderung 15a: Ab 2023 MUSS eine Authentifizierung über die von den gesetzlichen Kassen für ihre Versicherten anzubietenden sektoralen *Identity Provider* unterstützt werden muss. Da die Nutzung einer solchen Identität für die Versicherten freiwillig ist, muss eine DiGA jedoch in jedem Fall zusätzlich auch ein eigenes Authentifizierungsverfahren anbieten.

- Anforderung 11: Jede Authentifizierung MUSS über eine zentrale Komponente – faktisch einen Identity Provider des Herstellers – erfolgen. Hierfür müssen etablierte, erprobte Produkte eingesetzt werden, wie es sie z. B. mit Keycloak, openIAM oder CAS auch als Open Source verfügbar sind.

- Analog zu den aktuellen Entwicklungen bei den großen Plattformanbietern (google, Microsoft, etc.) sollte die betroffene Person zumindest die Möglichkeit haben, eine 2FA zu aktivieren. Eine DiGA sollte daher idealerweise 1FA und 2FA unterstützen.

- DiGA und DiPA erlauben die Möglichkeit einer durchgehend pseudonymen Nutzung. Die betroffene Person identifizierende Kontaktdaten wie z. B. die Handynummer oder die E-Mail-Adresse sollen nur erhoben werden, wenn dieses für den Zweck der Anwendung oder die Umsetzung einer gesetzlichen Verpflichtung erforderlich ist. Und auch in diesen Fällen soll die Nutzung strikt auf diesen Zweck beschränkt bleiben.

Kassen eID

Authentisierung

Es gibt keine Anforderung mehr, eine Authentisierung per eGK zu unterstützen! (Dennoch kann man das natürlich tun…)

- Anforderung 15a: Ab 2023 MUSS eine Authentifizierung über die von den gesetzlichen Kassen für ihre Versicherten anzubietenden sektoralen *Identity Provider* unterstützt werden muss. Da die Nutzung einer solchen Identität für die Versicherten freiwillig ist, muss eine DiGA jedoch in jedem Fall zusätzlich auch ein eigenes Authentifizierungsverfahren anbieten.

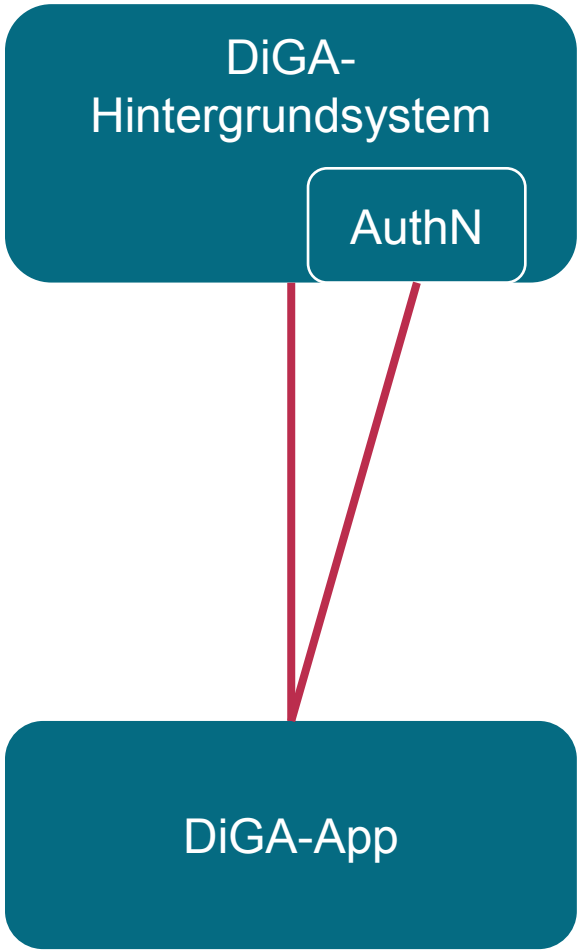
- Anforderung 11: Jede Authentifizierung MUSS über eine zentrale Komponente – faktisch einen Identity Provider des Herstellers – erfolgen. Hierfür müssen etablierte, erprobte Produkte eingesetzt werden, wie es sie z. B. mit Keycloak, openIAM oder CAS auch als Open Source verfügbar sind.

- Analog zu den aktuellen Entwicklungen bei den großen Plattformanbietern (google, Microsoft, etc.) sollte die betroffene Person zumindest die Möglichkeit haben, eine 2FA zu aktivieren. Eine DiGA sollte daher idealerweise 1FA und 2FA unterstützen.

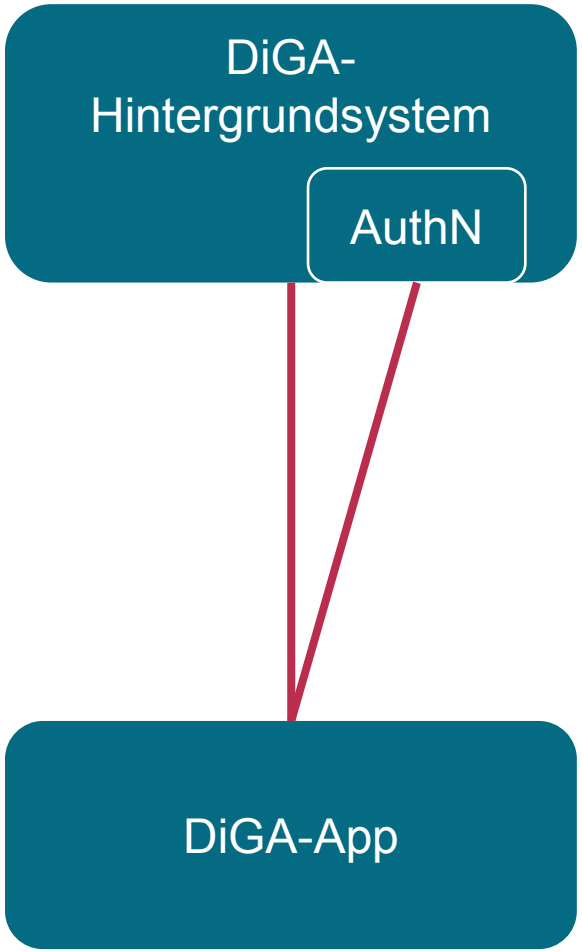
- DiGA erlauben die Möglichkeit einer durchgehend pseudonymen Nutzung. Die betroffene Person identifizierende Kontaktdaten wie z. B. die Handynummer oder die E-Mail-Adresse sollen nur erhoben werden, wenn dieses für den Zweck der Anwendung oder die Umsetzung einer gesetzlichen Verpflichtung erforderlich ist. Und auch in diesen Fällen soll die Nutzung strikt auf diesen Zweck beschränkt bleiben.

Pseudonyme Nutzung in dieser Form wird mit den ab 1.8.24 geltenden Datenschutzanforderungen verpflichtend!

Authentisierung: Umsetzungsempfehlung



Authentisierung: Umsetzungsempfehlung



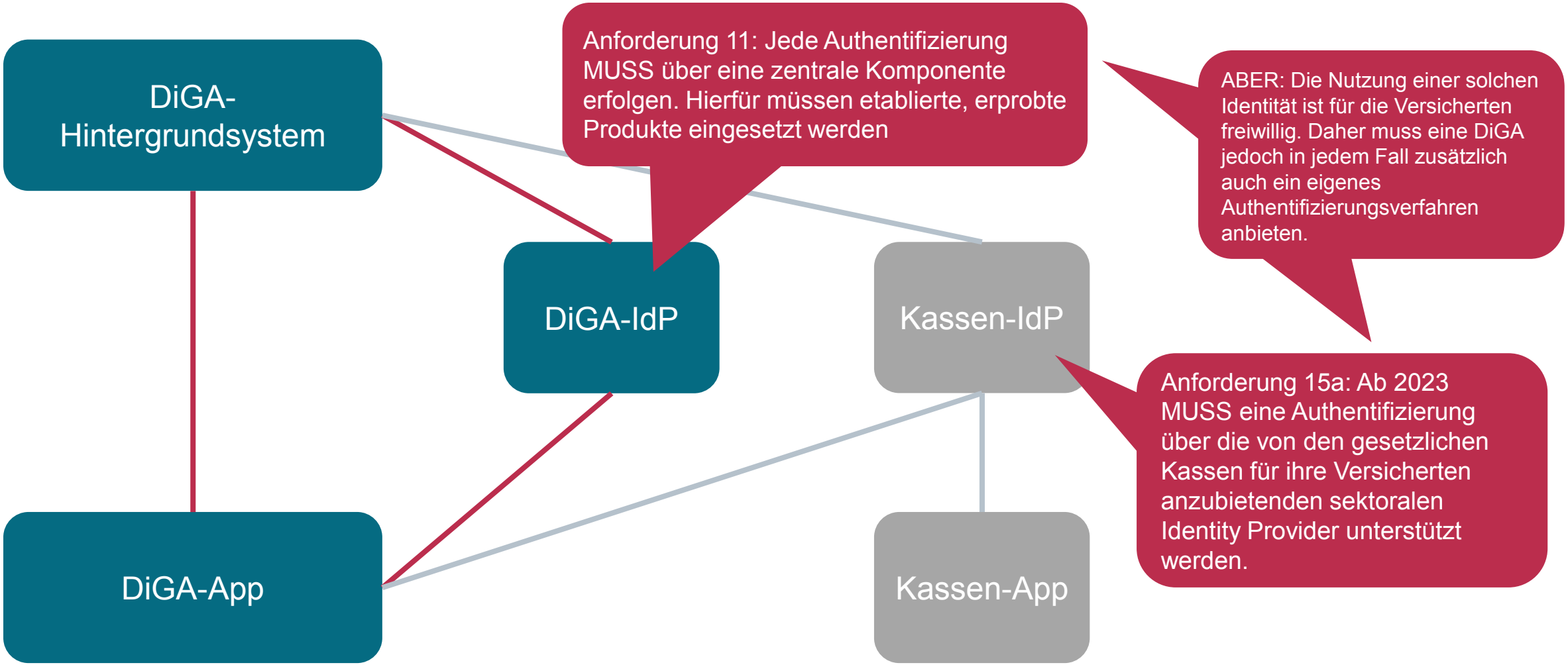
?

Anforderung 11: Jede Authentifizierung MUSS über eine zentrale Komponente erfolgen. Hierfür müssen etablierte, erprobte Produkte eingesetzt werden

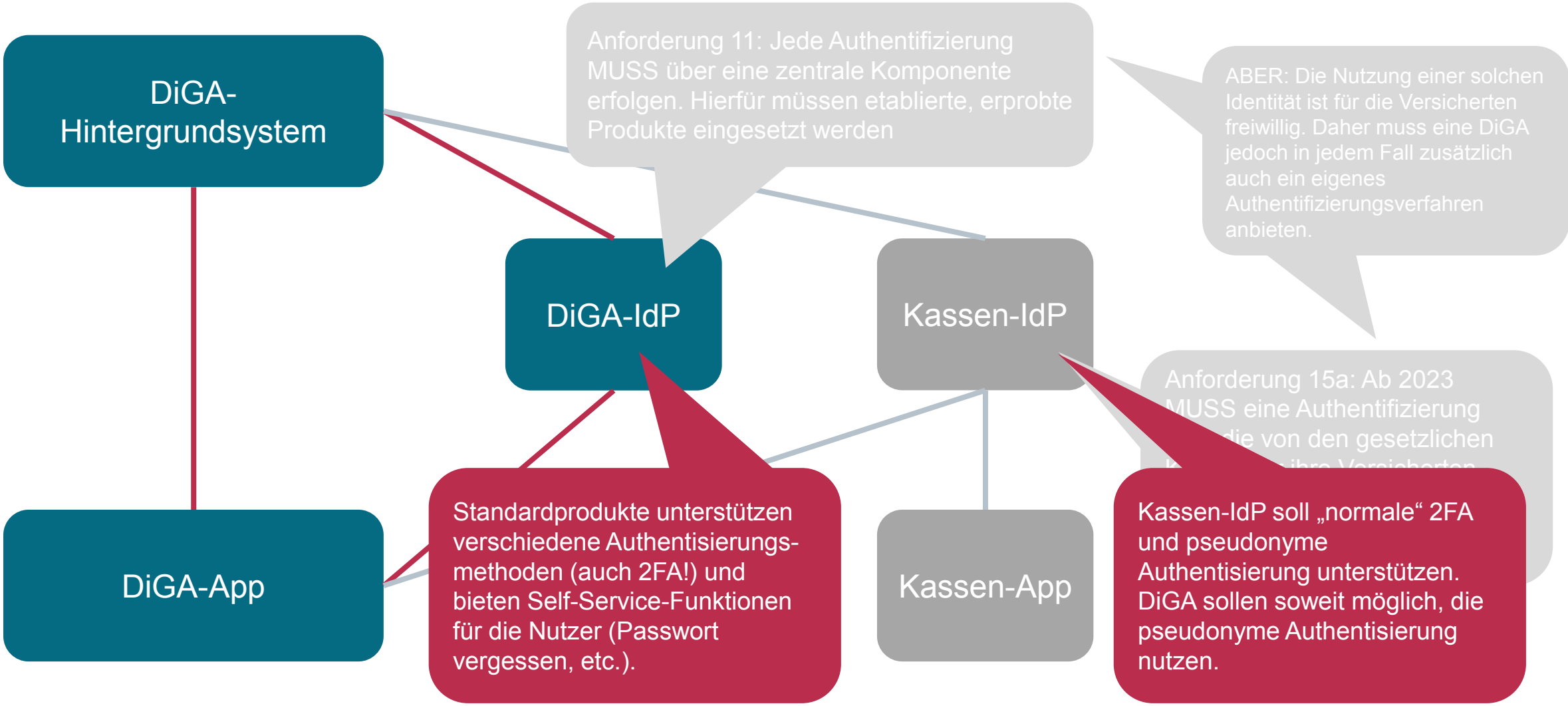
Anforderung 15a: Ab 2023 MUSS eine Authentifizierung über die von den gesetzlichen Kassen für ihre Versicherten anzubietenden sektoralen Identity Provider unterstützt werden.

ABER: Die Nutzung einer solchen Identität ist für die Versicherten freiwillig. Daher muss eine DiGA jedoch in jedem Fall zusätzlich auch ein eigenes Authentifizierungsverfahren anbieten.

Authentisierung: Umsetzungsempfehlung



Authentisierung: Umsetzungsempfehlung



Impuls: Kassen eID

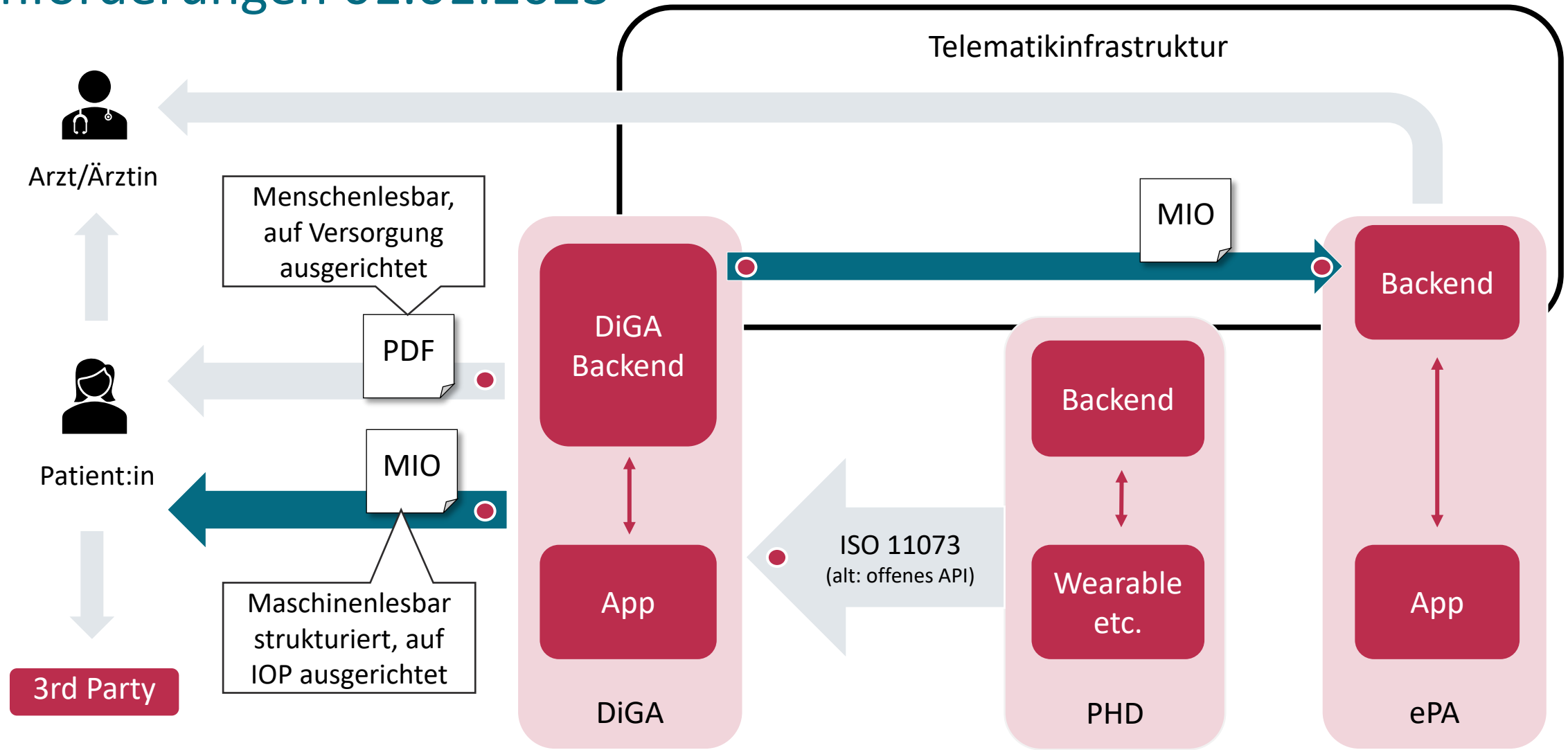
Q&A

Anforderungen an die Interoperabilität

ePA-Anbindung und DiGA MIO

_fbeta

Anforderungen 01.01.2023



Anforderungen an die Interoperabilität

ePA-Anbindung für DiGA

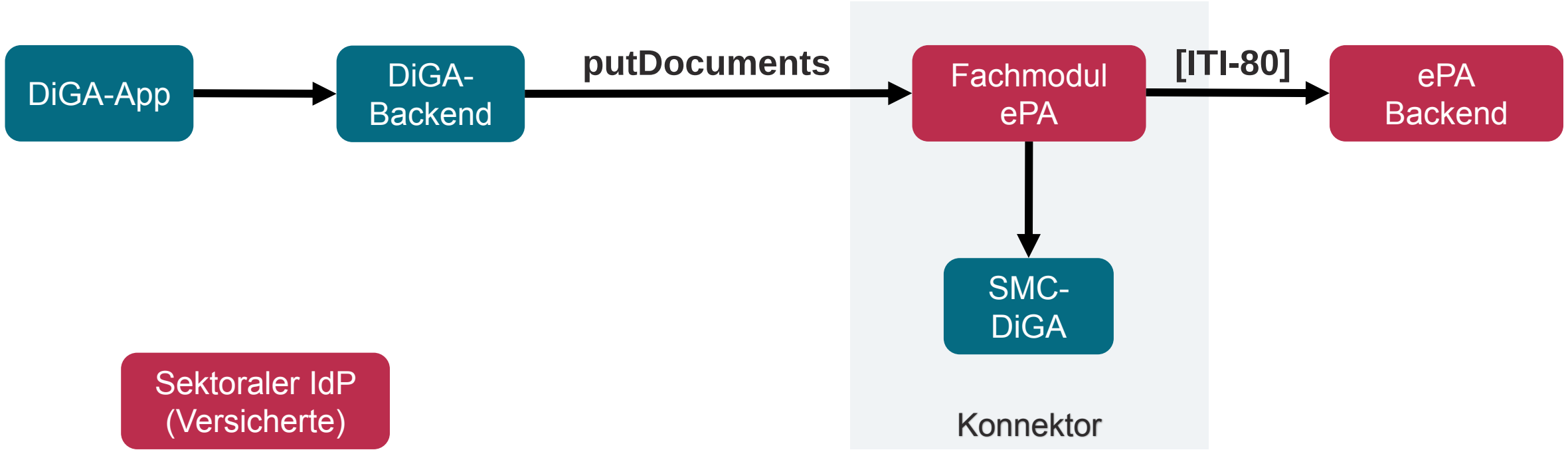
_fbeta

Schnittstelle DiGA / ePA

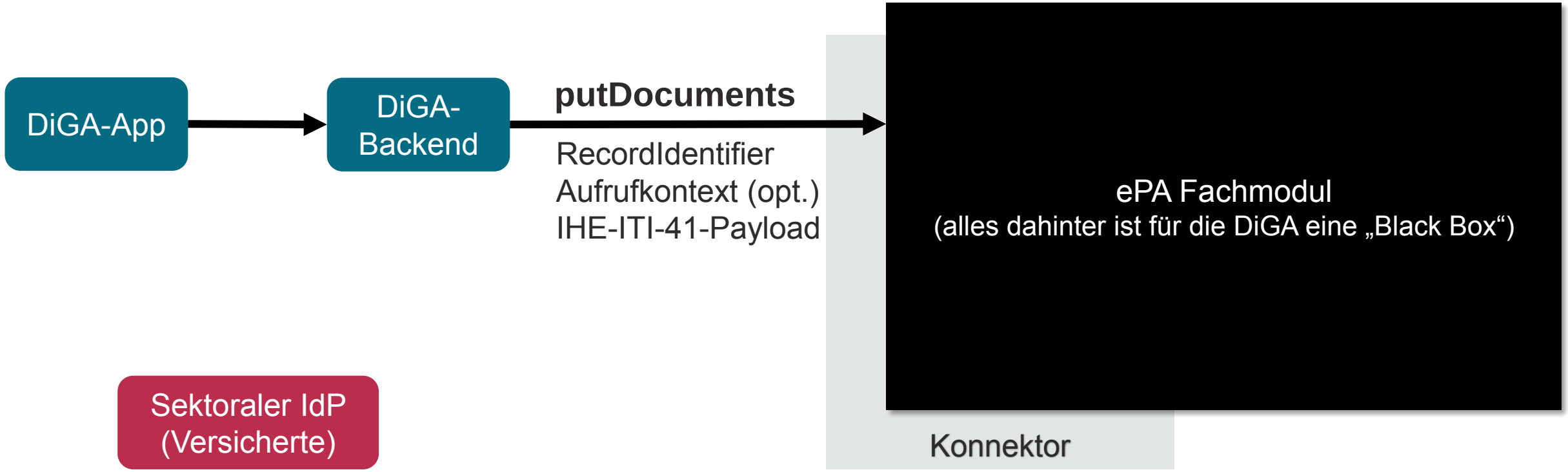
Schnittstelle DiGA/ePA ab ??.??.????:

- DiGA erhält in der ePA Schreibrechte, Attribut „Daten aus digitalen Gesundheitsanwendungen“ (DVPMG > § 341 Abs. 2 Nr. 9 SGB V)
- ePA muss Schnittstelle für DiGA anbieten (DVPMG > § 342 Abs. 2 Nr. 6 / § 351 Abs. 2 SGB V)
- jede gelistete DiGA muss eine ePA-Schnittstelle implementieren (DVPMG > neuer § 6a DiGAV)
- gematik gibt Komponenten zur Authentifizierung aus, BfArM bestätigt die Berechtigung (DVPMG > § 351 Abs. 3 SGB V)
- KBV spezifiziert MIOs für DiGA Datenexport in die ePA (DVPMG > § 355 SGB V)

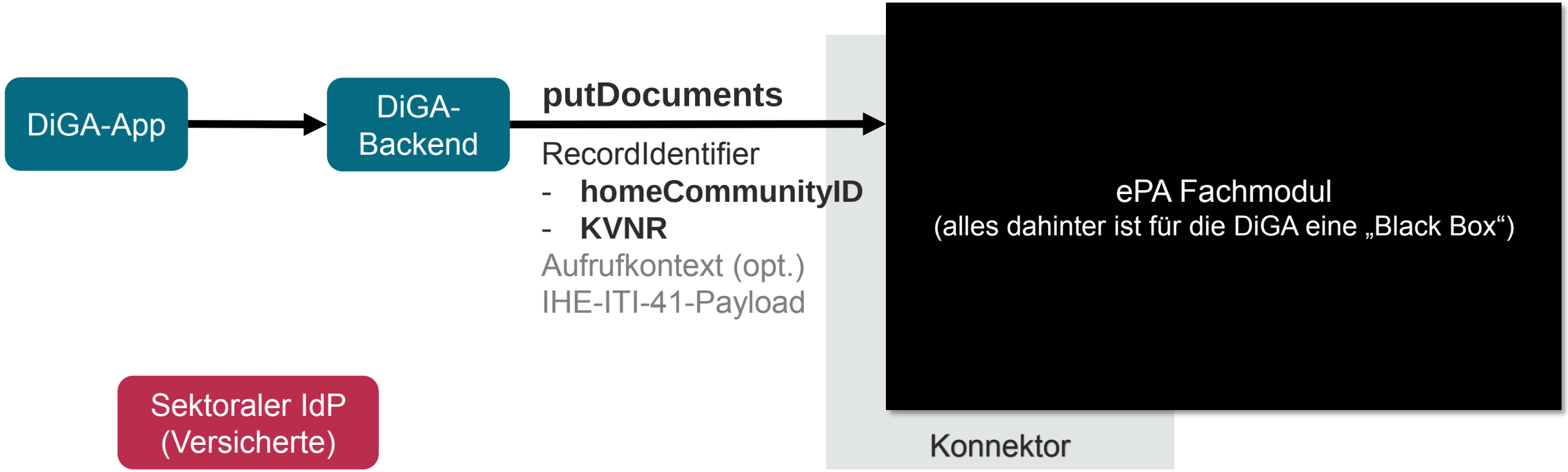
ePA Building Blocks (Schreib-Operation, schematisch)



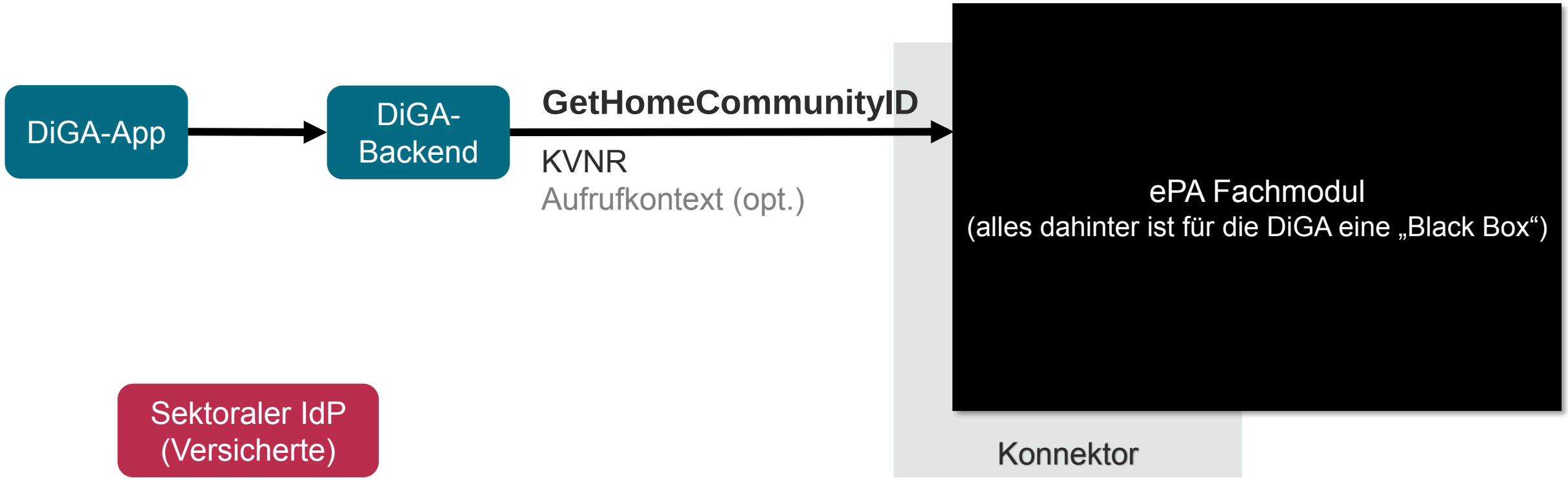
ePA Building Blocks (Schreib-Operation, schematisch)



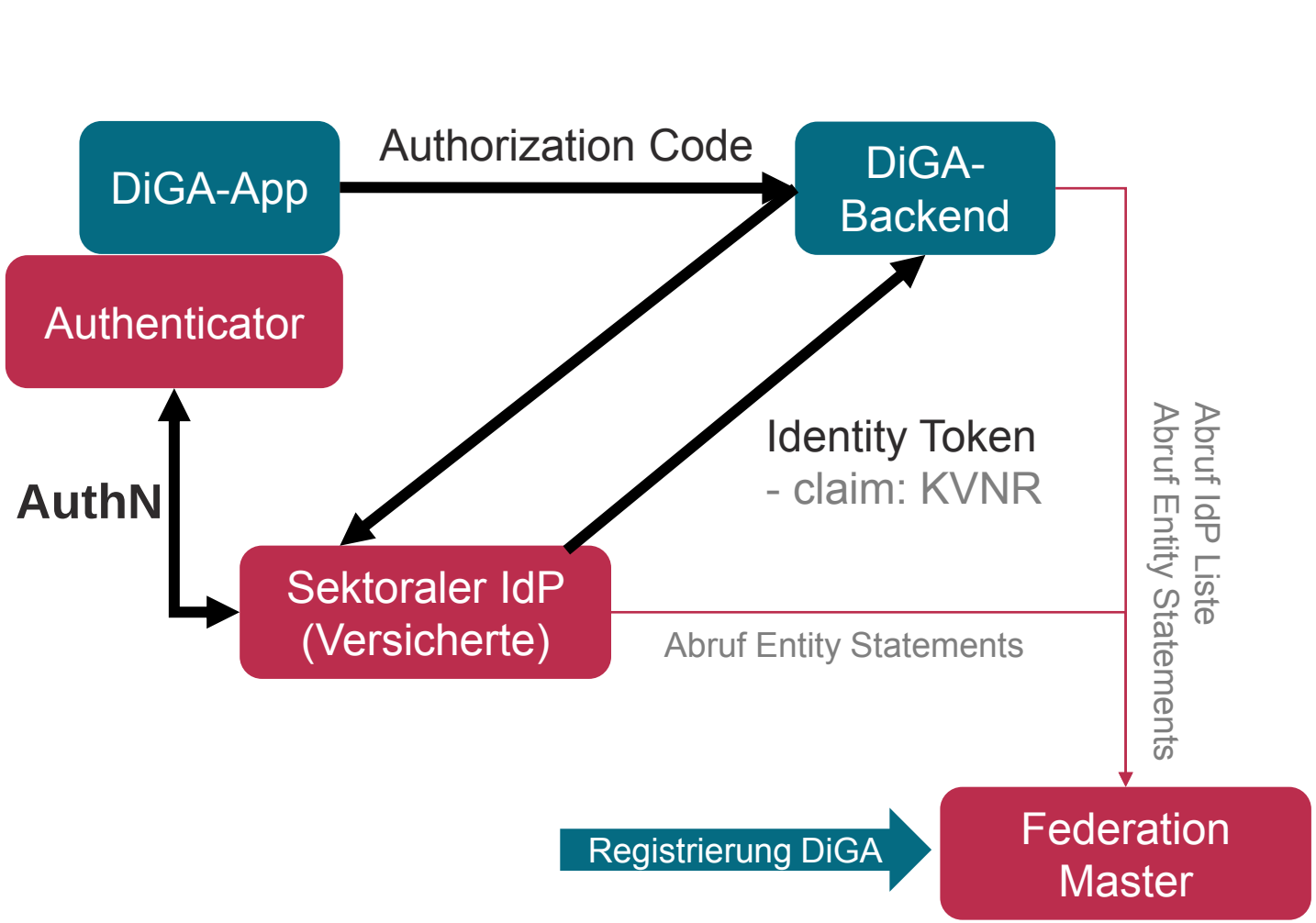
ePA Building Blocks (Schreib-Operation, schematisch)



Ermitteln der homeCommunityID (als Teil des RecordIdentifier)



Ermitteln der KVNR (als Teil des RecordIdentifier)



Impuls: ePA-Anbindung

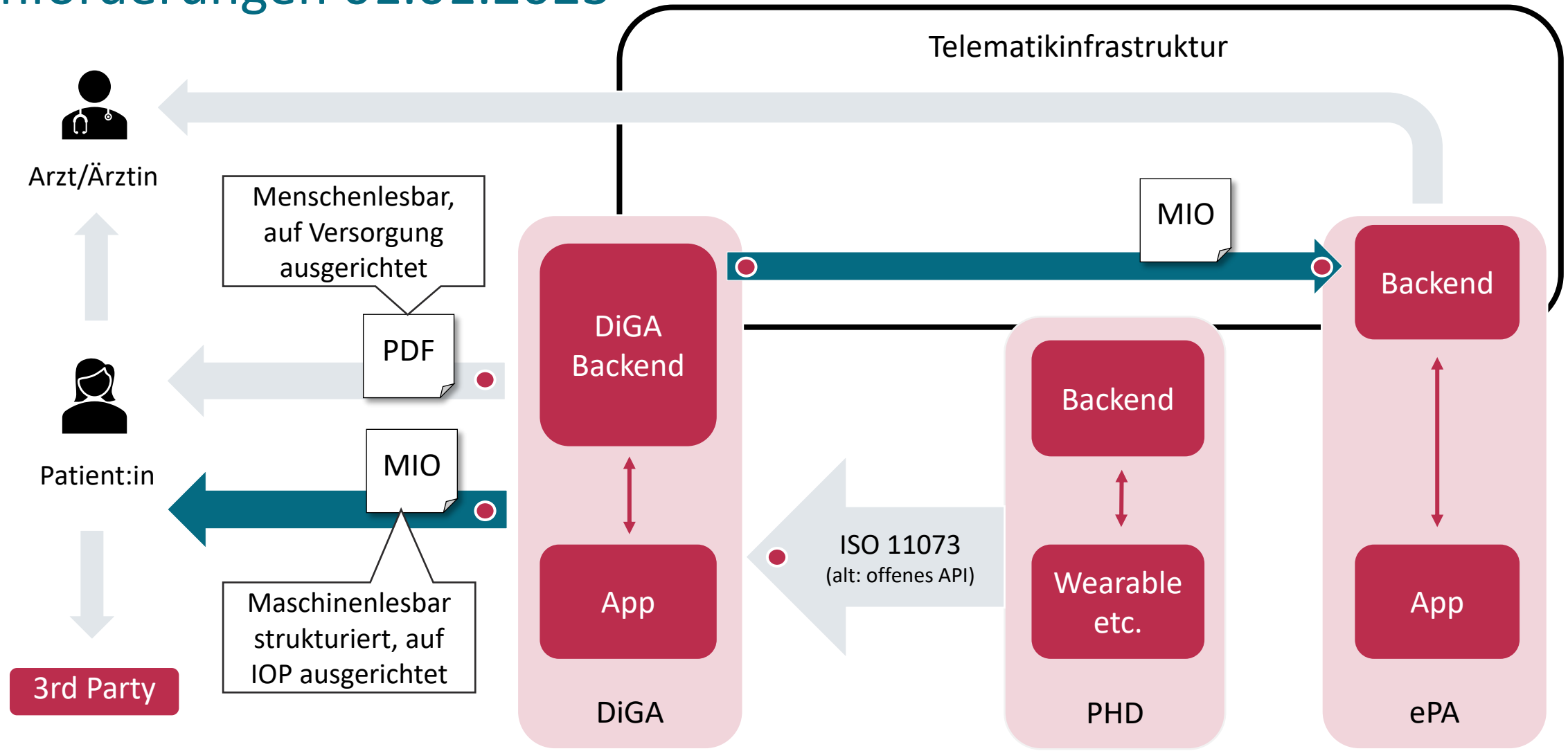
Q&A

Anforderungen an die Interoperabilität

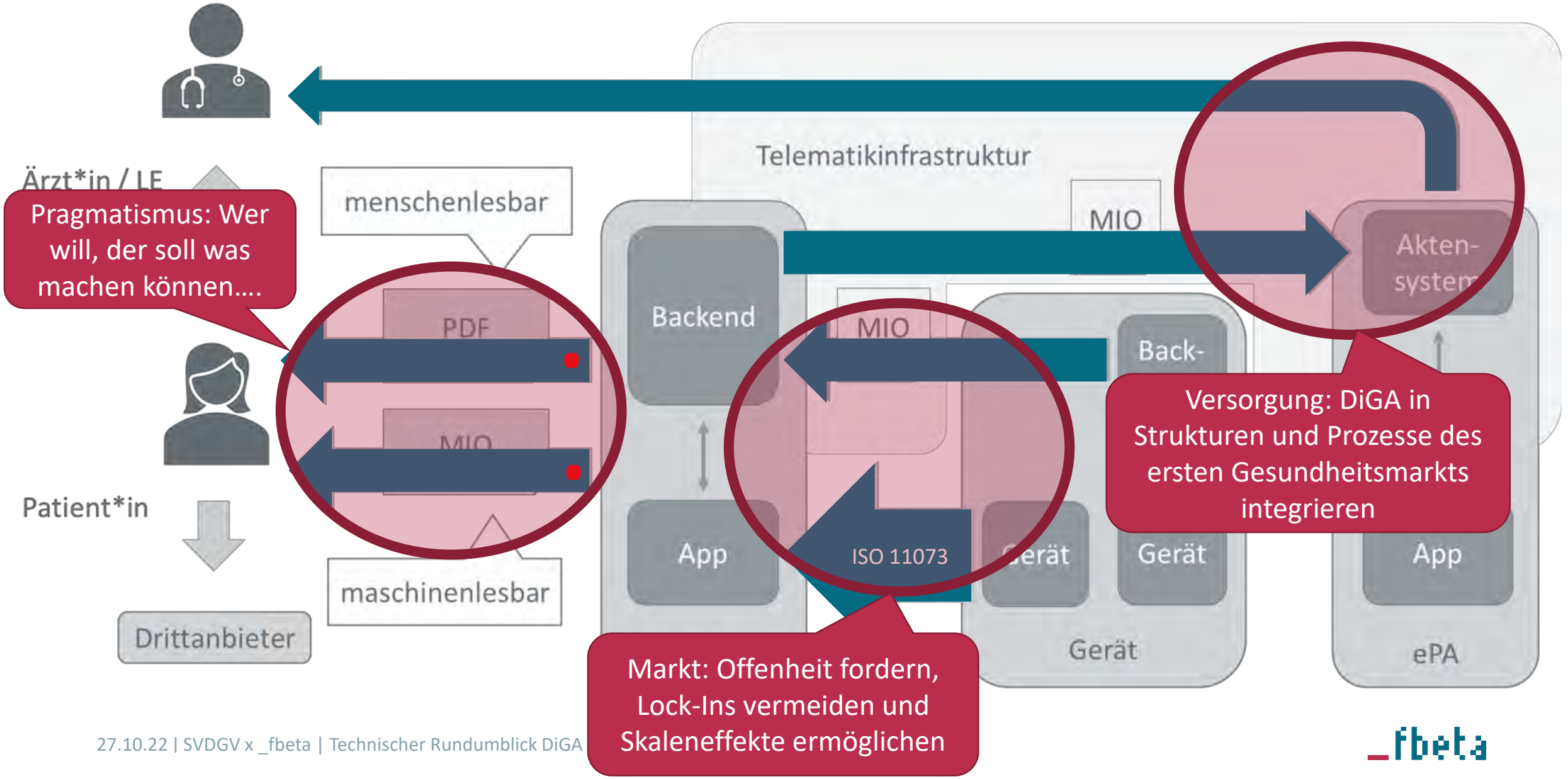
Best Practices für das DiGA MIO

_fbeta

Anforderungen 01.01.2023



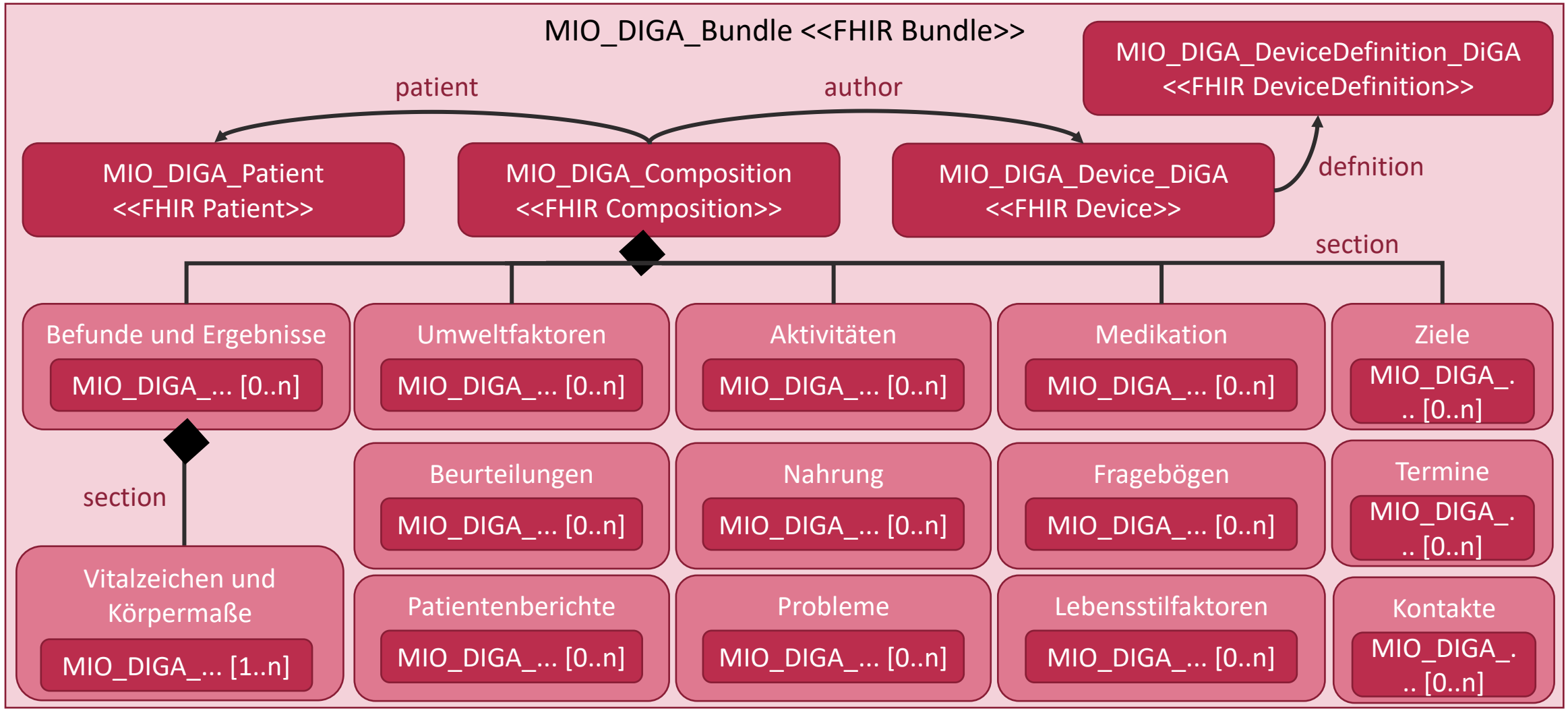
Jede Schnittstelle hat ihre eigene Motivation



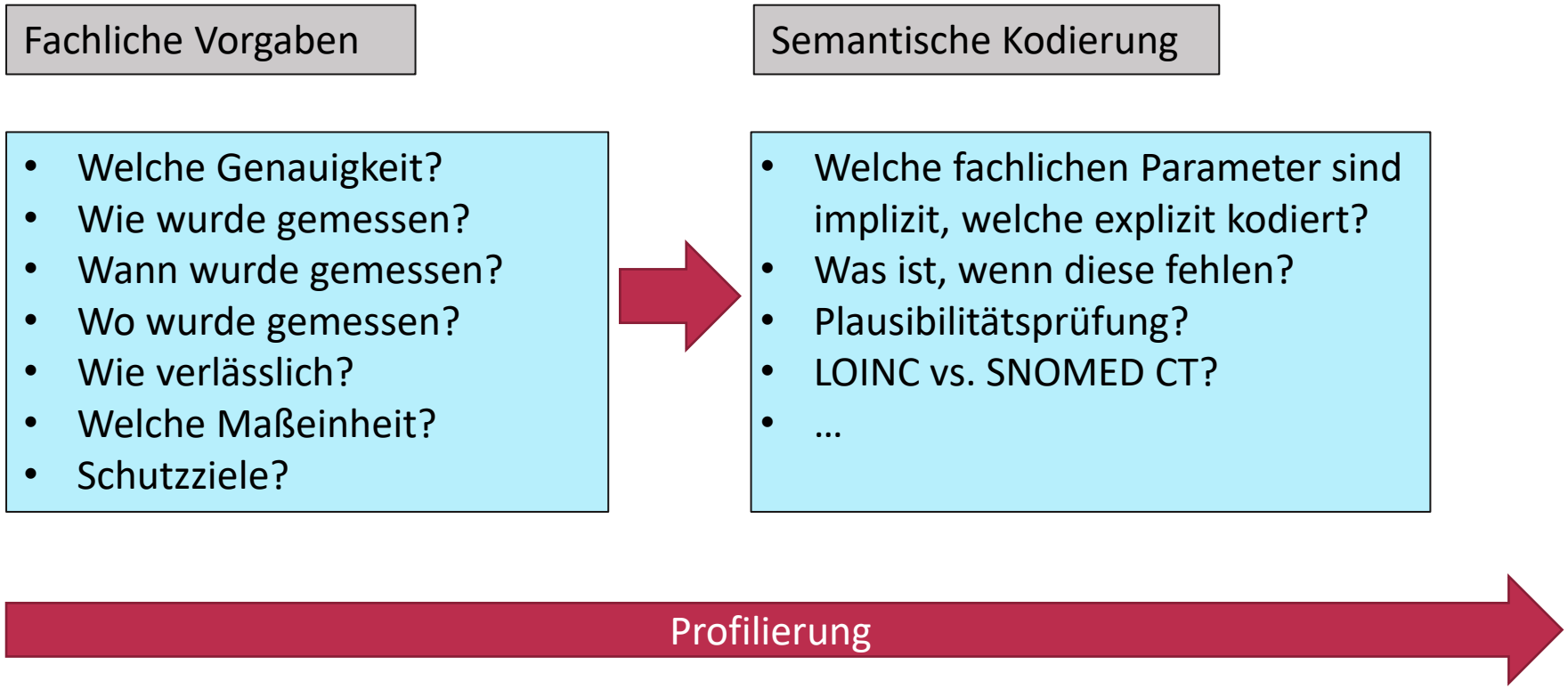
HL7 FHIR (Fast Healthcare Interoperability Resources)

- Fast: FHIR ist **einfach** zu verstehen und zu implementieren
- Healthcare: FHIR basiert auf einem **Domänenmodell** für das Gesundheitswesen
- Interoperability: FHIR ist ein **Austauschformat**, dessen Fokus auf technischer und semantischer und prozessualer Interoperabilität liegt
  - FHIR ist kein Datenbankschema oder Speicherformat
- Resources: FHIR basiert auf den Paradigmen einer **ressourcen-orientierten Architektur**
  - Ressourcen haben eine eindeutige Identität und einen Zustand
  - Standardisierte ReST-Operationen mit Ressource-Typ, Ressource-ID und Parametern in der URL
  - Aber: Über SOA, Microservices etc. kapselbar, um komplexe Operationen umzusetzen

KBV DiGA MIO als Baukasten: Gruppierung der Inhalte



Interoperabilität: Beispiel „Körpertemperatur“



Profilierung für eine Diät-App mit der der Patient täglich sein Gewicht erfasst

Fester Wert: final

Fester Wert: Code vital-signs aus dem System http://hl7.org/fhir/ValueSet/observation-category

Fester Wert: Code 29463-7 aus LOINC

Patient (Verweis auf FHIR *Patient* Ressource)

Zeitpunkt der Gewichtsmessung (Datum und ggf. Uhrzeit)

Patient (Verweis auf FHIR *Patient* Ressource)

Gewicht in Kilogramm (Code kg aus UCUM)

Impuls: Interoperabilität

Q&A

DiGA & DiPA:
Technischer Rundum- und Vorausblick

Dr. Jörg Caumanns
joerg.caumanns@fbeta.de

Cornelius Roll
cornelius.roll@fbeta.de

LinkedIn

_fbeta

Anhang

Links

Links

- DiGAV mit Anlage 1: https://www.gesetze-im-internet.de/digav/BJNR076800020.html
- KBV DiGA MIO Baukasten: https://mio.kbv.de/pages/viewpage.action?pageId=74557103
- DiGA MIO Baukasten (Spezifikation): https://simplifier.net/dtk
- FHIR Deutsche Basisprofile: https://ig.fhir.de/basisprofile-de/stable/
- DiGA Leitfaden: https://www.bfarm.de/SharedDocs/Downloads/DE/Service/Beratungsverfahren/DiGA-Leitfaden.pdf?__blob=publicationFile
- Kriterien zum Datenschutz nach § 139e Abs. 11: https://www.bfarm.de/DE/Medizinprodukte/Aufgaben/DiGA-und-DiPA/Datenschutzkriterien/_node.html