Die Verwaltung von GFP im EPD: Sisyphos ruft Herkules

Swiss eHealth Forum 2020

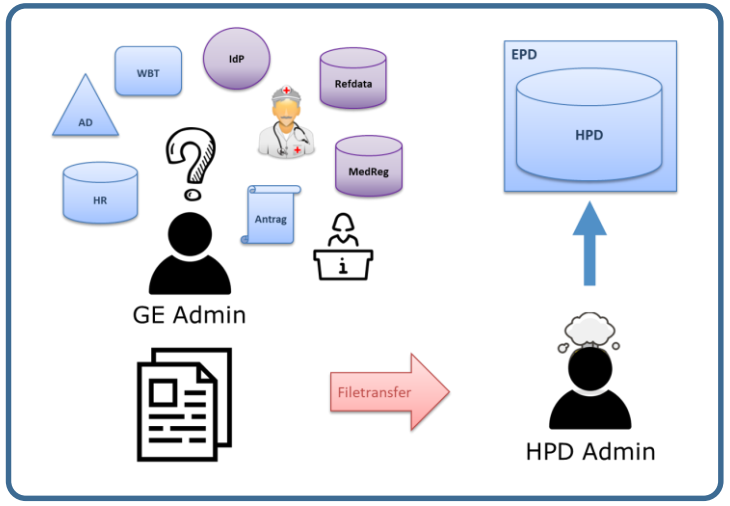
Solution Präsentation Do 14:00 – 14:30

Thomas Kessler, IT-Security Architekt, TEMET AG

05.03.2020

Worum es heute geht

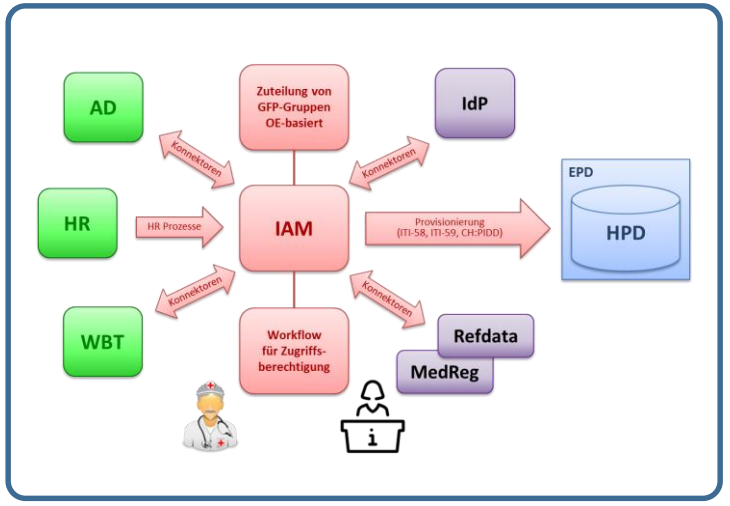
Manuelle GFP-Verwaltung



2020

2023

IAM-integriertes HPD



Glossar vorab

Abkürzung	Bedeutung
EPD	Elektronisches Patientendossier nach EPD-Gesetz
GE	Gesundheitseinrichtung, z.B. ein Spital, ein Heim oder eine Arztpraxis
GFP	Gesundheitsfachperson, z.B. ein Arzt oder ein Apotheker
GLN	Global Location Number, z.B. 7601002486385
HIP	Hilfsperson, z.B. ein Mitarbeiter eines medizinischen Sekretariats
HPD	Health Provider Directory; Verzeichnis aller GE, GFP und GFP-Gruppen im EPD
IAM	Identity and Access Management; Benutzer- und Berechtigungsverwaltung
IdP	Identity Provider; Herausgeber von Identifikationsmitteln
TOZ	Technische und Organisatorische Zertifizierungsvoraussetzungen

Agenda

- Einführung in das Identity and Access Management (IAM)
  - Kernfunktionen des IAM
  - Grundmodell für die Implementierung
  - IAM Evolutionsstufen
- IAM für Gesundheitsfachpersonen im EPD
  - Anforderungen aus dem Ausführungsrecht (insb. TOZ)
  - Minimallösung: Manuelle GFP-Verwaltung
  - Erste Etappe: Delegierte HPD-Administration
  - Zwischenziel: IAM-integriertes HPD
  - Vision: Das «Spital Schweiz»

Über den Referenten

Thomas Kessler

Dipl. Physiker ETH
MAS ZFH in Business Administration

IT-Security Architekt, Partner
In der IT-Security tätig seit 1991

Spezialgebiete
Security Architecture and Strategy
Strong Authentiction
Identity Provider (IdP)

Kontakt
Tel: +41 79 508 25 43
E-Mail: thomas.kessler@temet.ch

Über die TEMET AG

Die TEMET AG positioniert sich im Markt als unabhängige und auf Security fokussierte Firma, deren Berater fachliche Expertise mit Management und Projektkompetenz verbinden.

IAM Referenzprojekte (seit 1993)

- 2018, Bank: Zielarchitektur IAM Federation Services
- 2018, Spital: Ist-Aufnahme «Organisations- und Berechtigungs-Mgmt.»
- 2017, eCH: Co-Autor eCH-0107 (Gestaltungsprinzipien für das IAM)
- 2015, Telekommunikation: Federführung „IAM Vision und Strategie“
- 2013, Bank: Projektleiter „IAM – Way Forward“ Strategieprojekt
- 2008-2011, Versicherer: Architekt und Projektleiter „BrokerGate IdP“
- 2005, Bank: Vorstudie & Evaluation einer IAM Infrastruktur
- 1997, Bank: Teilprojektleiter 2FA-Lösung für erstes E-Banking
- 1993-1995, Bank: PL Bank-interne Einführung von SecurID-Token

EPD Referenzprojekte (seit 2015)

- Seit 2018 unterstützt die Temet vier grosse Häuser in allen DSDS-Aspekten der EPD-Anbindung (inkl. IAM-Integration)
- 2019/2020, Stammgemeinschaft: Projektleiter für die Zertifizierung
- 2019, eHS: Umsetzungshilfe „Funktionsabnahmen“
- *2019, Spital: Grobkonzept für die 2-Faktor Authentifizierung von GFP
- *2018, myEPD: DSDS-Verantwortlicher für den myEPD Pilotbetrieb
- *2017, USB: Sicherheitsreview myEPD-Anbindungskonzept
- *2016, eHealth NWCH: AKV für die Informationssicherheit im EPD
- *2015, BAG: Bedrohungs- und Risikoanalyse für das EPD

*: Öffentlich vorgestellte Projekte anlässlich der eHealth Foren 2016/2017/2018/2019/2020

Identity and Access Management (IAM)

Einführung in das IAM (1/4)

Die Hauptaufgaben des IAM sind:

- Die Verwaltung der Benutzer mit ihren Berechtigungen
- Die Authentifizierung und Zugriffskontrolle zur Laufzeit

Das IAM ist eine tragende Säule der Informationssicherheit und muss *Effizienz*, *Sicherheit* und *Benutzerfreundlichkeit* unter einen Hut bringen.

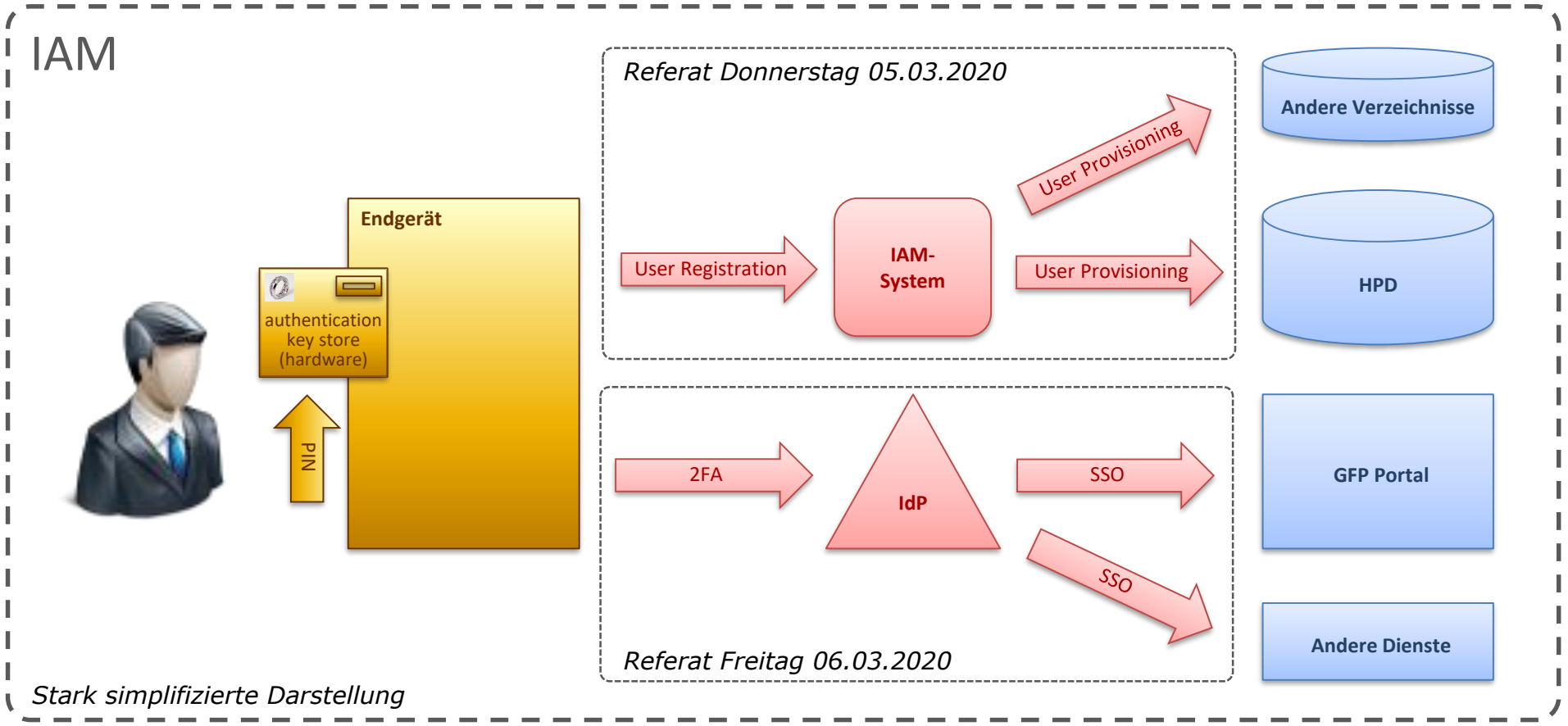
Das IAM muss die Entwicklung der IT-Landschaft unterstützen; aktuell insb. firmenübergreifende Geschäftsprozesse und Cloud-Services.

⇨ Das *EPD als Vorbild* für die sichere Nutzung externer Dienste (*!?!*)

Zwei Themen – zwei Referate

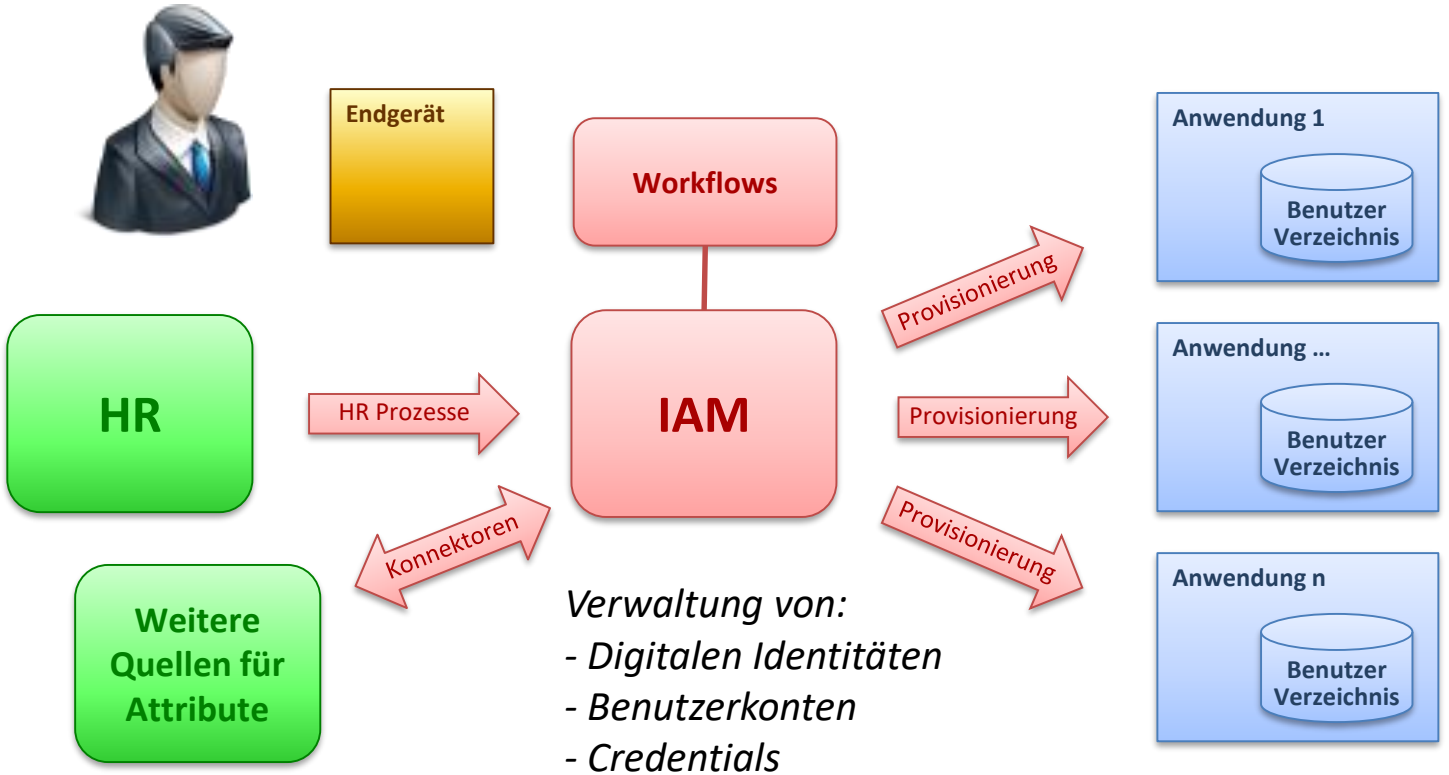
Einführung in das IAM (2/4)

Die *IAM-Infrastruktur* ermöglicht sichere und effiziente Prozesse:



Grundmodell der IAM Implementierung

Einführung in das IAM (3/4)



Verwaltung von:
- Digitalen Identitäten
- Benutzerkonten
- Credentials
- Berechtigungen

Bezug von:
- Organisationseinheit(en)
- Funktion(en)
- Adressen, Geräte-ID usw.

IAM-Infrastruktur:

- Drehscheibe für Benutzerattribute
- Anbindung von Quellen (Master pro Attribut)
- Konnektoren zu Zielsystemen (ggf. bi-direktional)
- Automatisierung verbessert Effizienz und Datenqualität

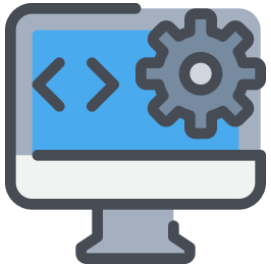
IAM-Evolutionsstufen

Einführung in das IAM (4/4)

Formularversand

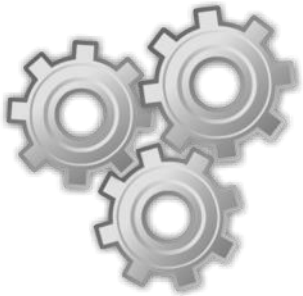
Steinzeit der IT (90er Jahre)

Delegierte Administration



Internet-Zeitalter (00er Jahre)

Systemintegration



Automatisierung (2010er Jahre)

Anforderungen des Gesetzgebers

IAM für Gesundheitsfachpersonen im EPD (1/6)

Die *TOZ* regeln die Verwaltung von Gesundheitsfachpersonen (GFP) und Hilfspersonen (HIP) sowie GFP-Gruppen in diversen Kapiteln, insb.:

1.3 Verwaltung von Gesundheitsfachpersonen (Art. 9 Abs. 2 Bst. a bis f EPDV)

1.3.1 Die Gemeinschaften legen die Prozesse für den Eintritt, die Verwaltung und den Austritt von Gesundheitsfachpersonen fest.

1.3.2 Sie stellen sicher, dass die Daten des Dienstes zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 41 EPDV aktualisiert werden.

1.5 Verwaltung von Gruppen von Gesundheitsfachpersonen (Art. 9 Abs. 2 Bst. a, c, d und f EPDV)

1.5.1 Gemeinschaften sind für die Verwaltung der Gruppen von Gesundheitsfachpersonen verantwortlich. Sie legen den Prozess zu deren Verwaltung fest.

Relevante Attribute

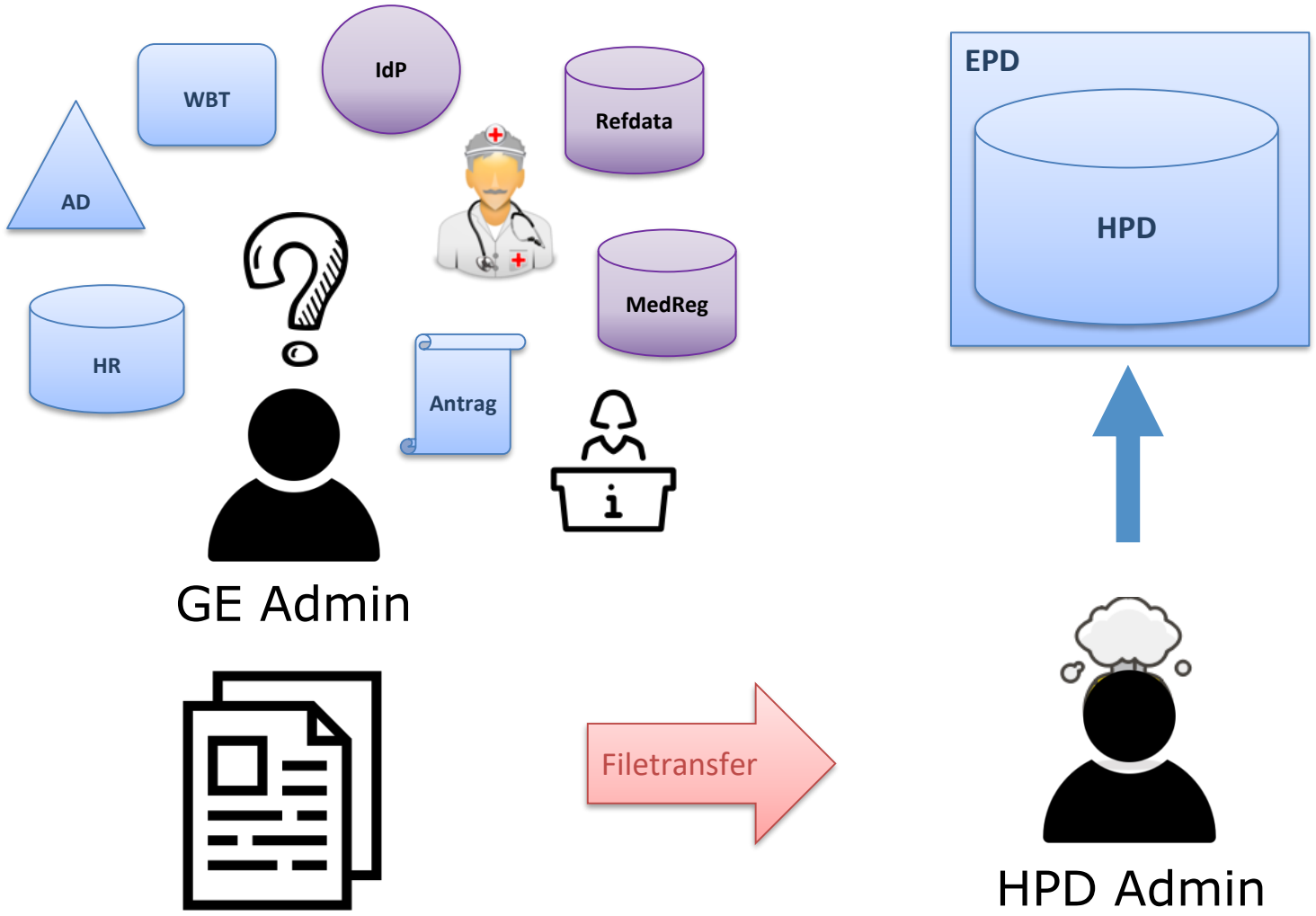
IAM für Gesundheitsfachpersonen im EPD (2/6)

ID	Attribute	Beschreibung	Quelle	Ref. TOZ
1	Attribute der zivilen Identität	Name, Vornamen, Geschlecht	Amtlicher Ausweis (via IdP)*	1.3.3.b
2	GLN	Eindeutiger Identifikator einer GFP oder HIP (Basis für die Berechtigungsvergabe)	Refdata	1.4.2
3	IdP-ID	Eindeutiger Identifikator eines EPD-Benutzers (Basis für den Login)	IdP für GFP und HIP	1.4.2
4	Beruf und Spezialisierung	Metadaten gemäss Anhang 9 der EPDV-EDI	Berufsregister (z.B. MedReg)	1.3.3.e
5	Schulungsnachweis	Basis für Erteilung EPD-Zugriffsberechtigung	Schulungssoftware (WBT)	1.3.3.a, 4.7.1.b
6	GFP-Verpflichtung	Basis für Erteilung EPD-Zugriffsberechtigung	Schulungssoftware (WBT)	1.3.3.a, 4.7.1.b
7	EPD-Zugriffsberechtigung	Basis für Eintrag im HPD	GE Admin? Vorgesetzter?	1.3.3.c
8	GFP-Gruppenzugehörigkeiten	Basis für effiziente Berechtigungsvergabe	GE Admin? Vorgesetzter?	1.5.1
9	Nur HIP: Verantwortliche GFP	Basis für Eintrag im HPD	GE Admin? Vorgesetzter? GFP?	1.6.1
10	Adressen	E-Mail Adresse, Telefonnummer, …	GE-interne Systeme (z.B. AD)	-
11	Organisationsdaten	OE-Zugehörigkeit(en), Funktion(en), …	GE-interne Systeme (z.B. HR)	-

*: Konsistenz Name/Vornamen zwischen IdP, Refdata, Berufsregister und GE HR ist heute nicht sichergestellt.

(1) Manuelle GFP-Verwaltung

IAM für Gesundheitsfachpersonen im EPD (3/6)

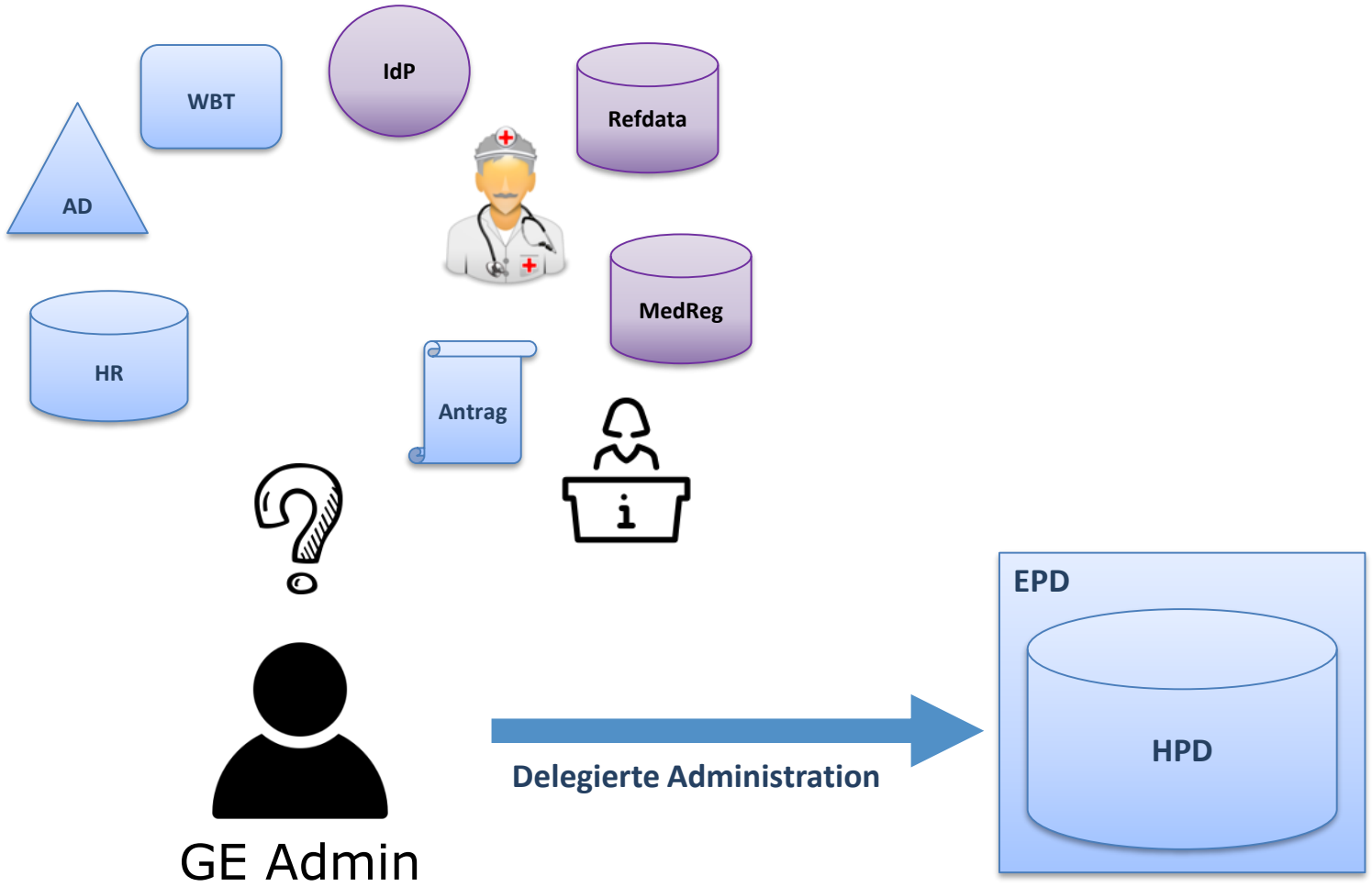


Fragezeichen und Zeitverlust

- Sammeln aller nötigen Attribute
- Nachführen bei allen Ein- Aus- und Übertritten
- HPD-Mutation via HPD-Admin bei der Gemeinschaft

(2) Delegierte HPD-Administration

IAM für Gesundheitsfachpersonen im EPD (4/6)

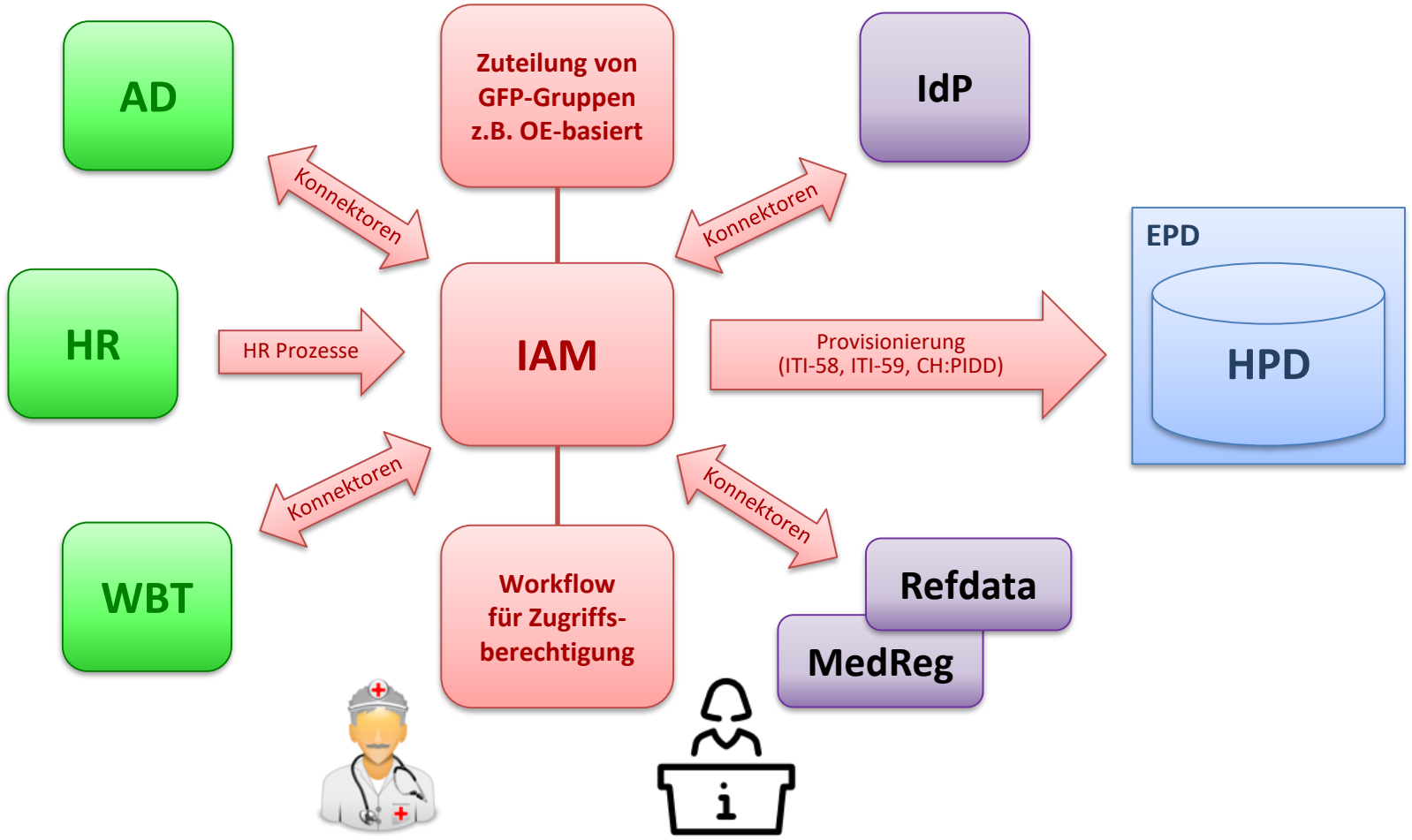


Fragezeichen bleiben

- Sammeln aller nötigen Attribute
- Nachführen bei allen Ein- Aus- und Übertritten
- HPD-Mutation via Self-Service GUI

(3) IAM-integriertes HPD

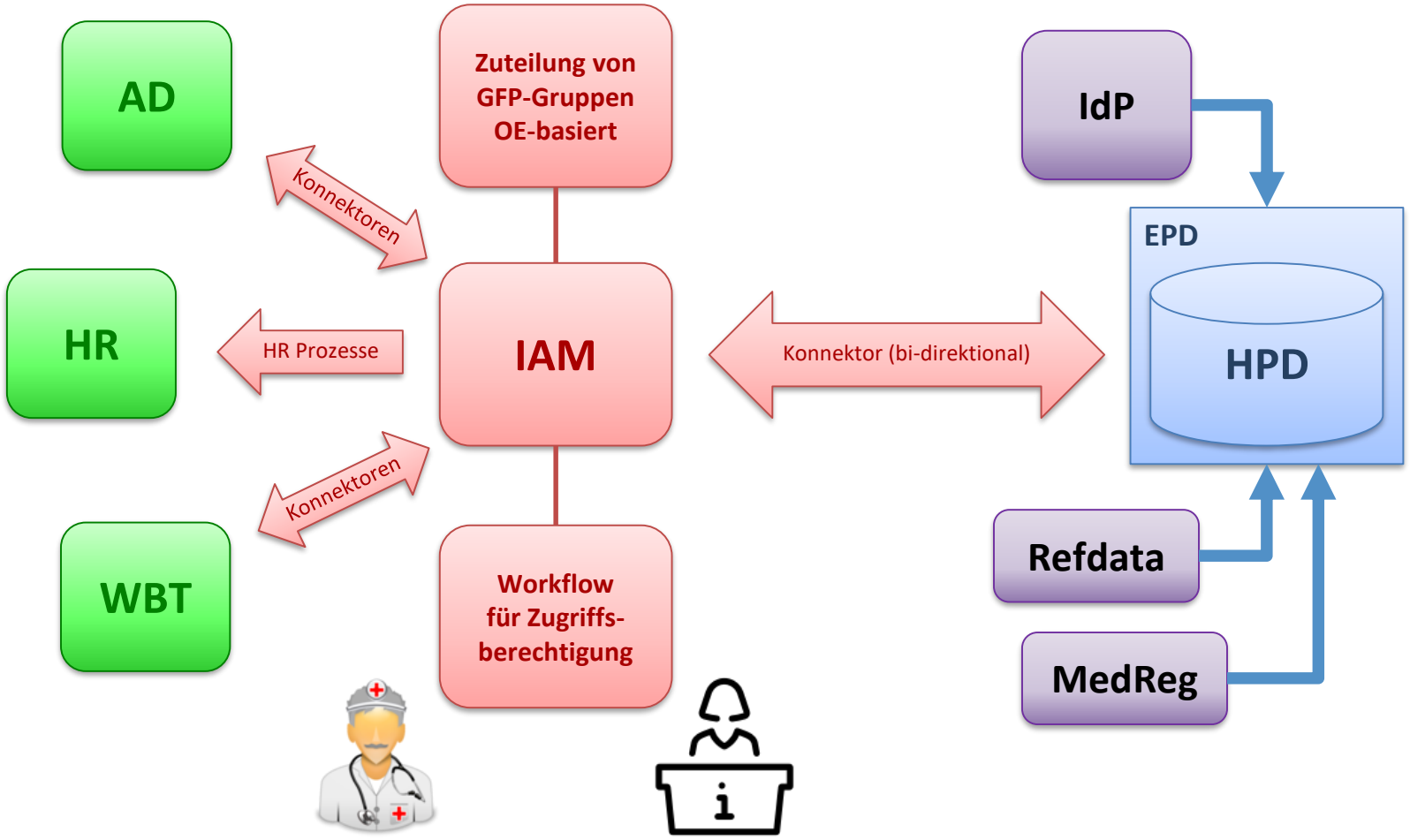
IAM für Gesundheitsfachpersonen im EPD (5/6)



- IAM-Integration des HPD
- Automatisierte Verwaltung der Attribute
- z.B. OE-basierte Zuteilung von GFP-Gruppen
- Workflow für manuelle Entscheidungen

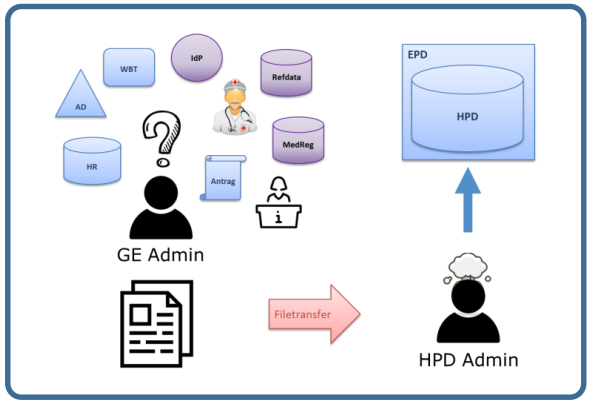
(4) «Spital Schweiz» als Vision

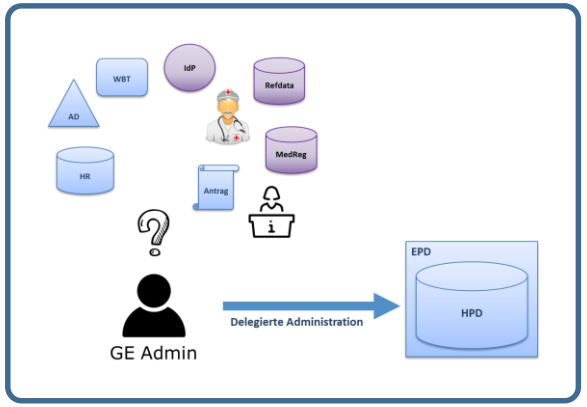
IAM für Gesundheitsfachpersonen im EPD (6/6)

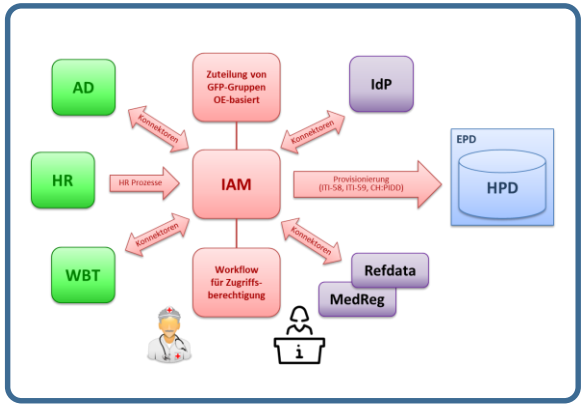


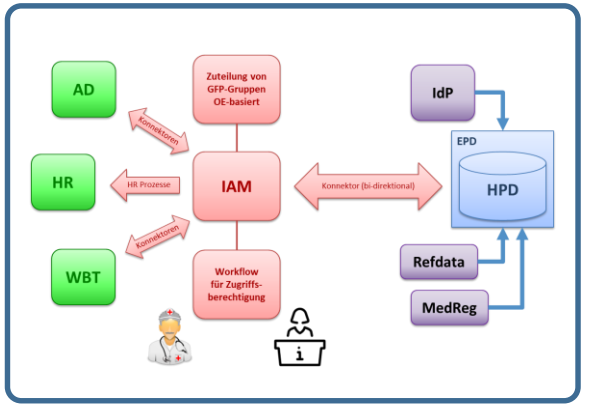
- Das nationale HPD wird zur Quelle für das GE-interne HR

IAM-Evolutionsstufen im EPD





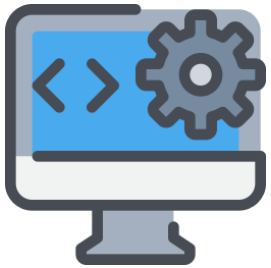




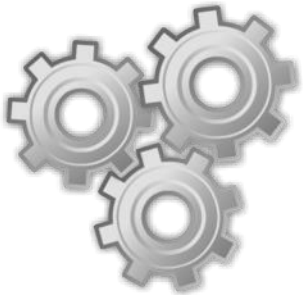
2020 **2021** **2023** **2030**

Steinzeit der IT **Internet-Zeitalter** **Automatisierung** ***t***

Formularversand



Delegierte Administration



Systemintegration

Fazit / Schlusswort

- Das EPD stellt hohe Anforderungen an die Gesundheitseinrichtungen in Bezug auf die Verwaltung von GFP, HIP und GFP-Gruppen.
- Eine manuelle Lösung ist in der Anfangsphase OK, skaliert aber nicht.

⇨ Wird das EPD ein Erfolg, dann müssen die IAM-Evolutionsstufen in den nächsten 2-3 Jahren durchlaufen werden.

Die gute Nachricht dazu:

- Die für die EPD-Anbindung aufgebaute Infrastruktur ist auch für andere Cloud-Services verwendbar.
- Gelingt die IAM-Anbindung des EPD (bzw. HPD), dann wird auch die Anbindung anderer Cloud-Services gelingen!

… zum Erfolg

Besten Dank
für Ihre Aufmerksamkeit!

TEMET AG
Basteiplatz 5
8001 Zürich
044 302 24 42
info@temet.ch
www.temet.ch