Identity Access Management (IAM) in der Praxis und zukünftige Entwicklungen

Health-IT Talk Berlin/Brandenburg
Berlin, 09. August 2021

Toralf Skeries, Stefan Zorn

BG Klinikum Unfallkrankenhaus Berlin

Das Unfallkrankenhaus Berlin (ukb) ist ein hoch spezialisiertes klinisches Zentrum zur Rettung, Behandlung und Rehabilitation von Erkrankten und Verletzten.

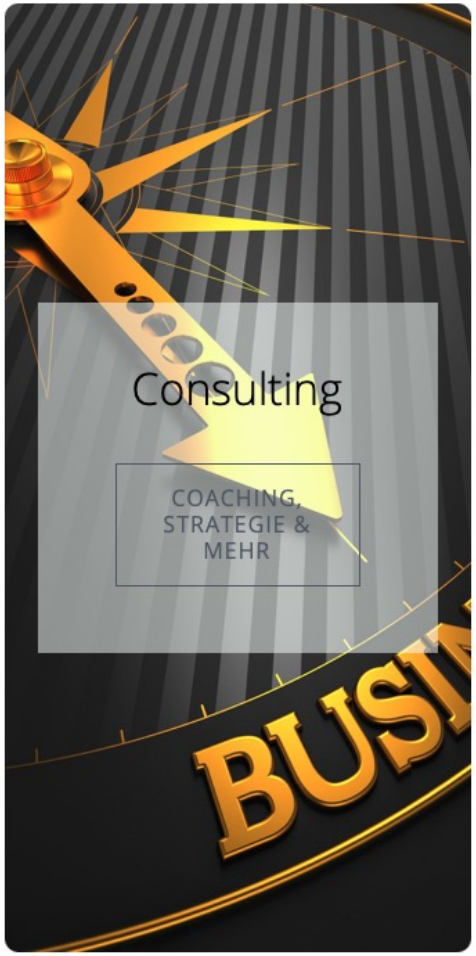
- 25 medizinischen Fachabteilungen, von verschiedenen chirurgischen Disziplinen über die leistungsstarke Kardiologie bis zur Neurologie.
- Internationale Spitzenposition in Therapie von Brand-, Rückenmark- und Handverletzungen
- Digitaler Radiologie, telemedizinischer Unterstützung von zahlreichen Krankenhäusern in mehreren Bundesländern, für Offshore-Windparks und Schiffe weltweit
- 2019 gegründete Medizinischen Akademie für die Ausbildung von Physio-, Ergotherapeuten und Logopäden.
- In 2020 eröffnete Reha-Klinik setzt neue Maßstäbe für die Behandlung der Patienten von der Akutversorgung bis zur Wiedereingliederung ins Berufsleben
- Zentrum für Notfalltraining im Haus der Zukunft, Angebot für bundesweite Simulationsteamtrainings für medizinisches Personal.

Zahlen & Fakten (2020)

1997 eröffnet – heute über 2.100 Mitarbeitende

- 27 Stationen mit insgesamt 730 Betten, 17 Operationssäle (4 ambulante OP)
- Jährlich rund 100.000 Patienten, davon ca. 23.300 stationär.
- 19.700 stationäre, 2.900 ambulante Operationen
- Rettungseinsätze 9.300, davon 1.400 mit dem Rettungshubschrauber, 6.000 Notarztwagen und 1.900 mit dem STEMO (Schlaganfall-Mobil)

imatics Health-IT Consulting GmbH



Es gibt nicht Gutes, außer man tut es (Erich Kästner)

WAS WIR TUN

Wir unterstützen Sie und Ihr Krankenhaus bei Ihrer Digitalen Transformation. Wir erstellen nachhaltige Konzepte und Strategien, begleiten Ihre Mitarbeiter, entwickeln Prozesse, wählen passende IT-Lösungen aus, kümmern uns um Datenschutz und IT-Sicherheit, entwickeln Ihr Project Management Office und begleiten die Veränderungen im Unternehmen.

1 **Verstehen**
Die Themen werden in Interviews und Begehungen analysiert und Probleme identifiziert.

2 **Miteinander sprechen**
Kommunikation ist (fast) alles: Interne und externe Beteiligte werden "an einen Tisch geholt"

3 **Strukturieren und Planen**
Zur Lösungsfindung werden Szenarien diskutiert und Prozesse und Strukturen optimiert.

4 **Begleiten und Unterstützen**
Die Umsetzung wird begleitet, imatics ist Sparringspartner, Aufpasser und Erinnerer

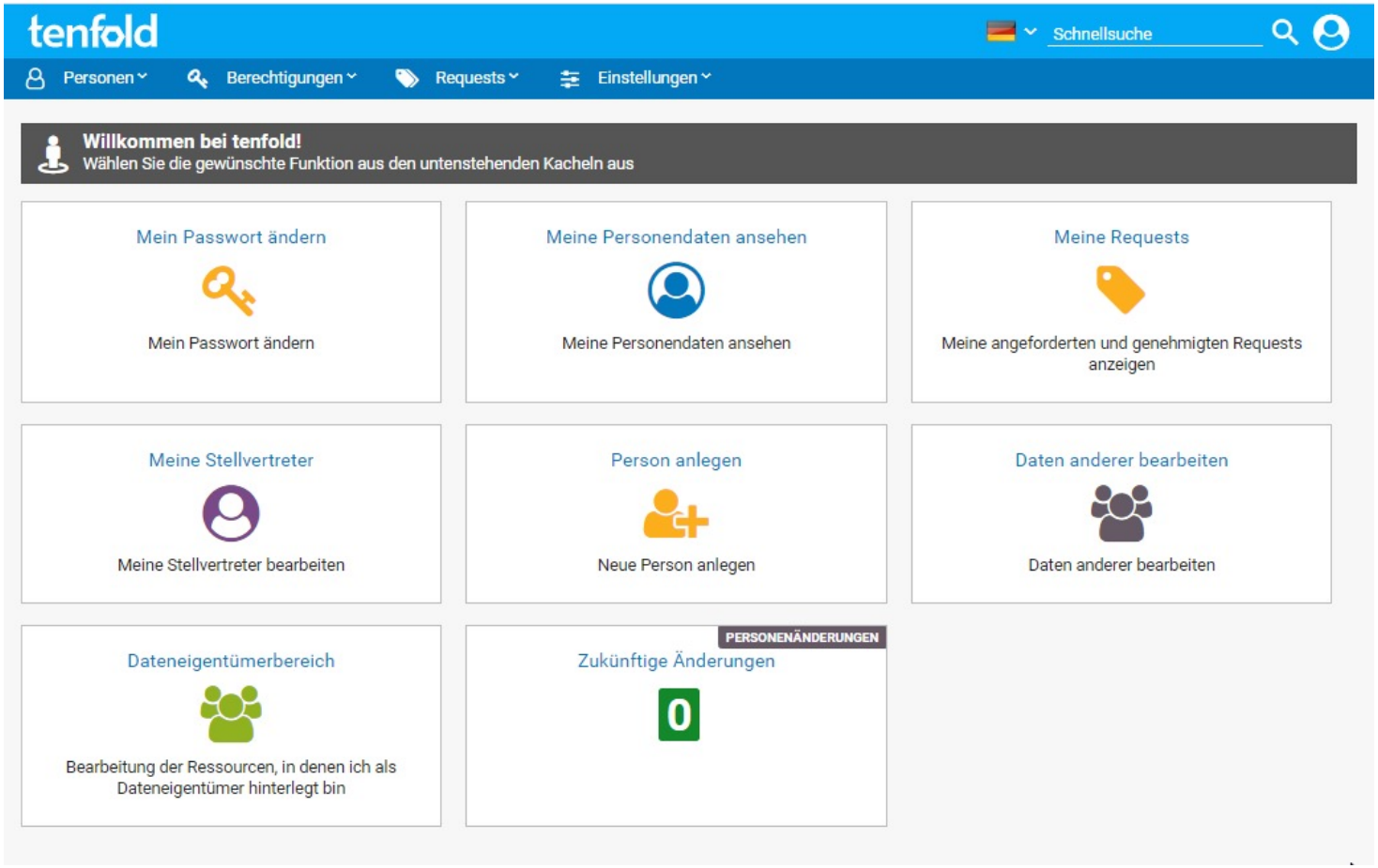
Identity- & Access-Management (IAM) am ukb

- Motivation für die Einführung des IAM ***Tenfold***: Nachvollziehbarkeit von Ressourcen (Dateifreigaben, Zugriff auf IT-Systeme etc.)

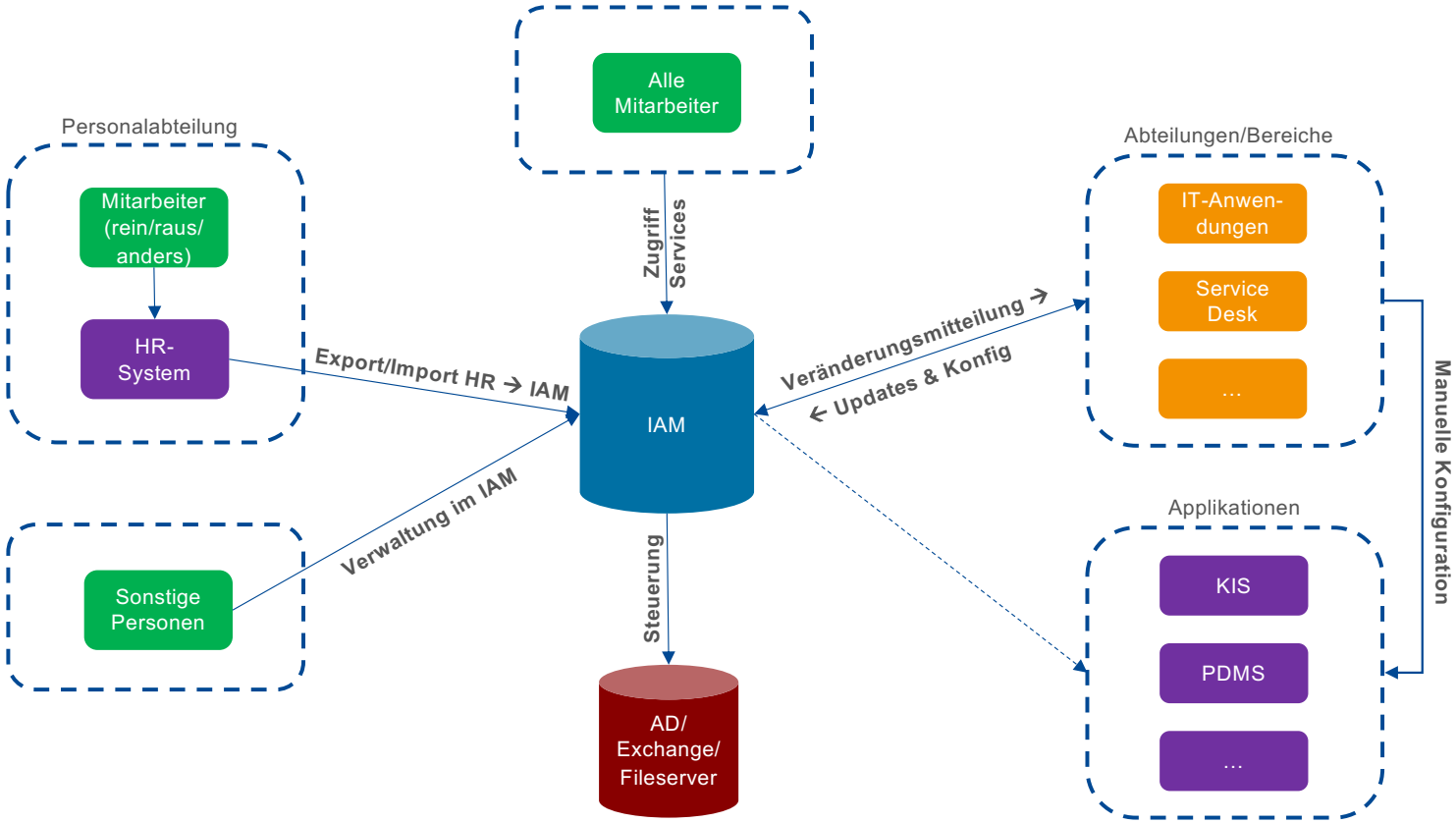
- Ziele
  - Vereinfachung von Prozessen
  - Verkürzung von Prozesslaufzeiten durch Optimierung und Automatisierung
  - Auskunftsfähigkeit (Audit)
  - Abbau von Medienbrüchen
  - Vermeidung von Mehrfacherfassung
  - …

- **Zentrales, unternehmensweit eingesetztes System für benutzerbezogene Services**

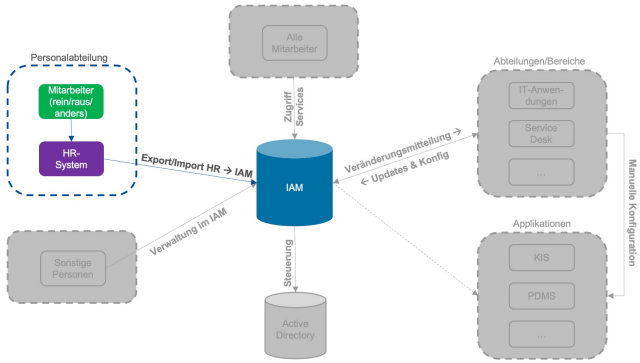
IAM am ukb: Tenfold – ein erster Eindruck



IAM Ecosystem

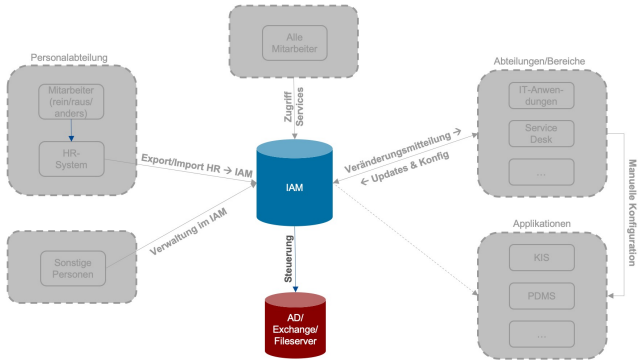


Die Mitarbeiter



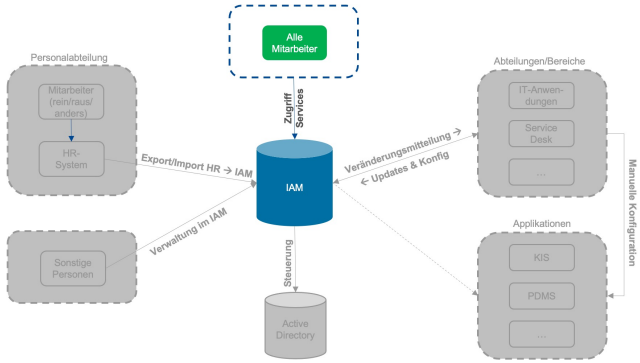
- Personalabteilung ist „Master of Desaster“
  - HR-System ist für **Datenqualität** verantwortlich
  - Alle Mitarbeiterbewegungen werden in HR ausgelöst
- Ergänzende Informationen werden im IAM gehalten. Beispiele:
  - Zusätzliche Telefonnummern
  - Qualifikationsnachweise
  - Mitarbeiterfoto
  - Informationen zur Schlüsselvergabe
- Mitarbeiterstammdatensatz beliebig erweiterbar

AD adé?



- Steuerung des **AD** zentral über IAM
- Synchronisation ausschließlich von IAM → AD
- Abbildung von sehr speziellen Attributen *nur in Ausnahmefällen* direkt im AD
- Steuerung von **Exchange-Konten** (Anlegen, Deaktivieren, Löschen)
- Steuerung des **Fileservers**

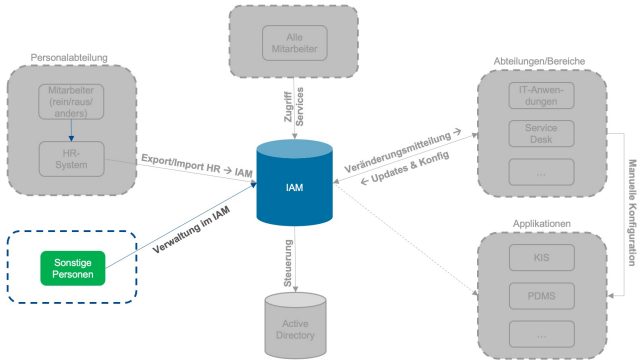
Me, myself and I



- Jeder IAM-Nutzer hat Zugriff auf seine eigenen Daten

- Änderung von Informationen
  - Direkte Änderung nur bei Daten möglich, die nicht über das HR-System kommen
  - Für Stammdaten aus HR-System muss Prozess etabliert werden, so dass HR entsprechende Änderungen ins HR-System einpflegen kann

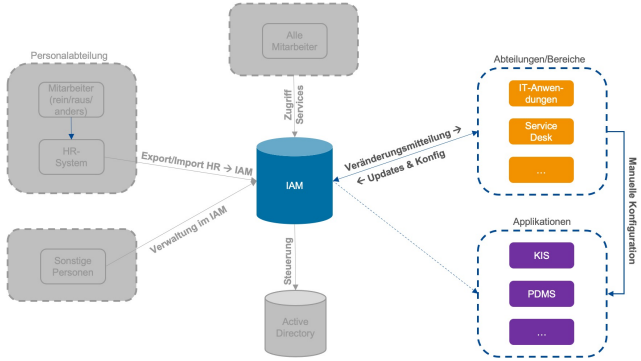
Und was passiert bei den Anderen?



- Verwaltung verschiedener Personengruppen, neben „normalen“ Mitarbeitern, die nicht im HR-System gepflegt werden, z.B.
  - Externe Dienstleister
  - Leiharbeitskräfte
  - Praktikanten, Famulanten, Doktoranden (Mitarbeiter ohne Bezahlung)

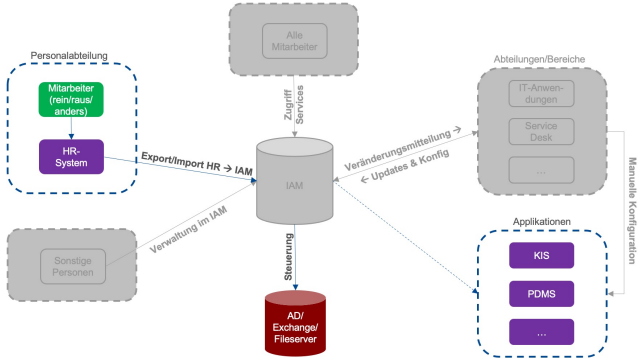
- Etablierung personengruppenspezifischer Attribute und Prozesse

Informationswege & Konfigurationen



- Automatische Informationen
  - über Änderungen an die beteiligten Abteilungen/Bereiche
  - Zu anstehenden Terminen (Reminder)
- Änderungen & Konfigurationen
  - Optimal: Konfigurationen über das IAM
  - Aber: Viele Systeme können nicht über ein externes System gesteuert werden → direkter Eingriff in jeweilige Anwendung. Bei Änderungen ist IAM „nur“ Vermittler für Arbeitsaufträge

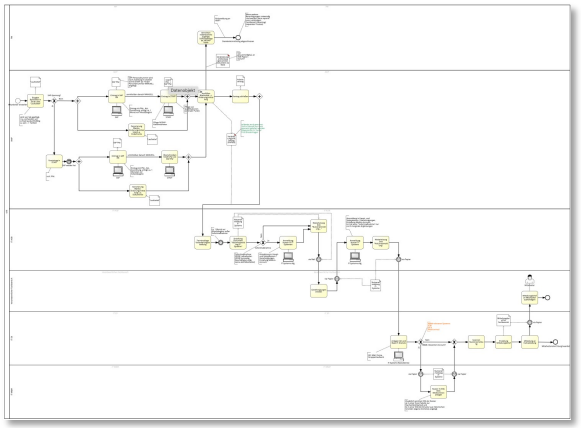
Was bin ich, wie heiße ich – Datenqualität



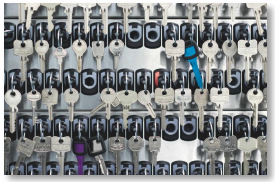
- Voraussetzung für einen reibungslosen Betrieb ist eine hohe Datenqualität
  - Kann eine längere Diskussion werden…
  - Evtl. Anpassungen in Subsystemen notwendig
- Beispiel Rollenbezeichnung
  - Anhand der Rollenbezeichnung werden Systeme manuell/automatisch konfiguriert
  - Einheitliche Bezeichnungen sollten in allen beteiligten Systemen angestrebt werden.
  - Und wie schon gesagt: Verbindliche Datenquelle soll am Ende das HR-System sein

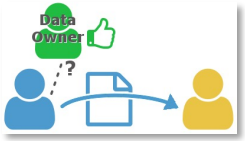
Was geht? Da geht noch viel! – Use Cases

- Nach initialem Aufsetzen, Datenbereinigung und stabilem Lauf können
  - weitere mitarbeiterzentrierte Prozesse digitalisiert werden
  - die Zusammenarbeit verschiedener Abteilungen optimiert werden (keine Medienbrüche, Verfügbarkeit von Informationen, Nachvollziehbarkeit)



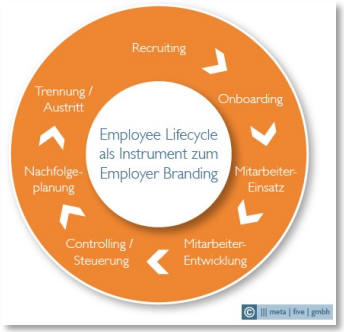
- Beispiele:
  - Karten- und Schlüsselverwaltung
  - Urlaubsantrag
  - Nutzungsanträge unterschiedlicher Art
  - Etablierung von Data Ownern





Start, Stopp, Weiter, Ende: User Lifecycle

- Klare Prozesse durch User Lifecycle Management für
  - Einstellung
  - Veränderungen während der Beschäftigung (Versetzung, längere Abwesenheiten wie z.B. Mutterschutz, Stammdatenänderung etc.)
  - Austritt

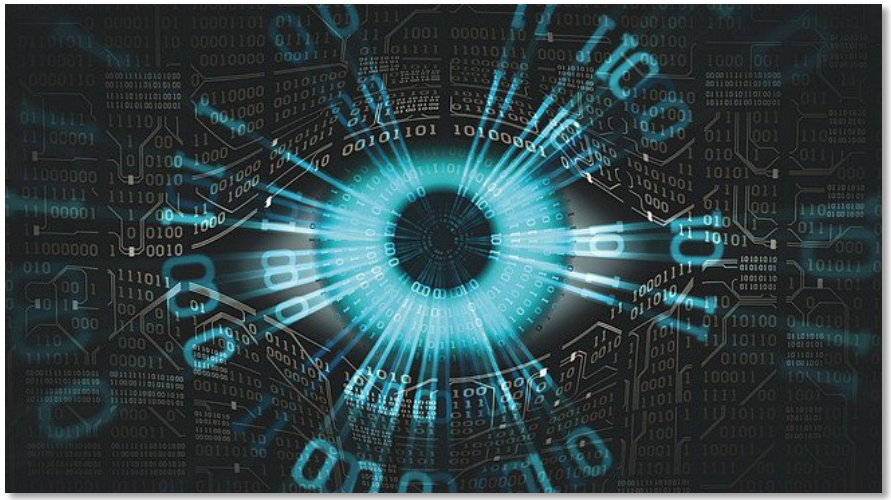


- Profilierung:
  - Wann werden welche Accounts (de-)aktiviert
  - Wann werden welche Zugriffe (de-)aktiviert
  - Wann werden Schlüssel (de-)aktiviert
  - Wann sollen welche Daten gelöscht werden

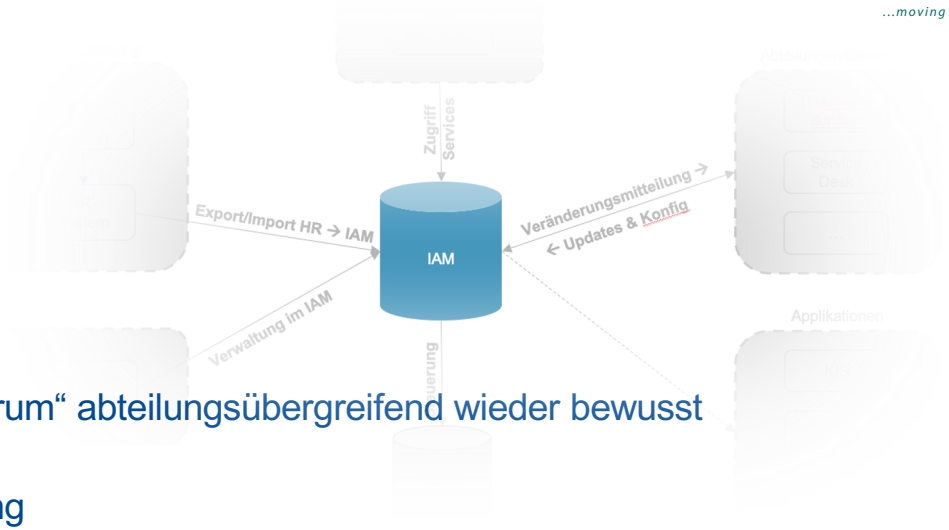
- Freie Definition der Lifecycle-Prozesse entsprechend der Anforderungen der Klinik sowie der rechtlichen Rahmenbedingungen

Ich weiß, was Du gestern getan hast… ☺

- Zentrale Haltung aller administrativen Aktivitäten
- Einfaches und revisionssicheres Auditing
- Im Falle eines Falles schneller Überblick und Einblick
- Kontrolle durch Genehmigungsworkflows
- Erleichterung in der Administration durch
  - Self Service Passwort
  - Data Owner
  - automatische Anlage von Nutzern
  - automatisierte Rechtevergabe (und –entzug)



Zusammenfassung



- Systeme können aktuell gehalten werden
  - Optimierung Lizenzen
  - Auditierfähigkeit ohne lange Vorbereitungszeit
- Optimierung von Prozessen
  - Alle Prozessbeteiligten werden sich des „Wie und Warum“ abteilungsübergreifend wieder bewusst
  - Starke Vereinfachung der betrachteten Prozesse
  - Schon im ersten Schritt hoher Grad an Automatisierung
  - Starke Reduzierung von Papier (Ausfüllen, Scannen, Versenden, Ausdrucken, Unterschreiben, Hauspost etc. gehört mehr und mehr der Vergangenheit an)
  - Deutlich erhöhte Prozessperformance
- Entlastung Service Desk durch Entfall von Standardaufgaben
- Es ist ein langer Weg (Prozessoptimierung, Datenqualität, Systemintegration etc.), aber er lohnt sich!

Vielen Dank

Toralf Skeries, toralf.skeries@ukb.de, 030/5681-1110

Stefan Zorn, s.zorn@imatics.de, 0175/1658151