Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
Bereich Digitale Transformation und IKT-Lenkung

Agile Lösung in hochsicherem Umfeld – unmöglich?

BäRN 26. August 2021

Vier Thesen für Agilität in der Sicherheit

- Agilität ist die (Führungs-)Fähigkeit schnell/kurzfristig einen (Teil-)Nutzen zu stiften (z.B. um Nutzenhypothesen zu verifizieren oder Nutzenengpässe befriedigen)
- Agilität braucht «Energie», Kreativität und ein präzises (nicht zwingend vollständiges) Verständnis der Bedürfnisse (andere Bezeichnung für «Wege zum Nutzen»)
- Lösungen brauchen Probleme; ohne «Problem» gibt es keine Beschreibungen von Bedürfnissen, sondern nur Spezifikationen von Lösungen; folglich bei Kollision zweier Lösungen keine Chance für «Vermittlung» und Priorisierung
- Jedes sozio-ökonomische System definiert / versteht «sicher» oder «hochsicher» anders; am Ende kommen aber alle bei den vier Schutz-/Sicherheitszielen (Vertraulichkeit, Verlässlichkeit/Integrität, Verfügbarkeit und Nachvollziehbarkeit) raus – sie konkretisieren die Ziele nur anders und gewichten sie unterschiedlich

Konkreter?
IAM Bund

in der Cloud wird die Identität zum letzten technischen Sicherheitsdispositiv – «Identity is the new (security)perimeter»

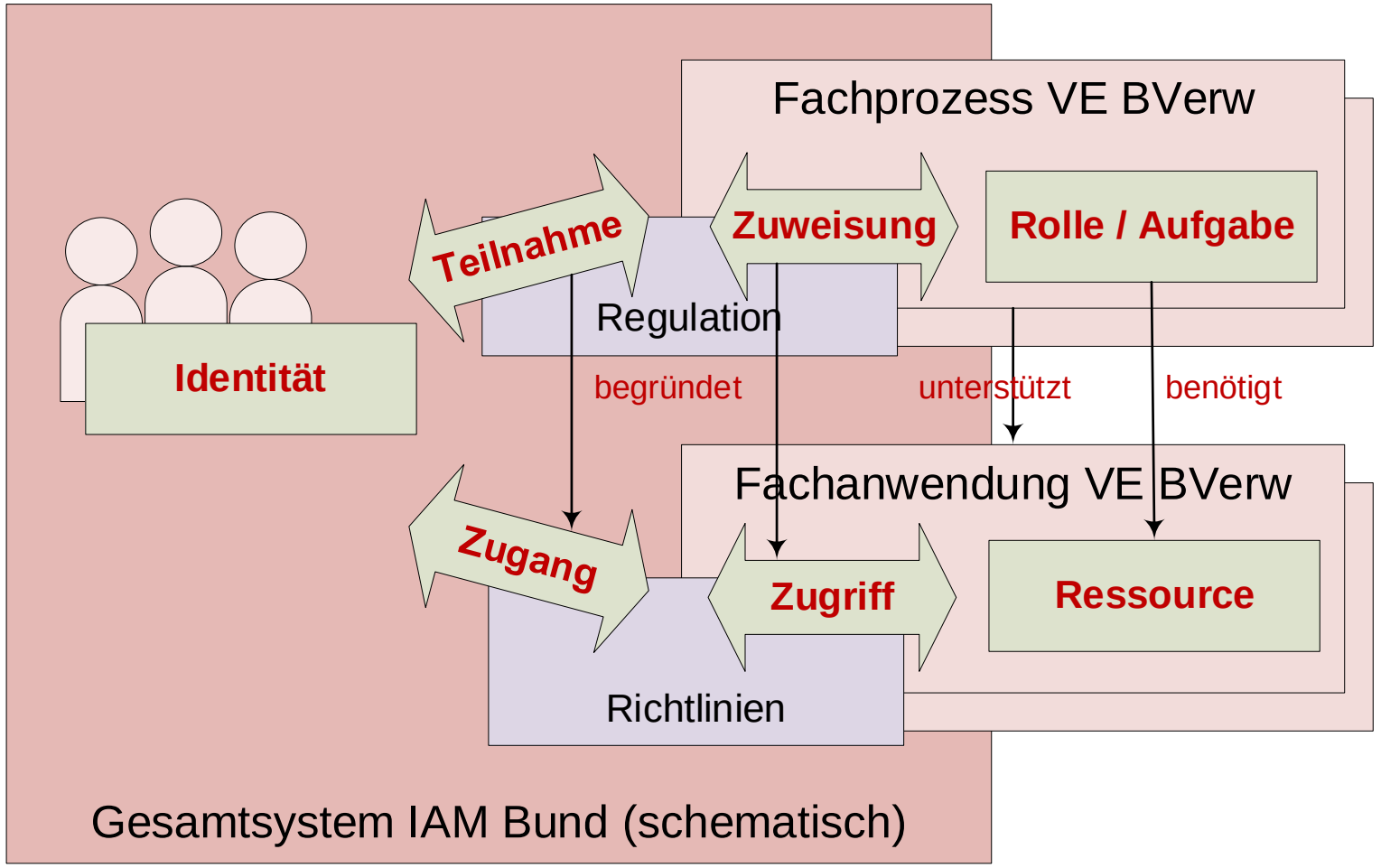
Steckbrief «Programm IAM Bund»

- Angetreten 2013 um «IAM in der Bundesverwaltung ‘aufzuräumen’»
- 2013/2014 umfassende Anforderungsanalyse (von der wir heute noch profitieren)
- Ursprünglich 25 Mio. Steuerfranken schwer; nur 11 Mio. bis 2016 investiert «Programm IAM Bund»; Rest sollte «später» kommen
- Bundesverwaltung: ca. 40’000 Personen, 10’000 FA, ca. 50 «Firmen» aus 8 «Holding» «keinen einzelnen Chef» – 8 Chefs
- Zeitweise 40 FTE in 6 Vorhaben aktiv – Kommunikation & Präzision überlebenswichtig
- Programm 2016 mit Go-Live des SD/IAM, der «IAM Steuerung» und über 1’000 Seiten «echtes Fach-Papier» abgeschlossen – seit dem «flaxile» Entwicklung / Umsetzung
- Ergebnis: Gesamtsystem IAM Bund, welches IAM in der Bundesverwaltung ganzheitlich als «infrastrukturelle Geschäftsfähigkeit IAM» tut

ganzheitlich «Gesamtsystem IAM Bund»?

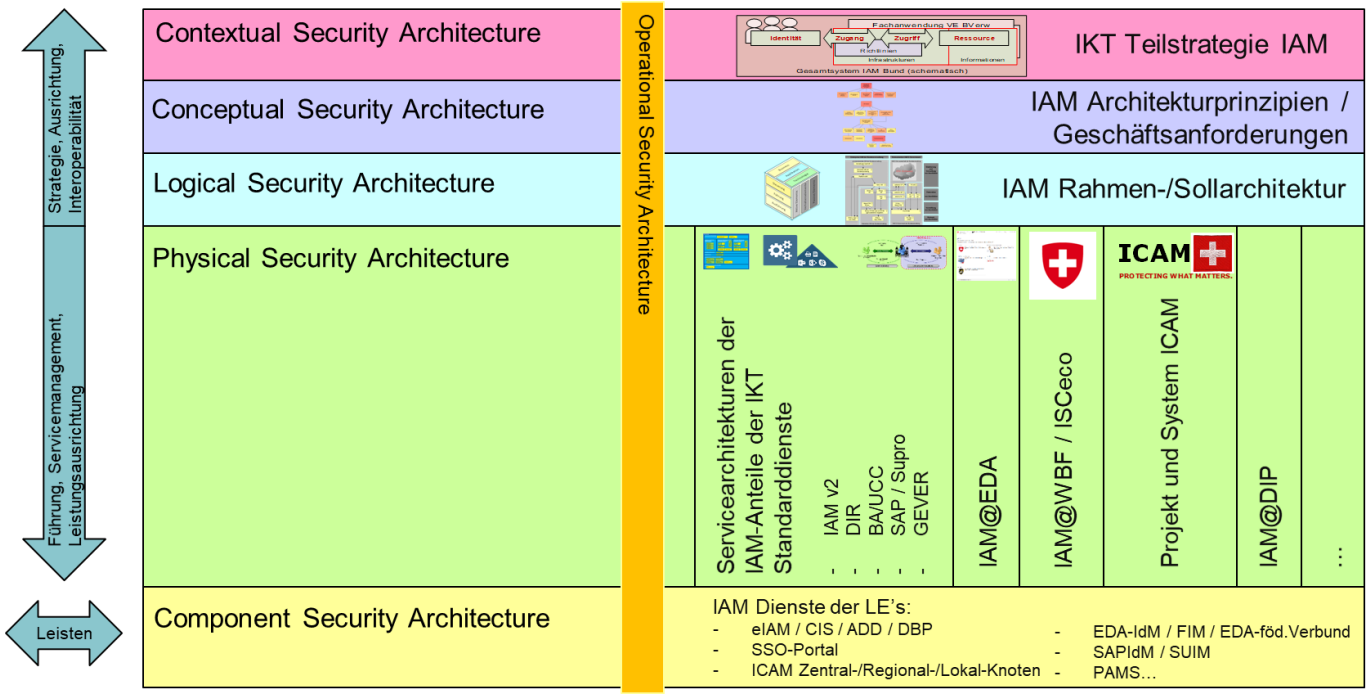
- Triviale Regel (aber für nicht-Architekten unbrauchbar):
- alle
  - Akteure (aktive Strukturen)
  - Dienstleistungen, Prozesse, Funktionen (Verhalten) und
  - Informationsobjekte, Produkte (passive Strukturen)
- mit einen Beitrag zur Antwort auf die vier grossen Fragen von IAM:
  - Wer bist du?
  - Woran erkenne ich dich?
  - Was darfst du oder wozu bist du autorisiert
  - Wie setze ich die Grenzen deiner Autorisation durch?
- unbeeindruckt einer Trennung in Governance, Management, Operation, IKT, Business..
- ABER: nur (Fach-)Prozesse in Eigentümerschaft der Bundesverwaltung

ganzheitlich «Gesamtsystem IAM Bund»?



Wie und Wo «agilisieren» wir in IAM Bund

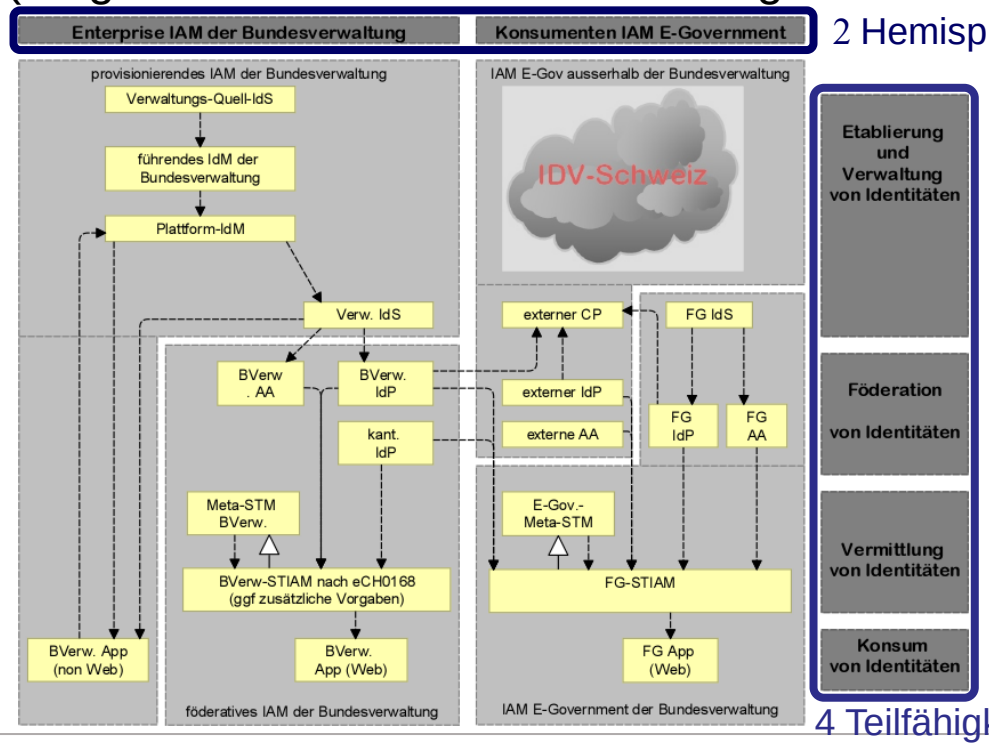
- Zwei Massnahmen fördern Agilität
  - Durch gestaltete (Fach-)Strukturen Bedarfsverantwortlichkeit zuweisen
    - Steuerungs-/Führungs-/Ausführungsstrukturen / oder –systeme → System-of-Systems-Approach (aufgrund organisatorischer Breite und Komplexität der Fachbedürfnisse)



Agilität in Organisation

Wie und Wo «agilisieren» wir in IAM Bund

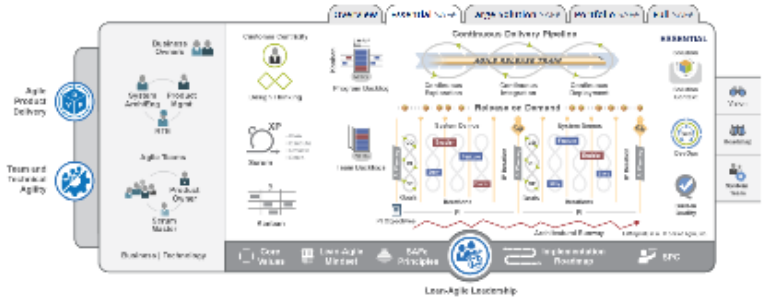
- Zwei Massnahmen fördern Agilität
  - Durch gestaltete (Fach-)Strukturen Bedarfs-Verantwortlichkeit zuweisen
    - Fachlich segmentiertes IAM oder Multi-Tier Identity Architecture (aufgrund technischer und technologischer Breite)



Agilität in Technik und Technologie

Wie und Wo «agilisieren» wir in IAM Bund

- Zwei Massnahmen fördern Agilität
  - Die meisten IAM-Services werden nach SAFe geführt / (weiter)entwickelt - CoE
    - Kein Full-SAFe – geht organisatorisch nicht; eher abgespeckter Large Solution SAFe
    - Jeder IAM Service ein ART (3 zentrale ART's) oder Team in ART (ca. 10 dezentrale ART)
    - BO «kommen» aus Führungssysteme haben aber «Proxy-BO's» in den PI-Plannings der Service-Trains
    - ART-Rollen entweder aus Führungssystem ge'staff't oder eng mit Führungsorganisation «verbunden»
    - Feature-Stories fliessen aus den «höheren Architekturebenen» in die Trains, werden in UserStories zerlegt, MVP's für Nutzenhypothesen oder Quickwins geplant und «fertig-fertig» implementiert



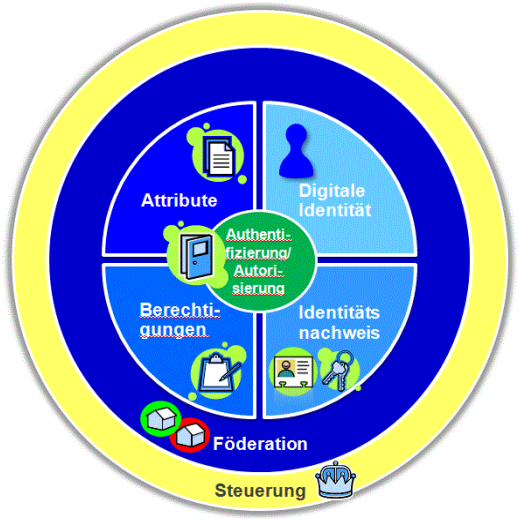
Agilität in Entwicklung

Funktioniert’s?

- Das «Überleben» des 5. Jahres gibt Anlass zur Hoffnung
- Viele 5-jahre alte Konzepte werden heute «wiederentdeckt» und begonnen zu nutzen

- Key-Learnings
  - Präzision insb. in den «höheren» Ebenen überlebensnotwendig; Modellierung hilft extrem
  - Alles wird herausgefordert; folglich braucht alles ein kommunizierbares WHY – «WHY is the new HOW»
  - «Kern» (die Steuerung) niemals organisatorisch oder verantwortlich fragmentieren und nicht mehr als 2-3 fachkompetente Personen; alles andere sollte einer gestalteten **teil**autonomen Fragmentierung entlang semantischer Anspruchsgrenzen folgen
  - Kommunikation ist nicht nur erzählen und «sich berieseln lassen»; es ist eine Kunst mit dem Willen zum Diskurs
  - Präzision verlangt Reflektionsvermögen und «nachdenken braucht Zeit»

Vielen Dank für ihr Aufmerksamkeit



Fragen ??

Anhang / Backup / Details

Der «Sand» des Architekturuniversums

- Drei Differenzierungslogiken
  - Konzeption (Problem) vs. Realisation (Lösung) – die «Mittel-Zweck-Beziehung»
    - Was ist die Idee zu einer Umsetzung – Was das Problem zu einer Lösung
    - Bsp. Idee/Konzept von Tisch → Tisch
    - Lösungen sind vergleichbar / ersetzbar, wenn sie das identische Problem haben
  - Abstraktion vs. Konkretisierung (Generalisierung vs. Spezifität) – «Klassifikationsbeziehung»
    - Ein Konzept (Lösung) bekommt zusätzliche (konkreter/spezifischer) oder weniger (abstrakter/generischer) Eigenschaften zugewiesen
    - Bsp. Höhere Säugetiere → Laurasiatheria → Unpaarhufer → Pferd
    - Jede zusätzliche Eigenschaft (in einem Konzept) schränkt den Lösungsraum ein
  - Grob vs. Fein – die «Verfeinerungs- oder Modularisierungsbeziehung»
    - Ein Konzept (Lösung) ist Bestandteil eines/r anderen Konzepts (Lösung)
    - Bsp. Mensch → Bein → Fuss → Zeh

Abstraktion und Präzision

- «*The purpose of abstraction is not to be vague, but to create a new semantic level in which one can be absolutely precise*» (Edsger W. Dijkstra 1971)
- Abstraktion oder Konkretisierung öffnen oder schliessen Freiheitsgrade in einer Konzeption
- Eine Definition ist umso präziser, je weniger **ungewollte** Freiheitsgrade eine Interpretation selbiger Definition (durch andere Individuen) zulässt.

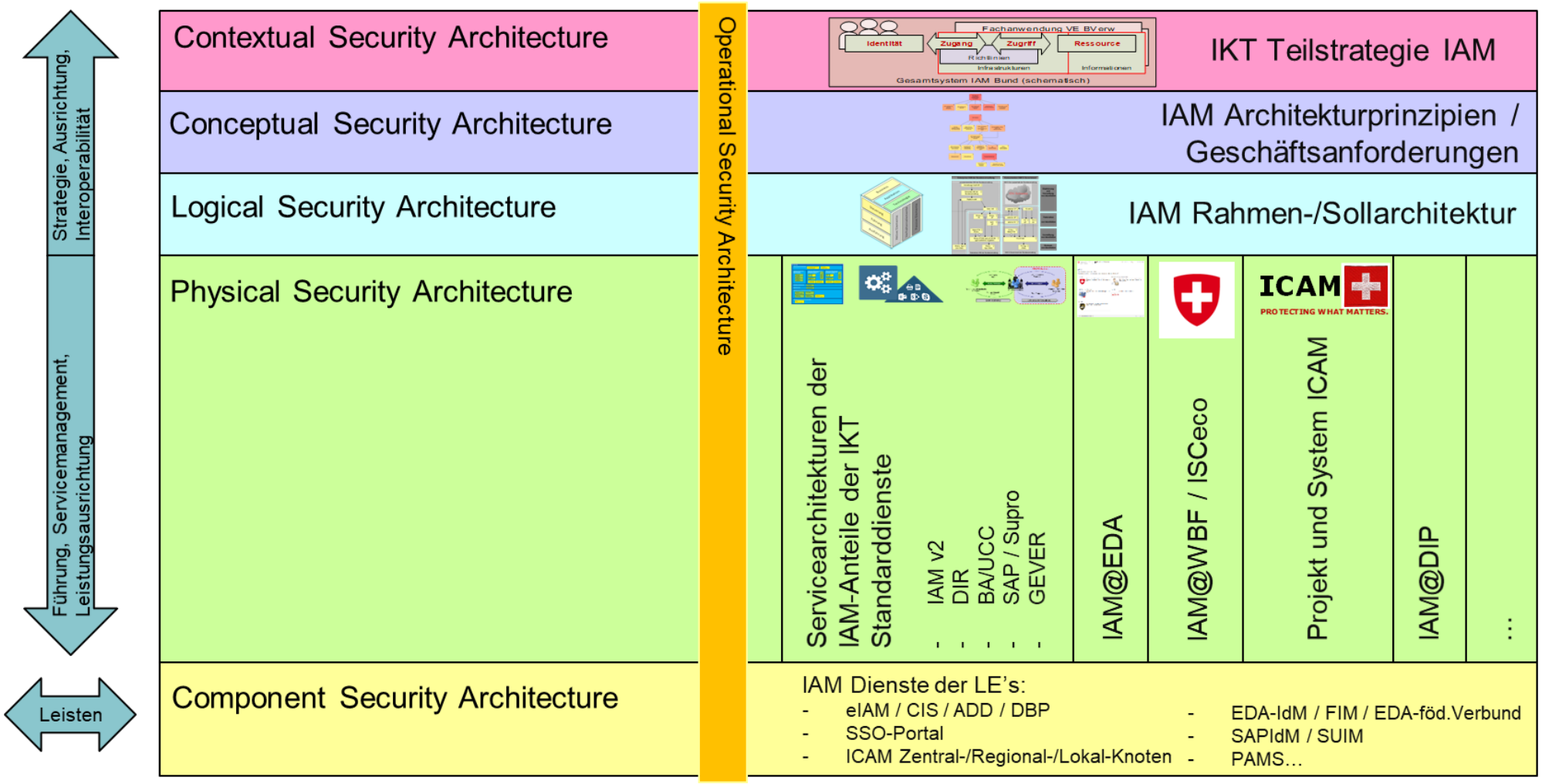
- drei Regeln für die Agilität (und Flexibilität):
  - So abstrakt/generisch wie möglich → lässt Lösungs-/Anwendungsräume offen
  - So konkret/spezifisch wie nötig → erlaubt Interoperabilitätssicherung
  - So präzise wie nötig aber nicht präziser → verhindert den Perfektionismus

Verständnis des Bedarfs oder «Weg zum Nutzen»

- Ist:
  - nicht nur eine (lange, flache) Liste von Anforderungen!!
  - Strukturierung von Motivationen (handlungs- und strukturtreibenden Gründen / Zwecken)
  - Aufgelöst (nach Mittel/Zweck-, Klassifikations/Spezifitäts- oder Verfeinerungs-beziehungen) bis zu einem Set «Root-Knoten» von Stakeholdern, denen es (quasi per Moral) «erlaubt» ist, etwas «Konkretes» einfach nur «zu wollen»
  - Asking and modeling WHY

- Führt zu:
  - Vollständigen (semantisches Niveau!) Beschreibbarkeit des Bedarfes oder Erwartungen des semantischen Problems → Semantik des Problems → Nutzen
  - Kenntnis über stakeholderspezifische Suboptima → Agilität

Fachstrukturen - Architekturdekomposition



Strategie, Ausrichtung, Interoperabilität
→ IAM Steuerung

- IKT-Teilstrategie und der IAM-Kontext
  - Wenig Konkretes, aber abgesegnet vom Bundesrat und damit starke Willenserklärung
  - Platz der Interoperabilität «nach aussen»
- Geschäftsanforderungen und Gestaltungsprinzipien
  - Requirements- und Motivationbasis – das grosse WHY und HOW mit Wirkung / Fokus auf Bundesverwaltung
  - Verschiedene Konkretisierungs- und Detaillierungsniveaus – Requirementsfundus auch noch für neue und laufende Vorhaben (insb. zur Ausrichtung)
- IAM-Rahmen- und Sollarchitektur
  - «Legokasten» von IAM Bund mit 21 abstrakten Bauanleitungen für IAM Services
  - die Gestaltung und Verteilung des Bedarfs – das grosse «WITH WHAT»
  - Platz der Interoperabilität «nach innen»

Servicemanagement, Leistungsorientierung
→ spezialisierte / fokussierte Führungssysteme

- Klassisches Servicemanagement nach gestalteten Führungsgrössen
  - **IAM der Standarddienste**: streng nach Narrativ «80% Bedarf zu 20% Kosten»
    - Ziel: Standardisierung, Wirtschaftlichkeit, Effizienz, Effektivität in der Breite
  - **IAM im EDA**: verlässliches IAM auf sandigem Untergrund
    - Ziel: Verlässlichkeit exakt auf Bedarf EDA zugeschnitten – hochflexibel und dennoch effizient
  - **IAM im WBF**: die Restanz, die eigentlich keinen Platz fand
    - Ziel: migrieren in die IAM-Leistungen der Standarddienste – Mergers & Akquisition «lernen»
  - **ICAM**: der Standarddienst des Militärs
    - Ziel: immer und jederzeit höchstverlässliches IAM («auch wenn die Welt in Flammen liegt, der Panzer schiesst, die Rakete fliegt»); Kosten spielen (fast) keine Rolle
  - **IAM der Digitalisierungsplattform**: der Herausforderer, der Inkubator, der «Reissnagel»
    - Ziel: Herausforderung der Standarddienste, Zeigen was möglich ist wenn man die Regeln «biegt»
  - **…..**: der Rest, das IAM in jedem Prozess, jeder Fachanwendung
    - Ziel: nicht alles kann man standardisieren / schubladisieren – aber es muss schrumpfen

Leisten
→ die Exekutive der IAM Services

- **That's what's all about** – alles andere ist Unterstützung, Effizienz, Planung und Orchestrierung, um das Richtige richtig zu tun
  - Drei zentrale Standard IAM-Services mit vielen verschiedenen Interfaces zu deren IAM-Leistungen – das, was wirklich jeder braucht, brauchen soll oder gebrauchen muss
  - IAM-Services anderer Gesamtsysteme plattformisiert und partiell autonom – Ausrichtung durch gestalteten Bedarf und nur Einschränkung aufgrund Interoperabilität
  - IAM-Services grosser technischer Plattformen (M/F, Unices, SAP) ebenfalls plattformisiert integriert und partiell autonom – aber strengere Guvernanz
- Plattformisierte IAM-Services leisten was immer die Plattform resp. deren Nutzer/Konsumenten/Teilnehmer brauchen → präzise (System-)Grenzen der Plattform und interoperabilitätszentrische Rahmenbedingungen → **Agilität**
- Bundesratsbeschluss (sog. Marktmodell) zwingt alle «Systeme» mit IAM-Funktionalitäten diese in IAM-Services einer Plattform oder des SD zu integrieren