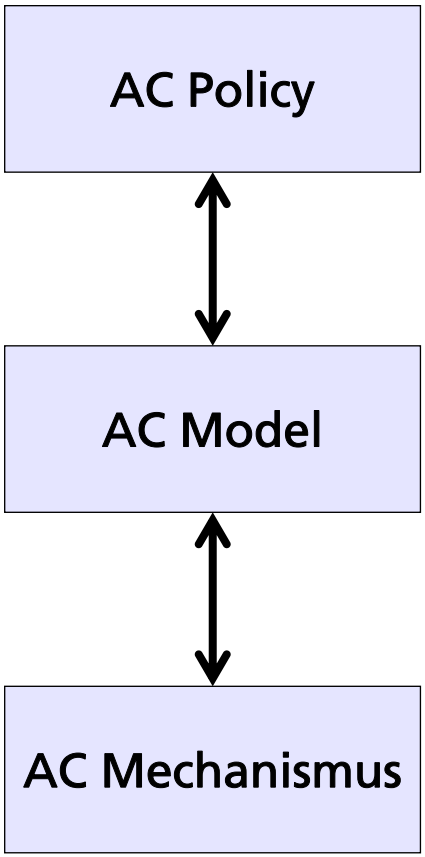
Identity und Access Management: Policies – Modelle – Mechanismen

Dr. Jörg Caumanns, Olaf Rode
Fraunhofer ISST Berlin

München, 07.03.08

Fraunhofer Institut Software- und Systemtechnik

Access Control: Abstraktionsebenen

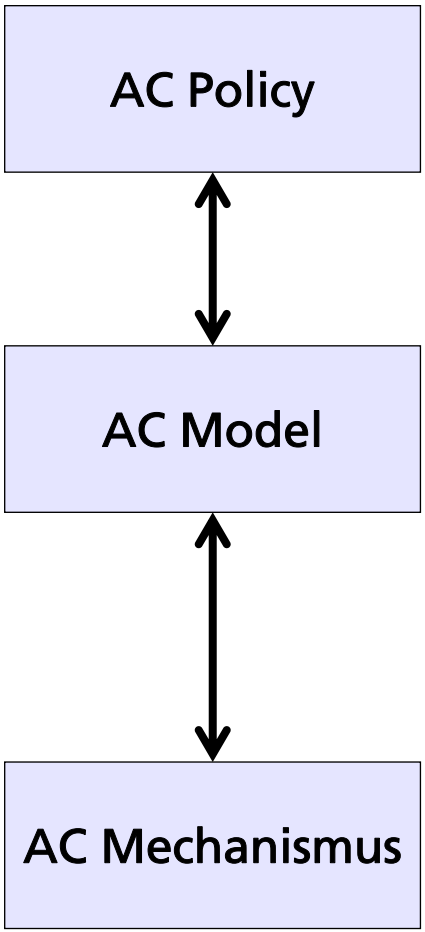


Richtlinien, die sich aus gesetzlichen Regelungen sowie den Abläufen und Objekten einer Anwendung (z. B. Einweisung) ableiten lassen.

Zuordnung von Berechtigungen zu Personen, wobei Rollen, Arbeitsabläufe, Nutzungsziele etc. als Indirektionsstufen genutzt werden können.

Verwaltung, Prüfung und Durchsetzung von Berechtigungen.
Identifizierung und Authentifizierung von Nutzern.

Access Control: Beispiel



Aufnahme -> {VSD, read}, {eEinweisung, read},...
Notaufnahme -> {VSD, read}, {NFD, read},...
med. Behandlung -> {eFA, read}, {eFA,write},...
...

Aufnahmenkraft -> Aufnahme, Notaufnahme
med. Personal -> med. Behandlung, Notaufnahme
...
Fr. Burger -> Verwaltung, Aufnahmekraft
Dr. Schulz -> med. Personal, Arzt, Kardiologe
...

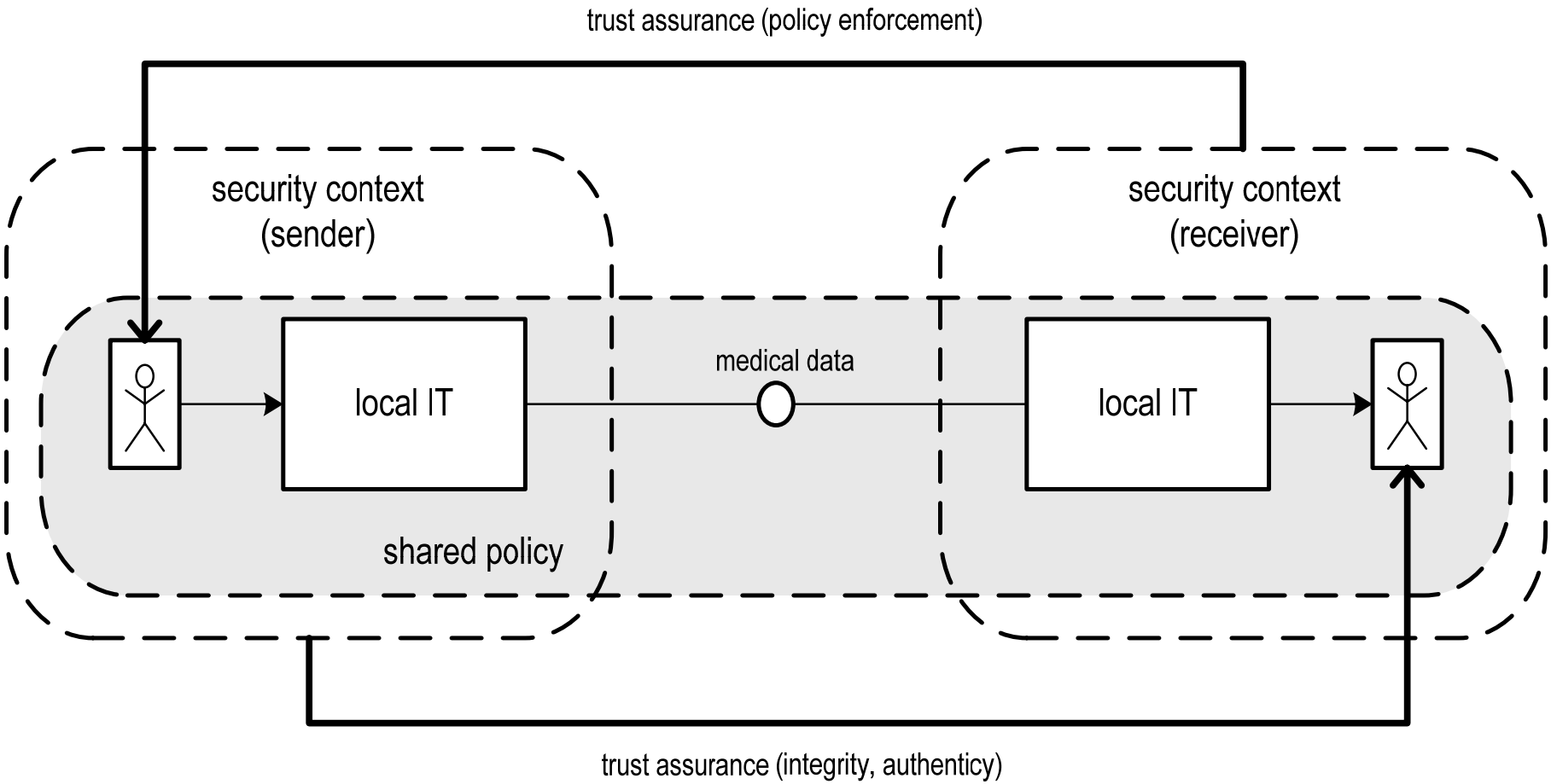
Aufnahme-PCs sind identifizierbar und haben gesonderte Accounts. Rechte der Aufnahmekräfte sind an die Arbeitsplätze gebunden. Policies, Rollen und Einschränkungen für med. Personal sind im KIS hinterlegt und werden dort geprüft. ...

Schweigepflicht

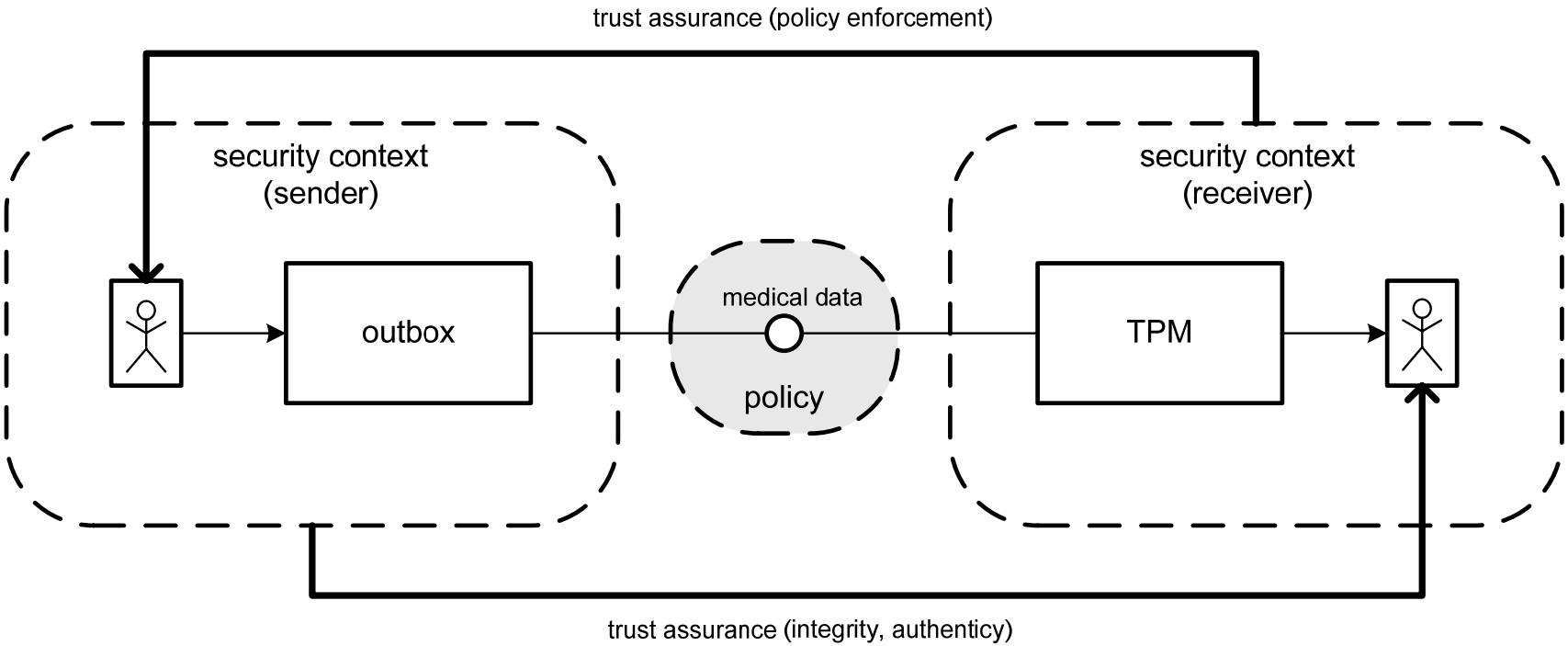
» Ein Arzt ist verpflichtet, vor einer Übermittlung zu prüfen, ob eine Befugnis zur Offenbarung der Daten an den Empfänger vorliegt. Würde ein Arzt die Patientendaten für einen Abruf durch andere Behandlungseinrichtungen bereithalten und käme es dann zum Abruf, der rechtlich nicht (z. B. durch eine Einwilligung des Patienten) legitimiert ist, so hätte sich der speichernde Arzt nach § 203 StGB strafbar gemacht. «

[Datenschutz und Telemedizin 2002 – Konferenz der Datenschutzbeauftragten des Bundes und der Länder]

Trust Assurance

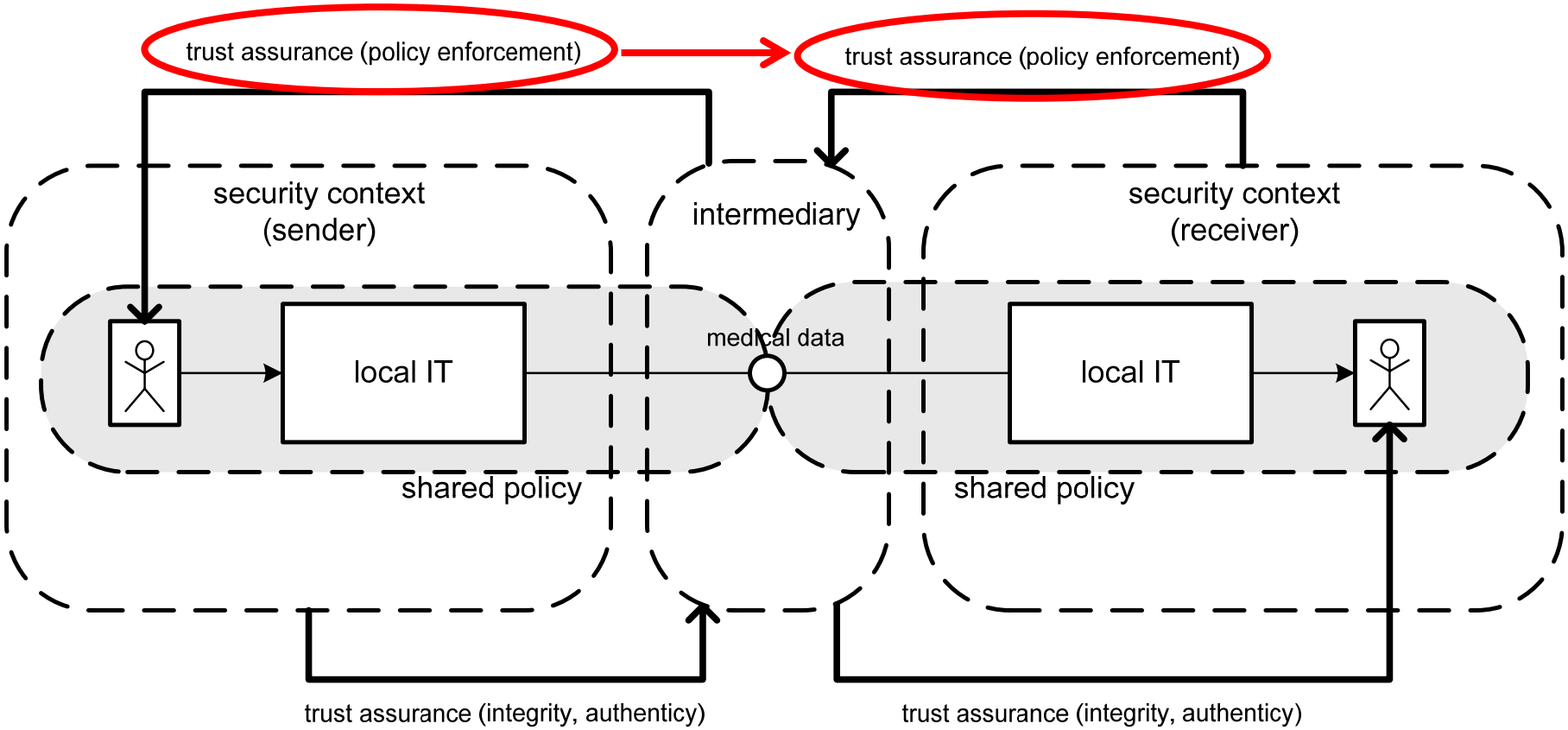


Trusted Computing Modell



Fraunhofer Institut Software- und Systemtechnik

Angepasstes Modell für den § 291a SGB V



Beispiel: Operationen auf den Anwendungen der eGK

§ 291a SGB V

	{ RETRIEVE, VSD }	{ READ, VSD }	{ CREATE, PRE_VOD }	{ READ, PRE_VOD }	{ UPDATE, PRE_VOD }	{ DELETE, PRE_VOD }	{ SIGN, PRE_VOD }	{ CREATE, VOD }	{ RETRIEVE, VOD }	{ READ, VOD }	{ UPDATE, VOD }	{ DELETE, VOD }	{ EXECUTE, VOD }	{ CREATE, PRE_NFD }	{ READ, PRE_NFD }	{ UPDATE, PRE_NFD }	{ DELETE, PRE_NFD }	{ SIGN, PRE_NFD }	{ CREATE, NFD }	{ RETRIEVE, NFD }	{ READ, NFD }	{ UPDATE, NFD }	{ DELETE, NFD }	{ RETRIEVE, EINWILLIGUNG }	{ READ, EINWILLIGUNG }	{ UPDATE, EINWILLIGUNG }
Administration																										
Patientenverwaltung																										
Voraufnahme/Disposition	-	-	-	-	-	-	-	-	x	x	-	-	-	-	-	-	-	-	-	-	-	-	x	x	-
Aufnahme	x	x	-	-	-	-	-	-	x	x	-	-	x	-	-	-	-	-	-	x	-	-	x	x	-
Entlassung	x	x	-	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-	x	-	x	x	-
Medizinische Versorgung																										
Vorbereitung																										
Dokumentenaufbereitung	x	x	x	x	x	x	-	-	-	-	-	-	-	x	x	x	x	-	-	x	x	-	-	x	x	-
Behandlung																										
Beratung / Datenaktualisierung	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Notaufnahme	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	x	x	-	-	x	x	-
Nachbereitung																										
Dokumentenbereitstellung	-	-	x	x	x	x	(x)	x	-	-	-	-	-	x	x	x	x	(x)	-	-	-	-	-	x	x	-

Fraunhofer ISST Institut Software- und Systemtechnik

AC Policy ⟷ AC Model ⟷ AC Mech.

Access Control: Modelle

Discretionary Access Control (DAC):

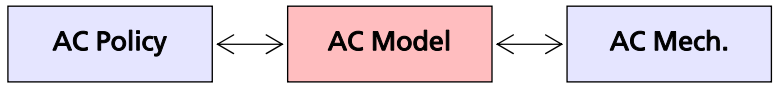
- Jedes Objekt hat einen Verantwortlichen, der Rechte zur Durchführung von Operationen auf dem Objekt an Subjekte (Personen, Gruppen) vergeben kann

Mandatory Access Control (MAC):

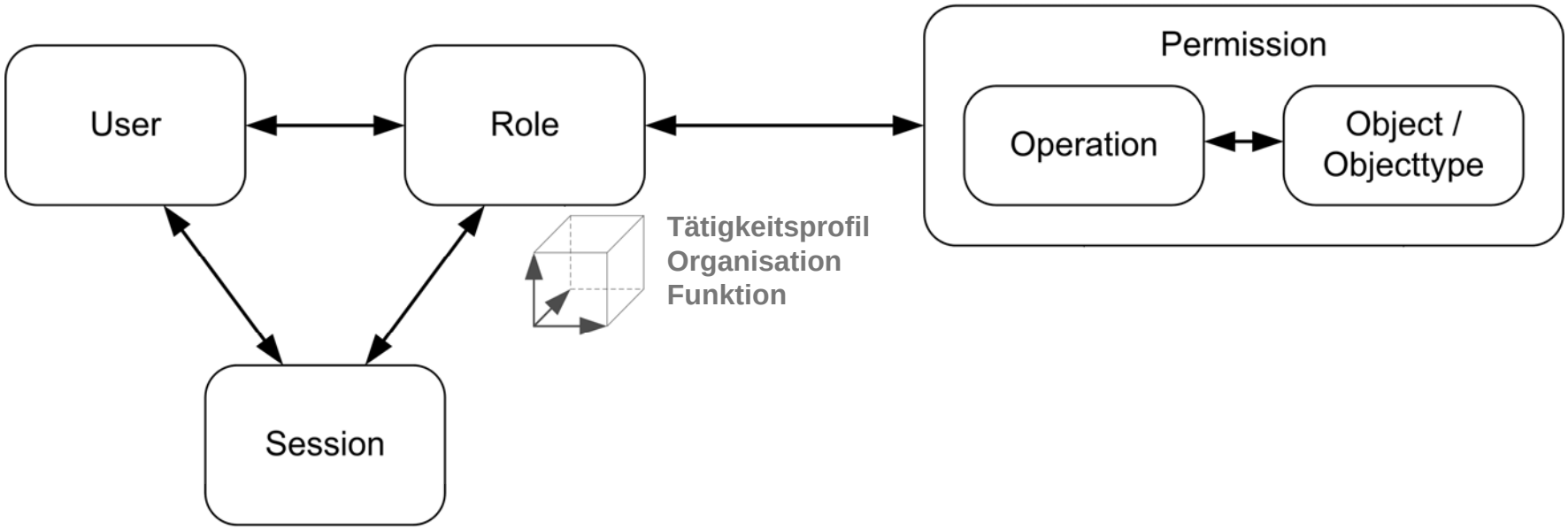
- Subjekte und Objekte sind Sicherheitsstufen (clearance/classification levels) zugeordnet
- *-property: no read up – no write down

Role-Based Access Control (RBAC):

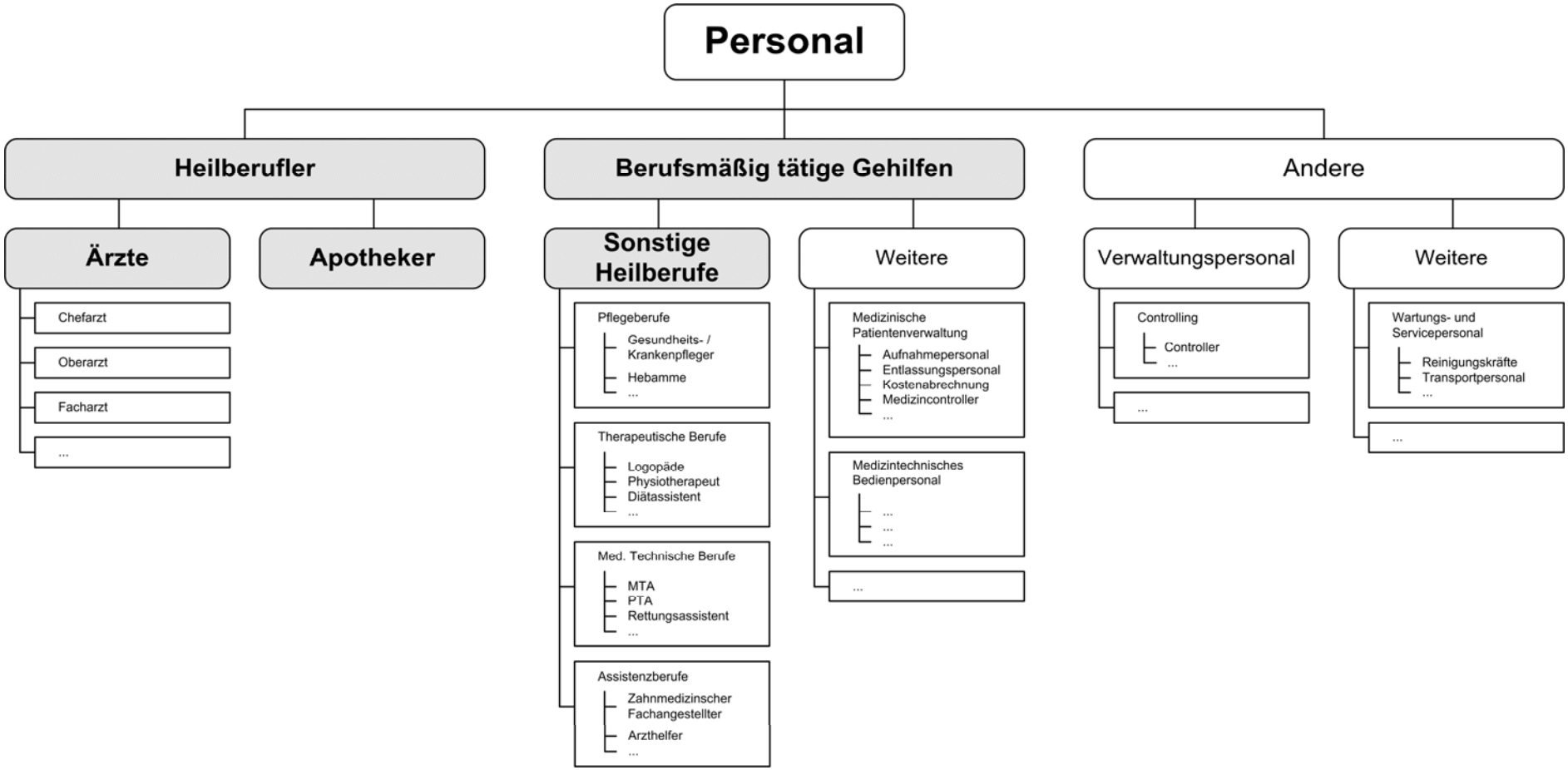
- Berechtigungen werden ausschließlich auf Rollen ausgestellt
- Berechtigungen werden zentral administriert
- Möglichkeit, Rollenhierarchien und –einschränkungen zu definieren



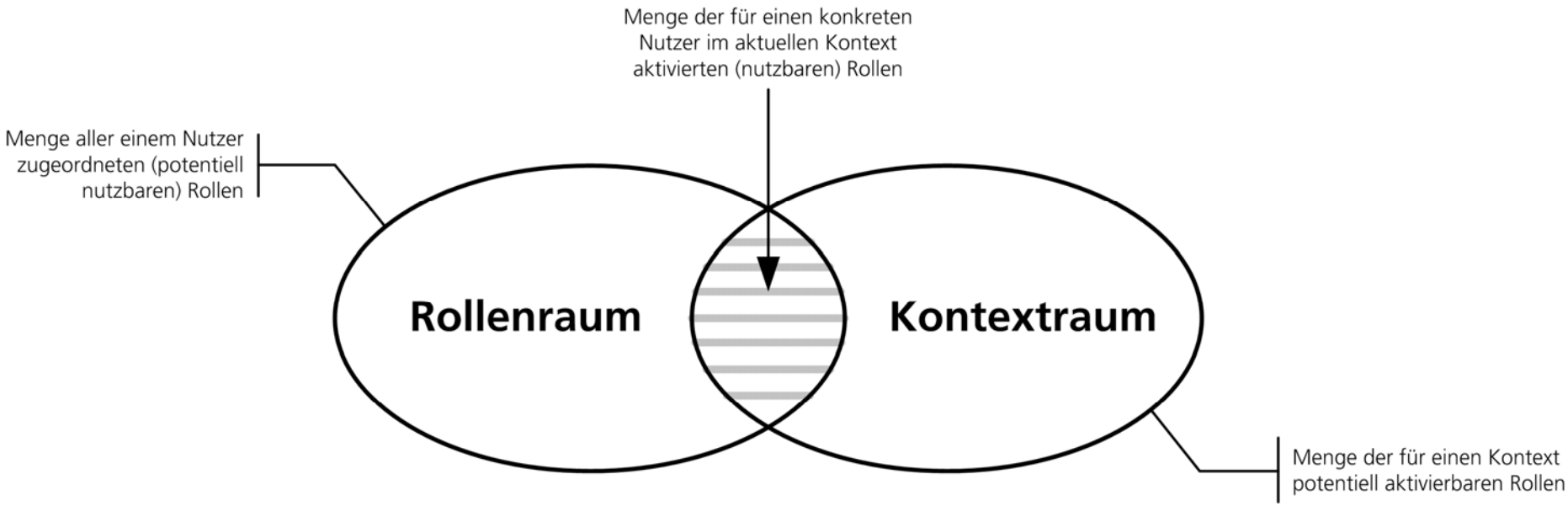
Role Based Access Control



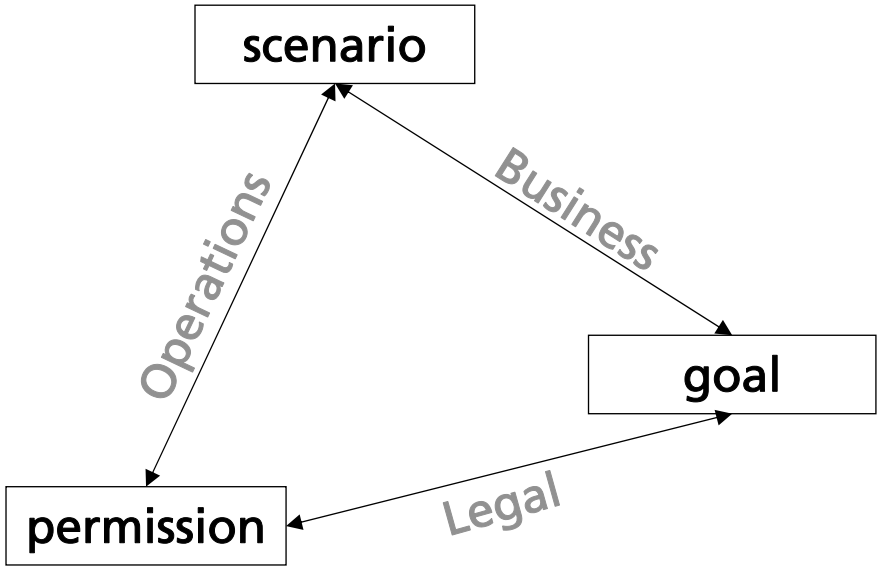
Beispiel: Tätigkeitsprofile



Role Activation



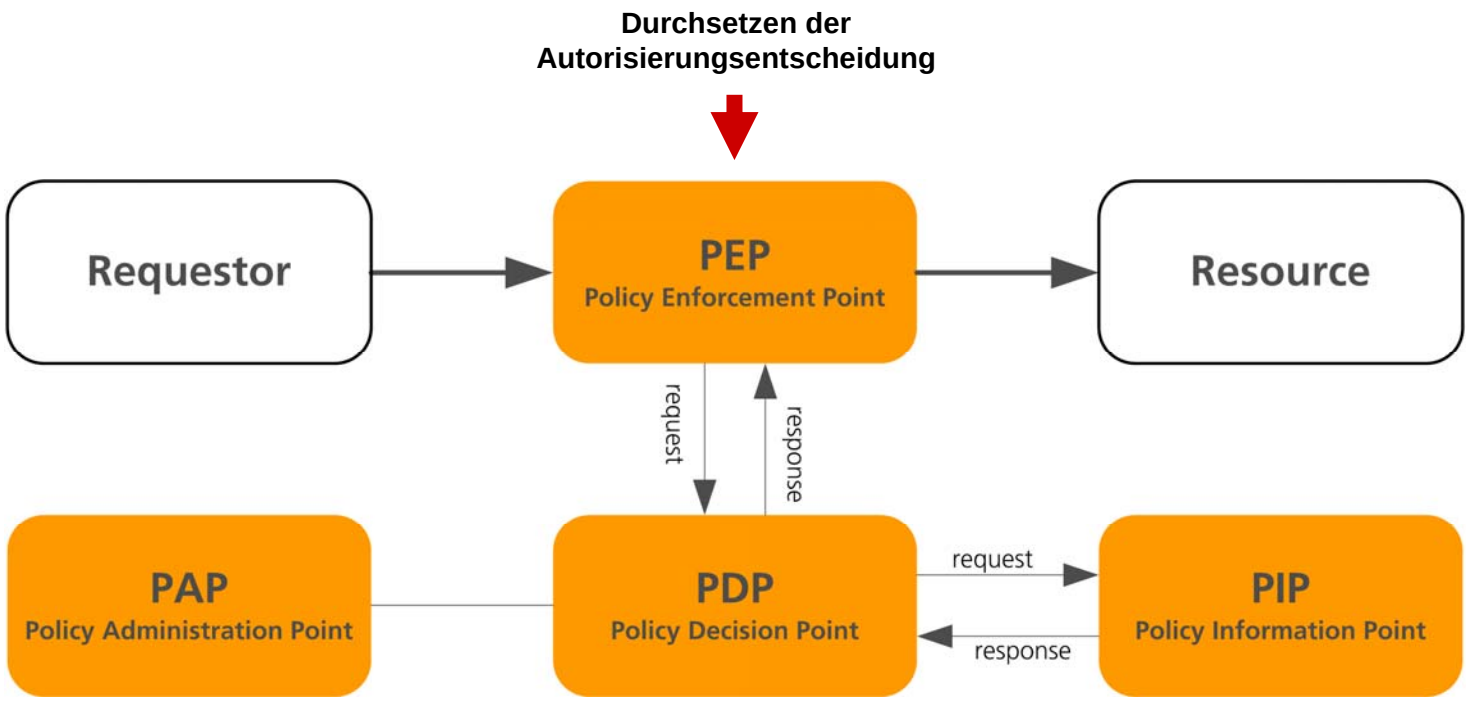
Role Engineering



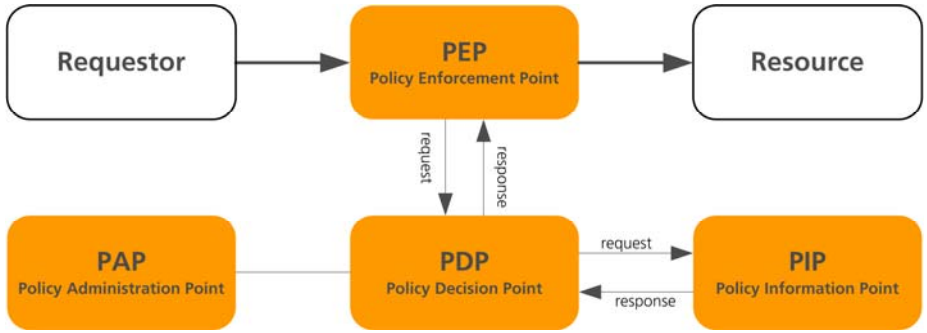
In der Theorie sind drei Vorgehensmodelle beschrieben:

- **scenario based**: Welche Szenarien/Ablaufschritte gibt es und welche Personen (Rollen) müssen dabei wie auf welche Daten zugreifen?
- **goal oriented**: Welche Geschäftsziele gibt es, welche Objekte sind damit verbunden und wer (Rolle) muss was mit diesen machen?
- **permission driven**: Welche Objekt-typen gibt es, welche Operationen darauf sind erforderlich und wer (Rolle) führt diese in welchem Kontext durch?

Komponenten des Access Managements

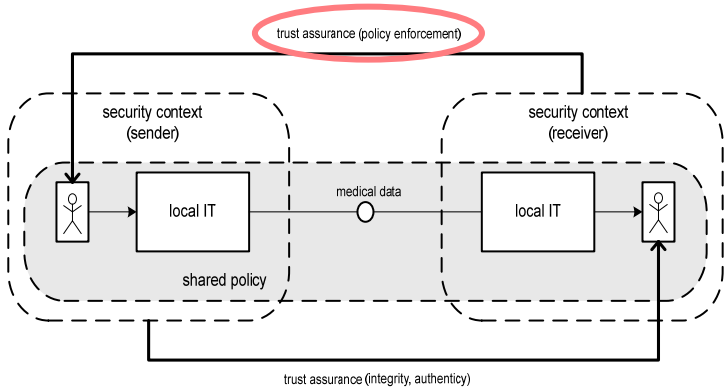


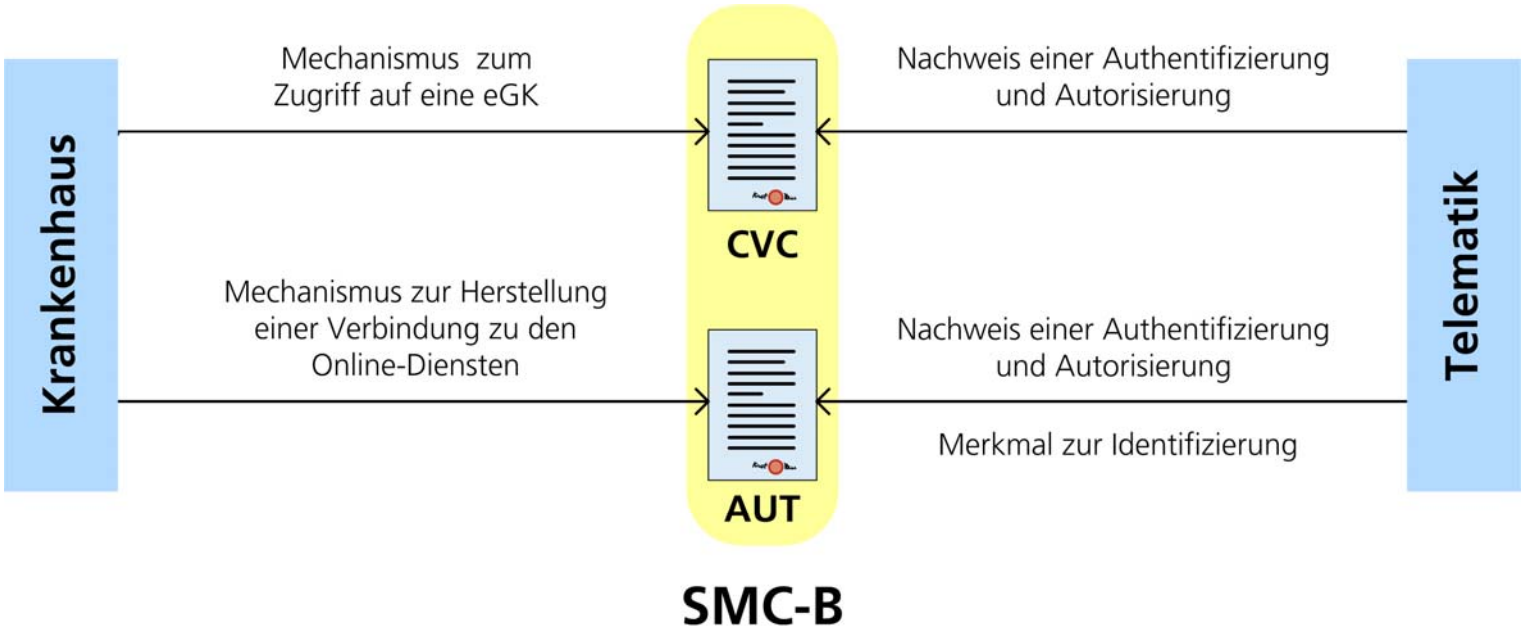
Semantik der SMC-B I



	Offline (Daten auf eGK)	**Online (Daten auf Server)**
Konnektor	[Policy Enforcement Point] [Policy Information Point]	[Policy Enforcement Point]
HBA	Policy Information Point	Policy Information Point
SMC	Policy Information Point	Policy Information Point
eGK	Policy Enforcement Point Policy Decision Point Policy Administration Point	-
Broker	-	[Policy Enforcement Point Policy Decision Point][4]
Fachdienst	-	Policy Enforcement Point Policy Decision Point Policy Administration Point

Semantik der SMC-B II

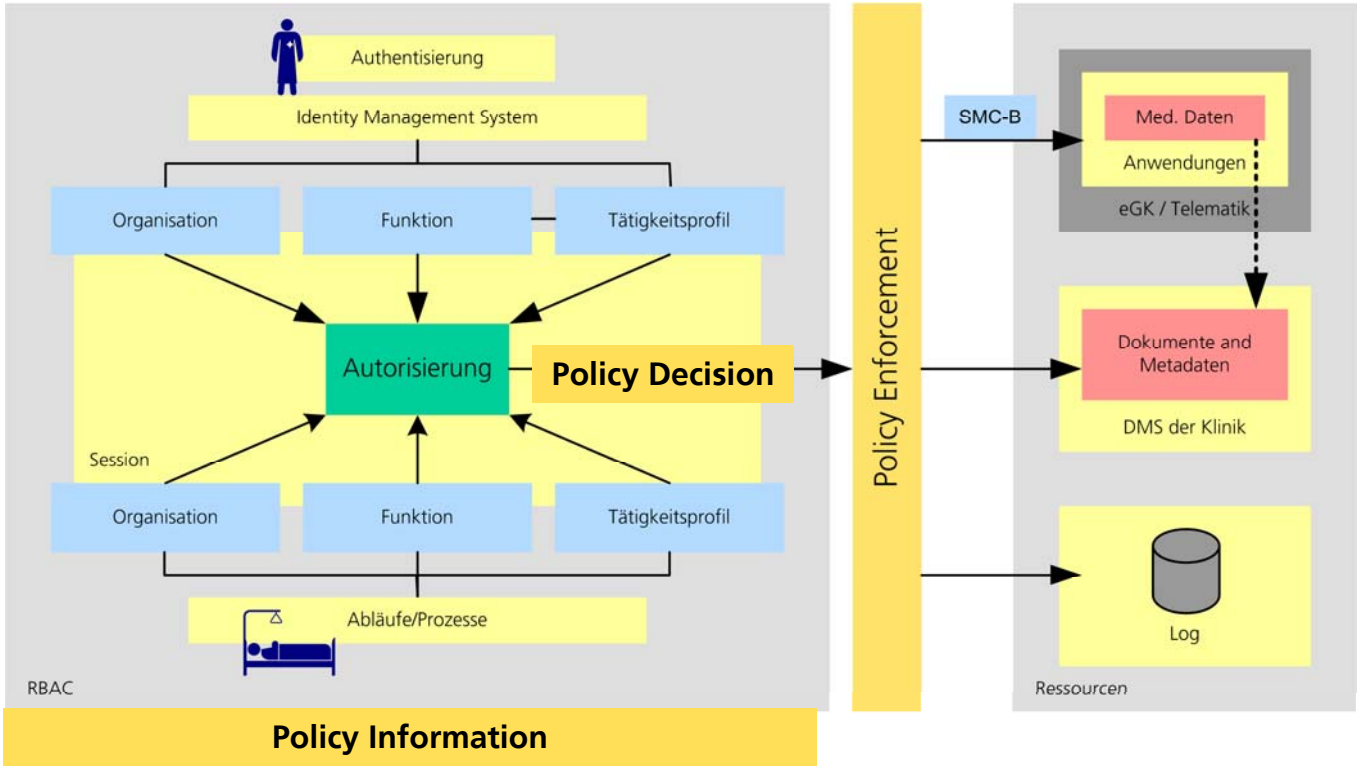




Fraunhofer Institut Software- und Systemtechnik

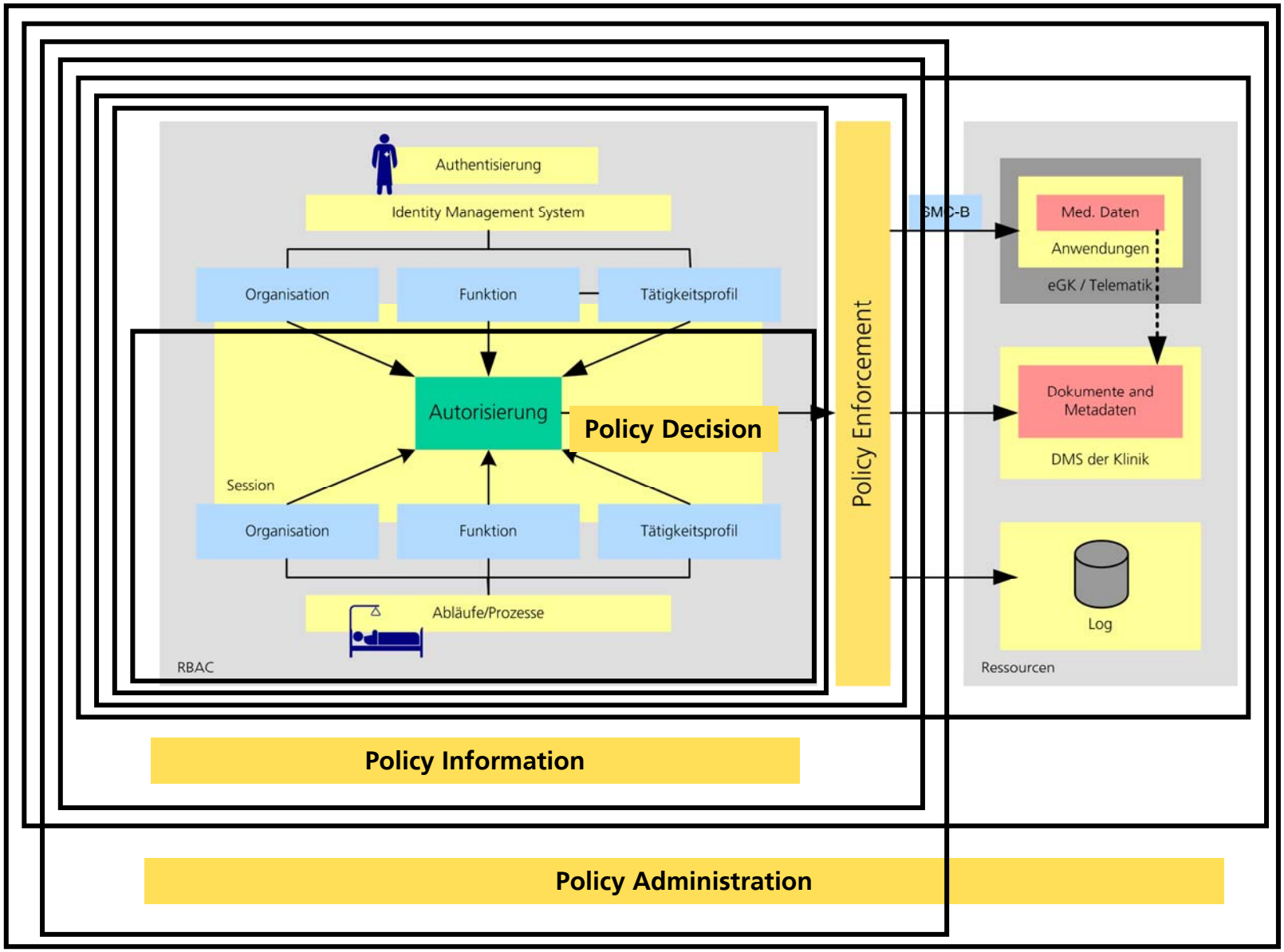
AC Policy ⟷ AC Model ⟷ AC Mech.

Entkopplung von Ressourcen



Fraunhofer Institut Software- und Systemtechnik

Funktionen des KIS: Jeder Kasten eine Option....



Kontakt

Dr. Jörg Caumanns
Fraunhofer ISST Berlin
joerg.caumanns@isst.fhg.de

Elektronische Fallakte
http://www.fallakte.de/