Datenschutz und Datensicherheit

- Kritische Erfolgsfaktoren für eHealth -

München, 18.Februar 2005

Prof. Dr.-Ing. Heinz Thielmann

Fraunhofer Institut Sichere Informationstechnologie SIT, Darmstadt

In Kooperation mit Dr. Lutz Kleinholz, healthpartner consulting GmbH, München

Fraunhofer SIT Institut Sichere Informations-Technologie

Datenschutz und Datensicherheit

- Der Bürger und Patient im Mittelpunkt
- Rechtliche Grundlagen, Rahmenbedingungen, Gesamtkonzept
- Die Kette: Bürger, Patient, Arzt, Apotheker, Klinik,....
- Die eGK: Daten, Personalisierung, Ausgabe, Zugriffsrechte
- Karten- und Rechtemanagement
- Dezentrale Dienste
- Zentrale Dienste
- Aktuelle Aufgaben in der Spezifikation der Lösungsarchitektur

Fraunhofer SIT Institut Sichere Informations-Technologie

Datenschutz und Datensicherheit

- **Der Bürger und Patient im Mittelpunkt**
- Rechtliche Grundlagen, Rahmenbedingungen, Gesamtkonzept
- Die Kette: Bürger, Patient, Arzt, Apotheker, Klinik,....
- Die eGK: Daten, Personalisierung, Ausgabe, Zugriffsrechte
- Karten- und Rechtemanagement
- Dezentrale Dienste
- Zentrale Dienste
- Aktuelle Aufgaben in der Spezifikation der Lösungsarchitektur

Fraunhofer SIT
Institut
Sichere Informations-
Technologie

Ausgangsthese

Das Vertrauensverhältnis zwischen

Patient und Arzt

ist ein hohes Gut, das durch die Einführung einer

Telematikinfrastruktur nicht abgewertet werden darf.

Der Bürger/Patient ist Herr seiner Daten.

Fraunhofer SIT Institut Sichere Informations-Technologie

Datenschutz und Datensicherheit

- Der Bürger und Patient im Mittelpunkt
- **Rechtliche Grundlagen, Rahmenbedingungen, Gesamtkonzept**
- Die Kette: Bürger, Patient, Arzt, Apotheker, Klinik,....
- Die eGK: Daten, Personalisierung, Ausgabe, Zugriffsrechte
- Karten- und Rechtemanagement
- Dezentrale Dienste
- Zentrale Dienste
- Aktuelle Aufgaben in der Spezifikation der Lösungsarchitektur

Fraunhofer SIT
Institut
Sichere Informations-
Technologie

Ärztliche Verordnungen mit Unterstützung der eGK

GMG §291a:

Die eGK „muss geeignet sein“, Angaben aufzunehmen für

- **die Übermittlung ärztlicher Verordnungen in elektronischer und maschinell verwertbarer Form“**

Zugriffsberechtigt sind:

a) Ärzte,

b) Zahnärzte,

c) Apotheker,

d) sonstiges Personal

e) sonstige Erbringer ärztlich verordneter Leistungen,

Fraunhofer SIT Institut Sichere Informations-Technologie

Einwilligung

GMG §291a:

Mit dem Erheben, Verarbeiten und Nutzen von Daten des Versicherten darf erst begonnen werden, wenn der Versicherte jeweils gegenüber dem Arzt, Zahnarzt oder Apotheker dazu seine Einwilligung erklärt hat. Die Einwilligung ist bei erster Verwendung der Karte vom Leistungserbringer auf der Karte zu dokumentieren; die Einwilligung ist jederzeit widerruflich und kann auf einzelne Anwendungen beschränkt werden.

Fraunhofer SIT Institut Sichere Informations-Technologie

Protokollierung

GMG §291a:

...durch technische Vorkehrungen ist zu gewährleisten,

dass mindestens die letzten fünfzig Zugriffe auf die Daten

nach Absatz 2 oder Absatz 3 für

Zwecke der Datenschutzkontrolle protokolliert werden.

Fraunhofer SIT Institut Sichere Informations-Technologie

Gesamtkonzept: Datenschutz und Datensicherheit (I)

- Erstellung einer Bedrohungsanalyse
- Erstellung und Abstimmung der aus der Bedrohungsanalyse folgenden Schutzprofile für Teilkomponenten der Telematikinfrastruktur
- Berücksichtigung der Datenschutzanforderungen und Patientenrechte
- Beteiligung von BfD, BSI, Patientenvertretern,...

Fraunhofer SIT Institut Sichere Informations-Technologie

Gesamtkonzept: Datenschutz und Datensicherheit (II)

Es geht um alle Bereiche

- **elektronische Gesundheitskarte eGK**
- **Heilberufeausweis HBA**
- **elektronische Patientenakte ePA**
- **Vernetzung: Connector, Server, Transaktionen,...**

Fraunhofer SIT Institut Sichere Informations-Technologie

Rechtliche Grundlagen

- GMG
- BDSG
- StGB
- Signaturgesetz
- IT-Grundschutzhandbuch
- Common Criteria
- SAGA (eGovernment-Handbuch)
- .....

Fraunhofer SIT Institut Sichere Informations-Technologie

Grundsätzliche Fragen für die technischen Lösungen

- wer darf auf was, wann, wie zugreifen ?, lesen, kopieren, ändern, löschen,.... ?
- was wird wann, durch wen, wo protokolliert ? Zugriffe, Orte, Häufigkeit, Aufbewahrungsdauer ?
- was passiert bei Kartenverlust, Kartenmissbrauch, Technikausfall ?
- Handhabung von Notfalldaten ? (national, international)
- Handhabung der Karte im Prozessablauf ? (ärztliche Praxis, Apotheke, Klinik,...)

Fraunhofer SIT Institut Sichere Informations-Technologie

Freiwillige Anwendungen

1. medizinische Daten, soweit sie für die Notfallversorgung erforderlich sind,

2. Befunden, Diagnosen, Therapieempfehlungen sowie Behandlungsberichte in elektronischer und maschinell verwertbarer Form für eine einrichtungsübergreifende, fallbezogene Kooperation (elektronischer Arztbrief),

3. Daten einer Arzneimitteldokumentation,

4. Daten über Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte sowie Impfungen für eine fall- und einrichtungsübergreifende Dokumentation über den Patienten (elektronische Patientenakte),

5. durch von Versicherten selbst oder für sie zur Verfügung gestellte Daten sowie

6. Daten über in Anspruch genommene Leistungen und deren vorläufige Kosten für die Versicherten (§ 305 Abs. 2).

Archivierungsangaben

Fraunhofer SIT Institut Sichere Informations-Technologie

Datenschutz und Datensicherheit

- Der Bürger und Patient im Mittelpunkt
- Rechtliche Grundlagen, Rahmenbedingungen, Gesamtkonzept
- **Die Kette: Bürger, Patient, Arzt, Apotheker, Klinik,....**
- Die eGK: Daten, Personalisierung, Ausgabe, Zugriffsrechte
- Karten- und Rechtemanagement
- Dezentrale Dienste
- Zentrale Dienste
- Aktuelle Aufgaben in der Spezifikation der Lösungsarchitektur

Fraunhofer SIT
Institut
Sichere Informations-
Technologie

Die elektronische Gesundheitskarte: Ein Paradigmenwechsel

KVK

Wenige Daten

Elektronische Gesundheitskarte eGK

- PIN
- Ausweisfunktion mit Sichtbild
- Signaturfähige Karte
- Anwendungen (eRezept, Notfalldaten, …)
- Datenspeicherung (Notfalldaten, Verweise, …)
- Zuzahlungsstatus
- Patientenfach
- Europäischer Versicherungsausweis
- Interaktion mit HPC (eHBA)

Fraunhofer SIT Institut Sichere Informations-Technologie

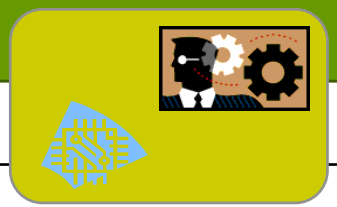
elektronischer Heilberufsausweis: neues Arbeitsmittel der Ärzte

Papierausweis

Keine elektronischen Prozesse

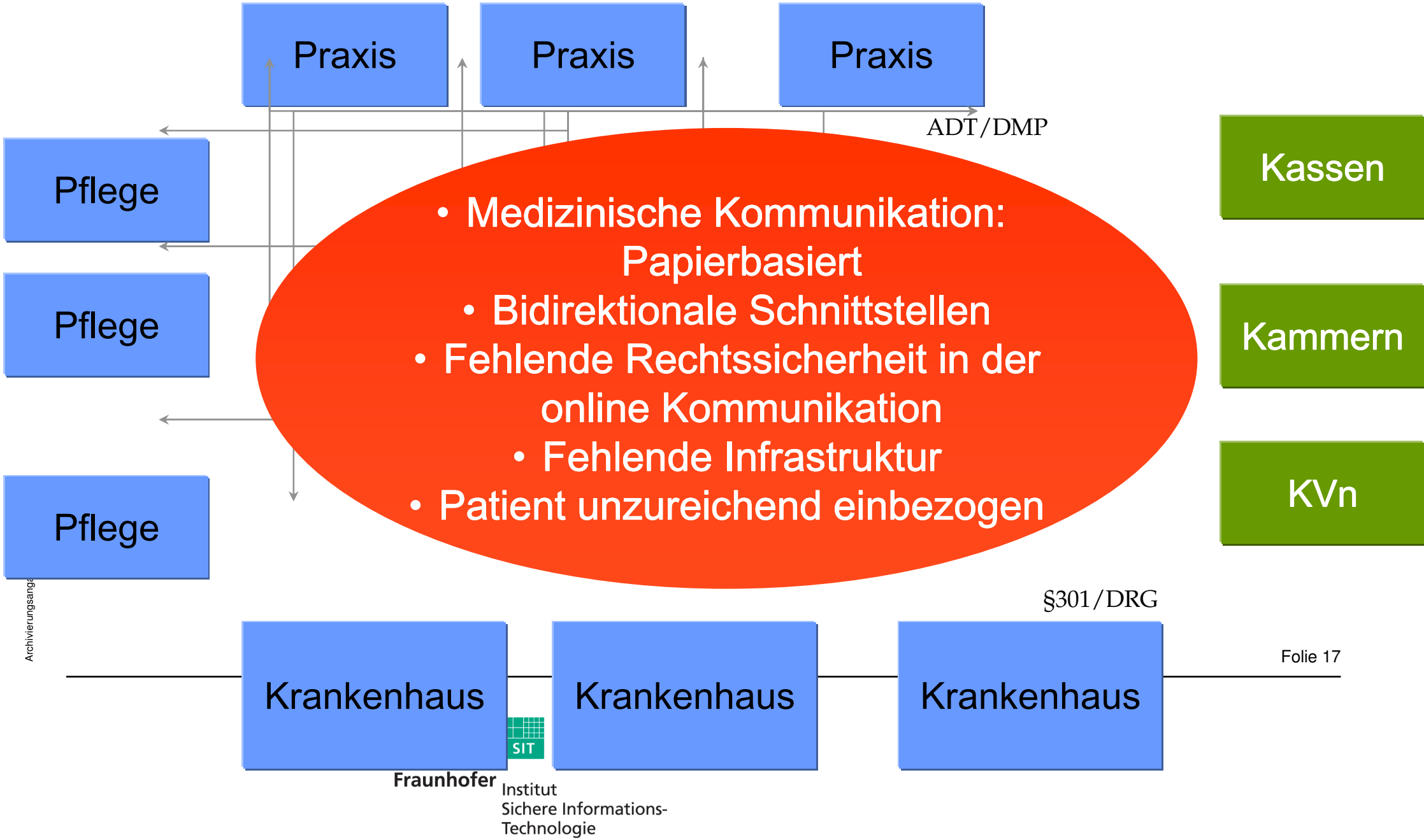
Elektronischer Arztausweis HBA

- PIN
- Ausweisfunktion mit Sichtbild
- Qualifizierte Signatur
- Auslösen rechtsgültiger Prozesse nach Signaturgesetz
- Anwendungen (eRezept, Notfalldaten, …)
- Aufbau sicherer Kanäle zu Zweitkarten (SMC)
- Interaktion mit eGK



Fraunhofer SIT Institut Sichere Informations-Technologie

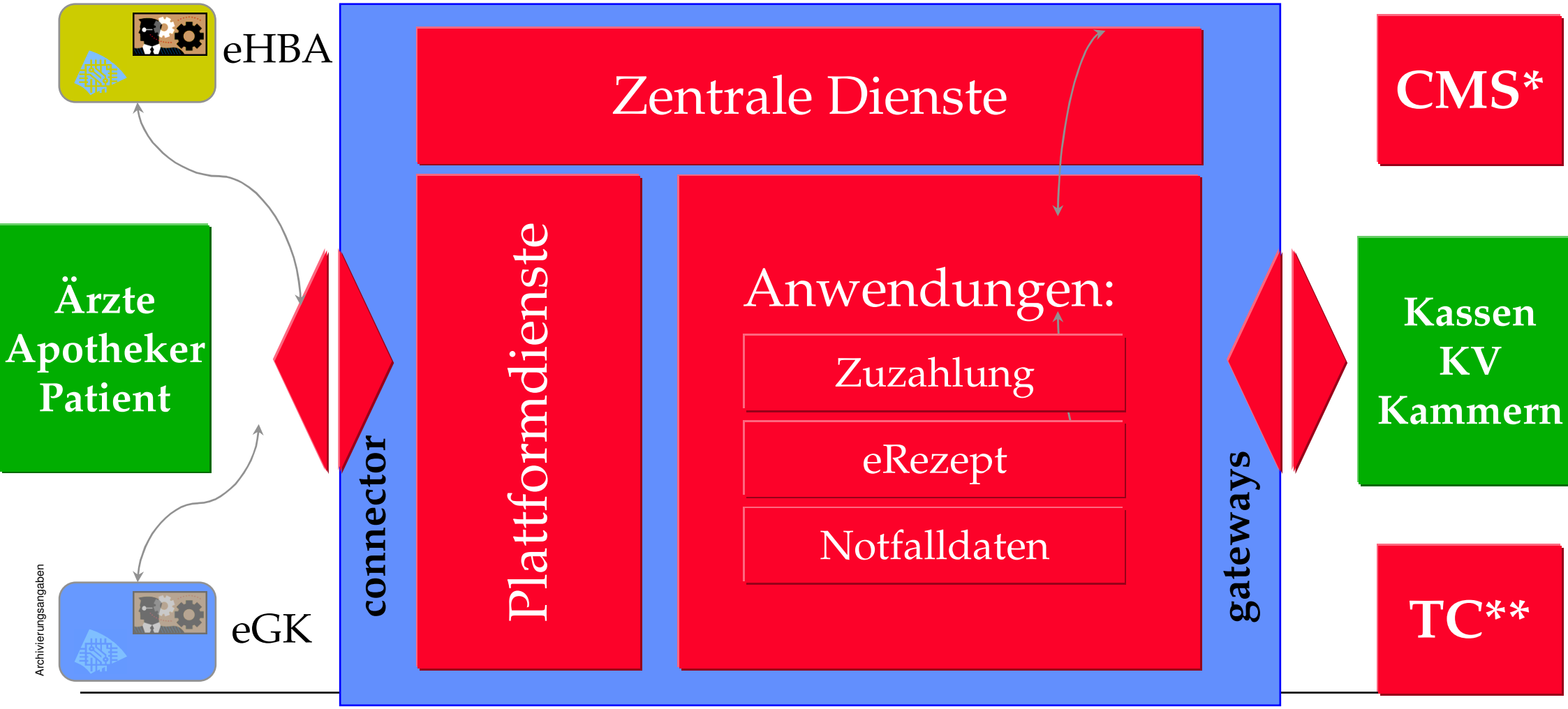
elektronische Kommunikation heute



Archivierungsange

Fraunhofer SIT Institut Sichere Informations-Technologie

einheitliche Infrastruktur: Die Autobahnen der modernen Medizin



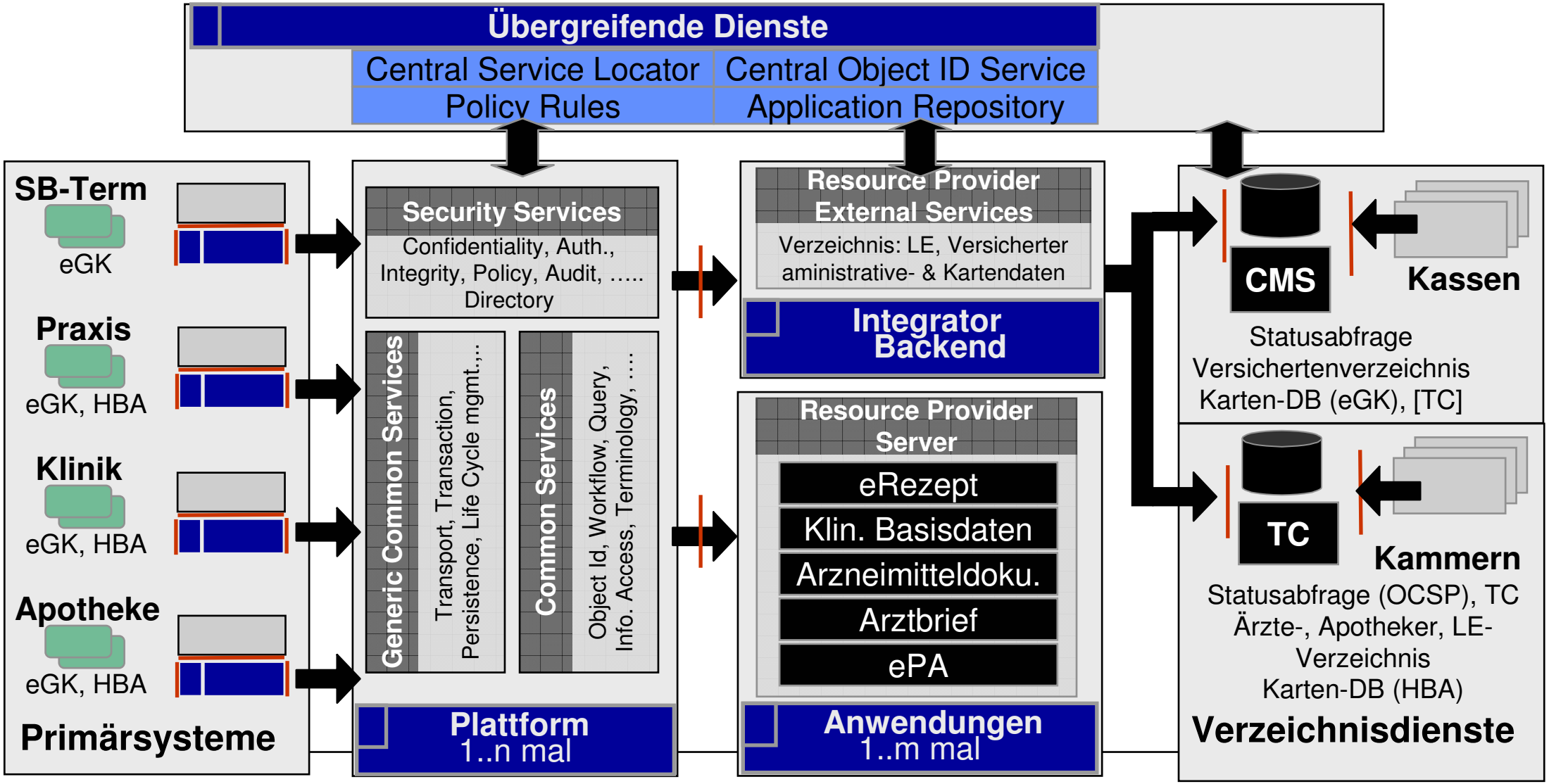
Archivierungsangaben

Fraunhofer SIT Institut Sichere Informations-Technologie

*Card Management System

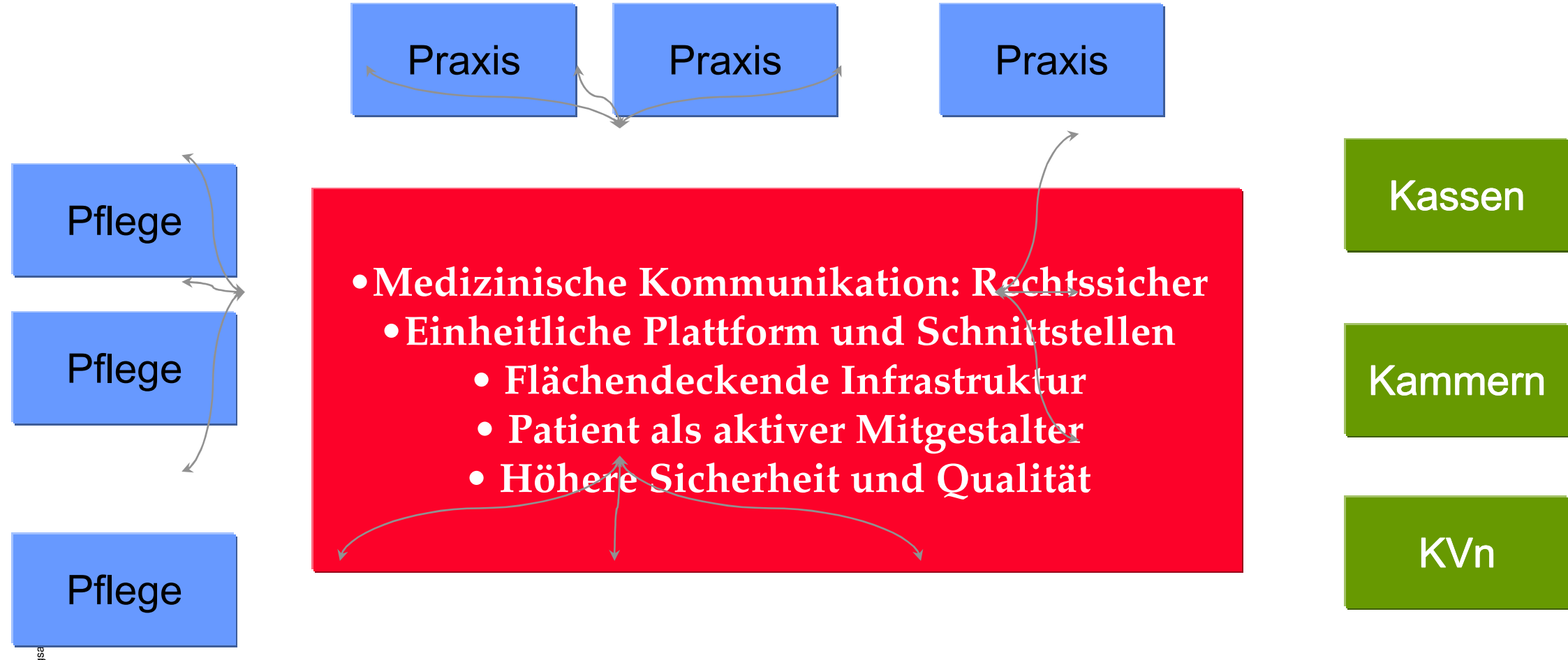
**Trust Center

Lösungsarchitektur: interoperable Telematikinfrastruktur



Fraunhofer SIT Institut Sichere Informations-Technologie

Die Auswirkungen der neuen Infrastruktur

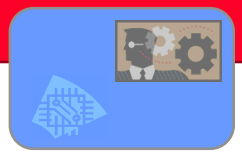


Archivierungsa

Institut
Sichere Informations-
Technologie

Auswirkungen auf die Prozesse im Krankenhaus allgemein

eGK



- Prüfung Zuzahlungsstatus
- Ausstellung eRezept in Ambulanz
- Management der Notfalldaten
- *Ausstellung Arzneimitteldokumentation ambulant und stationär !!*

eHBA

- Personalisierung der Karten
- Realisierung von Ausfallkonzepten (Verlust, Vergessen, Defekte, …)
- Signierung statt Unterschrift

connector

- Integration in IT Infrastruktur
- LDAP Server für Signaturen
- Komplexes Management von allen eGK und eHBA

Auswirkungen auf die medizinischen Prozesse

eRezept

- Signatur der Rezepte durch Ärzte
- Backupprozesse über Papier
- Umstellung der Rezeptausgabeprozesse

Notfalldaten

- Prüfung der Notfalldaten vor Aufnahme auf die Station
- Erstellung oder Pflege der Notfalldaten mit dem Patienten

Arzneimittel-dokumentation

- *Dokumentation der Verordnung auch im stationären Bereich*
- *Prüfung der Historie und erweiterte Kontraindikation durch diese Daten*
- *Signatur der Dokumentation durch den Arzt*

Datenschutz und Datensicherheit

- Der Bürger und Patient im Mittelpunkt
- Rechtliche Grundlagen, Rahmenbedingungen, Gesamtkonzept
- Die Kette: Bürger, Patient, Arzt, Apotheker, Klinik,....
- **Die eGK: Daten, Personalisierung, Ausgabe, Zugriffsrechte**
- Karten- und Rechtemanagement
- Dezentrale Dienste
- Zentrale Dienste
- Aktuelle Aufgaben in der Spezifikation der Lösungsarchitektur

Fraunhofer SIT
Institut
Sichere Informations-
Technologie

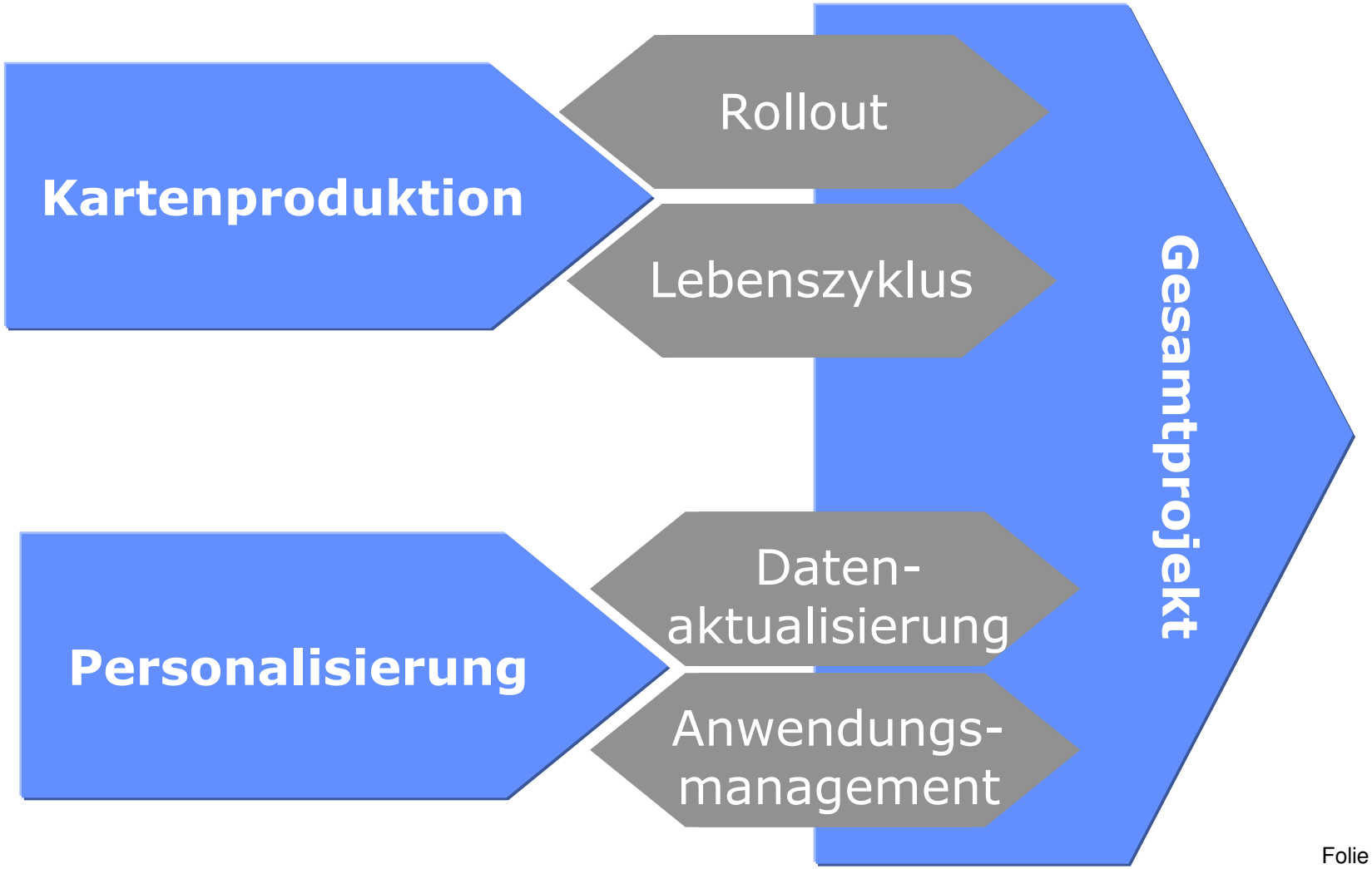
Personalisierung der eGK

- **Herzstück im Rahmen von Produktion und Herausgabe**
- **aktive Rolle und lebende Karte, die**
  - **gepflegt,**
  - **aktualisiert,**
  - **geändert und**
  - **nachstrukturiert werden muss**

Neue Anforderungen an die Einbettung der Personalisierung in der gesamten Prozesskette

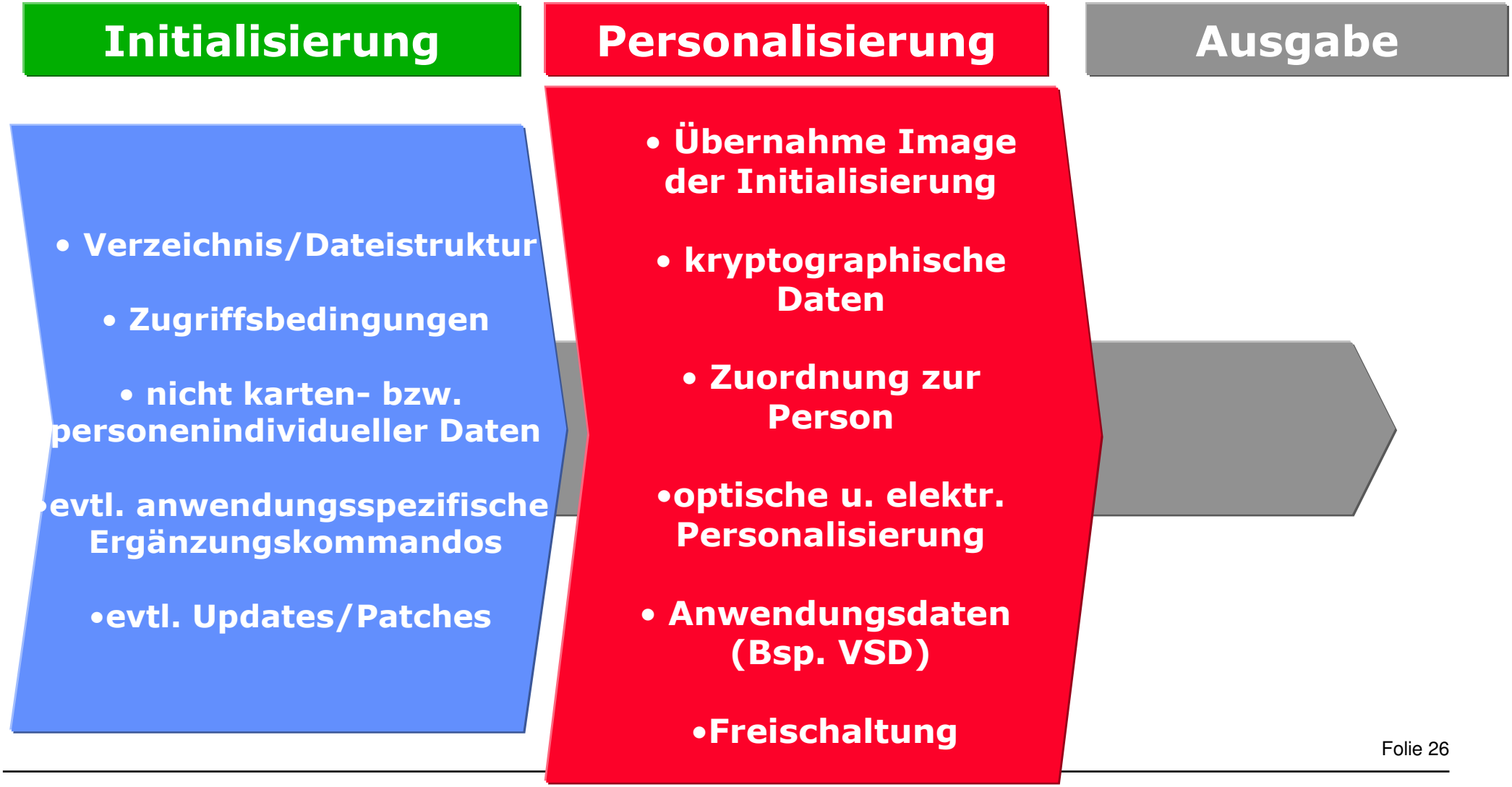
Fraunhofer SIT Institut Sichere Informations-Technologie

Einführung der eGK für alle Versicherten in Deutschland



Fraunhofer Institut
Sichere Informations-
Technologie

Produktion eGK



Fraunhofer Institut Sichere Informations-Technologie

Datenschutz und Datensicherheit

- Der Bürger und Patient im Mittelpunkt
- Rechtliche Grundlagen, Rahmenbedingungen, Gesamtkonzept
- Die Kette: Bürger, Patient, Arzt, Apotheker, Klinik,....
- Die eGK: Daten, Personalisierung, Ausgabe, Zugriffsrechte
- **Karten- und Rechtemanagement**
- Dezentrale Dienste
- Zentrale Dienste
- Aktuelle Aufgaben in der Spezifikation der Lösungsarchitektur

Fraunhofer SIT Institut Sichere Informations-Technologie

Rechte des Versicherten

Der Versicherte hat das Recht, Daten seiner eGK (z.B. Rezepte) zu verbergen.

Das kann z.B. über eService-Terminals geschehen.

Beispiel eines eService-Terminals mit Sicherheitsmodul SMC.X (Security Condition für Read Access zu Files mit medizinischen Daten z.B. EXT AUTH with SMC.X AND PIN.Cardholder)

Fraunhofer Institut Sichere Informations-Technologie

Patienten-Rechte-Management

- **Patient geht zu einem Touchscreen-PC (Aufstellungsort = überwachte Umgebungen z.B. Arztpraxis, Apotheke) und steckt eGK in das Kartenterminal („eKiosk“)**
- **Patient gibt seine PIN.HCA (Health Care Application PIN) ein**
- **Es findet eine Authentisierungsprozedur zwischen eGK und SMC.eKiosk statt**
- **Patient kann sich bestimmte Inhalte anschauen und Zugriffsrechte auf medizinische Datenobjekte verändern (Activate/Deactivate)**
- **Hinweis: Um Erpressbarkeit des Karteninhabers auszuschliessen (Gewalt in der Familie, Offenlegung medizinischer Daten bei Abschluss von Lebensversicherungen oder Einstellung bei Arbeitgeber, …) sollte Rechte-Management nur an speziellen Terminals mit SMC.eKiosk in überwachten Umgebungen möglich sein**

Fraunhofer SIT Institut Sichere Informations-Technologie

mögliche Abläufe in der Arztpraxis (1)

- Patient betritt Arztpraxis und meldet sich am Empfang
- Der Patient übergibt eGK und Arzthelferin prüft, ob Foto zum Patienten paßt
- Arzthelferin steckt Karte in Kartenterminal
- Versichertendaten werden aus eGK ausgelesen
- Prüfung durch Arztpraxis-Sytem in Verbindung mit KK-Datenbank, ob Versichertenverhältnis noch ok (falls Karteninhaber noch versichert und Zuzahlungsstatus stimmt: weiter, sonst Update mit SMC.KK initiieren)
- eGK wird auf Echtheit durch Security Module Card (SMC.Arztpraxis) geprüft (die SMC ist praktisch die Plug-in-Ausprägung eines Heilberufsausweises und wird durch eine PIN aktiviert)
- eGK prüft SMC.Arztpraxis und setzt Status „Certificate Holder Authorization of SMC.Arztpraxis successfully presented“

mögliche Abläufe in der Arztpraxis (2)

- **Arztpraxis-Software sucht elektronische Patientenakte in lokaler Arztpraxis-Datenbank**
- **Übernahme aller Daten, auf die die betreffende eGK Zugriff gewährt, z.B. Arzneimitteldokumentation (medizinische Daten nicht für Arzthelferin sichtbar), in das Primärsystem. Weitere Verwendung z.B. Ablage in Patientenakte**
- **Logging-Datensatz wird geschrieben (hier ist zu prüfen, ob es nicht ausreicht, einen Logging-Satz pro Arztbesuch bzw. pro „Card-Session“ zu erstellen)**
- **eGK wird aus Kartenterminal herausgenommen und verbleibt beim Empfang oder wird an Patient zurückgegeben**
- **Patient geht ins Wartezimmer und wird dann später gebeten, sich in den Behandlungsraum X zu begeben**
- **Im Behandlungsraum X ist ein PC, der gesperrt und dessen Bildschirm dunkel geschaltet ist, damit der Patient nicht unbefugt sich Zugang verschaffen kann**

Fraunhofer SIT Institut Sichere Informations-Technologie

mögliche Abläufe in der Arztpraxis (3)

- Der Arzt aktiviert PC (z.B. durch Präsentation eines Fingers am Kartenterminal im Behandlungsraum)
- Auf dem Bildschirm erscheint die elektronische Patientenakte des Patienten, die ihm durch die Arzthelferin bereitgestellt wurde (bei der SIT-Sichtweise sind Kartenterminals für die Nutzung der eGK in den Behandlungsräumen nicht zwingend erforderlich, d.h. der Arzt kann von dem ganzen eGK-Handling weitgehend entlastet werden!)
- Arzt führt Behandlung durch
- Arzt erstellt z.B. elektronischen Notfalldatensatz aus und signiert diesen mit seiner HPC (Notfalldatensatz wird in elektronische Patientenakte eingetragen, aber noch nicht in eGK)
- Arzt stellt nun ein eRezept aus (automatische Prüfung der Verträglichkeit der Medikamente mit Hilfe der im Primärsystem verfügbaren Infos zu bisheriger Medikation und patientenindividuellen Risiken) und signiert es
- Signiertes Rezept wird in elektronische Patientenakte eingetragen, aber noch nicht in eGK

Fraunhofer SIT Institut Sichere Informations-Technologie

mögliche Abläufe in der Arztpraxis (4)

- Arzt verabschiedet Patient, der sich zum Empfang begibt
- Arzthelferin steckt eGK wieder ins Kartenterminal
- Nach gegenseitiger Authentisierung zwischen eGK und SMC.Arztpraxis erscheint administrativer Teil der elektronischen Patientenakte des Patienten (damit Sicherstellung der Eintragung der richtigen Daten in die richtige eGK)
- Notfalldatensatz und elektronisches Rezept werden in die eGK eingetragen
- Logging-Datensatz wird geschrieben
- Die Rezept-Begleit-Info wird ausgedruckt und zusammen mit der eGK dem Patienten übergeben
- Patient verläßt Arztpraxis und begibt sich üblicherweise direkt zur Apotheke und löst Rezept ein.

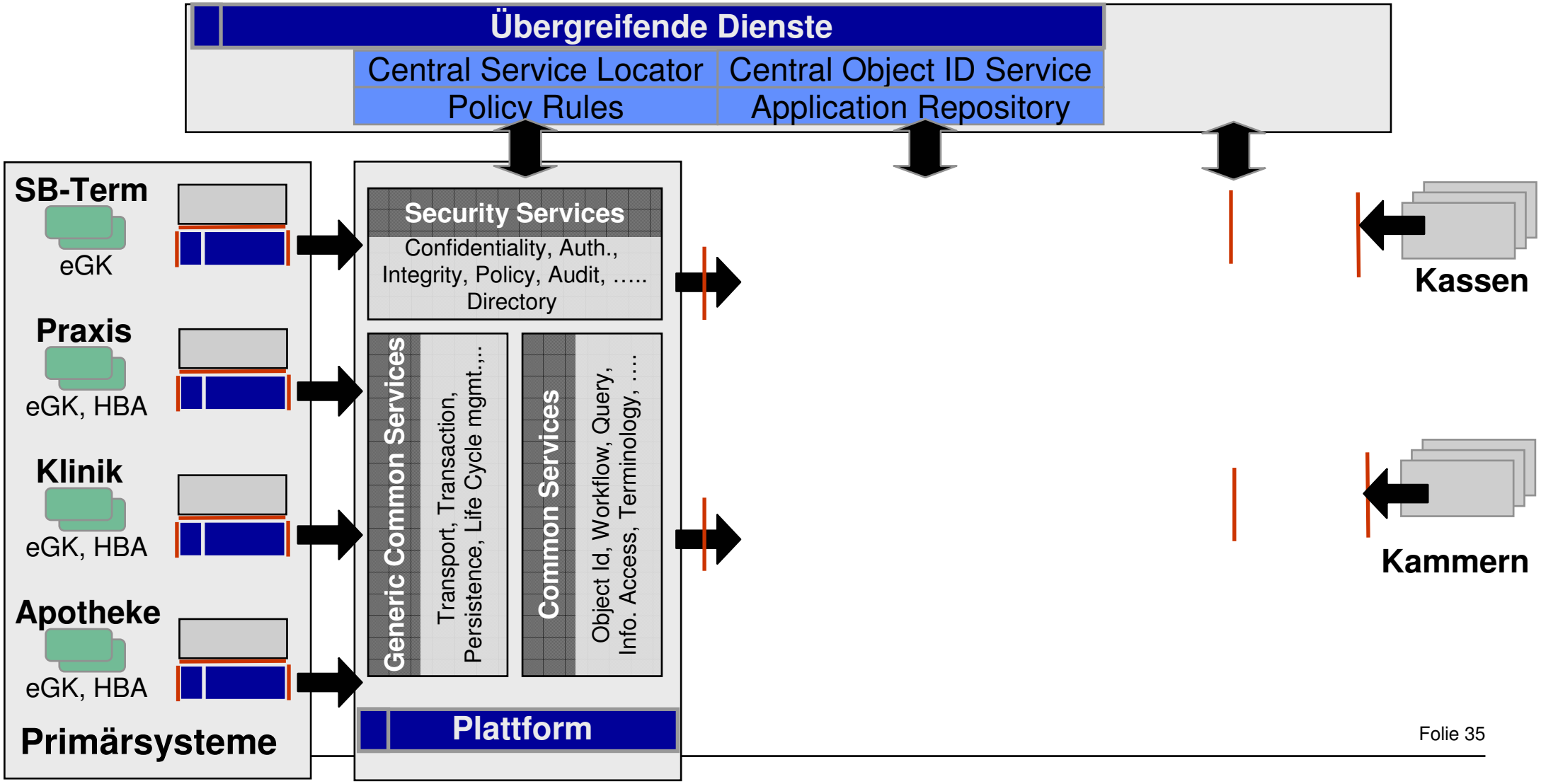
Fraunhofer SIT Institut Sichere Informations-Technologie

Datenschutz und Datensicherheit

- Der Bürger und Patient im Mittelpunkt
- Rechtliche Grundlagen, Rahmenbedingungen, Gesamtkonzept
- Die Kette: Bürger, Patient, Arzt, Apotheker, Klinik,....
- Die eGK: Daten, Personalisierung, Ausgabe, Zugriffsrechte
- Karten- und Rechtemanagement
- **Dezentrale Dienste**
- Zentrale Dienste
- Aktuelle Aufgaben in der Spezifikation der Lösungsarchitektur

Fraunhofer SIT Institut Sichere Informations-Technologie

Die Lösungsarchitektur für eine interoperable Telematikinfrastruktur



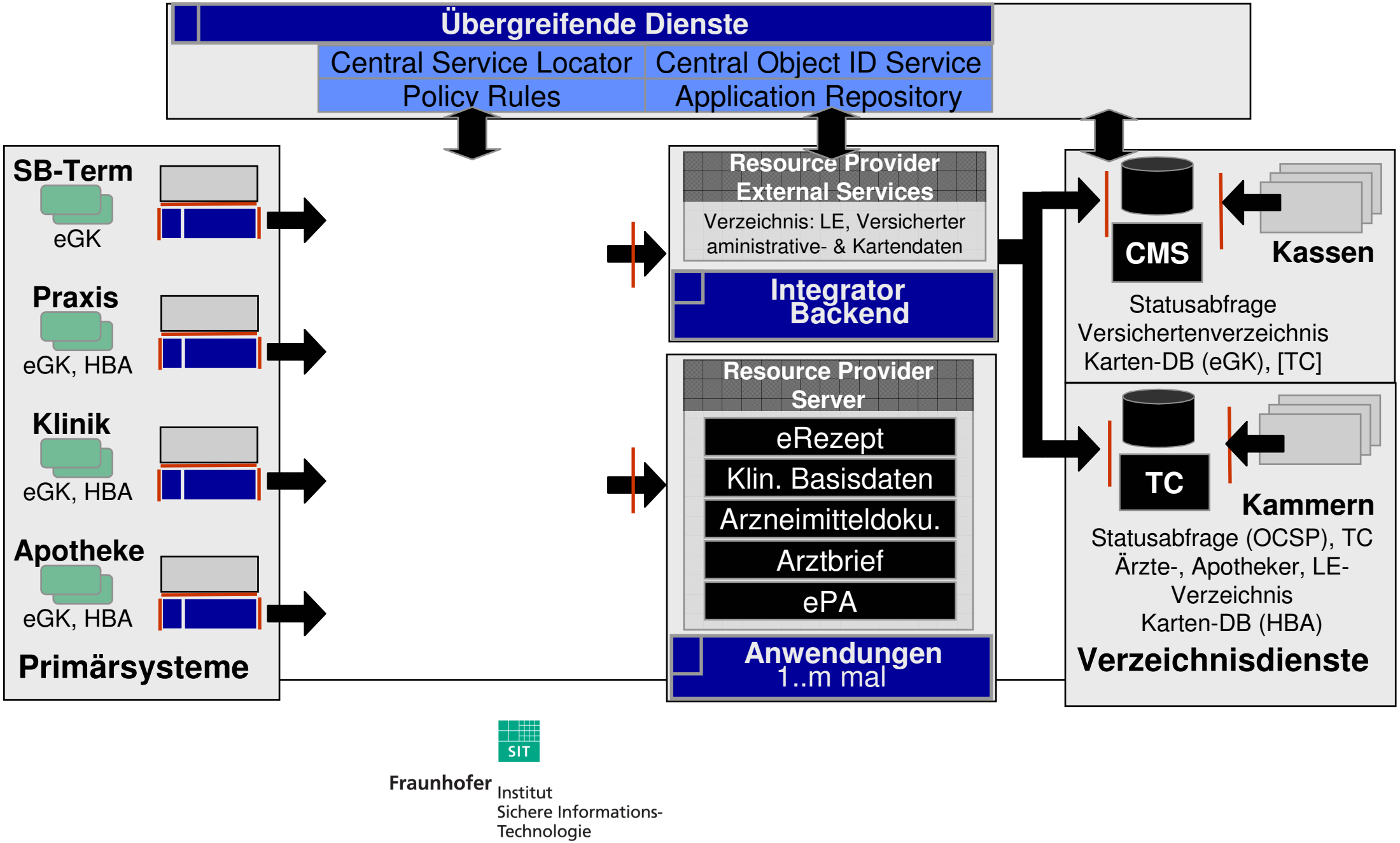
Fraunhofer Institut Sichere Informations-Technologie

Datenschutz und Datensicherheit

- Der Bürger und Patient im Mittelpunkt
- Rechtliche Grundlagen, Rahmenbedingungen, Gesamtkonzept
- Die Kette: Bürger, Patient, Arzt, Apotheker, Klinik,....
- Die eGK: Daten, Personalisierung, Ausgabe, Zugriffsrechte
- Karten- und Rechtemanagement
- Dezentrale Dienste
- **Zentrale Dienste**
- Aktuelle Aufgaben in der Spezifikation der Lösungsarchitektur

Fraunhofer SIT Institut Sichere Informations-Technologie

Die Lösungsarchitektur für eine interoperable Telematikinfrastruktur



Fraunhofer SIT Institut Sichere Informations-Technologie

Datenschutz und Datensicherheit

- Der Bürger und Patient im Mittelpunkt
- Rechtliche Grundlagen, Rahmenbedingungen, Gesamtkonzept
- Die Kette: Bürger, Patient, Arzt, Apotheker, Klinik,....
- Die eGK: Daten, Personalisierung, Ausgabe, Zugriffsrechte
- Karten- und Rechtemanagement
- Dezentrale Dienste
- Zentrale Dienste
- **Aktuelle Aufgaben in der Spezifikation der Lösungsarchitektur**

Fraunhofer SIT
Institut
Sichere Informations-
Technologie

Fachanwendungen

Konkrete IT Spezifikation der Fachanwendungen mit speziellen Fokus auf Versichertenstammdaten, eRezept, eVerordnung und Zugriffsrechte

- **Auf Basis der fachlichen Geschäftsprozessdefinition und des fachlichen Informationsmodells werden die IT Spezifikationen für die Fachanwendungen erstellt**

- **Ergebnisse:**
  - **Detaillierte Beschreibung der relevanten Use Cases (Sequenzdiagramme) undFestlegung der Fehlerfälle**
  - **Festlegung der Testfälle und des Testplans**
  - **Detaillierte Beschreibung der Sicherheitsmechanismen**

Fraunhofer SIT Institut Sichere Informations-Technologie

Connector Primärsysteme

Spezifikation des Connectors mit speziellen Fokus auf

- **Komponenten des Connectors**
- **Sicherheitsanforderungen und nicht funktionale Anforderungen**
- **Testplan und Zertifizierungsplan (Einbindung der CC)**
- **Abstimmung der Dienstschnittstellen zu Primärsystemen, Systemmanagementschnittstelle und Schnittstelle zu zentralen Diensten**
- **konkrete Spezifikation des Karten-API (KT-API)**

Fraunhofer Institut Sichere Informations-Technologie

Kartenterminal

Spezifikation des Kartenterminals mit speziellen Fokus auf

- **Komponenten (PIN-Pad, Netzanbindung, ...)**
- **Sicherheitsanforderungen und nicht funktionale Anforderungen**
- **Testplan und Zertifizierungsplan (Einbindung der CC)**
- **Abstimmung der Dienstschnittstelle zu Connector**

Fraunhofer SIT Institut Sichere Informations-Technologie

Kartenspezifikation HBA

- **Enge Zusammenarbeit und Abstimmung mit Datenschutz und Datensicherheit**

- **Ergebnisse:**
  - **Sicherheitsniveau**
  - **Schutzprofile**

Fraunhofer SIT Institut Sichere Informations-Technologie

Sicherheitsdienste, Verzeichnisdienste und -komponenten

- **Festlegung Definition, Abstimmung und Beschreibung der übergeordneten organisatorischen, rechtlichen und technischen Strukturen einer PKI im Gesundheitswesen. Festlegung der übergeordneten PKI Policies im Gesundheitswesen sowie der Zertifikatsprofile und CPS der PKI im Gesundheitswesen**

- **Security Server und Key Management: Detaillierte Beschreibung der Funktionalitäten sowie des Verhaltens der zentralen und dezentralen Sicherheitsdienste basierend auf dem Fachkonzept zur Virtuellen Poststelle. Detaillierte Beschreibung der XML Schnittstelle zum Aufruf der zentralen Sicherheitsdienste basierend auf der XML Schnittstellenspezifikation der Virtuellen Poststelle**

- **Zentrale Verzeichnisdienste: Makrodesign und Mikrodesign der Schnittstellen zu Verzeichnisdiensten**

- **Audit: Komponenten und Schnittstellen zur Nachweisbarkeit der auf Karte oder Server durchgeführten relevanten Aktionen**

Fraunhofer Institut Sichere Informations-Technologie

Fazit:

Datenschutz und Datensicherheit

sind technisch machbar

Die Handhabbarkeit ist der Schlüssel zur Akzeptanz

Fraunhofer Institut
Sichere Informations-
Technologie