Online-Texte der Evangelischen Akademie Bad Boll

eGesundheitskarte

Telematik und Sicherheit im Gesundheitswesen

Prof. Dr. Hartmut Pohl

Ein Beitrag aus der Tagung:

Die neue Gesundheitskarte

Bad Boll, 14. - 15. Januar 2006, Tagungsnummer: 410906

Tagungsleitung: Dr. Günter Renz, Prof. Dr. Friedrich-Wilhelm Kolkmann

---

Evangelische Akademie Bad Boll
Akademieweg 11, D-73087 Bad Boll
E-Mail: info@ev-akademie-boll.de
Internet: www.ev-akademie-boll.de

Telematik und Sicherheit im Gesundheitswesen

eGesundheitskarte

Evangelische Akademie Bad Boll 14. Januar 2006

Prof. Dr. Hartmut Pohl
Fachhochschule Bonn-Rhein-Sieg ◆ *ISIS* – InStitut für InformationsSicherheit, Köln

Unsicherheit der eGesundheitskarte

Prof. Dr. Hartmut Pohl
Fachhochschule Bonn-Rhein-Sieg ◆ *ISIS* – InStitut für InformationsSicherheit, Köln

Illusion !

Integrität?
Vertraulichkeit?
Verfügbarkeit?
Verbindlichkeit?

Internet!

'Während ich heute meinen **Glückwunsch** zum 8. Geburtstag meines Enkels der **E-Mail** anvertraute und **sicher** sein konnte, dass er **keine Probleme** hat, sie im **Empfang** zu nehmen, haben gleichzeitig Tausende Arzthelferinnen und Sekretärinnen **ärztliche Befundberichte** nach Diktat ihrer Chefs zu **Papier** gebracht und im günstigen Fall per **Telefax** weitergeleitet, im weniger günstigen aber kuvertiert, mit einer Briefmarke zu 55 Cent versehen und der guten alten **Post** anvertraut ... '

Wert, Bedeutung?

Direktverbindung – Internet!?

Post-Ident?

K. H. Schriefers, Koblenz, Mitglied der Chefredaktion 'Arzt und Krankenhaus', Editorial 6/2005

Mitglieder
Bürger
Presse
Über uns
Service
Kontakt

Suche nach Ärzten/ Psychotherapeuten

KVNO aktuell

Druckversion
Sitemap
Suche

Go

Home > Infos für Journalisten > Meldungen >

Kooperation in Sachen Telematik: "KV-Safenet" entlastet Ärzte und schafft Sicherheit für Patienten

Berlin, 2.3.2005 – Die Kassenärztlichen Vereinigungen (KVen) wollen auf dem Gebiet der Telematik auch im Hinblick auf die Einführung der elektronischen Gesundheitskarte enger zusammenarbeiten. So haben sich die KV Nordrhein, die KV Westfalen-Lippe und die KV Bayerns kürzlich in Berlin gemeinsam auf Grundsätze geeinigt, wie Arztpraxen einheitlich elektronisch eingebunden werden können, damit ein bundesweiter Datenaustausch möglich ist.

Eine Rahmenrichtlinie stellt sicher, dass nur diejenigen Netzdienstleister ein Zertifikat der KVen erhalten, welche den hohen Anforderungen an Sicherheit und Service genügen. Das Zertifikat berechtigt die Anbieter, so genannte „KV-Safenet-Anschlüsse" zu vertreiben, und wird von den beteiligten KVen gegenseitig anerkannt.

Das KV-Safenet selbst gewährleistet die völlige Sicherheit der Praxisdaten und verbindet die Praxisrechner der teilnehmenden Ärzte mit einer Datenstelle, in der die Daten verwaltet und ausgewertet werden. Ein Zugriff von außen ist ausgeschlossen, sodass die Daten nicht nur während der Übertragung vor Angriffen von Hackern geschützt sind, sondern auch auf den angeschlossenen Computern der Ärzte. Praxis-PCs können bedenkenlos an das Netz angeschlossen werden. KV-Safenet ist mit nahezu sämtlichen Betriebssystemen verwendbar. Der Zugang kann installiert werden, ohne dass die Stabilität der Praxissoftware beeinträchtigt oder gefährdet wird.

Ein Zugriff von außen ist ausgeschlossen

Dazu Dr. Leonhard Hansen, Vorstandsvorsitzender der KV Nordrhein: „Diese Telematiklösung ist ein echter, innovativer Entwicklungsschritt, der Ärzten die Verwaltungsarbeit und Patientenversorgung erheblich erleichtert." Sein Vorstandskollege von der KV Westfalen-Lippe, Dr. Ulrich Thamer, ergänzt: „Dass drei der großen KVen an einem Strang ziehen, ist hoffentlich auch ein Signal an die anderen KVen, sich zu beteiligen. Denn bei den Herausforderungen in der

EXIT **Mehr Infos zur KV Westfalen-Lippe**

Kooperation in Sachen Telematik: "KV-Safenet" entlastet Ärzte und schafft Sicherheit für Patienten

Berlin, 2.3.2005 – Die Kassenärztlichen Vereinigungen (KVen) wollen auf dem Gebiet der Telematik auch im Hinblick auf die Einführung der elektronischen Gesundheitskarte enger zusammenarbeiten. So haben sich die KV Nordrhein, die KV Westfalen-Lippe und die KV Bayerns kürzlich in Berlin gemeinsam auf Grundsätze geeinigt, wie Arztpraxen einheitlich elektronisch eingebunden werden können, damit ein bundesweiter Datenaustausch möglich ist.

Eine Rahmenrichtlinie stellt sicher, dass nur diejenigen Netzdienstleister ein Zertifikat der KVen erhalten, welche den hohen Anforderungen an Sicherheit und Service genügen. Das Zertifikat berechtigt die Anbieter, so genannte „KV-Safenet-Anschlüsse" zu vertreiben, und wird von den beteiligten KVen gegenseitig anerkannt.

Das KV-Safenet selbst gewährleistet die völlige Sicherheit der Praxisdaten und verbindet die Praxisrechner der teilnehmenden Ärzte mit einer Datenstelle, in der die Daten verwaltet und ausgewertet werden. Ein Zugriff von außen ist ausgeschlossen, sodass die Daten nicht nur während der Übertragung vor Angriffen von Hackern geschützt sind, sondern auch auf den angeschlossenen Computern der Ärzte. Praxis-PCs können bedenkenlos an das Netz angeschlossen werden. KV-Safenet ist mit nahezu sämtlichen Betriebssystemen verwendbar. Der Zugang kann installiert werden, ohne dass die Stabilität der Praxissoftware beeinträchtigt oder gefährdet wird.

Ein Zugriff von außen ist ausgeschlossen

1. Regel

Die Politik will Ergebnisse

dementsprechend ist die Wortwahl.

Jede neue Technik birgt Chancen und Risiken. Risiken werden verschwiegen

...

Technik und Sicherheit der eGesundheitskarte

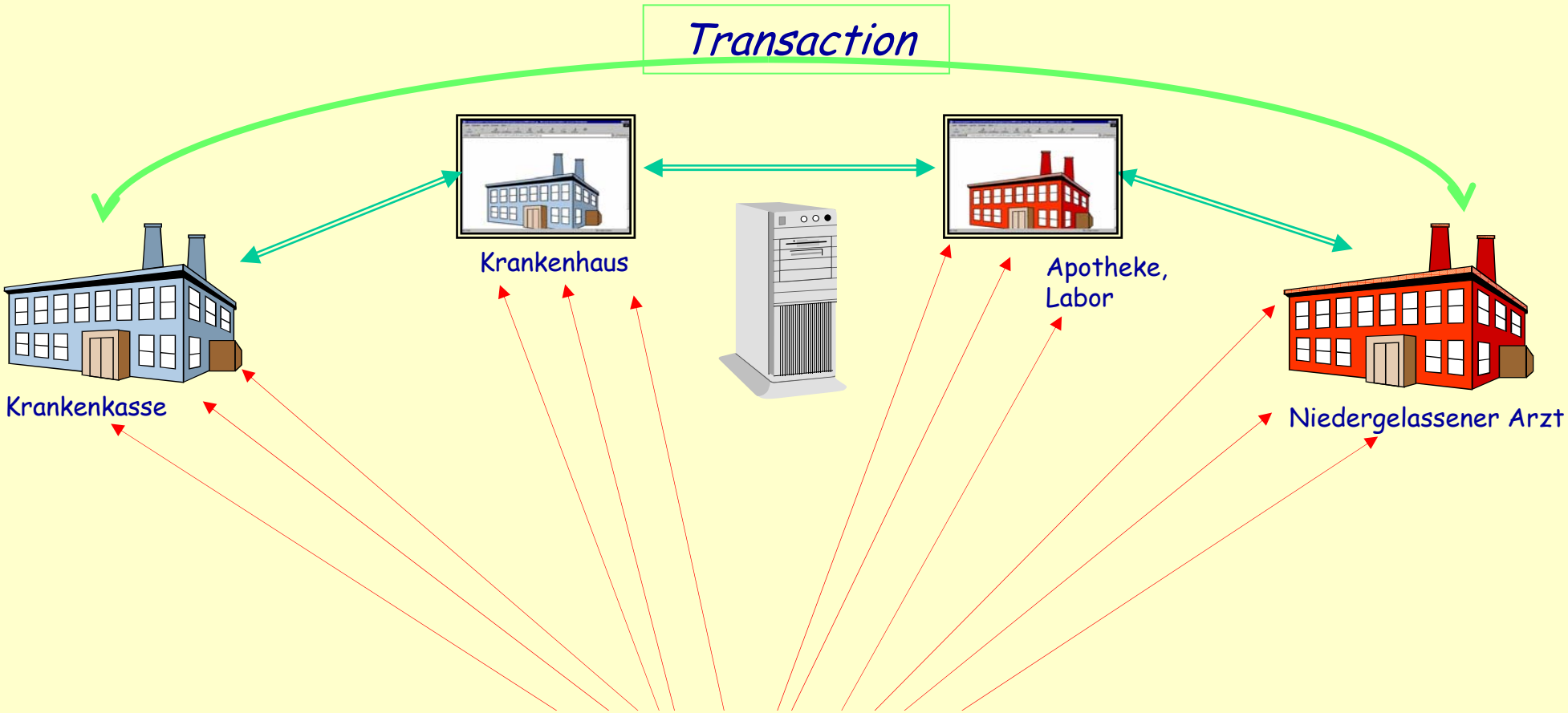
1. Illusion oder Wirklichkeit:
   Technik der Gesundheits-Telematik
   Wo werden *meine* Daten gespeichert?
   Angriffe, Risiken, Haftung

2. Nicht behebbare strategische Fehler

3. Kosten: Patient, Arzt

4. Zusammenfassende Forderungen

Internet Security

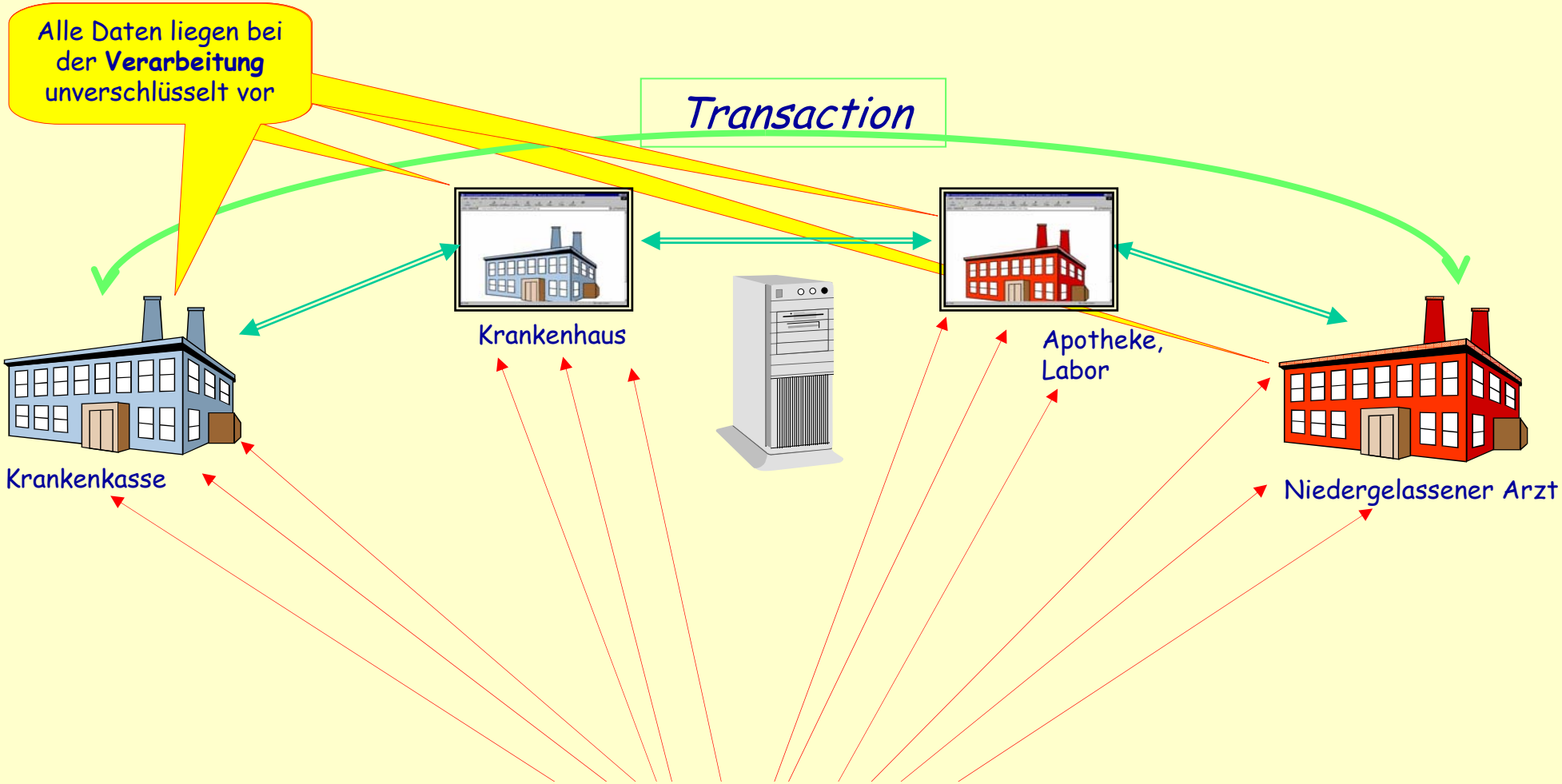


Attacks

Espionage, Sabotage

Masquerading, Eavesdropping,
Manipulation, Denial of Service

Internet Security

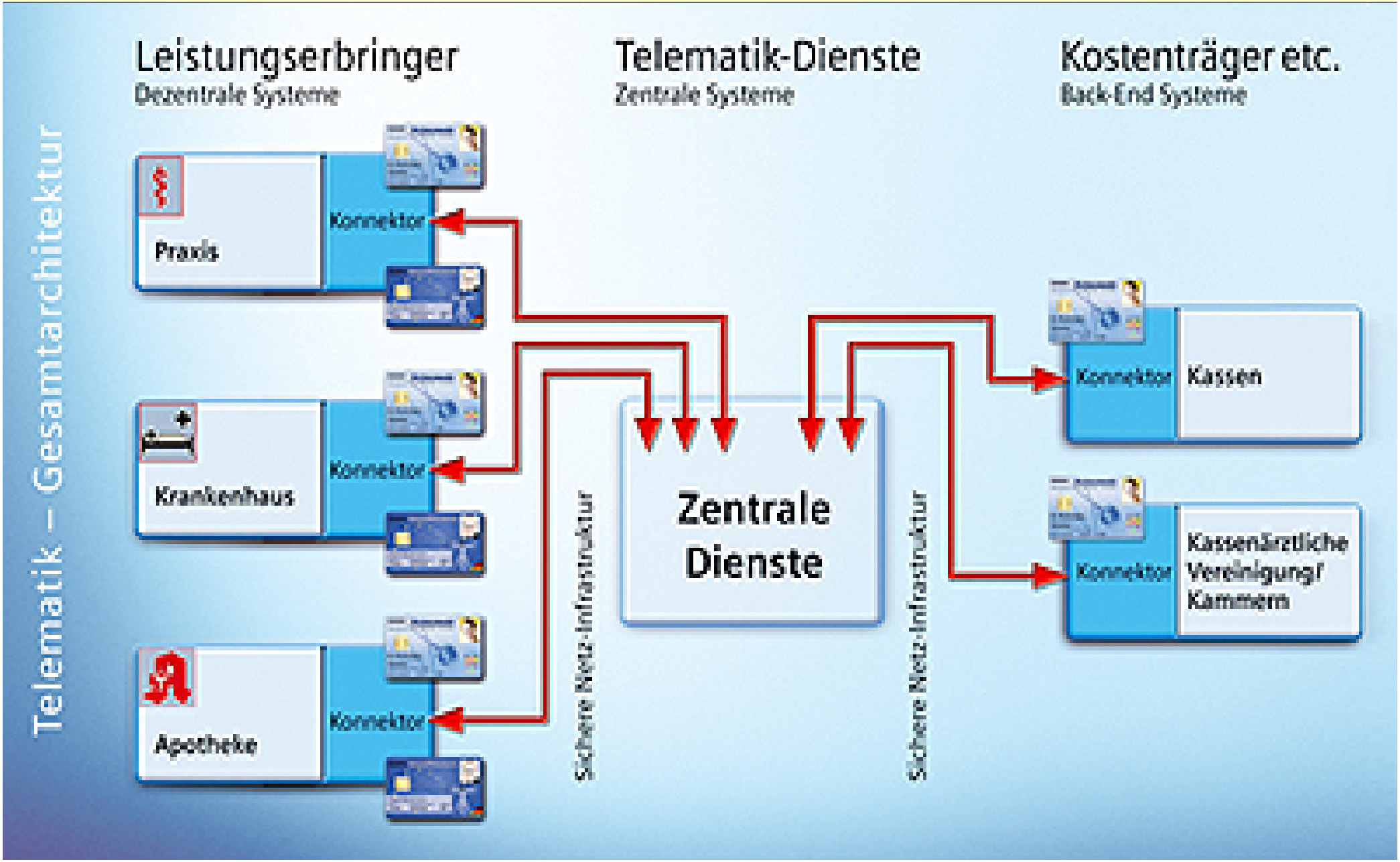


Attacks

Espionage, Sabotage

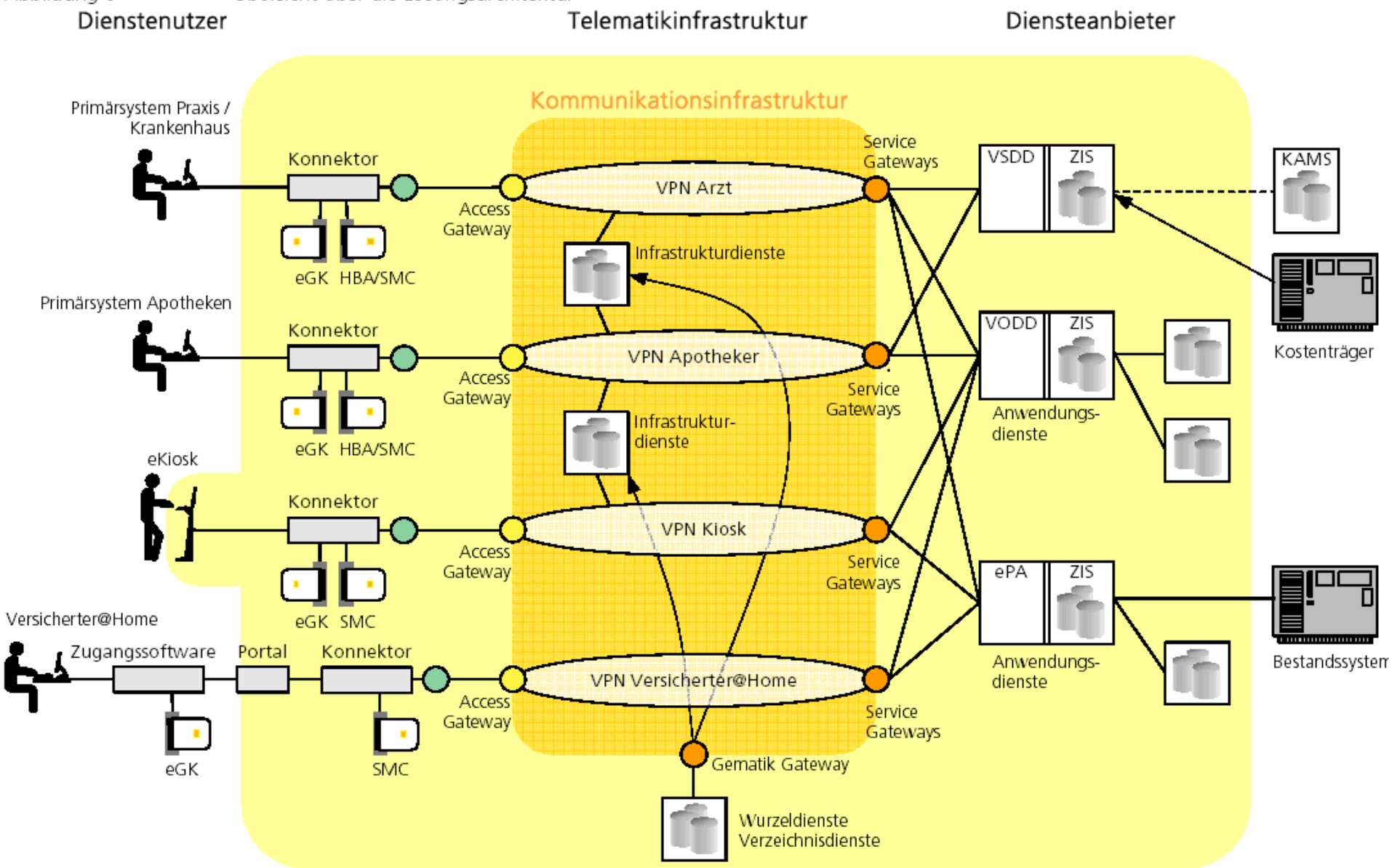
Masquerading, Eavesdropping, Manipulation, Denial of Service

Telematik Gesamtarchitektur



Telematik Gesamtarchitektur

Abbildung 6 Übersicht über die Lösungsarchitektur



Alles graue Theorie!?

Wo soll hier was passieren?

Apotheken-CD

- Kopien aller Rezepte: Rezeptrecherche
- Versicherten-Datenbank:
  Krankenversichertennummer, Verordnungsvolumen, Medikamentenlisten
- Ärzte-Datenbank (Arztnummer und Verordnungen):
  Auswertung des individuellen Verschreibungsverhaltens: Pharmazeutische Beratung

2. Regel

Keine Dezentralität im Internet

Clients, Workstations, Server, Peers, ... überall auf der Welt, im Flugzeug ...

Papierakten waren dezentral

Funktionsweise der Gesundheitstelematik

- eGesundheitskarte
  Name etc., Rezept, Identifizierung/Authentifizierung
- Health Professional Card
  Arzt, Apotheker, Heilpraktiker, Masseur, Helferin, ...
- Stammdatensatz

Inhalte der Karte Einführung bis 2010

PIN

Verschlüsselung

Versichertendaten

Zuzahlungsdaten

Rezept

Notfalldaten***

Doku Arzneien

Behandlungen/Brief

Patientenakte

Patientenfach*

**

* Eigentümer kann nur auf die Daten des Patientenfachs zugreifen!
Alle anderen Daten sind nur mit HPC zugreifbar.

** Derzeit noch freiwillig

*** Blutgruppe, chronische Erkrankungen, Implantate, Allergien/Unverträglichkeiten

Falsche Begriffe

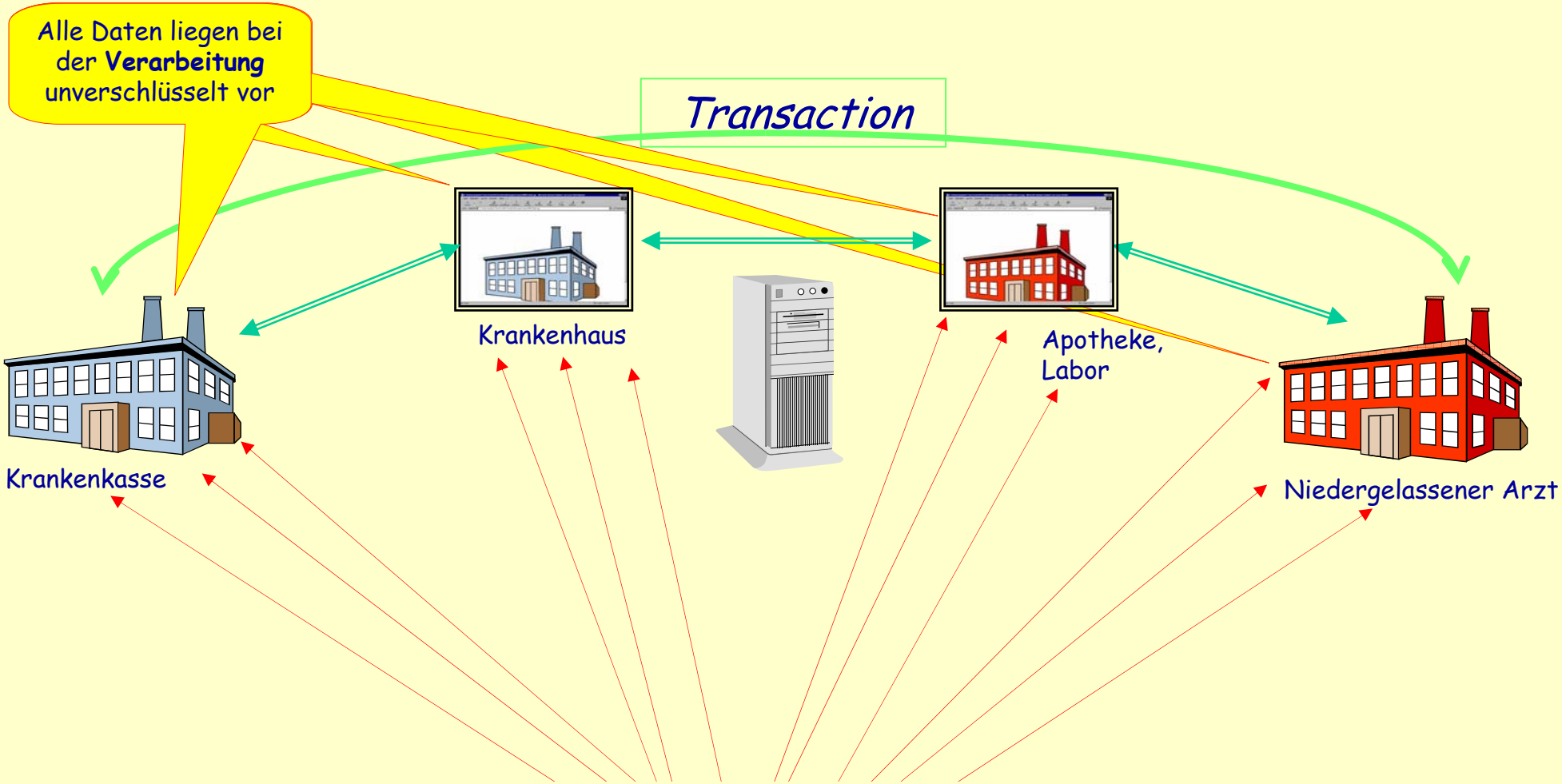
- Sicherheit: Relative Sicherheit, nicht 100% !
- Mißbrauch: Erschwerung – nicht Vermeidung!
  Verordnungsmißbrauch: Foto auf der eGesundheitskarte
  Hauptanteil (!) der Einsparungen von 1.7 Mrd. €
- ...

Herausforderungen

- Medienbrüche ←→ Protokollierung, (vollständige) Speicherung
  eRezept
- Bürokratie ←→ eArztbrief: Austausch digitaler Dokumente
  Kasse, (andere) Ärzte, ...

  Patientenakte: Vollständigkeit! Internet!
  Symptome, Untersuchungen, Ergebnisse,
  Erkrankungen, Therapien, ...
- Forschung ←→ Anonymisierte Daten???

Internet Security



Attacks

Espionage, Sabotage

Masquerading, Eavesdropping, Manipulation, Denial of Service

3. Regel

Das Internet vergisst nicht

Google, ... Archive, Protokollierung, Back-up,
Mails (Yahoo, GMX, ...), VoIP ...

Wertvolle, schutzwürdige Daten? Vollständige Patientenakten, Rezepte, ...

13 Schritte zum Rezept

Handhabung durch Health Professionals

Beispiel Rezeptausstellung

1. Patient stellt eGesundheitskarte (eGK) zur Verfügung
2. Patient schaltet eGK mit PIN frei
3. Arzt gibt HPC ein und PIN
4. Arzt prüft Authentizität der eGK
5. Arzt prüft Notfalldaten, Allergien etc.
6. Arzt lädt Patientenakte aus dem Internet
7. Arzt prüft Patientenakte
   Gesamte Historie: Verträglichkeit, Wirksamkeit
8. Arzt verordnet durch Eintrag in seinen Computer
9. Arzt schreibt Rezept auf eGK (liegt im Lesegerät)
10. Arzt tippt PIN ein zur Freigabe des Signaturverfahrens
11. Arzt veranlaßt Signierung des ausgestellten Rezepts
12. Arzt entnimmt die eGK und übergibt sie dem Patienten
13. Arzt deaktiviert HPC und entnimmt sie

Handhabung durch Patienten

Beispiel Rezept

- Überprüfung durch Patienten ?
- Ausland ?
- Nachbarn, Pflegedienst ?
- ... ?

Mengengerüst

80.000.000 Versicherte (70 + 10)

43.000 HIV-Infizierte und
2.000 Neu-Infizierte p.a. und
5.000 HIV-Kranke

Hepatitis Binfizierte?

Zwei eGK ?

350.000 Ärzte* (inkl. Zahnärzte)

22.000 Apotheken*

2.200 Krankenhäuser*

700 Labore*

260 Krankenkassen*

* Mit jeweils durchschnittlich 2, 5, 200, 3.000 Mitarbeitern := ~ 100 Millionen Zugriffsberechtigte

Beschreibungsparameter

- Massengeschäft! Per se nicht absicherbar
  - 11 Milliarden Transaktionen p.a.
  - Datenaufkommen > 23.6 Terabyte p.a.
- Anschluss ans Internet ⇒ Zugriff weltweit möglich
- Verknüpfungen: Patientendaten mit Genomdatenbanken, Mautdatenbank, gespeicherten Verbindungsdaten (Kommunikation), Bankkonten, Straßenkontrollen, Buchungsdaten von Flügen
- Sicherheit ist nie 100%
  - Updates/Patches für Software
  - Organisatorische Anpassungen
  - Einweisung, Ausbildung
  - Sicherheit ist nicht umsonst
- Gefühlte Sicherheit
  - Bürger entscheidet 'aus dem Bauch heraus'

Erwartete 'Angriffe'

- Helferin wird abgelenkt und gibt Akte der Patientin für Dritten frei
- Arzt überträgt Patientenakte persönlich an Kollegen.
  Verschlüsselung ist zu Wartungszwecken disabled
- Helferin speichert das Rezept der vorhergehenden Patientin
- Fälschung von Rezepten, Unterschriften, Patientenakten ...
  für Gutachten, Schadenersatzprozesse, ...

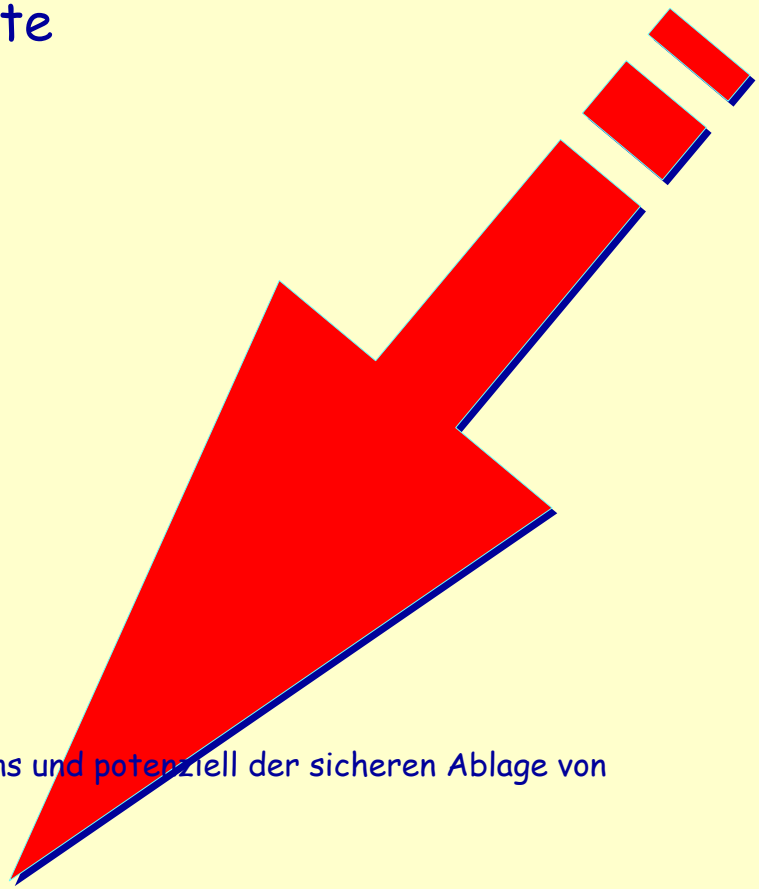
Die Chipkarte ist hochsicher, die Verschlüsselungsalgorithmen sind hochsicher
– und die Menschen? Und die Programme?

Erwartete 'Angriffe'

- Krankenkassen, Lebensversicherer:
  Gesundheitsrisiken
- Schulen, Hochschulen, Ausbildung: Lebenserwartung
- Arbeitgeber: Erbliche Disposition – genetische Selektion
- Banken:
  Kreditausfallrisiken (Lebenserwartung)
- ...

Akteure/Rollen der Geschäftsprozesse

Zugriffsberechtigte



- (Patient)
- (Versicherter)
- Verordnungsgeber
- Leistungserbringer
- Kostenträger
- Übergreifende Funktionen

  Einrichtungen zur Kontrolle und Steuerung des Gesundheitswesens und potenziell der sicheren Ablage von gesundheitsbezogenen Informationen.
  Karten für Funktionen und Fachverwaltungspersonal
  - Prüfung der Authentizität der übermittelten Daten
  - Entschlüsselung und Integritätsprüfung der übermittelten Daten
  - Nachweisbare Übermittlung z.B. statistische Auswertungen an Berechtigte im Gesundheitswesen
- Versandapotheke
- Kartenherausgeber

FhG, IBM, SAP et al. (Hrsg.): Erarbeitung einer Strategie zur Einführung der Gesundheitskarte. Sicherheitsanforderungen. 4.2 Schutzbedarf der Geschäftsprozesse. S. 14. Berlin Version 1.1 vom 12. August 2004

4. Regel

Angriffe durch eigene Mitarbeiter

Innentäter! Fahrlässigkeit, Sabotage, unberechtigte Kenntnisnahme, ...

Aber Hacker? Cracker? Crasher? Phisher? ...

Übergreifende Anforderung: Verfügbarkeit

Manuelle Ersatzverfahren sind bei Technikausfall für den Prozessschritt vorzusehen. Durch die elektronischen Prozesse sollen bei dem Ausfall einzelner Komponenten keine zusätzlichen Risiken für die Versicherten entstehen. Das derzeitige Niveau muss mindestens erreicht werden.

Für jeden neuen und veränderten Geschäftsvorfall soll ein analoger, papierbasierter Prozess existieren. Die Telematikinfrastruktur unterstützt daher

- Die **Bereitstellung aller relevanten Informationen in Papierform**.
- den zeitnahen Abgleich der Datenbstände zwischen elektronischen Prozessen und papierbasierten Ersatz- und Notfallprozessen.
- Die nachträgliche Übernahme der Daten der Ersatzprozesse.

Die existierenden Prozesse dienen dabei als Basis der zu definierenden Notfallprozesse. Damit wird das zusätzliche Risiko durch den Ausfall einzelner Komponenten der Telematikinfrastruktur auf das heute akzeptierte Gefährdungspotential zurückgeführt.

FhG, IBM, SAP et al. (Hrsg.): Erarbeitung einer Strategie zur Einführung der Gesundheitskarte. Sicherheitsanforderungen. 4.3 Übergreifende Anforderungen S. 19. Berlin Version 1.1 vom 12. August 2004

Organisatorische Maßnahmen

U.a. wird der mögliche Schaden durch organisatorische und vertragliche Regelungen begrenzt. Insbesondere sind für das Gesundheitswesen organisatorische Ersatzprozesse bei der Gefährdung der körperlichen Unversehrtheit bereitzustellen. Um dies für den **Ausfall jeder IT-Komponente** der Telematikinfrastruktur sicherzustellen, sind daher **zusätzliche begleitende Papierinformationen** für die Versicherten zu berücksichtigen. Damit wird das zusätzliche Risiko durch den Ausfall einzelner Komponenten auf das heute akzeptierte Gefährdungspotential zurückgeführt.

FhG, IBM, SAP et al. (Hrsg.): Erarbeitung einer Strategie zur Einführung der Gesundheitskarte. Sicherheitsanforderungen. 5.1.1 Anforderungen aus der medienbruchfreien elektronischen Übertragung der Geschäftsvorfälle S. 25. Berlin Version 1.1 vom 12. August 2004

5. Regel

IT ist völlig unsicher

Programmsteuerung: BIOS, Betriebssysteme, Anwendungsprogramme, Sicherheitsprogramme

⇔ Klassisch-materielle Komponenten (USV)

Technik und Sicherheit der eGesundheitskarte

1. Illusion oder Wirklichkeit: Technik
2. Nicht behebbare strategische Fehler
3. Kosten: Patient, Arzt
4. Zusammenfassende Forderungen

Verantwortlichkeiten

- Standard-Vorentwicklung: IBM
- Standards: Gematic (Organe der Selbstverwaltung)
- Bayern: Siemens, BMW
- NRW: T-Systems
- ...
- Sicherheit ?

Kein Verantwortlicher

Noch nicht einmal verantwortliches Konsortium (TollCollect)

Anonymisierung - Pseudonymisierung

- **Authentifizierung und Autorisierung:**
  Patient muss entscheiden können, wer Daten erhält
  (Informationshoheit z.B. auftragsbezogene Zugriffsberechtigungen).
- Eine **Pseudonymisierung** des Versicherten- und Leistungserbringerbezugs wird von der Vertrauensstelle durchgeführt und findet in der Form statt, dass **bundesweit periodenübergreifende Auswertungen zu einem Versicherten und Leistungserbringer durchgeführt werden können**.
  Pseudonyme enthalten bestimmte Bestandteile (Geburtsdatum, Geschlecht, PLZ, u.a. siehe § 303c SGB V/GMG). Sie enthalten einen stabilen Teil, der auch nach Kassenwechsel periodenübergreifende Auswertungen zulässt.
- Anonymisierung und Pseudonymisierung von Daten muss unterstützt werden.
- Unterschiedliche **Pseudonymisierungsverfahren** werden gefordert:
  rückführbar, ***nicht-rückführbar,*** lebenslang gültig.

Hervorhebungen durch die B4H-Autoren.

FhG, IBM, SAP et al. (Hrsg.): Erarbeitung einer Strategie zur Einführung der Gesundheitskarte. Sicherheitsanforderungen. 5.1.1 Anforderungen aus der medienbruchfreien elektronischen Übertragung der Geschäftsvorfälle S. 34 – S. 38. Berlin Version 1.1 vom 12. August 2004

6. Regel

Es gibt keine Anonymität

im Internet, in der Behörde, ... bei den Krankendaten

Bewertung in der Risikoanalyse

'Wie in obiger Abbildung dargestellt, sind die sekundären Bedrohungen für die Betrachtung des Gesamtrisikos nicht mehr vernachlässigbar. Selbst im Fall einer geringen Eintrittswahrscheinlichkeit für primäre Bedrohungen, so daß ein akzeptables Restrisiko für den direkt betroffenen Geschäftsprozess entsteht, ist die gesamte **Schadenshöhe** auf Grund der sekundären Bedrohungen **nicht mehr zu begrenzen**. Eine direkte Abwägung der Bedrohungen gegen organisatorische und technische Sicherheitsmaßnahmen einer Komponente reicht also nicht mehr aus, wenn die Kompromittierung einer Komponente der Telematikinfrastruktur zu Kompromittierungen weiterer Komponenten führen kann.'

FhG, IBM, SAP et al. (Hrsg.): Erarbeitung einer Strategie zur Einführung der Gesundheitskarte. Sicherheitsanforderungen. 5.1.2 Anforderungen resultierend aus der Schwachstellenanalyse S. 29. Berlin Version 1.1 vom 12. August 2004

Folgen der Gesundheitstelematik

- Vollständige Patientenakte
  Ärzte, Diagnosen, Therapien, Medikamente ...
- Jederzeitiger Zugriff
- Kontrolle durch jeden HP
  Medikament auch gekauft? Welches Medikament? Diagnose?
- Notfalldaten Zugriff durch Betriebsarzt
  vor Einstellung (Asthma, Diabetes, ...)
- Krankenversicherung, Haftpflicht (PKW)? ...
- Kontrolle/Überwachung der Ärzte, Apotheker ...
  Fehler, Behandlungserfolge ... Haftung
- **Die gesamte Infrastruktur ist gegen bestimmten Angriffe nicht absicherbar**

Folgen der Sicherheitsmaßnahmen

Patient soll Bereiche seiner eGK sperren können

Vertrauensverhältnis zum Arzt?

Definition Hochsicherheit

Nach heutigen Erkenntnissen

sind diese Verfahren nicht in den nächsten 10 Jahren zu knacken

Programmgesteuerte Angriffe

- Sehr schnell – kein menschlicher Eingriff
- Ubiquitär: Internet – von überall auf der Welt aus
- Verteilte Angriffe: Von Tausenden von Computern

- Protokollierung?

Mängel der Gesundheitstelematik

1. Patient ist nicht Herr seiner Daten ⇔ Verschlüsselung
   Unbemerkte Auswertungen durch Dritte
   Pseudonymisierung ⇔ Anonymisierung

2. Sicherheitsmaßnahmen völlig unzureichend
   entsprechen nicht dem Stand der Technik
   Verschlüsselungsverfahren nicht frei wählbar - vorgeschrieben
   Angriffen schutzlos ausgeliefert

3. Überwachung und Kontrolle der Sicherheitsmaßnahmen
   Zertifizierung

Technik und Sicherheit der eGesundheitskarte

1. Illusion oder Wirklichkeit: Technik
2. Nicht behebbare strategische Fehler
3. Kosten: Patient, Arzt
4. Zusammenfassende Forderungen

Monatlicher Gesamtaufwand Sicherheit

Maßnahme	Kosten in €			
	Hardware	Software	Personal	Summen
Informationswertanalyse, Risk assessment			1.000	
Back-up Hardware und Software	300	200		
Einweisung, Ausbildung			500	
Firewall	300	500		
Parametrisierung			500	
File-Verschlüsselung gespeicherter Daten	500			
Einweisung, Ausbildung			500	
File-Übertragung-, mail-Verschlüsselung	1.000			
Einweisung, Ausbildung			500	
Passwort, Token	100		500	
Security Management (inkl. Kontrollen) implementieren			1.000	
Change Management, Updates, Patches installieren			300	
Summen	2.200	700	4.800	
50% Aufschlag für erhöhte Verfügbarkeit	1.100			
Gesamtsumme Einmalaufwand Sicherheit				**8.800**
Abschreibung auf 3 Jahre monatlich				244
Monatl. Personalaufwand für Kontrollen: 15% des o.g.			720	
Virensoftware monatlich		20		
Intrusion Protection System monatlich		100		
Monatl. für Hardware, Updates und Patches 5%	165	35		
Monatlicher Gesamtaufwand für Sicherheit				**1.284**

Datenträger Kapazität

	Giga-Bytes	Aktenordner	Gewicht
USB-Stick	1	800	
*	5	4.000	
Microdrive	8	6.400	14
*	50	40.000	

- Auf 3 Jahre hochgerechnet
- Windows mobile 5.0 unterstützt Platten in Handys, PDA etc.

40 GB Magnetplatte 300.- €

7. Regel

Gefühlte Sicherheit ??

der Gesundheitstelematik / Gesundheitskarte

Kein Recht auf Einsicht in die eigene Patientenakte!

Technik und Sicherheit der eGesundheitskarte

1. Illusion oder Wirklichkeit: Technik
2. Nicht behebbare strategische Fehler
3. Kosten: Patient, Arzt
4. **Zusammenfassende Forderungen**

Forderungen der Bundesärztekammer

zur Einführung der eGK und Telematik-Infrastruktur

1. Schaffung eines rechtlich, organisatorisch und technisch **vertrauenswürdigen** Rahmens unter Wahrung der ärztlichen Schweigepflicht und des Datenschutzes der Ärzte.
2. Sicherung des Anspruchs der Patienten auf **absolute Vertraulichkeit**. **Entscheidungsfreiheit** des Patienten über Zugänglichkeit und Weiterleitung seiner Daten.
3. Die Nutzung von Telematik ist am Bedarf des Patienten und nicht am Wunsch der uneingeschränkten Ökonomisierung der Versorgung auszurichten.
4. Einfache und sichere **Handhabbarkeit** der technischen Systeme.
5. Angemessene **Vergütung** der mit Einführung der Telematik verbundenen Kosten. Der Nutzen der Telematik muss langfristig die Kosten übersteigen (die Investitionskosten für die Einführung der Telematik liegen nach von der DKG publizierten Schätzungen zwischen 1,0 und 1,4 Milliarden Euro).
6. Wissenschaftliche Begleitung der Einführung der Telematik.
7. Anpassung des unrealistischen Zeitplans mit Gewährleistung angemessener Test-, Lern- und Einführungsphasen.

Unterschiedliche Qualität

Dezentrale Papierakten - zentrale Speicherung Internet

Recht auf informationelle Selbstbestimmung ?

Programmsteuerung macht IT völlig unsicher

- Schufa
- Kraftfahrtbundesamt, Flensburg
- Vorratsspeicherung der Kommunikationsdaten:
  Telefon (auch mobil mit Lokalisierung!), Internet - ohne Zweckbindung
- Zwangsuntersuchung Neugeborener auf Erbkrankheiten
- Zentrale Zwangs-Speicherung der Patientenakten
- Datenbanken der Arbeits- und Sozialversicherung
- Bankkontenkontrolle ohne Anlass oder gar Grund
- Kreditkarten/Bargelloses Zahlen, Payback
- Autobahn-Maut
- Bibliotheken
- eBAy, iPod, Amazon, ...
- Flugdaten
- Ärzte: Behandlungen, Verschreibungspraxis, ...
- ...

Stasi ?

Forderungen

Digitalisierung des Gesundheitswesens!

1. **Wahrhaftigkeit der Funktionäre**: KVN, AA-Netz

2. **Sensibilisierung** der Bürger: Gesellschaftliche Zustimmung

3. **Beherrschbarkeit**
   Keine Pflicht-Speicherung im Internet: **Alternativen, Kontrolle ?**
   Verbesserung der Exportfähigkeit

4. **Einen Verantwortlichen** / Sicherheitsbeauftragten:
   Öffentliche Prüfberichte/Kontrollen der Sicherheit, Haftung

Prof. Dr. Hartmut Pohl

Informationssicherheit – Fachhochschule Bonn-Rhein-Sieg - ISIS – InStitute für InformationsSicherheit

- **Management Consulting**: Absicherung von Intranets und Extranets, Mobilkommunikation
  in großen und mittleren Unternehmen: Chemie, Pharma, Energieversorger, Kommunikation, Sicherheitsbehörden
- **Begutachtung** von Sicherheitsprojekten – Bewertung und Auswahl von Produkten
- **Coaching** von Sicherheitsbeauftragten und Beratern. **Projektmanagement**
- **Sicherheitsstrategien** und Richtlinien, Sicherheits-Benchmarking, Risk-Management
  Securing Outsourcing, Outsourcing Security - Managed Security, Trust Infrastructures
  Implementierung von Standards: ISO 20 000 (17799 / BS 7799), Grundschutzhandbuch.
- **Fälschungschutz** von und mit Transpondern (RFID), cloning

Max-Pechstein-Str. 4 - 50858 Köln
Tel.: 0221 - 4847 - 553. Fax.: - 529
Hartmut.Pohl@sang.net
http://www.inf.fh-bonn-rhein-sieg.de/Pohl.html