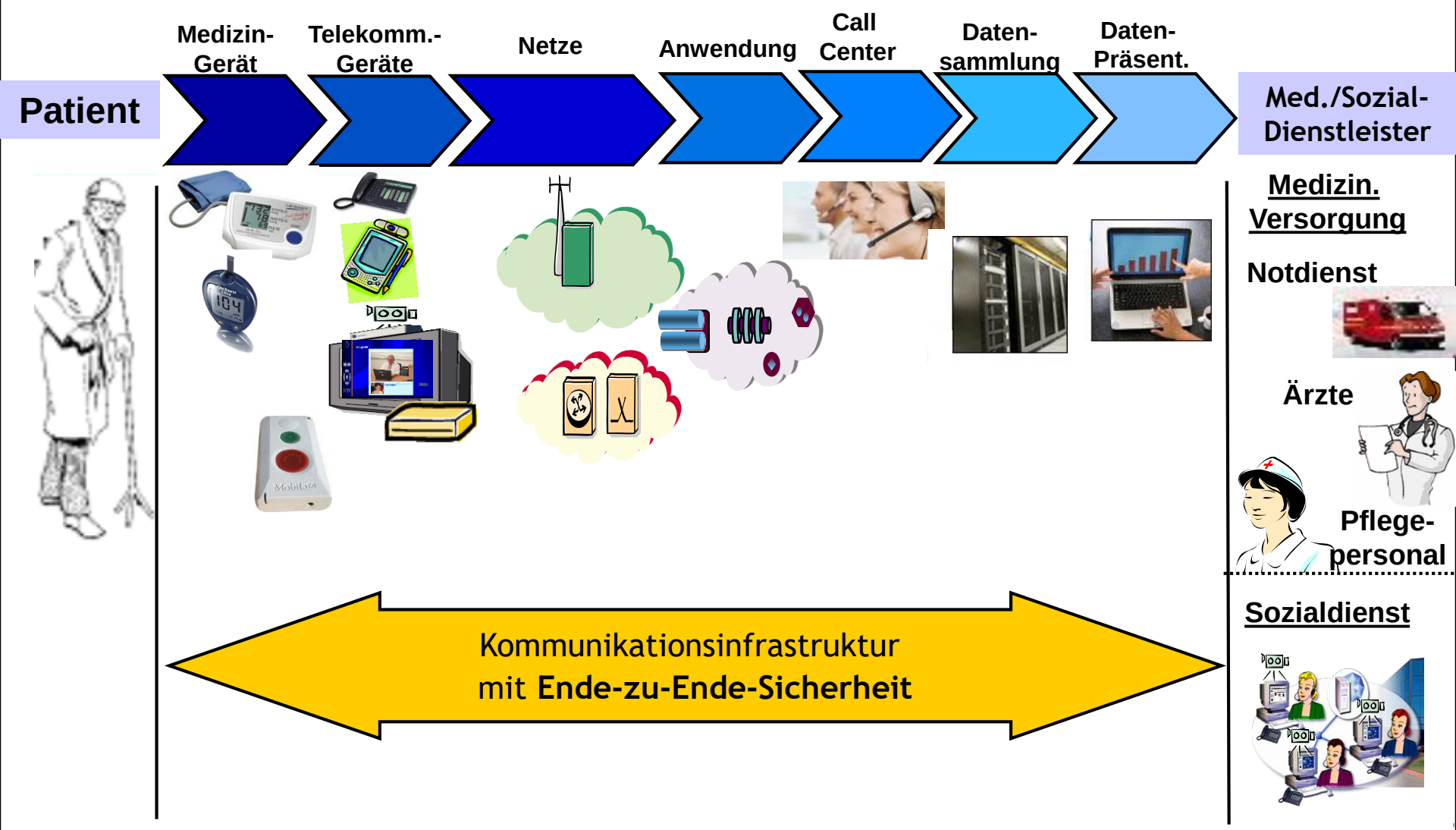
Sichere Kommunikationsinfrastruktur

Kurt Lösch, Alcatel-Lucent Bell Labs Germany

Münchner Kreis, 6. Juli 2009

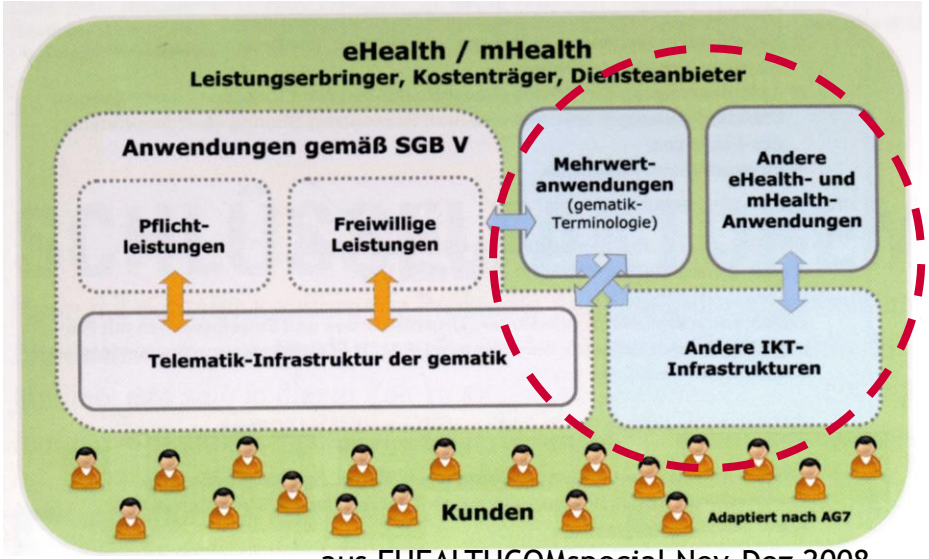
Elemente des Telemonitoring



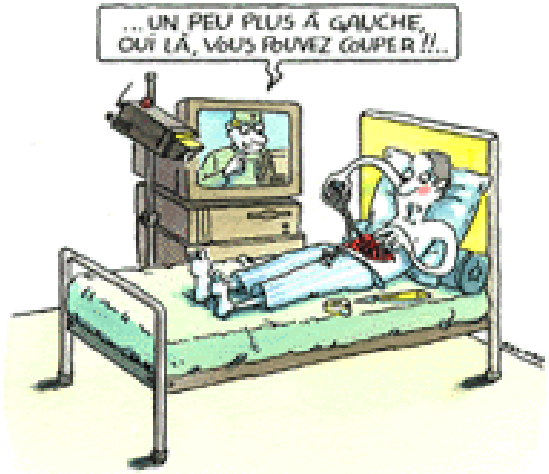
Alcatel·Lucent

Inhalt

- **Allgemeine Anforderungen an die IKT-Infrastruktur**
- **Konzepte zur Umsetzung der Anforderungen**
  - Verfügbarkeit
  - Datentransport
  - Speichern von Daten und Zugriff
  - Umsetzungsbeispiele
- **Standards**
- **Zusammenfassung und Ausblick**



aus EHEALTHCOMspecial Nov-Dez 2008



Allgemeine Anforderungen an die Infrastruktur

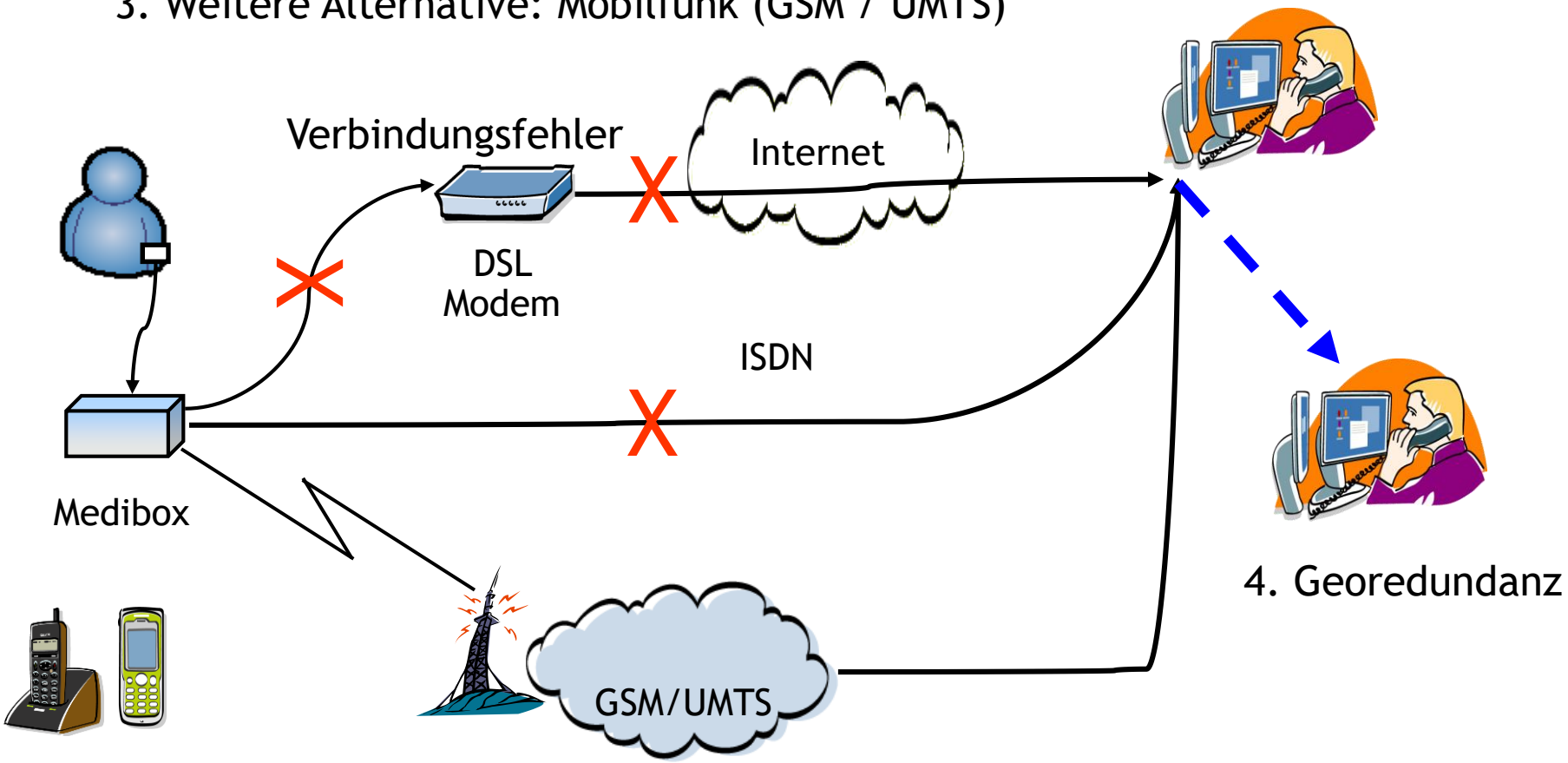
- Einhaltung der Datenschutzbestimmungen (z.B. keine Vorratserhebung)
- Einhaltung der Vorgaben des Sozialgesetzbuches (SGB 1 §35: Sozialgeheimnis, §36a: Elektronische Kommunikation), von Krankenhausgesetzen etc
  soweit im konkreten Fall erforderlich
- Sicherstellung der "ärztlichen Schweigepflicht" bei der Informationsverarbeitung
- Umsetzung der Patientenrechte (Benachrichtigung, Einsicht, Löschung, ...)
- Authentizität, Integrität, Vertraulichkeit der Patientendaten (Missbrauch von Zugangsberechtigungen verhindern)
- Zugriff auf Teil der Patientendaten im Notfall (Notfalldaten)
- Permanente Verfügbarkeit

Anforderungen: Sicherheit …

- bei der Übertragung
  - Authentisierung beider Kommunikationspartner
  - Pseudonym für Nutzer/Patient
  - Integrität der übertragenen Daten
  - Nachweisbarkeit des Datenursprungs und der Zustellung
- bei der Datenspeicherung
  - nachweisbare Urheberschaft und Integrität der Daten,
  - Wahrung der Pseudonymität; bei Weitergabe für Studien: Anonymisierung
  - Auskunft, Berichtigung und Löschung von Daten auf Verlangen des Patienten
  - Langzeitarchivierung bestimmter Datensätze
  - Vermeidung von dauerhafter Speicherung und redundanter Datenhaltung außerhalb der Primärspeichersysteme
- beim Zugriff
  - Authentisierung und Autorisierung
  - Zugriff nur auf die für den konkreten Behandlungskontext erforderlichen Daten
  - Protokollierung der Zugriffe

Umsetzungskonzept: Permanente Verfügbarkeit

1. Standardverbindung über WLAN & DSL
   2. Alternativer Verbindungsaufbau über ISDN
      3. Weitere Alternative: Mobilfunk (GSM / UMTS)



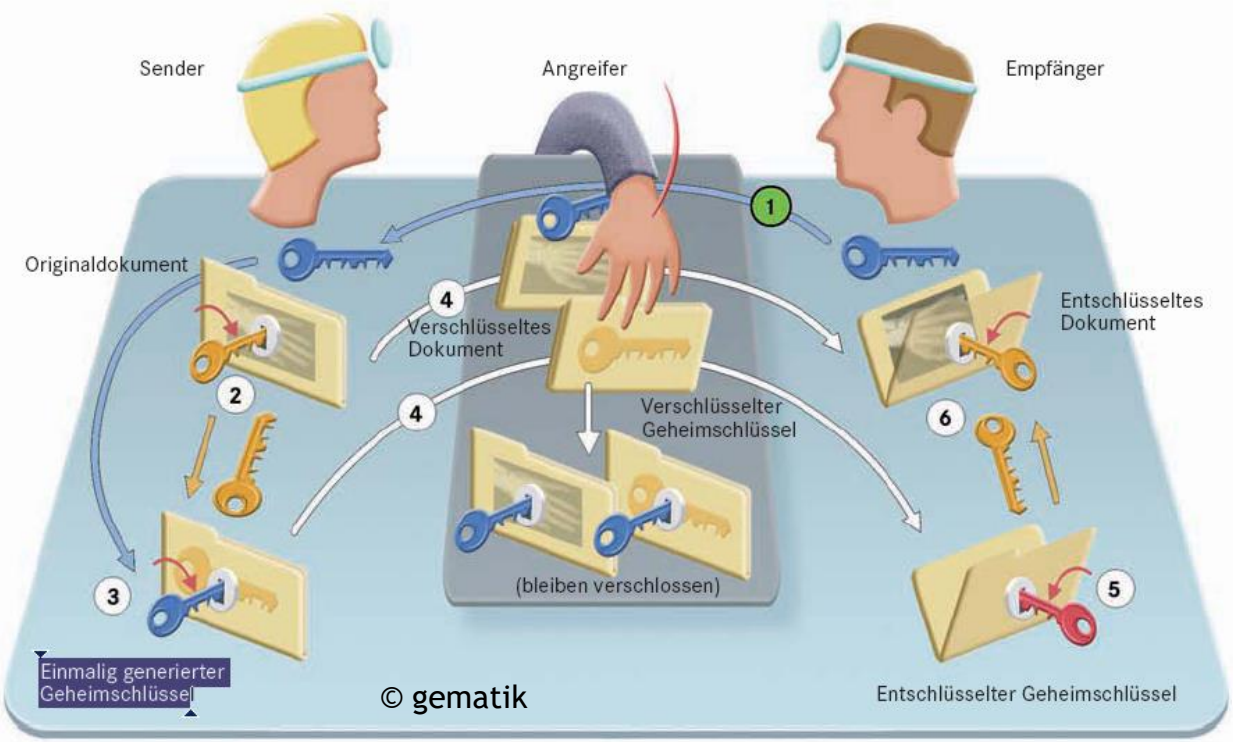
Umschalten muss ohne Nutzerinteraktion erfolgen, d.h. ohne erneute Authentifizierung

Umsetzungskonzept: Datentransport/Kommunikation

- Die Kommunikation erfolgt über Virtual Private Network (VPN)-Verbindungen mit Hilfe des IPSec-Protokolls (Punkt-zu-Punkt).
- Zu Beginn müssen sich beide Seiten authentifizieren.
- Nach erfolgreichem Aufbau der VPN-Verbindung werden die gewünschten Daten verschlüsselt übertragen.
- Der Empfänger sendet eine signierte Empfangsbestätigung zurück.
- Personenbezogenen Daten werden pseudonymisiert und getrennt von Nutz-/Vital-/Messdaten übertragen.

IPSec: Internet Protocol Security (für IPv6 obligatorisch))

Hybride Verschlüsselung (aus Whitepaper „Sicherheit“ der gematik)



Vorbedingung:

der Empfänger (rechts) gibt seinen öffentlichen Schlüssel dem Sender (links) ❶.

Ablauf:

Der Sender kodiert das Dokument mit einem geheimen Schlüssel, den er selbst erzeugt hat ❷. Dieser geheime Schlüssel wird nun mit dem öffentlichen Schlüssel des Empfängers verschlüsselt ❸.
Sowohl der codierte Schlüssel als auch das verschlüsselte Dokument gehen über einen Transportweg zum Empfänger❹.

Dass dabei der Angreifer beide Dokumente abfangen kann, beeinträchtigt die Sicherheit nicht, denn er verfügt nur über den öffentlichen Schlüssel des Empfängers.

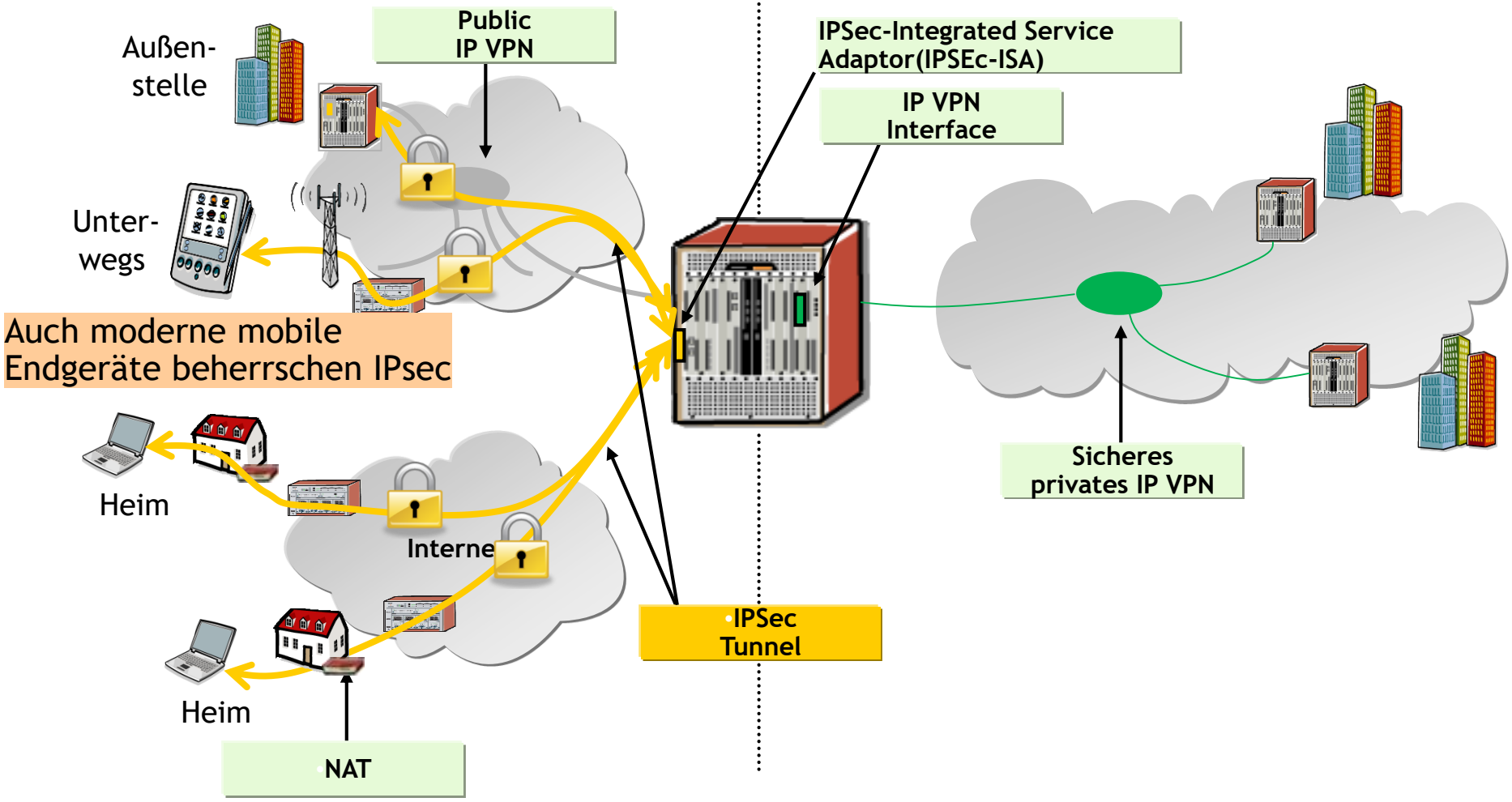
Der Empfänger verwendet anschließend seinen privaten Schlüssel, um den codierten Geheimschlüssel zu dechiffrieren ❺.

Damit kann er das Originaldokument erfolgreich öffnen ❻.

Vorteile:

- Absender und Empfänger können den Geheimschlüssel austauschen, ohne dass er in die Hände des Angreifers fallen kann.
- Nicht alle Schlüssel müssen geheim bleiben, nur der private Schlüssel des Empfängers und der einmalig verwendete Geheimschlüssel.
- Der Empfänger darf seinen öffentlichen Schlüssel jedem frei zur Verfügung stellen.
- Das Verfahren nimmt relativ wenig Rechenzeit in Anspruch.

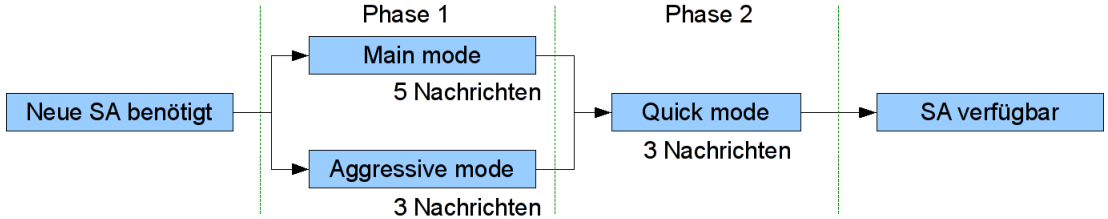
Umsetzungsbeispiel:
IPSec- Konzentrator (Remote-Access Concentrator (RAC)) in einem Service Router

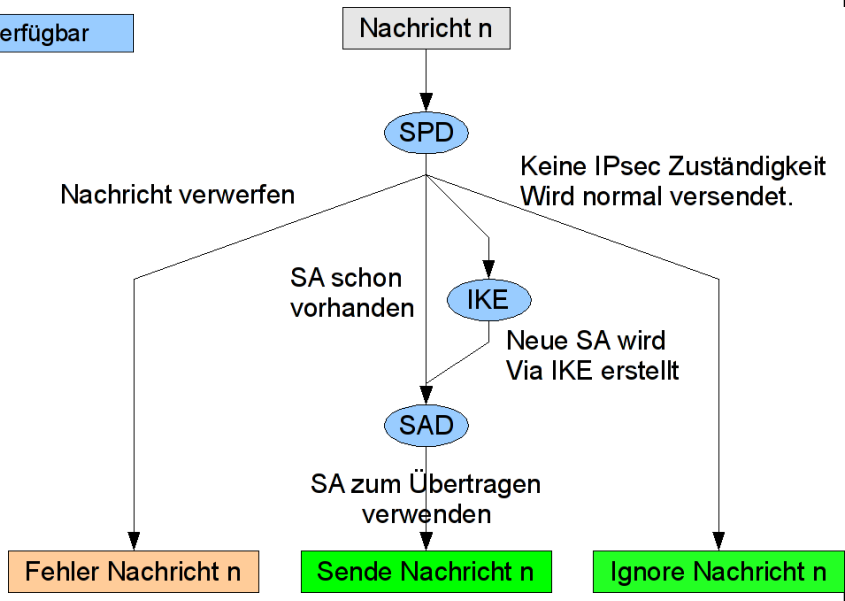


More Info: http://all.alcatel-lucent.com/wps/portal/wireline/ip Select IP/MPLS Routers =/x/opgproduct/a7750sr.jhtml

Ausführungsbeispiel für Service Router

- NAT traversal: Nutzer können private IP-Adressen beibehalten
- Schlüsselverteilung: IKE-Protokoll (oder manuell)
  gemeinsames Geheimnis durch Perfect Forward Secrecy (PFS)





- IPSec-Sicherheit
  - Verschlüsselung: AES-128, -192, -256
  - Authentifizierungs-Hashing: HMAC-MD5, HMAC-SHA1
- bis 32,000 gleichzeitige IPSec Sessions
- IPSec Bandbreite ab 64 Kb/s

NAT: Network Address Translation
IKE: Internet Key Exchange, MobIKE (Wechsel der IP-Adr. während Session)
SA: Security Associate, SPD: Security Policy Database, SAD: Security Association Database
PFS: Abfangen eines Schlüssel hat keine Auswirkung auf nachfolgende, da diese unanbhängig
AES: Advanced Encryption Security, Ziffern= Schlüssellänge in bit
AES-256 Zahl der Versuche zum Finden des Schlüssels = ca. $2^{n/2} = 2^{128} = 3{,}4 \times 10^{38}$ (10^{22} Jahre bei 10^9 Versuche/s)

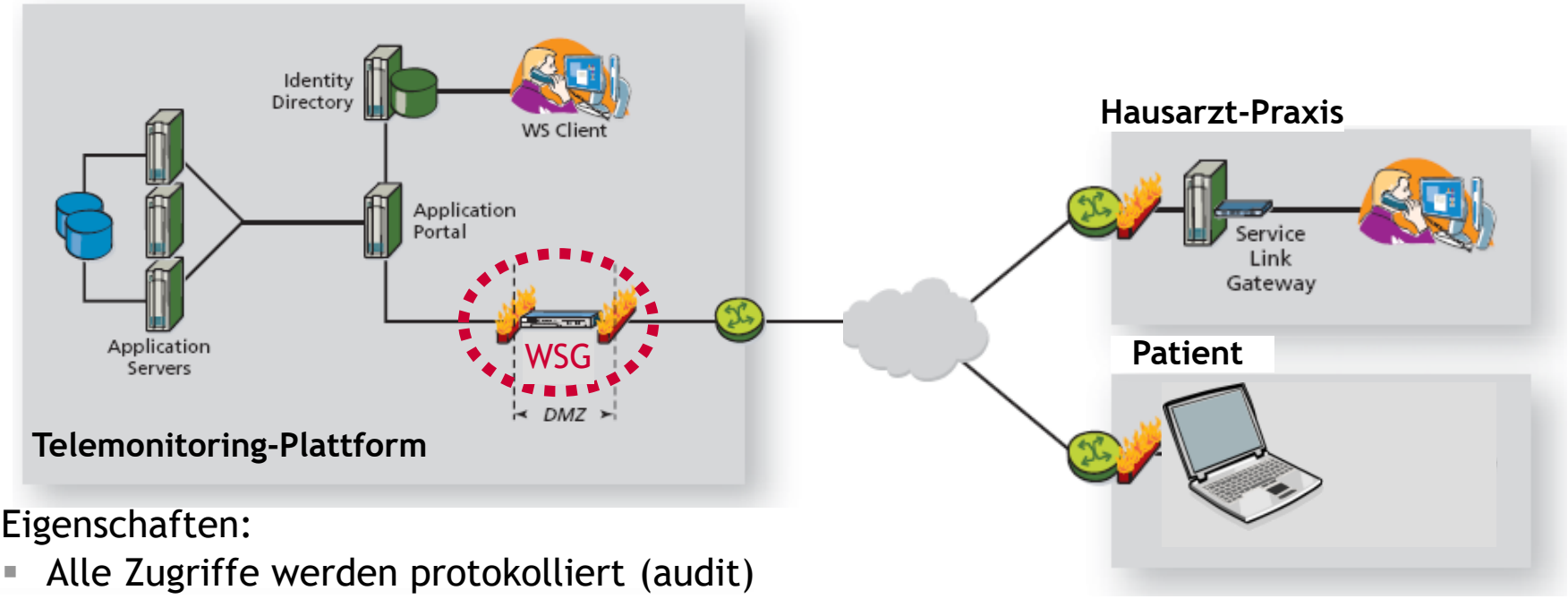
Umsetzungskonzept: Speichern von Daten

- Personenbezogene Daten werden verschlüsselt abgelegt
- Vitaldaten können ebenfalls verschlüsselt abgelegt werden
- Daten der Telekommunikationsanwendungen wie Video-Kommunikation usw. werden nach den heute üblichen Regeln behandelt
- Logging in der Datenbank
  Alle Veränderungen in der Datenbank werden protokolliert um die Frage „wer hat wann welchen Eintrag eingefügt, modifiziert oder gelöscht?“zu einem späteren Zeitpunkt juristisch einwandfrei beantworten zu können.
- Zugriffshierarchie
  Gesteuert durch verschiedene Profile wird sichergestellt, dass entsprechend der Vorgaben nur autorisierte Nutzer Zugang zum System oder zur Datenbank, bzw. fallbezogen zu Teilen aus der Datenbank für einen Patienten bekommen.

  Profilbeispiele:
  - Betreiber / Administratoren der Netzes oder der Server
  - Krankenhausarzt
  - Hausarzt
  - Pfegepersonal
  - Notarzt
  - Patient
  - Angehörige des Patienten bei entsprechender Verfügung des Patienten

    …

Umsetzungsbeispiel: WebService Gateway (WSG)



Eigenschaften:

- Alle Zugriffe werden protokolliert (audit)
- Single-Sign-On: einmalige Anmeldung auch für Dienste auf einem anderen System
- Übertragung von Sicherheitsklassen/Zugriffsrechten auf verbundene Systeme (trusted)
- Unterschiedliche, nutzerspezifische Sicherheitsklassen
- Alle Daten werden verschlüsselt abgelegt
- Einsatzgebiete:
  - an der Schnittstelle zweier Systeme/Netze für Datenaustausch (wie im Bild oder auch zw. Krankenkasse und Leistungserbringer für Abrechnungszwecke
  - Für Gastzugang in anderem Netz (z.B. Pfleger beim Hausbesuch)

Umsetzungskonzept: Weitere wichtige Punkte

- Löschen von temporären Daten
  - Alle temporären Daten im System werden nach einer abgeschlossenen Transaktion gelöscht, um eventuellen Missbrauch auszuschließen.
- Schulung zugangsberechtigter Personen
  - Alle zugangsberechtigten Personen müssen auf die Gefahren des Missbrauchs durch unsachgemäßen Umgang mit ihrer Zugangsberechtigung hingewiesen werden
- Die Verwaltung aller Accounts und Profile für das komplette System erfolgt an einer einzigen Stelle
- Passwortregeln entsprechend heute üblichen Regeln für Systeme mit hohen Sicherheitsanforderungen
- Alle Komponenten des Systems sind durch eine Firewall, die IPSec unterstützt, gegen Angriffe aus dem Internet geschützt.

Relevante Standards und Allianzen

- Allgemeine Sicherheit (siehe Wikipedia Transport Layer Security)
  - *IPSec Internet Protocol Security (für IPv6 obligatorisch) mit*
    - *ESP: Encapsulating Security Payload*
    - *AH: Authentication Header*
    - *IKE: Internet Key Exchange, MobIKE (Wechsel der IP-Adr. während Session)*
  - *TLS (Transport Layer Security, IETF RFC2246 (1999)→ RFC5246 (2008)) oder alte Bezeichnung SSL (Secure Sockets La*
  - *PFS:* Perfect Forward Secrecy (Wikipedia deutsch: Folgenlosigkeit)
  - *AES: Advanced Encryption Security (IETF RFC3686, Jan. 2004)*
- eHealth
  - Continua Health Alliance: global agierende Unternehmen; Ziel: Interoperabilität für zweiten und dritten Gesundheitsmarkt
  - HL7 (Health Level; Standards für Datenaustasuch in OSI-Schicht 7 (Applikationsebene), VITAL (ISO11073) (Dateiformat), DICOM (Dig. Imaging & Commun.in Medicine)
  - Bluetooth Medical Device Protocol (und IEEE-11073 Personal Health Data (PHD))
  - Imprimo Plattform für Vitaldatenerfassung über mobile Endgeräte (BMWi Projekt)
  - XACML (eXtensible Access Control Markup Language) der Organization for the Advancement of Structured Information Standards (OASIS) für Beschreibung von Zugriffsrichtlinien
  - SOAP: Protokoll für Datenaustausch zwischen Systemen und Fernaufruf von Prozeduren
    früher Simple Object Access Protocol oder Service Oriented Architecture Protocol genannt, jetzt Eigenname
- Endgeräte
  - UPnP: Universal Plug and Play Protokoll
  - USB: Universal Serial Bus (Schnittstelle und Protokoll)
  - Bluetooth; ZigBee; UWB (Ultra Wide Band) für low power Wireless Body Area Networks (WBAN)
  - URC: Universal Remote Control (Middleware)

Zusammenfassung und Ausblick

- Sicherheitsanforderungen für Telemonitoring können mit bestehenden Verfahren der Informations- und Kommunikationstechnik erfüllt werden.
- Diese müssen konsequent und nahtlos eingesetzt werden.
- Bedeutung der Anbindung über Mobilfunk wird stark zunehmen.
- Für rasche Verbreitung und Marktdurchdringung sind proprietäre Lösungen und Schnittstellen hinderlich.
  EU Recommendation " ..development of overall European eHealth interoperability by the end of 2015" (COMMISSION RECOMMENDATION of 2nd July 2008 on cross-border interoperability of electronic health record systems)
- Bausteinprinzip: bedarfsgerechter Einsatz von Telemonitoring-Funktionsmodulen bei einheitlicher Gesamtarchitektur
- Telemonitoring sollte in Ambient-Assisted-Living-Lösungen integrierbar sein → einfacher Übergang von „Komfortlösungen" zu medizinischen Diensten

Ausblick: Beispiel für Integration **SmartSenior-Allianz**

Übersicht Zielsetzung *(xxx= Bezug zu Telemonitoring)*

A **Sicher unterwegs sein**

- Erhöhung von objektiver und subjektiver Sicherheit
- ***Erweiterte Notfall-Assistenz mit Vital-datenübertragung***
- Sichere Nothalte-Funktion
- Erweiterte Ortungssysteme

B **Gesund werden und bleiben**

- ***Telemedizinische Nachsorge und Betreuung zu Haus***
- ***Standardisierte Übermittlung von Vitalparametern***
- Integration von Pflege- und Versorgungsdiensten

Erhaltung des Lebensstandards alter Menschen aus ökonomischer, gesundheitlicher und sozialer Sicht

- Unterstützung im häuslichen Alltag, Einbindung sozialer und quartiersbezogener Dienste
- ***Sicherheit zu Hause, Notfallvermeidung und -erkennung***
- Einfache integrierte Kommunikationsmöglichkeiten mit sozialem Umfeld und Dienstleistern

C **Länger selbstständig im häuslichen Umfeld leben**

Integration der Lösungen in ein Gesamtkonzept durch einheitliche Informationslogistik und organisationsübergreifende Datenvernetzung

Vielen Dank

Back-up-Folien

Quellenangaben

http://de.wikipedia.org/wiki/RSA-Kryptosystem

http://en.wikipedia.org/wiki/HMAC-MD5

http://en.wikipedia.org/wiki/Birthday_attack

http://en.wikipedia.org/wiki/Cryptographic_hash_function

http://de.wikipedia.org/wiki/Hash

http://de.wikipedia.org/wiki/HL7

Virtuelles Privates Netz (ISi-VPN); BSI-Leitlinie zur Internet-Sicherheit (ISi-L), 2009; http://www.bsi.bund.de oder http://www.isi-reihe.de

SmartSenior: Pressemitteilung 25.5.09: http://www.bmbf.de/press/2557.php

Ablauf zu Internet Key Exchange (IKE)

Main Mode [Der Main Mode (dem *Aggressive Mode* vorzuziehen) wird in der ersten Phase der Verschlüsselungsvereinbarung und Authentisierung (Internet Key Exchange) genutzt. Hierbei handeln der Initiator (derjenige, der die Verbindung aufnehmen will) und der Antwortende (der Responder) miteinander eine ISAKMP-SA aus. Diese „Verhandlung“ geschieht in folgenden Schritten:

1. Der Initiator sendet einen (zur Not auch mehrere) Vorschläge mit Authentisierungs- und Verschlüsselungsalgorithmen.
2. Der Responder wählt aus den angebotenen und den von ihm unterstützten Algorithmen den sichersten aus und sendet das Auswahlergebnis an den Initiator.
3. Der Initiator sendet seinen öffentlichen Teil vom Diffie-Hellman-Schlüsselaustausch und einen zufälligen Wert (die Nonce).
4. Der Responder sendet ebenfalls seinen öffentlichen Teil vom Diffie-Hellman-Schlüsselaustausch und einen zufälligen Wert. Dieser Wert dient im Schritt 5 der Authentisierung.

Da nun beide (der Responder und der Initiator) die öffentlichen Teile für den Diffie-Hellman-Schlüsselaustausch kennen, wird dieses Verfahren genutzt, um den geheimen Schlüssel zu berechnen. Dieser wird dann für die Verschlüsselung nach dem vereinbarten Schlüsselverfahren für die folgenden Schritte verwendet. Der berechnete (Diffie-Hellman-)Schlüssel wird auch für die Erzeugung eines weiteren Schlüssels genutzt, der für die Authentifikation verwendet wird.

Schritt 5 ist die Authentisierung. Dabei müssen sich beide Beteiligten als zugriffsberechtigt ausweisen. Hierbei kommen zwei unterschiedliche Verfahren zum Einsatz:

1. die Authentisierung mittels vereinbartem Geheimnis (im englischen Pre-Shared-Keys, PSK) oder
2. zertifikatsbasiert.

Die zertifikatsbasierte Authentisierung verwendet X.509-Zertifikate und ist im Wesentlichen eine Public-Key-Infrastruktur, wie sie auch für SSL und S/MIME verwendet wird. PGP-Zertifikate sind ein anderer Ansatz und können hierfür nicht verwendet werden.

Die Authentisierungsmethoden unterscheiden sich zwar, jedoch ist die grundsätzliche Vorgehensweise immer die gleiche: Es wird immer ein Hashwert über das mit dem Diffie-Hellman-Schlüsselaustausch erzeugte Geheimnis, die Identität, die ausgehandelten Kryptoverfahren sowie die bisher versandten Nachrichten gebildet, verschlüsselt und versendet. (In der Literatur werden manchmal *Cookies* erwähnt: ein Hashwert über ein erzeugtes Geheimnis, IP-Adresse und Zeitmarke.) Der Schlüssel, der hier für die Verschlüsselung genutzt wird, ist jedoch nicht der aus dem Diffie-Hellman-Schlüsselaustausch, sondern ein Hashwert über diesen sowie die versandten Nachrichten.

PSK-Authentisierung [

Bei diesem Verfahren erfolgt die Authentisierung aufgrund eines einzigen gemeinsamen Geheimnisses. Es kann angewendet werden, wenn eine überschaubare Teilnehmermenge an das IPsec-VPN angeschlossen ist. Der wesentliche Nachteil ist: Erhält jemand unberechtigten Zugriff auf diesen Schlüssel, müssen auf allen beteiligten Hosts die Schlüssel ausgetauscht werden, um die Sicherheit wiederherzustellen. Soll ein Rechnernetz wachsen, ist dieses Verfahren auch dann abzulehnen, wenn zuerst nur wenige Knoten beteiligt sind. Der Mehraufwand für die zertifikatsbasierte Authentisierung amortisiert sich in der Regel bereits nach kurzer Zeit.

Zertifikatsbasierte Authentisierung

Diese Authentisierung hat einen anderen Ansatz. Dabei werden X.509-Zertifikate verwendet. Dieses System basiert auf vertrauenswürdigen CAs (Certification Authorities, z. B. mit eTrust) oder einer Hierarchie aus diesen. Das Prinzip hierbei ist, dass jeder einzelne Endpunkt seine CAs (Vertrauensstellen) kennt und alle Zertifikate, die durch diese Vertrauensstellen signiert sind, als gültig anerkennt. In der Praxis bedeutet dies, dass alle Zertifikate von vertrauenswürdigen CAs eingespielt werden und somit alle von diesen CAs ausgestellten Zertifikaten Zugriff haben. Zertifikate können von bekannten CAs bezogen werden (VeriSign, eTrust uvm.). Damit kann gewährleistet werden, dass auch unbekannte VPN-Partner authentisiert werden können. Leider ist dies in der Praxis nicht so leicht, weil weitere Parameter (z. B. Rechnernetzadressen) eine Rolle spielen und diese mit bereits bestehenden VPN-Verbindungen kollidieren können. Es hat sich daher durchgesetzt, eine private PKI (Public Key Infrastructure) einzusetzen. Mit einer eigenen PKI sollen aber nur bekannte und vertrauenswürdige Hosts Zugriff auf das VPN haben.

Die zertifikatsbasierte Authentisierung erfolgt wie die PSK-Authentisierung. Der Unterschied ist: Je nach Verbindung kann ein anderes Zertifikat zum Einsatz kommen. Und wer sein CA-Zertifikat nicht veröffentlicht, kann gezielt steuern, wer zugreifen darf.

Ein weiterer Vorteil einer zertifikatsbasierten Authentisierung: Die CA darf einzelne Zertifikate widerrufen. In der sogenannten CRL (Certificate Revocation List) werden alle Zertifikate, die irgendwie ungültig geworden sind, gesperrt. Bei einer PSK-Authentisierung ist dagegen der Austausch aller Schlüssel erforderlich.

Aggressive Mode [Im "Aggressive Mode" werden die obigen Schritte auf drei zusammengefasst. Hierbei fällt dann die Verschlüsselung des obigen fünften Schrittes weg. Stattdessen werden die Hashwerte der PSKs im Klartext übertragen. Die Sicherheit des Verfahrens ist eng mit der Stärke des "pre shared keys" und des Hashverfahrens gekoppelt. Ein guter Schlüssel ist eine zufällige Wertefolge in der maximalen Schlüssellänge. Da in der Praxis gute Schlüssel oft aus Bequemlichkeit nicht gewählt werden, sollte man diesen Modus mit Vorsicht einsetzen.

Ein Grund für den Einsatz dieses Modus kann jedoch gegeben sein, wenn die Adresse des Initiators dem Responder a priori nicht bekannt ist, und beide Seiten pre-shared Keys zur Authentisierung einsetzen wollen. Weitere Anwendungsszenarien sind gegeben, wenn ein schnellerer Verbindungsaufbau gewünscht ist und die „policies“ des Responders hinlänglich bekannt sind. *Beispiel:* Angestellter will aus der Ferne auf das Firmennetz zugreifen – Richtlinien (z. B. Verschlüsselung mit AES, Hashing mit SHA und Authentisierung mit RSA Signaturen, die durch die Zertifizierungsstelle der Firma signiert wurden) sind soweit bekannt.

NAT traversal and IPsec

In order for IPsec to work through a NAT, the following protocols need to be allowed on the firewall:

* Internet Key Exchange (IKE) - User Datagram Protocol (UDP) port 500
* Encapsulating Security Payload (ESP) - IP protocol number 50

or, in case of NAT-T:

* IPsec NAT-T - UDP port 4500

Often this is accomplished on home routers by enabling "IPsec Passthrough".

The default behavior of Windows XP SP2 was changed to no longer have NAT-T enabled by default, because of a rare and controversial security issue[1]. This prevents most home users from using IPsec without making adjustments to their computer configuration. To enable NAT-T for systems behind NATs to communicate with other systems behind NATs, the following registry key needs to be added and set to a value of 2:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IPsec\AssumeUDPEncapsulationContextOnSendRule[1]

IPsec NAT-T patches are also available for Windows 2000, Windows NT and Windows 98.

One usage of NAT-T and IPsec is to enable opportunistic encryption between systems. NAT-T allows systems behind NATs to request and establish secure connections on demand.

SmartSenior: Beteiligte Funktionen

- Verschlüsselung

DataGrid

Dienste-Infrastruktur und -Plattform

Firewall

Krankenhaus, …

Data

Verwandte Person

VPN über IP sec Tunnel

Internet, PSTN, GSM/UMTS, WLAN

Teleservice Center z.B. Pflegedienst

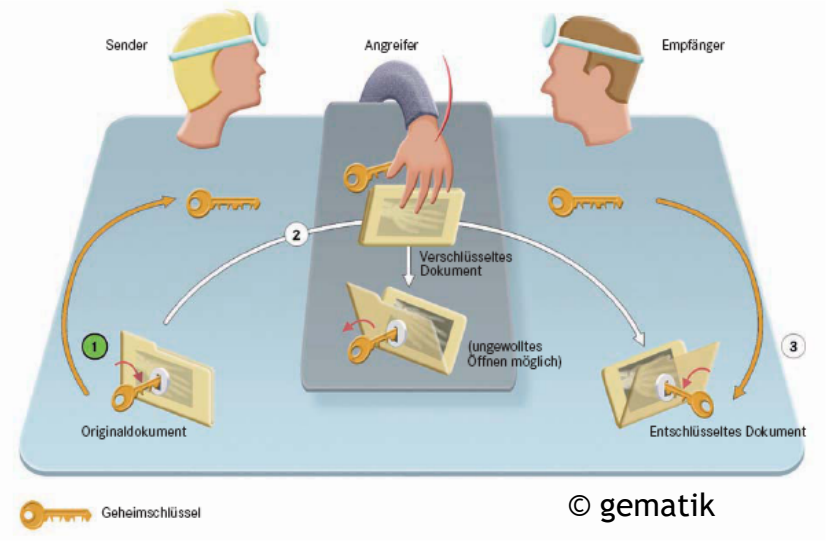
Senior Zuhause

IP-TV-Provider

Senior Unterwegs

Alcatel·Lucent

Symmetrische und asysmmetrische Verschlüsselung (© gematik)



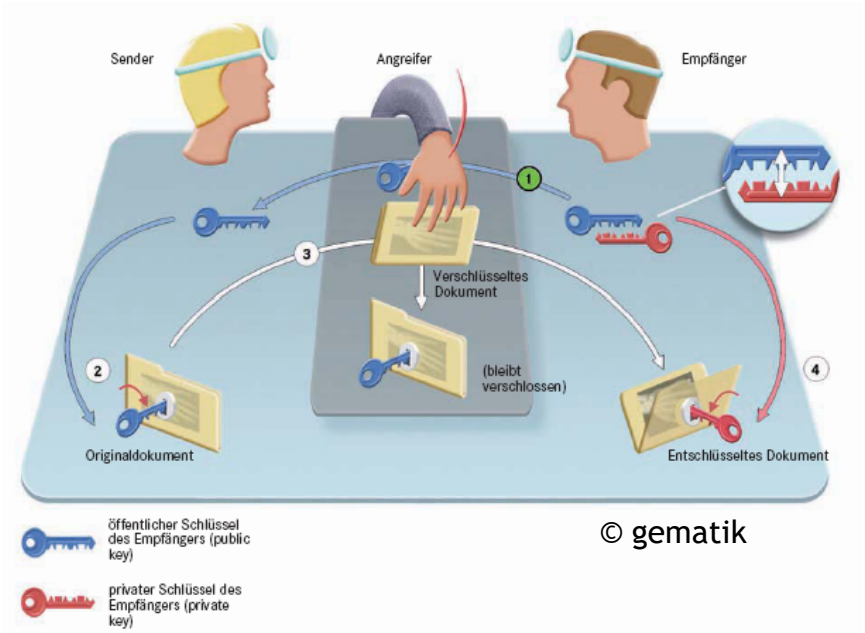
© gematik

Abbildung 1a:
Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung wird ein geheimer Schlüssel zum Verschlüsseln der Nachricht verwendet ❶. Die für die Sicherheit wichtigste Frage ist: Wie transportiert der Sender (links) seinen geheimen Schlüssel zum Empfänger (rechts)? Der Empfänger braucht diesen Schlüssel, um die codierte Nachricht lesen zu können. Dabei werden ihm das verschlüsselte Dokument und der geheime Schlüssel über zwei getrennte Transportwege ❷ zugeschickt. Ein möglicher Angreifer (Mitte) kann sowohl die Nachricht als auch den Schlüssel abfangen. Verfügt er über beides, kann er das Originaldokument lesen. Der Empfänger merkt beim Öffnen der Nachricht ❸ nicht, ob der Schlüssel von einem Angreifer kopiert wurde.

Vorteil:
- Das Verfahren nimmt relativ wenig Rechenzeit in Anspruch und ist deshalb sehr schnell.

Nachteile:
- Sender und Empfänger müssen den Schlüssel sicher austauschen.
- Für den Versand des Schlüssels muss ein zusätzlicher Kanal geschaffen werden, der eine höhere Sicherheit bietet, als der Transportkanal für das verschlüsselte Dokument.



© gematik

Abbildung 1b:
Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung benutzen Sender (links) und Empfänger (rechts) das Schlüsselpaar des Empfängers. Dieses besteht aus einem öffentlichen und einem privaten Schlüssel: Mit dem öffentlichen Schlüssel können Dokumente ausschließlich codiert werden. Dechiffrieren lassen sie sich nur mit dem privaten Schlüssel. Die Bedingung für diese Art der Verschlüsselung ist, dass der Empfänger seinen öffentlichen Schlüssel allen zur Verfügung stellt, die ihm Dokumente zuschicken möchten ❶. Damit kann ein Sender nun ein Dokument zuschließen/verschlüsseln ❷. Das codierte Dokument erreicht über einen unsicheren Transportweg ❸ den Empfänger. Dass auch der Angreifer (Mitte) über den öffentlichen Schlüssel des Empfängers verfügt, beeinträchtigt die Sicherheit nicht – er kann damit die Nachricht nicht öffnen. Nur der Empfänger kann das verschlüsselte Dokument mit seinem privaten Schlüssel dechiffrieren ❹. So bleibt das Dokument für den Angreifer geheim.

Vorteile:
- Der Empfänger kann seinen öffentlichen Schlüssel jedem frei zur Verfügung stellen, denn damit lassen sich Dokumente nur verschlüsseln, nicht entschlüsseln.
- Der private Schlüssel muss nie über einen unsicheren Transportkanal verschickt werden, sondern bleibt immer beim Empfänger.

Nachteil:
- Das Verfahren ist relativ rechenintensiv.

Verschlüsselung und Datentransport in der Telematikinfrastruktur (© gematik)

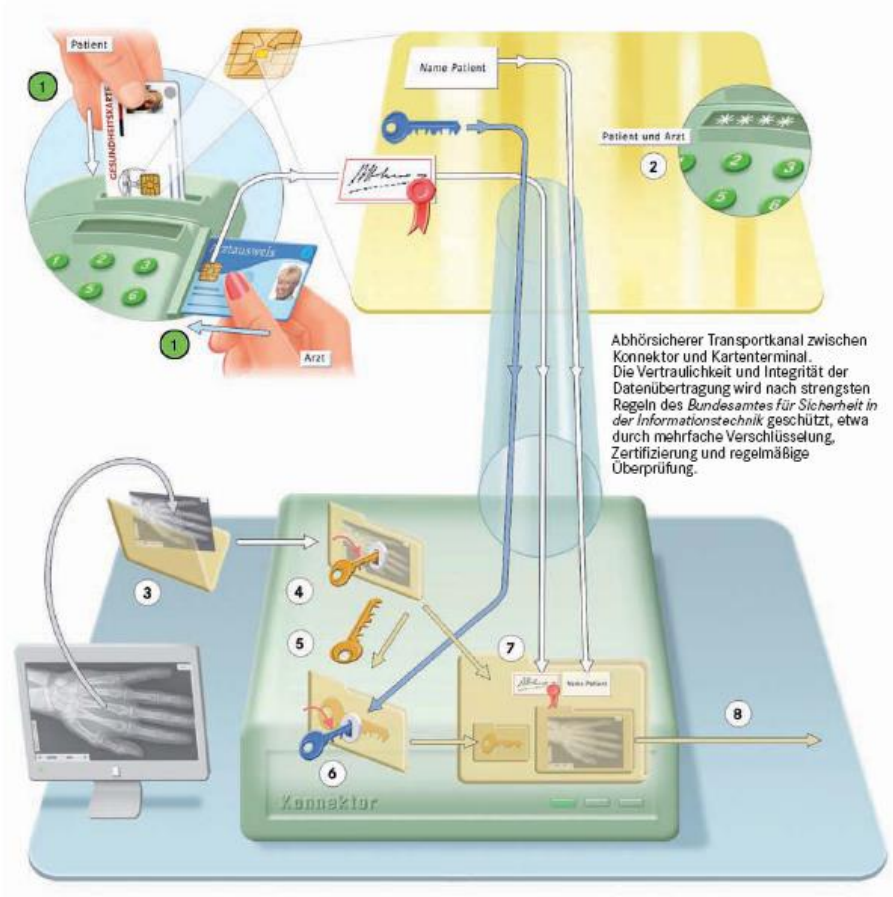


Abbildung 3a:
Verschlüsseln von Gesundheitsdaten

Für die Verschlüsselung von Gesundheitsdaten greift das Zweikartenprinzip:

Nur wenn sich beide Karten im Kartenlesegerät befinden ❶ und bei beiden Karten die richtige PIN eingegeben wird ❷, können Daten in die Telematikinfrastruktur geschickt werden. Die Dechiffrierung folgt dem Prinzip der asymmetrischen Verschlüsselung > Abb. 1c.

Die Gesundheitsdaten werden zuerst zu dem Konnektor geschickt ❸.

Dieser generiert nach dem Zufallsprinzip nun einen einmalig zu verwendenden Geheimschlüssel und codiert damit symmetrisch die Gesundheitsdaten ❹. Der geheime Schlüssel wird mit dem öffentlichen Schlüssel der elektronischen Gesundheitskarte verschlüsselt ❺ ❻. Um sicherzustellen, dass die Daten wirklich zum Patienten gehören und vom Arzt signiert wurden, wird noch ein Zertifikat beigefügt ❼. Alle Daten werden danach in einen digitalen Ordner gepackt und zum Versand bereitgestellt ❽.

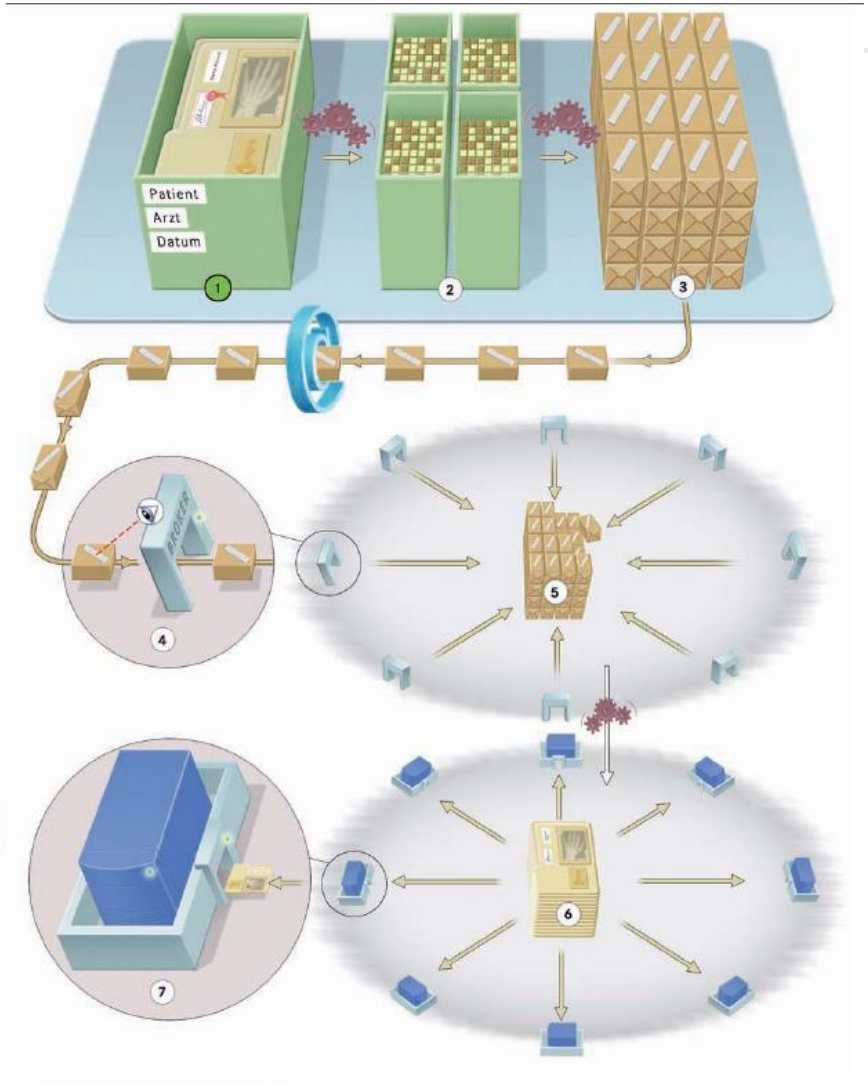


Abbildung 4:
Datentransport in die Telematikinfrastruktur

Die verschlüsselten Gesundheitsdaten ❶ werden für den Datentransport zweimal in Datenpakete geteilt und anschließend verschlüsselt: zuerst auf Anwendungsebene mit dem „Secure Sockets Layer"-Protokoll (SSL) ❷. Mittels des „Internet Protocol Security"-Verfahrens (IP sec) werden die SSL-Datenpakete danach nochmals in kleinere Transportpakete geteilt ❸. Die Datenpakete werden von dem Broker kontrolliert und entgegengenommen ❹. In der Telematikinfrastruktur werden sie wieder zugeordnet ❺, zusammengesetzt ❻ und in Rechenzentren abgelegt ❼.

Qualifizierte Elektron. Signatur (QES) und Zertifikat

Eine **qualifizierte elektronische Signatur** (*QES*) ist nach dem deutschen Signaturgesetz eine fortgeschrittene elektronische Signatur, die auf einem (zum Zeitpunkt ihrer Erzeugung gültigen) qualifizierten Zertifikat beruht und mit einer sicheren Signaturerstellungseinheit (SSEE) erstellt wurde.

Jeder geheime, auf asymmetrischen Verschlüsselungsverfahren basierende Signaturschlüssel hat immer einen einzigen korrespondierenden öffentlichen Signaturprüfschlüssel.

Ein Zertifikat des Zertifizierungsdiensteanbieters (ZDA) ist die elektronische Bescheinigung, dass der Signaturprüfschlüssel und damit auch der korrespondierende Signaturschlüssel **einer Person zugeordnet wurde und die Identität dieser Person bestätigt werden kann (vgl. § 2 Nr. 6 Signaturgesetz).**

Bei der elektronischen Signatur enthält das Zertifikat den öffentlichen Schlüssel, mit dem der während der Signaturerstellung verschlüsselte Hashwert (Prüfsumme) des elektronischen Dokuments entschlüsselt und gegen einen neu erstellten Hashwert verglichen und damit die Authentizität des elektronischen Dokuments überprüft werden kann.

Akkreditierte Anbieter qualifizierter Zertifikate sind
TC TrustCenter, T-Systems mit Telesec, die Sparkassen-Finanzgruppe mit S-TRUST,
die DATEV mit e:secure, D-TRUST (Bundesdruckerei-Gruppe), die Deutsche Post AG mit Signtrust, die Bundesnotarkammer sowie die DGN Deutsches Gesundheitsnetz Service und die medisign der Deutschen Apotheker- und Ärztebank.

Aus: http://de.wikipedia.org/wiki/Qualifizierte_elektronische_Signatur

SHL-Telemedizin: CardioSen‘C EKG mit eingebauter Mobilfunk-Schnittstelle

Simultane 12-Kanal-EKG Ableitung in Echtzeit (innerhalb von drei Sekunden) für eine verbesserte Daten-Qualität und eine schnellere Datenübertragung.

Das eingebaute Mobilfunkmodem ermöglicht eine Übermittlung von digital verschlüsselten EKG Daten für eine maximale Genauigkeit. Im Vergleich zur akustischen, analogen Übertragung über ein herkömmliches Telefon treten dabei keine Hintergrundgeräusche auf.

Falls kein Mobilfunknetz vorhanden ist, kann das 12-Kanal-EKG akustisch über einen Festnetzanschluss übermittelt werden.

Das medizinische Team im Telemedizinischen Zentrum kann das CardioSen'C aus der Ferne steuern. Dies ermöglicht eine klare und akkurate Übermittlung mit minimalem Aufwand auf der Benutzerseite.

Das CardioSen'C verfügt über ein innovatives Design mit moderner Ergonomie, wozu auch das große LCD Display und gesprochene Bedienungsanweisungen gehören.

Die neu entwickelten Elektroden garantieren einen besseren Hautkontakt und verfügen über eine optimierte Leitfähigkeit.

Zulassung der der amerikanischen Arzneizulassungsbehörde (FDA)

CE Zulassung

CardioSen'C ist ein eingetragenes Warenzeichen der SHL Telemedizin.

Relevante Standardisierungsgremien

- Deutsches Institut für Normung e. V. (DIN)
  Fachbereich NA 063-07 Medizinische Informatik
  Arbeitsausschuss NA 063-07-02 Interoperabilität
- CEN TC 251 Health Informatics
  Working Group IV Technology for Interoperability
- ISO TC 215 Health Informatics
  Working Group VII Health Care Devices
- CLSI Clinical and Laboratory Standards Institute
- HL7 International
  Special Interest Group Health Care Devices
- HL7 Deutschland
- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)
- E-Health Competence Center, Regensburg

Frequenzbänder und Funkdienste von ca.27 MHz bis 24 GHz

26,957 MHz – 27,283 MHz	ISM
40,66 MHz – 40,70 MHz	ISM
433,05 MHz – 434,79 MHz	ISM
870 MHz – 876 MHz, 915 MHz – 921 MHz	TETRA (nur in Deutschland)
868 MHz – 870 MHz	ISM
890 MHz – 915 MHz, 935 MHz – 960 MHz	GSM
1880 MHz – 1900 MHz	DECT, DPRS, GSM
2400 MHz – 2483,5 MHz	ISM, WLAN, IEEE802.11b, Bluetooth, ZigBee HomeRF
1900 MHz – 1980 MHz, 2110 MHz – 2170 MHz	UMTS
5150 MHz – 5350 MHz, 5725 MHz – 5825 MHz	WLAN IEEE 802.11a
5725 MHz – 5875 MHz	ISM
24000 MHz – 24250 MHz	ISM

ISM: Industrial, Scientific, and Medical Band

Die ISM-Bänder werden von einer Vielzahl von ISM- und anderen Anwendungen genutzt:

Funketiketten (*Smart Tags*) (13,56 MHz)
Modellbau-Fernsteuerungen (27 MHz, 40,6 MHz, 2,4 GHz)
Babyphone (27 MHz, 433 MHz)
Funk-Thermometer (433 MHz) , Funk-Schalter, wie z.B. Autoschlüssel, Funk-Steckdosen (433 MHz)
Funk-Alarmanlagen (433 MHz), Funk-Kopfhörer oder Funk-Lautsprecher (auslaufend bei 433 MHz)
Drahtlose Videoübertragungssysteme (2,4 GHz)
WLAN (nach IEEE 802.11b / IEEE 802.11g) (2,4 GHz), Bluetooth (2,4 GHz) , IEEE 802.15.4 (*ZigBee*) (2,4 GHz)
Mikrowellenherde (2,4 GHz)
Radar-Bewegungsmelder (24 GHz)

Siehe http://de.wikipedia.org/wiki/ISM-Band

SmartSenior: Mit dem **Standard TM7** soll
die Etablierung eines Qualitätslabels für Geräte und Services erfolgen
die Sicherstellung der Kompatibilität von Diensten national und international forciert werden
die Kompatibilität von Diensten und Produkten zu sichern, um die Attraktivität für Kunden zu erhöhen und telemedizinische Dienste in die Fläche zu bringen.
Durch den Aufbau einer Zertifizierungsstelle gemeinsam mit DIN und ETSI soll die Verbreitung des Standards TM7 gesichert werden.
•Standardisierung von Diensten in TP7
parallel betrachtet und in einem generischen, Service orientierten Ansatz zusammengeführt. Dies führt dazu, dass die o.g. Probleme aufgelöst werden:
Die große, proprietäre Vielfalt der telemedizinischen Technologie wird durch ein modulares Dienstekonzept aufgebrochen.
Mit TM7 wird ein die internationalen Basisstandards (VITAL, Videokonferenz, DICOM, HL/7, CDA, …) nutzender, darüber hinaus gehender Standard für Kommunikationsprotokolle und Dienste entwickelt.
Für die relevanten Geschäftsmodelle der einzelnen Anwendungen (siehe z.B. SmartSenior TP 2, 3 und 4) werden die Mechanismen zu deren Implementierung in der Plattform realisiert. Dies beginnt bei der Abbildung der Rollen und endet mit den Abrechnungsmodellen.
Die wichtigsten Bereiche für die Standardisierung sind: Ontologie; Geräte; Patientenakte; Abrechnung; Imaging; Verschlüsselung; Klinische Studien
Das TM7 Modell wird in 4 Bereiche unterteilt: Patientendaten; Medizin; Geräte und Kommunikation; Anwendungen

In dem Projekt **Strokenet** wurde ein System entwickelt werden, dass die Versorgung von Schlaganfallpatienten im Notfall bereits vor Ort und im Rettungswagen durch den Einsatz von IuK-Technologien optimiert und damit dazu beiträgt, mögliche Folgeschäden zu reduzieren. Die im Rahmen des vorgeschlagenen Projektes neu zu entwickelnden Systeme sind mobil einsetzbar (Rettungswagen) und stationär nutzbar (Rettungsleitstelle, StrokeUnit). Dabei werden vorhandene Infrastrukturen und bereits etablierte Organisationsstrukturen in Berlin genutzt. Im Projekt StrokeNet wird bereits ein Videoconferencing und eine Vitaldatenübertragung aus fahrenden Krankenwagen heraus vorgenommen. Dabei werden die Übertragungskanäle (WLAN, UMTS, WiFi) in Abhängigkeit von der besten Übertragungsqualität automatisch und nahtlos umgeschaltet.

- www.strokenet.de

Die **Continua Health Alliance (CHA)** will einheitliche Telemedizin-Standards etablieren, die eine Integration verschiedenster Technologien und Anwendungen ermöglichen und damit in einem besseren und kosteneffektiveren und hier insbesondere in einem persönlichen Gesundheitsmanagement resultieren. Die CHA sucht hierfür die Zusammenarbeit mit führenden Institutionen des Gesundheitswesens und setzt auf eine Mitgliederstruktur, die speziell global agierende Unternehmen umfasst. Die wesentlichen Anwendungsfelder für die mit etablierten Qualitätslabel und Standards der CHA entwickelten Produkte und Dienste sind der zweite und dritte Gesundheitsmarkt. Der hier gegenüber im Projekt zu entwickelnde TM7-Standard fokussiert stärker die technische Interoperabilität von Telemedizinlösungen für den ersten Gesundheitsmarkt. Basierend auf bereits bestehenden medizinischen / medizintechnischen Standards werden hierbei Lösungen für bestehende Interoperabilitätsprobleme entwickelt. Zudem wird ein Standard für die Übertragung von Funktionalität definiert. Durch die Beteiligung vieler KMU und die frühzeitige Einbindung entsprechender Normierungsgremien (DIN, ETSI, CEN, ISO) in TM7 wird sichergestellt, dass sich der neue Standard durchsetzt. Kurzfristig ist mit der Formulierung einer PAS eine schnelle markttaugliche Lösung zu erwarten.

Bluetooth-Eigenschaften

Bluetooth, along with other ISM radio technologies, operates in the 2.4–2.485-GHz band, and its radio meets the set of power and spectral emissions specifications defined by ETSI ETS300-328 in Europe and CFR 47 Part 15 in the United States.
Bluetooth uses the following set of parameters:

- Frequency-hopping, spread-spectrum 79 channels, 1600 hops/sec.
- Gaussian frequency shift modulation (GFSK).
- 1-Mb/sec raw data rate, realizable throughput >700 Kb/sec.
- 83.5 MHz of spectrum, divided into 1-MHz channels.
- Power control based on received signal strength indicator (RSSI) feedback from receiving device (Class I requirement).
- 0 dBm (1 mW) without power control (Class III, 10-m range).
- 20 dBm (100 mW) with power control (Class I, 100-m range).

The Bluetooth Host Stack for eHealt/medical applications includes the

- Multichannel Adaptation Protocol (MCAP) and the
- Bluetooth Health Device Protocol (HDP).

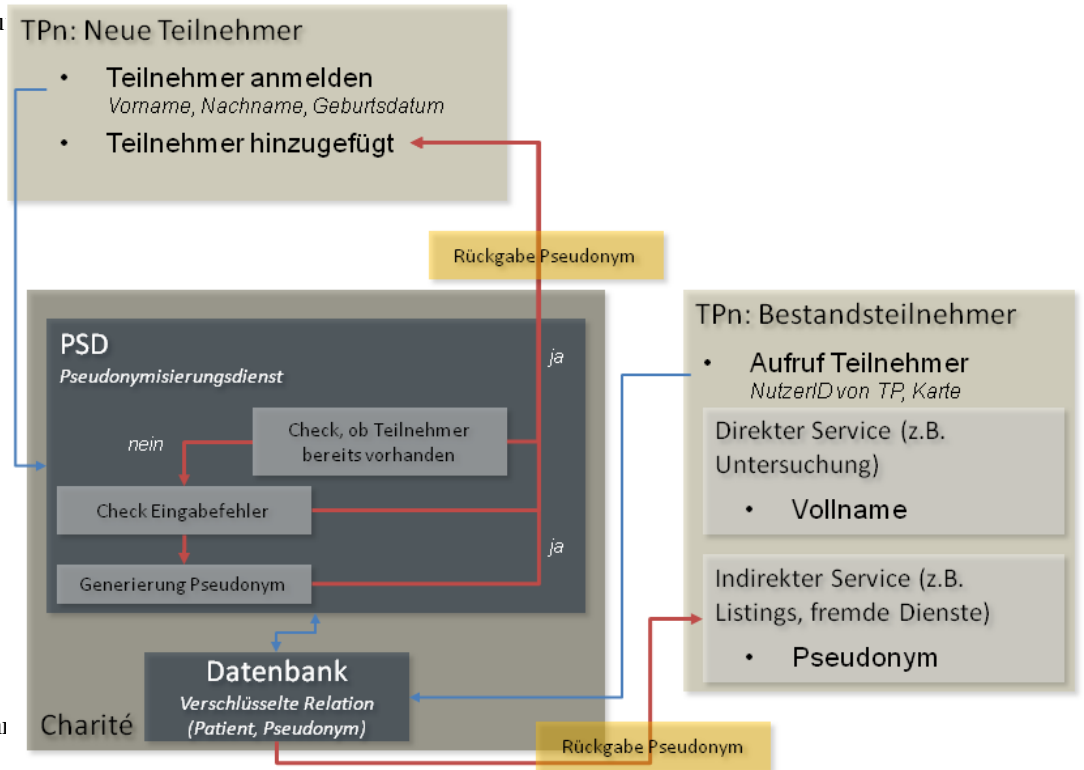
MCAP and HDP are specifications that are specific to Bluetooth health/medical devices. MCAP allows for a robust connection, including support for streaming data. The Health Device Profile (HDP) is the Bluetooth application profile that allows for source devices, such as blood pressure monitors, weight scales, glucose meters to exchange data with sink devices such as mobile phones, laptops and health appliances

Nach http://www.devicelink.com/mddi/archive/04/06/001.html und
http://www.ifoundrysys.com/downloads/6whitepapers/Designing%20Bluetooth%20Medical%20Devices.pdf

SmartSenior: Sicherheitskonzept

Neben dem Gebot der **Vertraulichkeit** gibt es eine weitere Reihe von Kriterien, die erfüllt werden müssen:

- **Authentizität**: es muss klar nachvollziehbar sein, wer für eine bestimmte Aktionen/Leistungen verantwortlich ist oder diese ausgelöst hat. Dies kann sich sowohl auf Personen wie auch au Geräte beziehen, die z.B. Messwerte liefern.
- **Korrektheit**: es muss zu jedem Zeitpunkt sichergestellt sein, dass die Daten in allen Phasen der Verarbeitung vollständig, echt, korrekt und ohne Widersprüche sind.
- **Nutzbarkeit**: Neben der Korrektheit der Daten ist ebenso sicherzustellen, dass die Daten die für den jeweiligen Nutzungszweck erforderliche Qualität und Aktualität haben und in einer für die relevanten Systeme les- und verarbeitbaren Form vorliegen
- **Verfügbarkeit**: es müssen die für eine Behandlung oder für einen Vorgang relevanten Daten jeweils zum richtigen Zeitpunkt verfügbar sein. Grundsätzlich kann dies bedeuten, dass Daten in Echtzeit zur Verfügung stehen, wenn dies erforderlich ist, Daten aber genau dann übertragen werden, wenn eine Aktion oder Reaktion erforderlich ist.
- **Dokumentation**: Für den Arzt und das Krankenhaus besteht die Pflicht, Behandlungen zu dokumentieren. Dies bindet im Fall des Einsatzes von Telemedizin damit auch das Erfordernis ein, lückenlos nachvollziehen zu können, wer wann welche Informationen verarbeitet hat. Dies betrifft insbesondere auch die Dokumentation zum konkreten Fall: Wer hat wann welche Daten an wen verschickt, bzw. von wem empfangen.
- **Rechtssicherheit**: Eng verbunden mit der Dokumentation und wesentlich darauf aufbauend ist es, dass beweiskräftig nachvollziehbar wird, wer auf welcher Grundlage welche medizinischen Entscheidungen getroffen hat. Hierfür ist es genauso relevant die Rollen und Rechte der Teilnehmer rechtskonform in telemedizinischen Anwendungen abzubilden.
- **Skalierbare Nutzerrechte**: für alle anfallenden medizinischen Daten muss festgelegt werden können, welche Nutzer(gruppen) diese Daten lesen und/oder verarbeiten dürfen und für welche Gruppen Nutzungsrechte ausgeschlossen werden



Pseudonymisierungsdienst

REST

Der Begriff **Representational State Transfer** bzw. das Akronym **REST** bezeichnen einen Softwarearchitekturstil für verteilte Hypermedia-Informationssysteme wie das World Wide Web .

REST setzt auf ein zustandsloses Client/Server-Protokoll. Dabei enthält jede HTTP-Botschaft alle Informationen, die notwendig sind, um die Nachricht zu verstehen. Deshalb muss weder der Server noch der Client Zustandsinformationen zwischen zwei Nachrichten speichern. Eine derartig strikte Trennung der Zuständigkeiten zwischen Client und Server führt dazu, dass ein REST-konformer Webservice als zustandslos (stateless) bezeichnet werden kann: Jede Anfrage eines Clients an den Server ist in dem Sinne in sich geschlossen, als dass sie sämtliche Informationen über den Anwendungszustand beinhaltet, die vom Server für die Verarbeitung der Anfrage benötigt werden.
Dies gilt z. B. auch für Authentifizierungsinformationen; statt "login via cookie" wird in jeder URI z. B. ein Passwort-Hashcode übertragen.

Zustandslosigkeit in der hier beschriebenen Form wirkt sich begünstigend auf die Skalierbarkeit eines Webservice aus. Beispielsweise können eingehende Anfragen im Zuge des Load Balancing unkompliziert auf beliebige Maschinen verteilt werden: da jeder Request in sich geschlossen ist und Anwendungsinformationen somit ausschließlich auf der Seite des Clients vorgehalten werden, ist auf der Seite des Servers kein Session Handling erforderlich. In der Praxis nutzen jedoch viele HTTP-basierte Anwendungen Cookies und andere Techniken, um Zustandsinformationen zu behalten.