Kompetenznetz Angeborene Herzfehler

TMF Workshop Sicherheitskonzepte
11. Dezember 2006

Bericht aus dem Kompetenznetz Angeborene Herzfehler

Dipl. Inform. Michael Beckmann

Prof. Dr. Ulrich Sax

Abt. Medizinische Informatik

Bereich Humanmedizin Universität Göttingen

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

KN-AHF Einführung 1/3
Angeborene Herzfehler

- Angeborene Herzfehler (AHF) sind mit einer Inzidenz von 0,7 – 0,8 % bei allen Lebendgeborenen die häufigsten angeborenen Erkrankungen (pro Jahr ca. 6000 Neugeborene mit AHF)
- Durch medizinische Fortschritte erreichen heute ca. 90 % das Erwachsenenalter; z. Zt. leben ca. 200.000 bis 300.000 Patienten mit AHF in Deutschland
- die Mehrzahl bleibt lebenslang chronisch krank → Einschränkungen der Lebensqualität, Leistungs- und Arbeitsfähigkeit
- die Forschung auf dem Gebiet der primären Korrektur der AHF ist weit fortgeschritten, die Forschung bei der Behandlung der chronischen Folge-erkrankungen und die Versorgungsforschung ist unzureichend entwickelt
- die relativ kleinen Patientenzahlen in den einzelnen Herzzentren bzw. in den einzelnen AHF-Diagnosen ließen bisher keine Studien mit aussagekräftigen Ergebnissen zu

KN-AHF Einführung 2/3
Ziele des KN-AHF

Das Kompetenznetz Angeborene Herzfehler trägt zur besseren Versorgung herzkranker Kinder und zunehmend auch Erwachsener bei. Bei seinen Aktivitäten in Krankenversorgung und Wissenschaft werden regelmäßig sensible Daten der Patienten und Angehörigen verarbeitet. Um dies sicher und datenschutzrechtlich korrekt leisten zu können, hat das KN-AHF den Datenschutz in seiner Satzung verankert.

Das Nationale Register für angeborene Herzfehler strebt die deutschlandweite Erfassung möglichst aller Patienten an. Es bildet somit die Grundlage für epidemiologische Studien, die bisher international fehlen.

KN-AHF Einführung 3/3 Organisationsstruktur

- Netzwerkzentrale am Deutschen Herzzentrum Berlin
- Telematik und Informationsdienste in der Abt. Med. Informatik Göttingen
- Zentraler Biometrischer Dienst am Institut für Biometrie Magdeburg
- Studienmanagement KKS Charite Berlin
- Kinderkardiologische Zentren, Universitätskliniken und niederg. Ärzte

Überblick

content security (Integrität)

Kommunikationssicherheit (Vertraulichkeit)

Zugangssicherheit (Nicht-Abstreitbarkeit, Authentizität)

Management von Sicherheit (Policies)

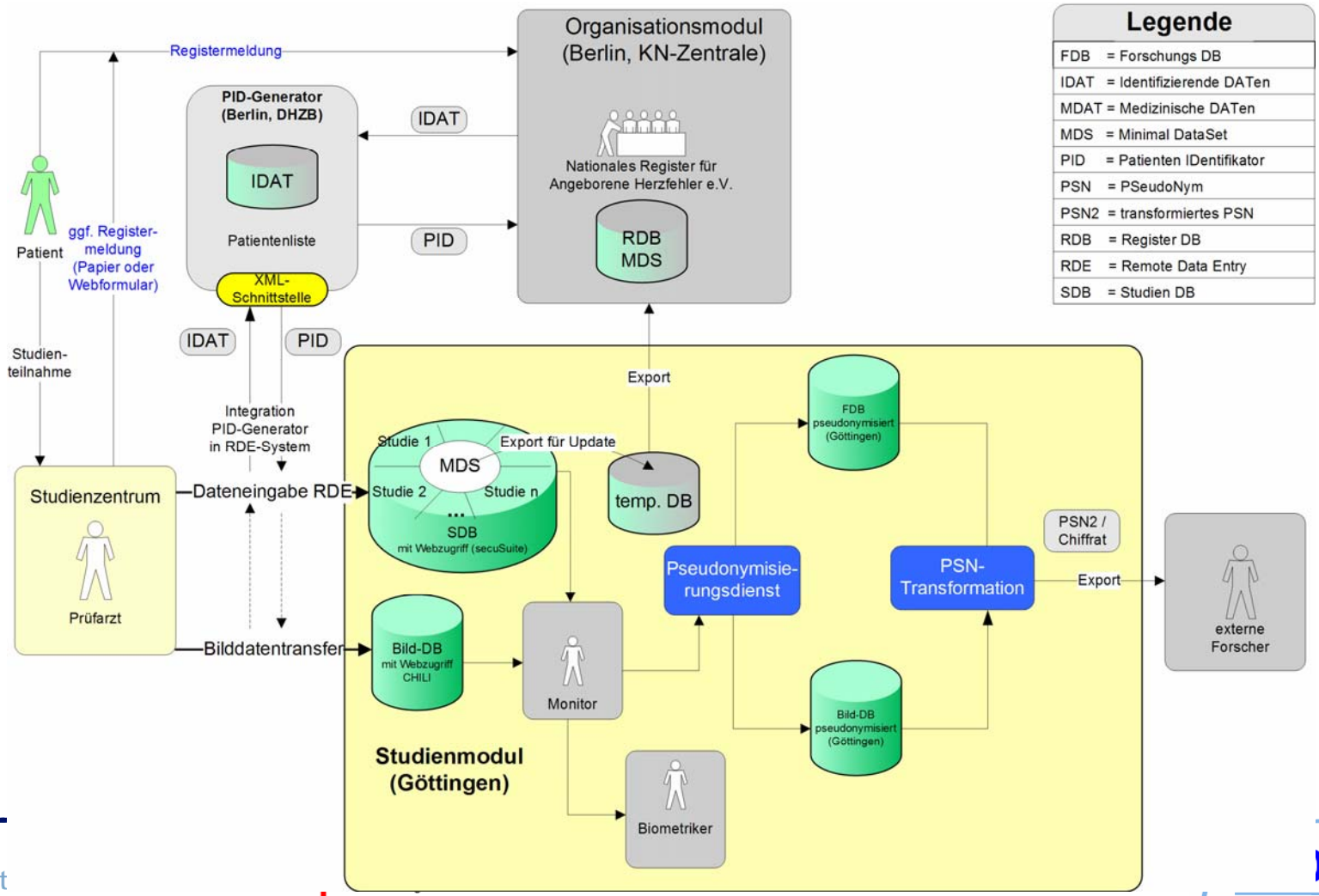
Pragmatische Beschreibung von Sicherheit aus Werkzeug-Sicht; modifiziert nach Titterington [1]

Datenschutzkonzept KN-AHF

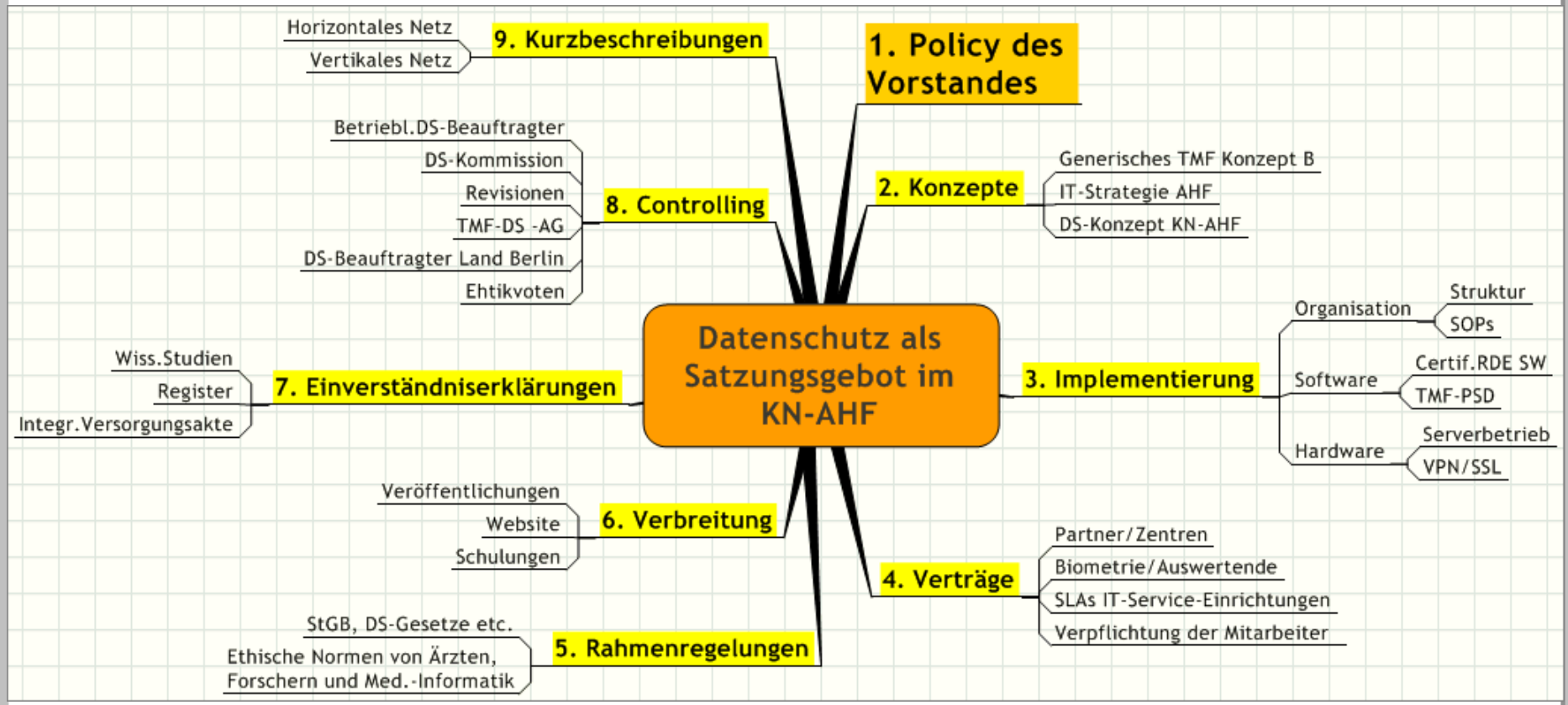
Vorlage TMF-Konzept B (forschungszentriert)

- erhobene Daten stammen nicht aus Behandlungsprozess, sie werden in speziell konzipierten Studien gewonnen
- es existiert keine unmittelbare Rückwirkung von den Studien auf die Behandlung
- das RDE-System erlaubt dezentrale Erhebung in einer Studiendatenbank mit zentraler Vergabe eines PID vom TMF-PID-Generator
- Qualitätssicherungsstufe ist in RDE-System integriert
  → Monitor-Rolle
- qualitätsgesicherte Daten werden über den Pseudonymisierungsdienst in die Forschungsdatenbank transferiert, wo sie externen Forschern auf Antrag in anonymisierter oder pseudonymisierter Form zur Verfügung stehen

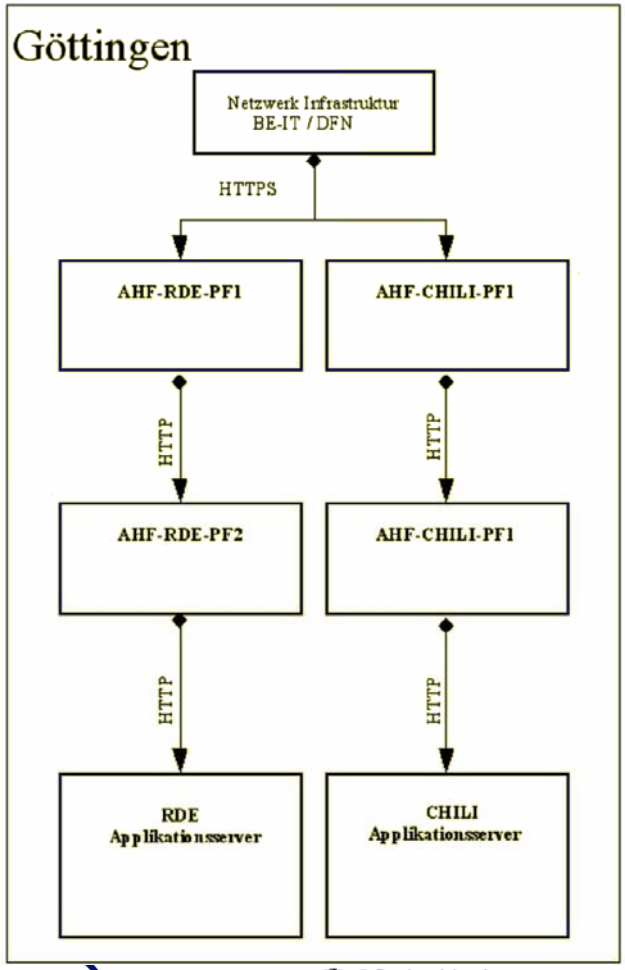
Überblick: Funktionen und Standorte



Umsetzung der Datenschutzanforderungen



Sicherheitsmanagement
Überblick zu den Systemen



Bereitgestellte Dienste AHF-RDE/CHILI-PF1:

Webserver
Stateful Packetfilter
Intrusion Detection System
Intrusion Prevention System

Kurzbeschreibung AHF-RDE/CHILI-PF1:

- Nimmt gewollte Verbindungen aus dem Internet entgegen
- Überprüft alle ankommenden Daten auf Schadroutinen
- Übernimmt für gewollte Verbindungen die Vermittlungsrolle zwischen Applikationsserver und berechtigtem Client

Bereitgestellte Dienste AHF-RDE/CHILI-PF2:

Stateful Packetfilter
Intrusion Detection System
Intrusion Prevention System
Datenbank für Intrusion Detection Logs

Kurzbeschreibung AHF-RDE/CHILI-PF2:

- empfängt Anfragen von PF1
- Überprüft die genutzten Protokolle auf Schadroutinen
- leitet Anfragen von PF1 an den Applikationsserver

Getroffene Sicherheitsmaßnahmen

- Paketfilter – insgesamt zwei Paketfilternde Instanzen
- Proxy-Modul (Apache)
- Netzwerkbasiertes Intrusion Detection System (NIDS) Snort
- Hostbasiertes Intrusion Detection System Tripwire
- Maßnahmen zur Härtung des OS:
  - Kernelbasierter Buffer-Overflow-Schutz (PaX)
  - Betriebssystembasierte-Sicherheitsmaßnahmen wie z.B. Sicherheitsfördernde Kernelparameter (Verhinderung von Source-Routing, Verweigerung der ICMP-Redirect Meldungen, usw.)

Inhaltliche Sicherheit

Rechenzentrum UKG

- Zugangskontrolle
- HW-Überwachung
- USV
- Feuerschutz (CO_2 – Löschanlage)
- Safe für Backup-Medien

GWDG: Bandroboter zur Sicherung des Bild-DB

Kommunikationssicherheit
Technische Umsetzung

PKI (GWDG):

- Server
- Client
  (Gruppenzertifikat + pers. Zertifikate)
- RBAC in Applikationen
  (Application gateway prüft Zertifikate)
- Teleradiologie-WS werden über VPN verbunden
- alle Verbindungen über HTTPS

Knackpunkte

- TMF-Datenschutzkonzept (B) verlangt mehrere Standorte (Biomaterialbank-Konzept noch mehr)
- Jeder der Standorte muss
  - SLA abschliessen
  - Sicherheitsmanagement durchführen
  - über entsprechenden Applikationsadmin verfügen
  - Billing (Kosten, insbesondere bei Industrie)

Knackpunkte

- Standorte / Netze
  - sind unerfahren mit SLAs
  - können Daten sichern, aber
  - komplexe Applikationen nicht administrieren
  - Industrie (ComputaCenter, SerNet, etc.) reduziert Hosting auf funktionale Bereitstellung (Black box)

Vielen Dank für Ihre Aufmerksamkeit!

Literatur

[1] Titterington G, Bassanese P,

Chappell C. E-business Security New Directions and Successful Strategies. London: Ovum Ltd., 2000.