Sicherheitskonzepte in der vernetzten medizinischen Forschung
TMF-Workshop, Berlin, 11.12.2006

Bericht aus dem Kompetenznetz Pädiatrische Onkologie und Hämatologie (KPOH)

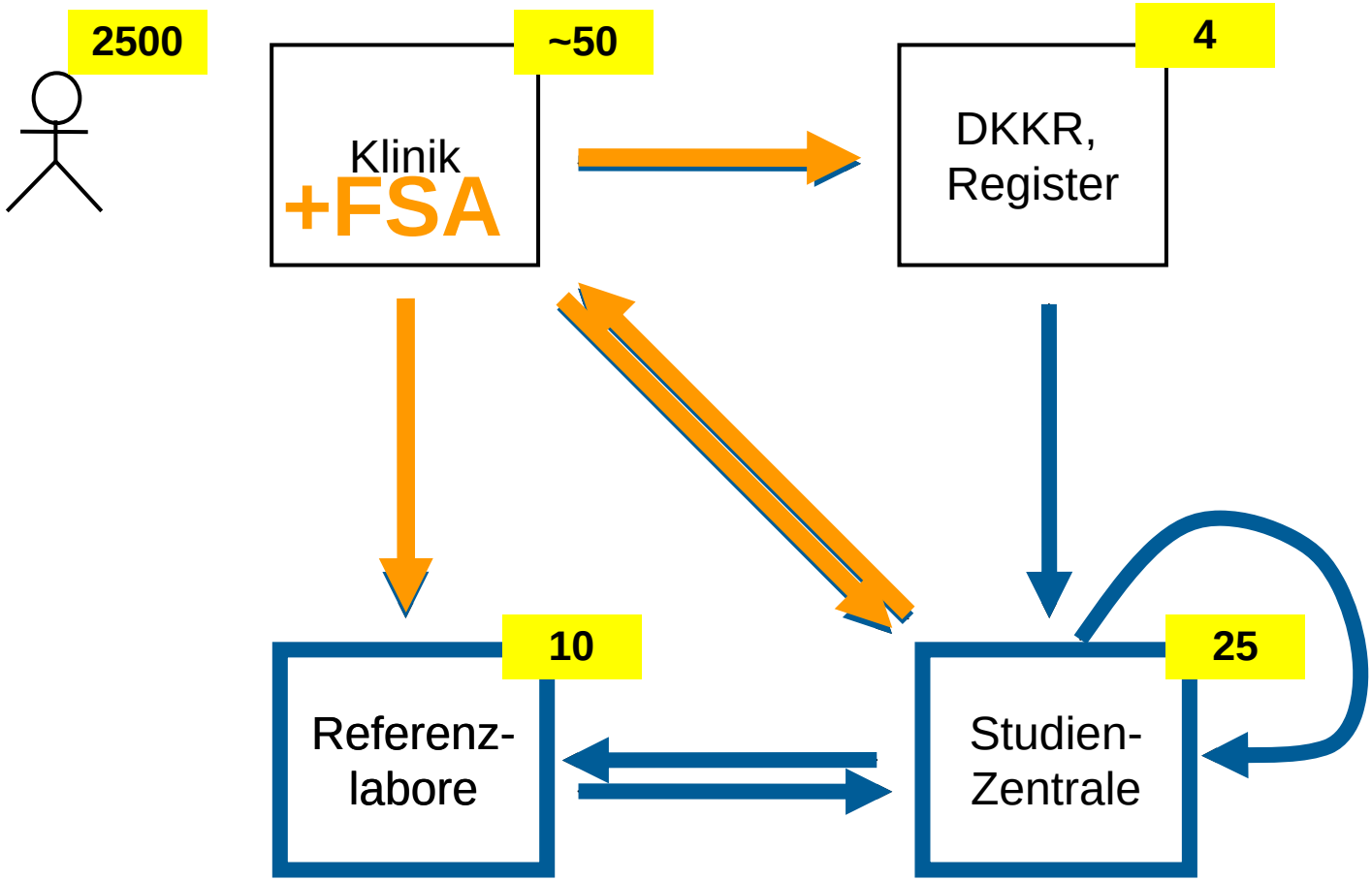
Smartcards in Health Professional IT-Services

Ralf Herold Koordinationszentrale
Kompetenznetz Pädiatrische Onkologie und Hämatologie
Charité – Universitätsmedizin Berlin

Gliederung

- Übersicht KPOH
- Übersicht rechnerbasierte Anwendungssysteme
- Begründung und Historie der Smartcard-Lösung
- Smartcard und Lesegerät
- Nutzerseitige(r) Inbetriebnahme und Betrieb
- Serverseitige(r) Inbetriebnahme und Betrieb
- Betrieb im Netz / Dezentrale Verzeichnisdienste
- Probleme / Nachteile *vs.* Mehrwerte / Vorteile
- Weiteres

Übersicht KPOH



Übersicht Rechnerbasierte Anwendungssysteme

- Studienzentralen
  - Datenbanken meist Einzelplatz-Anwendung *in house*
- Webserver
  - Informationsportal kinderkrebsinfo.de
    - Nutzergruppen = Arbeitsgruppen Netz / Fachgesellschaft
    - Keine Patientendaten, geschützte Fachinhalte
    - Content-Management-System
  - PID-Dienst = Patientenidentifikator
  - Bilddaten-Clearinghouse
  - Bilddaten-Kommunikation
  - Studien-Software
  - Therapieplanung-Software
- E-Mail
  - Pretty Good Privacy, Smartcard
- Sporadisch elektronischer Patientendatenaustauch

Informationen zu Krebs- und Blutkrankheiten bei Kindern und Jugendlichen

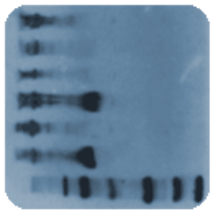
für Kinder, Jugendliche, Familien, Studenten, Ärzte, Wissenschaftler, das medizinische Fachpersonal, die interessierte Öffentlichkeit und alle auf unterschiedliche Weise Betroffenen.

Die Erkrankungen

Informationen zu Krankheiten, Heilungsaussichten und der Behandlung, für Arztgespräche, zum Nachlesen und mit Fachinformationen

Impressum · Was ist Krebs? · Suche

--- Erkrankungen ---



Aktuell & Allgemein

Die aktuellen Neuigkeiten, Ergebnisse aus der Forschung und unsere Veröffentlichungen bieten allgemeine Informationen.

Behandlungserfolge · Die Mitteilungen · Newsletter · Presse · Termine

Das Kompetenznetz

Hier forschen und kooperieren Experten für Kinderkrebsheilkunde zur Verbesserung der Gesundheitsversorgung krebskranker Kinder und Jugendlicher. Das Kompetenznetz trägt auch dieses Informationsportal.

Kompetenznetz

Die GPOH

In der Gesellschaft für Pädiatrische Onkologie und Hämatologie (Krebs- und Blutheilkunde) arbeiten viele Ärzte, Wissenschaftler, Pflegende und Psychologen zusammen für die erkrankten Kinder und Jugendlichen

Satzung · Studienregeln · GPOH

--- Arbeitsgruppen ---

kinderkrebsinfo.de wurde Ende 2002 begonnen. Zu Krebserkrankungen bei Kindern und Jugendlichen haben wir Informationen neu recherchiert, dem aktuellen Wissensstand angeglichen

Seite » weiter

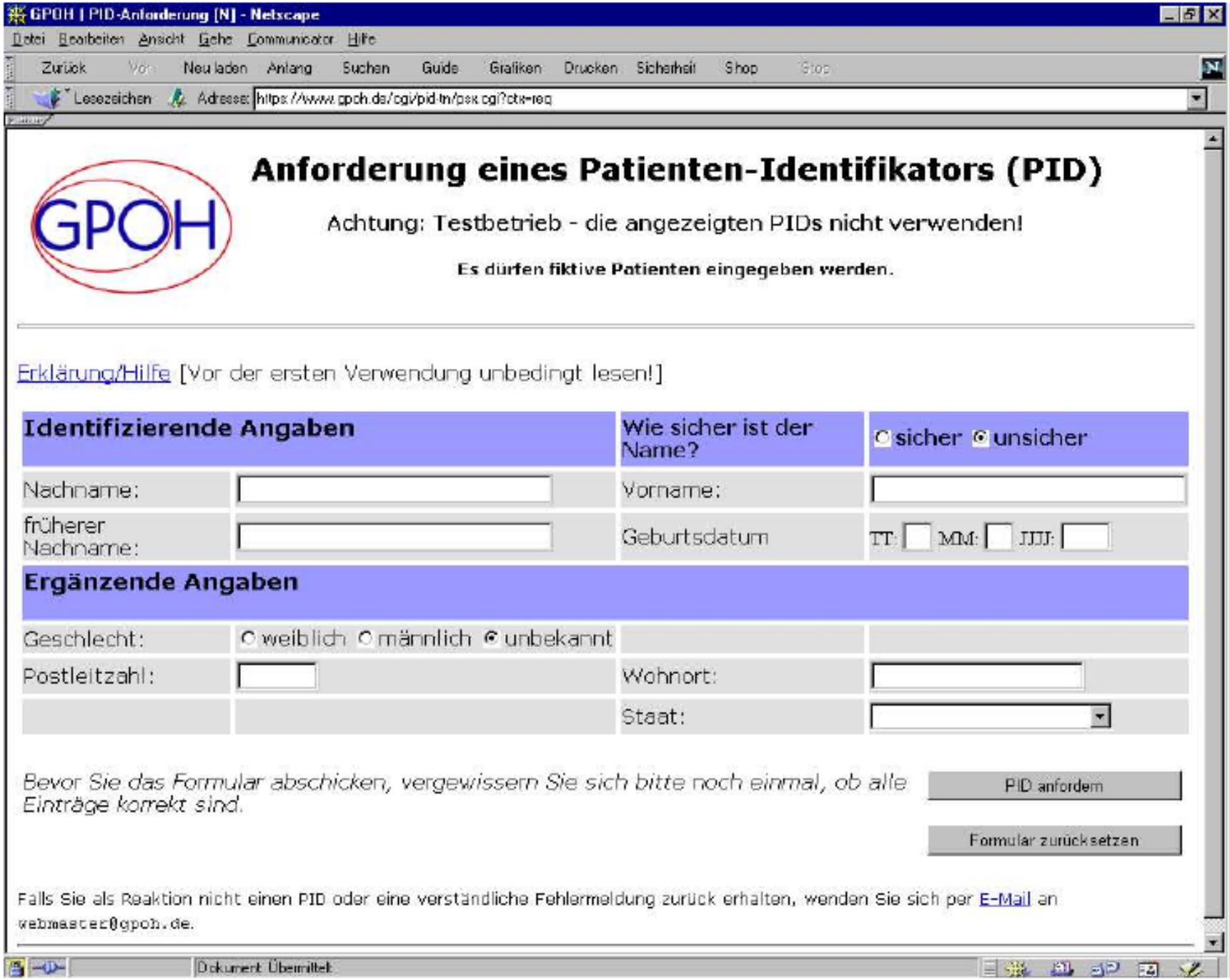
Informationsportal
Aktuelles
Presse
Impressum
GPOH
Kompetenznetz
Suche

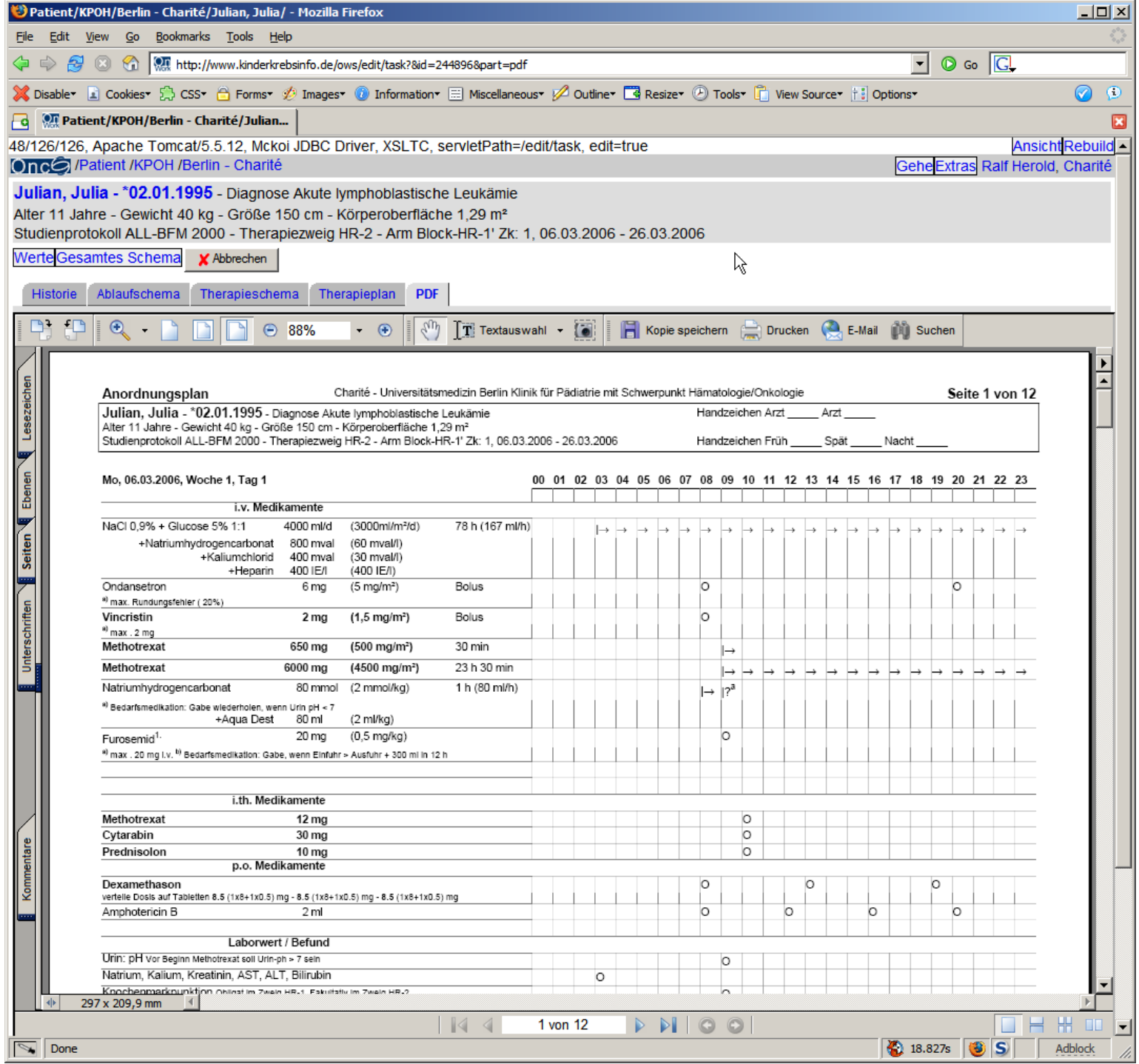
Aktuelle Umfrage

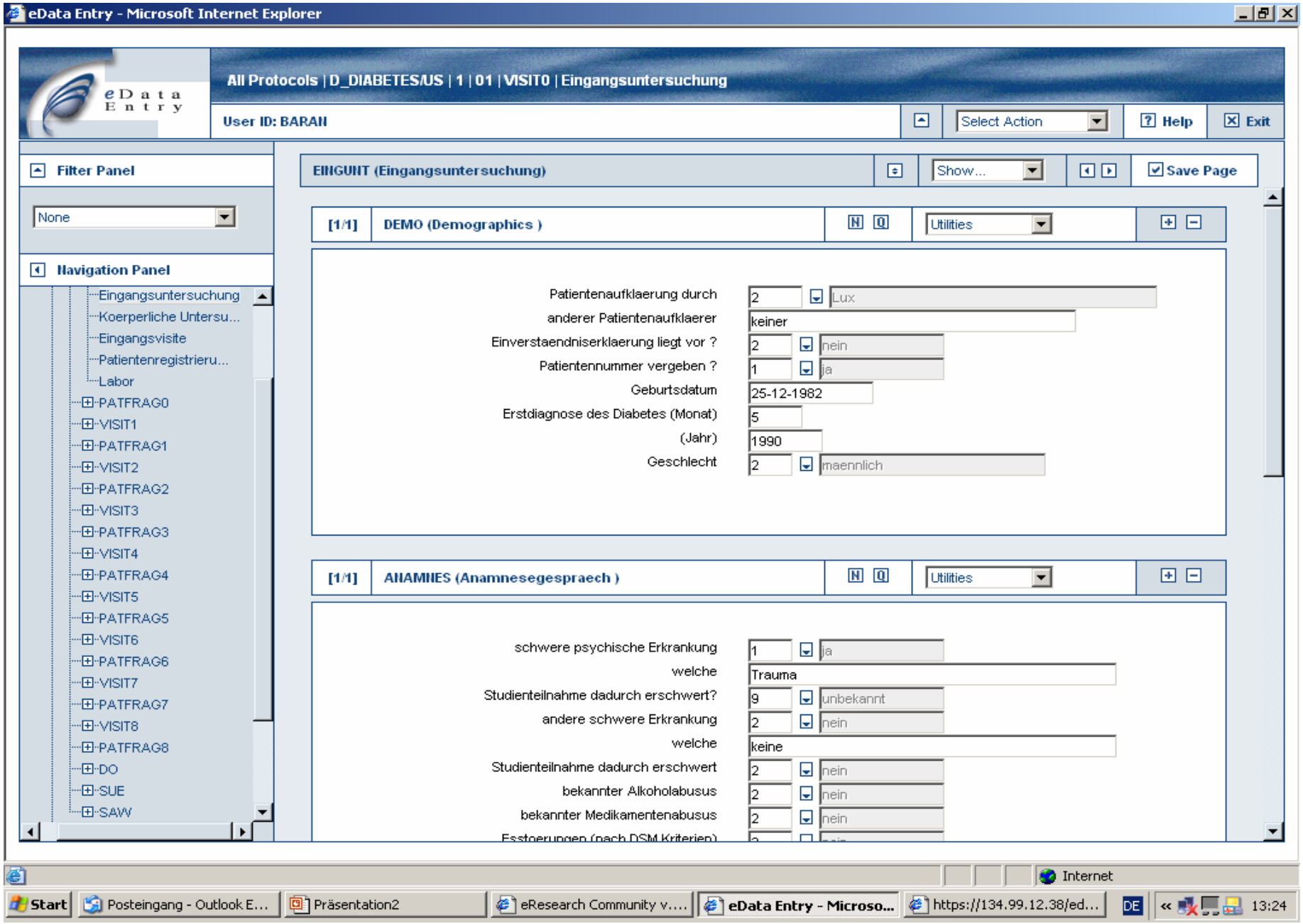
Wie beurteilen Sie die Infos von kinderkrebsinfo.de?

Gemeinsamer Text

der deutschen Infodienste zu Krebs- Erkrankungen bei Kindern und Jugendlichen


GPOH | PID-Anforderung [N] - Netscape
Datei Bearbeiten Ansicht Gehe Communicator Hilfe
Zurück Vor Neu laden Anfang Suchen Guide Grafiken Drucken Sicherheit Shop Stop
Lesezeichen Adresse: https://www.gpoh.de/cgi/pid-tn/pix.cgi?ctx=req
Anforderung eines Patienten-Identifikators (PID)
Achtung: Testbetrieb - die angezeigten PIDs nicht verwenden!
Es dürfen fiktive Patienten eingegeben werden.
Erklärung/Hilfe [Vor der ersten Verwendung unbedingt lesen!]
Identifizierende Angaben
Wie sicher ist der Name?
sicher unsicher
Nachname:
Vorname:
früherer Nachname:
Geburtsdatum
TT: MM: JJJJ:
Ergänzende Angaben
Geschlecht:
weiblich männlich unbekannt
Postleitzahl:
Wohnort:
Staat:
Bevor Sie das Formular abschicken, vergewissern Sie sich bitte noch einmal, ob alle Einträge korrekt sind.
PID anfordern
Formular zurücksetzen
Falls Sie als Reaktion nicht einen PID oder eine verständliche Fehlermeldung zurück erhalten, wenden Sie sich per E-Mail an webmaster@gpoh.de.
Dokument Übermittelt


Patient/KPOH/Berlin - Charité/Julian, Julia/ - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.kinderkrebsinfo.de/ows/edit/task?8id=244896&part=pdf
Go
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options
Patient/KPOH/Berlin - Charité/Julian...
48/126/126, Apache Tomcat/5.5.12, Mckoi JDBC Driver, XSLTC, servletPath=/edit/task, edit=true
Ansicht Rebuild
/Patient /KPOH /Berlin - Charité
Gehe Extras Ralf Herold, Charité
Julian, Julia - *02.01.1995 - Diagnose Akute lymphoblastische Leukämie
Alter 11 Jahre - Gewicht 40 kg - Größe 150 cm - Körperoberfläche 1,29 m²
Studienprotokoll ALL-BFM 2000 - Therapiezweig HR-2 - Arm Block-HR-1' Zk: 1, 06.03.2006 - 26.03.2006
Werte Gesamtes Schema
Abbrechen
Historie Ablaufschema Therapieschema Therapieplan PDF
88%
Textauswahl
Kopie speichern
Drucken
E-Mail
Suchen
Lesezeichen
Ebenen
Seiten
Unterschriften
Kommentare
Anordnungsplan
Charité - Universitätsmedizin Berlin Klinik für Pädiatrie mit Schwerpunkt Hämatologie/Onkologie
Seite 1 von 12
Julian, Julia - *02.01.1995 - Diagnose Akute lymphoblastische Leukämie
Alter 11 Jahre - Gewicht 40 kg - Größe 150 cm - Körperoberfläche 1,29 m²
Studienprotokoll ALL-BFM 2000 - Therapiezweig HR-2 - Arm Block-HR-1' Zk: 1, 06.03.2006 - 26.03.2006
Handzeichen Arzt _____ Arzt _____
Handzeichen Früh _____ Spät _____ Nacht _____
Mo, 06.03.2006, Woche 1, Tag 1
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23
i.v. Medikamente
NaCl 0,9% + Glucose 5% 1:1 4000 ml/d (3000ml/m²/d) 78 h (167 ml/h)
+Natriumhydrogencarbonat 800 mval (60 mval/l)
+Kaliumchlorid 400 mval (30 mval/l)
+Heparin 400 IE/l (400 IE/l)
Ondansetron 6 mg (5 mg/m²) Bolus
a) max. Rundungsfehler (20%)
Vincristin 2 mg (1,5 mg/m²) Bolus
a) max . 2 mg
Methotrexat 650 mg (500 mg/m²) 30 min
Methotrexat 6000 mg (4500 mg/m²) 23 h 30 min
Natriumhydrogencarbonat 80 mmol (2 mmol/kg) 1 h (80 ml/h)
a) Bedarfsmedikation: Gabe wiederholen, wenn Urin pH < 7
+Aqua Dest 80 ml (2 ml/kg)
Furosemid1. 20 mg (0,5 mg/kg)
a) max . 20 mg i.v. b) Bedarfsmedikation: Gabe, wenn Einfuhr > Ausfuhr + 300 ml in 12 h
i.th. Medikamente
Methotrexat 12 mg
Cytarabin 30 mg
Prednisolon 10 mg
p.o. Medikamente
Dexamethason 8.5 (1x8+1x0.5) mg - 8.5 (1x8+1x0.5) mg - 8.5 (1x8+1x0.5) mg
verteile Dosis auf Tabletten
Amphotericin B 2 ml
Laborwert / Befund
Urin: pH Vor Beginn Methotrexat soll Urin-ph > 7 sein
Natrium, Kalium, Kreatinin, AST, ALT, Bilirubin
297 x 209,9 mm
1 von 12
Done
18.827s
Adblock


eData Entry - Microsoft Internet Explorer
eData Entry
All Protocols | D_DIABETES/US | 1 | 01 | VISIT0 | Eingangsuntersuchung
User ID: BARAN
Select Action
Help
Exit
Filter Panel
None
Navigation Panel
Eingangsuntersuchung
Koerperliche Untersu...
Eingangsvisite
Patientenregistrieru...
Labor
PATFRAG0
VISIT1
PATFRAG1
VISIT2
PATFRAG2
VISIT3
PATFRAG3
VISIT4
PATFRAG4
VISIT5
PATFRAG5
VISIT6
PATFRAG6
VISIT7
PATFRAG7
VISIT8
PATFRAG8
DO
SUE
SAW
EINGUNT (Eingangsuntersuchung)
Show...
Save Page
[1/1] DEMO (Demographics)
Utilities
Patientenaufklaerung durch 2 Lux
anderer Patientenaufklaerer keiner
Einverstaendniserklaerung liegt vor ? 2 nein
Patientennummer vergeben ? 1 ja
Geburtsdatum 25-12-1982
Erstdiagnose des Diabetes (Monat) 5
(Jahr) 1990
Geschlecht 2 maennlich
[1/1] ANAMNES (Anamnesegespraech)
Utilities
schwere psychische Erkrankung 1 ja
welche Trauma
Studienteilnahme dadurch erschwert? 9 unbekannt
andere schwere Erkrankung 2 nein
welche keine
Studienteilnahme dadurch erschwert 2 nein
bekannter Alkoholabusus 2 nein
bekannter Medikamentenabusus 2 nein
Internet
Start
Posteingang - Outlook E...
Präsentation2
eResearch Community v....
eData Entry - Microso...
https://134.99.12.38/ed...
DE
13:24

KPOH Bilddaten-Clearinghouse

Home [nicht angemeldet]

Willkommen!

Überblick

Um das Programm nutzen zu können, wechseln Sie bitte auf eine sichere SSL-Verbindung:

» **Zertifikate installieren**
» **Sichere Version**

Nirk-Testumgebung

» **zur Testumgebung**

Wozu Bilddatenkommunikation?

Das Clearinghouse unterstützt den weltweiten, sicheren Austausch von Dokumenten und Bilddaten im Rahmen multizentrischer Studien über das Internet. Dabei umfasst das System alle Standardfunktionalitäten eines Dokumentenmanagementsystems erweitert um die speziellen Anforderungen im medizinischen Umfeld, wie z.B. DICOM-Netzwerkkommunikation und die Konvertierung medizinischer Bildformate. Die besonderen Anforderungen im Bereich des Datenschutzes erfüllt das Clearinghouse durch eine an webbasierte Systeme angepasste Umsetzung des TMF-Datenschutzkonzeptes.

Ziel ist es, Zeitabläufe und Kosten, die mit dem traditionellen Postversand von Röntgenfilmen verbunden sind, zu optimieren und gleichzeitig eine Plattform für weitergehende Nutzungen der gesammelten Bilddaten in Forschung und Lehre bereitzustellen.

Clearinghouse starten

Weitere Informationen zum Produkt Clearinghouse erhalten Sie hier.

Hilfe und Support für Anwender des Systems erhalten Sie hier.

Das Clearinghouse wird derzeit im Rahmen der Ewing-Studie getestet.

Sicherheitshinweis

Über unverschlüsselte Verbindungen können andere Zugriff auf Ihr Kennwort und damit auf sensible Daten erhalten. Aus Sicherheitsgründen ist das Clearinghouse deswegen nur über eine sichere Verbindung zugänglich.

Vor dem allerersten Zugriff müssen zu diesem Zweck zwei Zertifikate installiert werden. (Es geht zwar auch ohne, aber dann erscheinen eventuell jedesmal Warnhinweise oder Fehlermeldungen, wenn die Clearinghouse-Startseite aufgerufen wird.)

Installationsanweisung für die Zertifikate in eigenem Fenster

Danach kann das Clearinghouse unter folgender Adresse erreicht werden:

TMI-Server - Service zum sicheren und effizienten Austauschen und Speichern von medizinischen Bild- und Textdaten für die Forschung

Navigation

Start
Hilfe
Impressum

Unterstützung

OFFIS e.V.
BMBF
TMF e.V.
Charité

Login - Sie sind noch nicht angemeldet

Zertifikatsidentität der Sicherheitskarte

nicht übermittelt

Login

Benutzername rherold

Kennwort ******

Login

Support +49-30-450-566 834, ralf.herold@charite.de · Applikation 02.12.2006 16:30 · Cookies bitte zulassen
https://tmiserver.charite.de/ · 10.12.2006 09:01

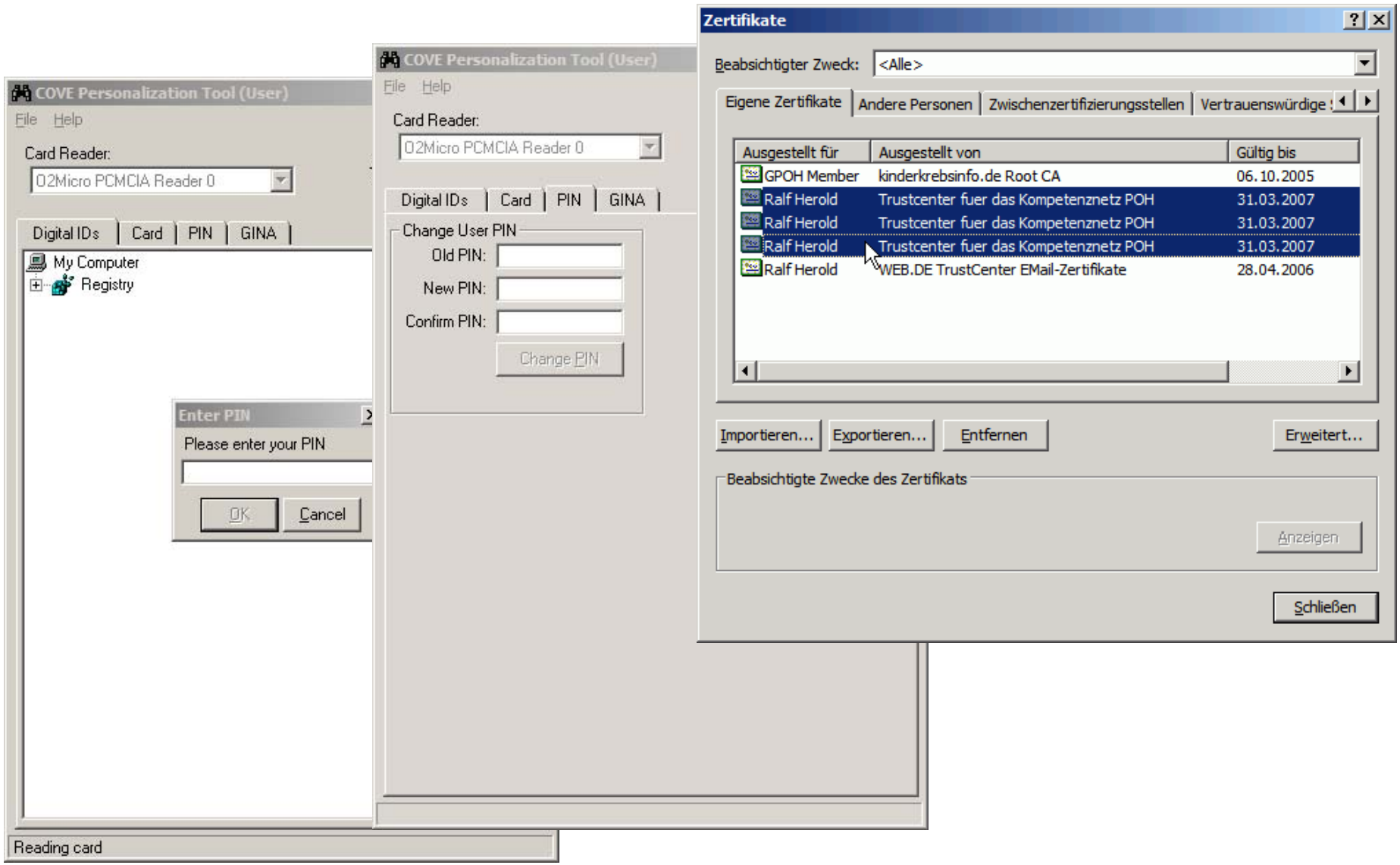
Begründung und Historie der Smartcard-Lösung

- Von Gutachtern 1999 als *state-of-the-art* identifiziert, dementsprechend für KPOH empfohlen
- Während TMF Phase 1 FhISST-Projekt
  - Ausschreibung und Anbieterauswahl
  - Entwicklung von Komponenten für PSD
- KPOH
  - Vorbereitung 2003 (Policies, „Dezentraler Teilnehmerservice“)
  - Auslieferung ab 03/2004
  - Verbreitung
    - 260 Karten ausgegeben
    - 120 Kartenleser ausgegeben
  - Einsatz
    - Monatlich 100 PID-Erzeugungen
    - Gelegentlich Zugriff Informationsportal
  - Neuausstellung ca. 50 Karten

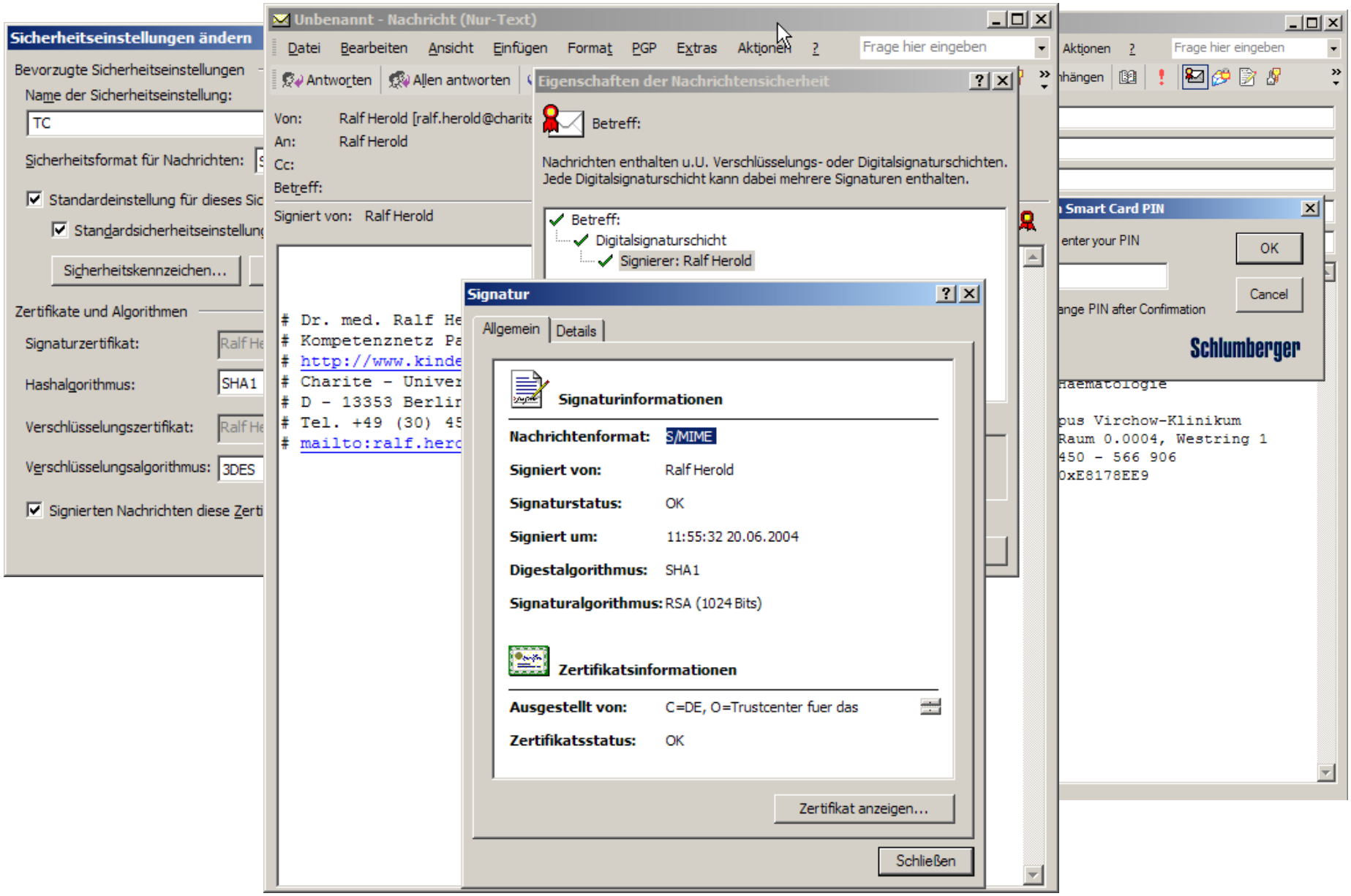
Smartcard und Lesegerät

+ Wurzel- und Knotenzertifikate (*Certificate Chain*)
+ CDROM für Hardware-Treiber
+ CDROM für Middleware (OS-nahes Zertifikatmanagement)

Nutzerseitige(r) Inbetriebnahme und Betrieb



Beispiel Nutzung für E-Mail



Serverseitige(r) Inbetriebnahme und Betrieb

- Server-Zertifikate
  - Reine Softzertifikate; nicht kennwortgeschützt (anbieterbedingt)
  - Je Domäne genau ein Server-Zertifikat (prinzipbedingt)
- Apache-Zusatzmodule
  - obligat **mod_ssl**
    - weithin bekannt, zumindest für SSL allgemein
    - sehr gute Konfigurierbarkeit (u. a. REGEX)
    - einfach als „dropin“ zur Authentifizierung
    - Ralf S. Engelschall, Open Source, BSD-Style Licence
    - http://www.modssl.org/
  - fakultativ **mod_authz_ldap**
    - mutmaßlich geringe Verwendung (im Internet)
    - Andreas Müller, 30.03.2004, Gnu General Public Licence (GPL)
    - **Z**ertifikatnutzung, LDAP-Anbindung, nicht trivial (DSO, APX)
    - http://authzldap.othello.ch/

Beispiel Apache `httpd.conf`

```
<VirtualHost 134.93.126.100:443>
  ServerName    mi2.imsd.uni-mainz.de

  SSLEngine on
  SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:
  SSLCertificateFile /.../ssl.crt/mi2.imsd.uni-mainz.de.crt
  SSLCertificateKeyFile /.../ssl.key/mi2.imsd.uni-mainz.de.key
  SSLCACertificateFile /.../ssl.crt/IMBEI-MI-CA.crt
  SSLOptions   +StdEnvVars

  # (a) fuer zope ueber name / kennwort login
  RequestHeader append SSL_CLIENT_S_DN   %{SSL_CLIENT_S_DN}e
  RequestHeader append SSL_CLIENT_VERIFY %{SSL_CLIENT_VERIFY}e

  # (b) fuer zope in remote authentication modus
  RewriteCond %{LA-U:ENV:SSL_CLIENT_S_DN} (..*)
  RewriteRule (.*) - [E=REMOTE_USER:%1,C]
  RewriteRule  .*   %{REQUEST_URI}

</VirtualHost>
```

Beispiel Apache `httpd.conf`

```
<Directory "/sys/web/pub/sec/KPOH-DB">
   AuthType Basic
   AuthUserFile  /.../nopub/.htpassword
   AuthGroupFile /.../nopub/.htgroups

   AuthzLDAPServer mi.imsd.uni-mainz.de
   AuthzLDAPUseCertificate on

   # Name / Kennwort - Login zulassen
   SSLVerifyClient optional
   AuthzLDAPAuthoritative  off

   AuthzLDAPUserBase ou=Personen,o=KPOH
   AuthzLDAPUserKey uid
   AuthzLDAPMapBase ou=AuthzLDAPCertmap,o=KPOH
   AuthzLDAPGroupBase      ou=Rechte,o=KPOH
   AuthzLDAPMemberKey      member

   # Gruppen bei Verwendung von Zertifikaten im LDAP definiert
   require group  Admin Web-Verwaltung
</Directory>
```

Betrieb im Netz / Dezentrale Verzeichnisdienste

- Papierbasierte Versendung
  - Anträge
    - Neuanträge Endnutzer
    - Neuanträge Server
    - Austräge
  - Nutzer-Ausweis obligat
  - Institutionsnachweis nur für Serverzertifikat obligat
  - Keine direkte Arbeit am LDAP
- Vorgehen entsprechend Policies

- Zentraler Verzeichnisdienst = Trustcenter
  - Schlumberger, jetzt Atos Origin

Probleme und Nachteile

- Nutzer
  - E-Mail: Verschlüsselung, jedoch keine Signatur möglich
  - Lesegerät: PIN-Eingabe nicht möglich
  - Betriebssystem: Middleware nur für Windows verfügbar
  - Falschversuche (ec-Card-ähnliche Policy)
- Serverbetreiber
  - Umstellung bei kommerziellen Anwendungen nicht möglich
  - Meist größerer Aufwand für Integration
  - Geringe Zahl an verfügbaren Lösungsmodulen
  - „Work around“-Implementationen
- Netz
  - Geringe Service-Nutzung (!)
  - Hohe Kosten für Anschaffung, Betrieb, Pflege, PKI-Wechsel
  - Trustcenter fehlerverursachend, unzuverlässig, unzufriedenstellend
  - Certificate Revocation List (CRL) unzuverlässig
  - Nicht ohne weiteres für SSH verwendbar

Mehrwerte und Vorteile

- Sicherheit („funktioniert“)
- Netz
  - Organisation wird modelliert (LDAP)
  - Vollständige und unbeschränkte, zentrale Nutzerverwaltung
  - Vielseitig einsetzbarer Datenkorpus
- Nutzer
  - Single Sign On
    - potenziell (wenn in Anwendung integriert)
    - prinzipiell (solange Browsersession offen)
  - Identifikation, Mitgliedschaft, Einbeziehung, Prozeßbewußtsein
- Serverbetreiber
  - Abstrahierung der Authentifizierung
  - Fortgeschrittene Nutzung von Standardmechanismen
  - Delegation der Nutzerverwaltung

Ausfallvorkehrungen

- Netz
  - Softzertifikate selber machen
  - Telefon Zentrale bereitstellen
  - Bisher nur Idee: Notfall-TAN
- Serverseitig
  - Zweifach-Betrieb für (virtuell gedoppelte) Webserver
    - Smartcard und Softzertifikat
    - Smartcard und Name/Kennwort
  - CRL-Verwendung ausschalten
  - Applikationsserver auf verschiedenen Wegen zugänglich halten
- Nutzer?
  - Betriebssystem als Backup-Image
  - Smartcard des Kollegen
  - Lokalkopien der Daten ...

Weitere wichtige Detailaspekte der Sicherheitskonzepte

- Grundschutz?
- Start 1999 mit Einführung PGP (Pretty Good Privacy)
- Für Smartcard Vereinbarungen getroffen
- PID (Patientenidentifikator) nicht als PSD verwenden
- Schutz auch der Daten der Netzbeteiligten
- E-Mail-Formulare und -weiterleitung absichern
- Disclaimer für „offizielle“ E-Mails verwenden
- Serverseitige IP-Adressenspeicherung überdenken
- ...