Kommunikationskonzept für das Schlaganfall-Netzwerk Rheinland-Pfalz

Engelmann U[1], Schroeter A[1], Schweitzer T[2], Meinzer HP[1]
[1] Deutsches Krebsforschungszentrum, Abt. Medizinische und Biologische Informatik, Im Neuenheimer Feld 280, D-69120 Heidelberg; U.Engelmann@DKFZ-Heidelberg.de
[2] Steinbeis-Transferzentrum Medizinische Informatik, Im Neuenheimer Feld 517, D-69120 Heidelberg, http://www.chili-radiology.com

Dieser Artikel beschreibt das Kommunikationskonzept für ein regionales Stroke-Netzwerk zum Austausch medizinischer Bilder und Befunde. Der Datentransfer erfolgt ausschließlich per E-Mail (SMTP). Die medizinischen Bilder werden dabei als Mail-Attachments gem. DICOM-Standard (Suppl. 54) angehängt. Den Erfordernissen des Datenschutzes wird durch Public-Key-Verschlüsselung Rechnung getragen. Alle verwendeten Protokolle sind standardisiert oder de facto Standards und erlauben eine herstellerübergreifende Kommunikation. Verschiedene Probleme und Möglichkeiten der Realisierung des Konzeptes werden diskutiert.

3

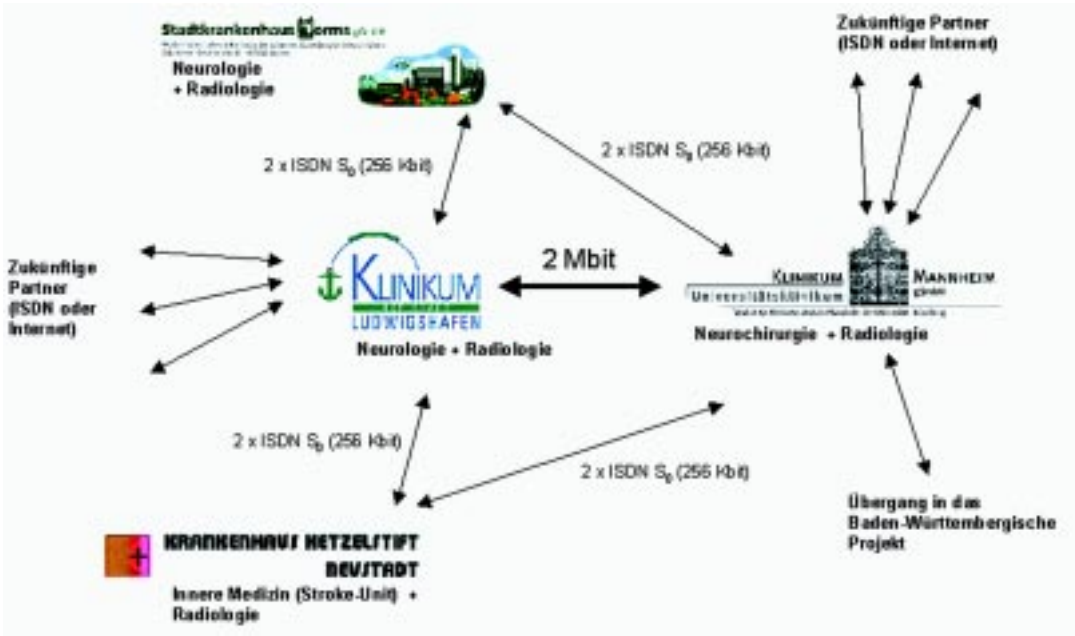
1 Einführung

Zeit ist einer der wichtigsten Faktoren bei der Erstellung einer Diagnose, der Therapie und Prognose eines Schlaganfalls (engl. Stroke). Das Bundesland Rheinland-Pfalz fällte die politische Entscheidung die Einrichtung eines landesweiten Kompetenznetzwerks zu unterstützen. Das Hauptanliegen ist, die schnelle und zuverlässige Verteilung medizinischer Bilder für die Schlaganfalldiagnostik und deren Therapie.

Der erste Schritt ist die Etablierung (und Finanzierung) eines Pilot-Netzwerks, welches die Krankenhäuser in Neustadt und Worms (Stroke-Units 2. Ordnung) mit den Kompetenzzentren in Ludwigshafen und Mannheim (Stroke-Units 1. Ordnung) verbindet (s. Abb. 1). Grundlegende Anforderungen an ein zu beschaffendes System wurden in den Ausschreibungsbedingungen definiert. Die Ausschreibung wurde von einer Beratungsfirma (Pergis, Ludwigshafen) organisiert. Eine kleine Gruppe von Teleradiologie-Experten (Dr. Weisser, Mannheim, und PD Dr. Walz, Eschborn) erarbeitete das grundlegende technische Konzept:

- Volle DICOM-Kompatibiliät für den Austausch von Daten mit bildgebenden Modalitäten.
- Archivierung von Daten in einer Datenbank,
- Funktionen für die Darstellung und Analyse medizinischer Bilder von verschiedenen Modalitäten.

Abbildung 1
Das initiale Schlaganfall-Netzwerk Rheinland-Pfalz



- Das bedeutet, dass kein spezielles Kommunikationssystem sondern ein integriertes System für Befundung und Kommunikation erforderlich war.
- Der standardisierte Datentransfer sollte per E-Mail (SMTP) realisiert werden und das neue DICOM-Supplement 54 berücksichtigen. Der Hauptgrund dafür war, dass E-Mails in der Regel durch Firewalls geschickt werden können ohne irgendwelche Änderungen in deren Regeln vornehmen zu müssen. Ein weiterer Grund war die Verfügbarkeit von standardi-

Autoren: Engelmann U, Schroeter A, Schweitzer T, Meinzer HP
Titel: Kommunikationskonzept für das Schlaganfall-Netzwerk Rheinland-Pfalz
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Ober-Mörlen, Ausgabe 2003; S.

sierten Verschlüsselungsmethoden für E-Mails.
- Das System sollte die automatische Weiterleitung von Daten an bestimmte Empfänger unterstützen.
- Die Konvertierung zwischen den DICOM- und Mail-Protokollen sollte automatisch ohne Benutzerinteraktion erfolgen.
- Die Übermittlung aller Daten sollte verschlüsselt erfolgen.
- Alle Kommunikationskanäle sollten mit bereits existierenden und zukünftigen Firewall-Lösungen ohne Beeinträchtigung der Sicherheit funktionieren.

Verschiedene Teleradiologie- und PACS-Anbieter reichten Angebote ein. Die Auswahl des Lieferanten basierte auf der Präsentation von Lösungen und der Prüfung von Konzepten mit Softwaredemonstrationen. Ausgewählt wurde das CHILI (Tele-) Radiologiesystem des Steinbeis-Transferzentrums Medizinische Informatik Heidelberg.

2 Methode

CHILI ist eine radiologische Workstation mit einem umfangreichen und flexiblen Funktionsumfang für die Teleradiologie und Befundung. Es unterstützt verschiedene Protokolle und offene Standards zur Bildübertragung und die interaktive Telekonferenz auf medizinischen Bildern [1]. Ein wichtiges Merkmal des Systems ist sein Sicherheitskonzept und die implementierten Datenschutzmaßnahmen, die auf symmetrischer Verschlüsselung und Public-Key-Verfahren basieren [2].

Eines des unterstützten Transferprotokolle ist SMTP (simple mail transfer protocol). Hiermit können Benutzer medizinische Bilder und zusätzliche Daten als reguläre E-Mail verschicken. Verschiedene Bildformate, wie DICOM, JPEG, GIF, usw. werden unterstützt.

Die meisten der geforderten Funktionalitäten der Ausschreibung waren bereits in der CHILI-Software vorhanden. Einige zusätzliche Funktionen mussten für das Projekt noch eingebaut werden, wie die automatische Verschlüsselung/Entschlüsselung von E-Mails und die automatische Konvertierung des Protokolls zwischen DICOM und SMTP. Zusätzliche Sicherheitsmaßnahmen, wie z.B. das Schlüsselmanagement, basierend auf offenen Standards, wurden integriert. Die flexible Protokollkonvertierung zu und von SMTP erlaubt eine einfache Ausweitung des Radiologie-Netzwerkes um andere Datentypen und liefert die Basis für ein generelles Telemedizin-Netzwerk.

4 Konzepte

Abbildung 2 zeigt die prinzipiellen Komponenten des Netzwerks. Die Medizinische Indikation und der Ablauf der Konsultationen wurden zwischen den beteiligten Häusern, bzw. Ärzten explizit definiert und vertraglich geregelt.

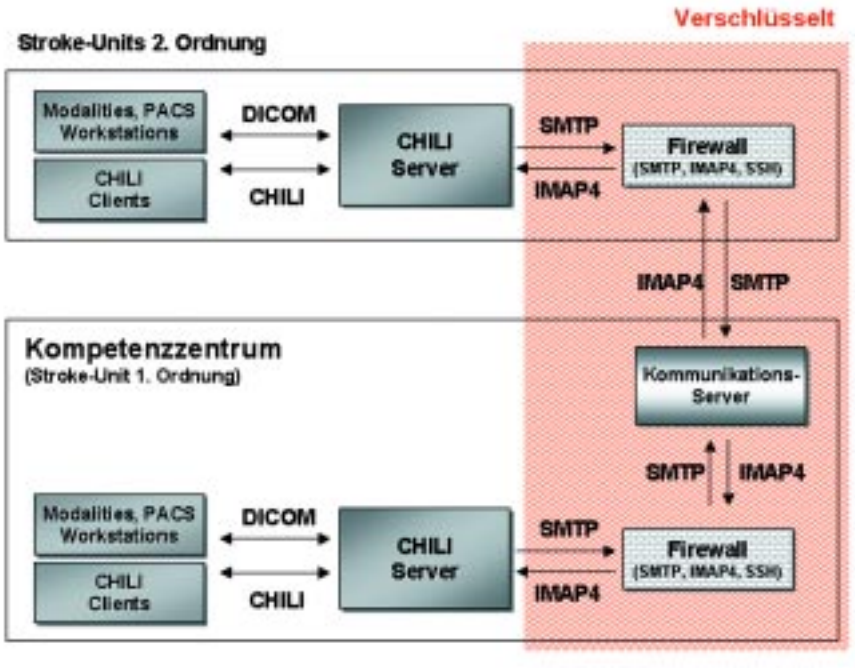
Die beteiligten Einweiser (ohne Experten in Neuroradiologie, Neurologie und Neurochirurgie) wurden mit je zwei CHILI-Workstations ausgestattet (PCs unter Linux). Eine Workstation dient jeweils als Server und die anderen als Clients, die auf die Daten und Dienste des Servers zugreifen. Der Server erhält die Bilder von den bildgebenden Modalitäten (z.B. CT, MR), vom PACS oder von den vorhanden DICOM-Workstations über das DICOM-Protokoll [3]. Der Server archiviert die Daten in einer relationalen Datenbank (PostgreSQL). Die CHILI-Clients greifen auf die Datenbank des Servers zu und können die dort gespeicherten Daten abrufen und bearbeiten. Zwischen allen CHILI-Systemen sind interaktive Telekonferenzen möglich.

Die Daten werden per E-Mail mit dem Simple Mail Transfer Protocol (SMTP) in das Kompetenzzentrum übertragen [4, 5]. Die erste Version dieses Protokolls konnte nur 7-bit-Textnachrichten übertragen. Die MIME-Erweiterungn (Multipurpose Internet Mail Extentions) erlauben inzwischen die Übertragung von mehrteiligen Nachrichten (Multipart messages) von beliebigen Datentypen [6]. Der DICOM-Standard definiert im Supplement 54 den DICOM MIME Typ [7]. Dieser erlaubt nun auch die standardisierte Übertragung medizinischer Bilder per E-Mail.

Da DICOM-Bilder personenbezogene Daten enthalten, ist es nach nationalen und internationalen Gesetzen nicht erlaubt, diese unverschlüsselt über ungeschützte Leitungen zu übermitteln. Also müssen entsprechende Sicherheitsmaßnahmen implementiert werden. Die wichtigsten Maßnahmen sind die Verschlüsselung und digitale Signatur der Daten, bzw. von Teilen der E-Mail.

Im RFC 1847 (Security Multiparts for MIME) wurde von Galvin et al. definiert, wie E-Mails digital signiert und verschlüsselt werden sollen [8]. Mit MIME Security with OpenPGP [9, 10] wurde dies im Projekt umgesetzt. Die Daten werden mit dem privaten Schlüssel des Absenders digital signiert,

Abbildung 2
Komponenten und verwendete Protokolle im Schlaganfall-Neztwerk Rheinland-Pflalz



um die Integrität und Authentizität der Daten zu gewährleisten. Die Verschlüsselung erfolgt mit dem öffentlichen Schlüssel des Empfängers [2].

Beim Versand von großen Datenmengen per Mail ist zu beachten, dass Mailgateways in der Regel nur Mails bis zu einer maximalen Größe durchlassen. Typische Größen sind 1 oder 2 MByte. Da die zu versendenden Datenmengen in der Regel weit darüber liegen (z.B. 20 MByte bei 40 Bildern), werden diese automatisch in viele kleine Mails aufgesplittet und auf der Empfangsseite wieder zusammengeführt.

Der Datenversand kann entweder interaktiv oder automatisch per Autorouting erfolgen. Es können Regeln definiert werden, an wen über welches Protokoll, auf welchem Weg und wann der Autorouter die Daten schicken soll. Dabei tritt das Problem auf, dass keine natürliche Person, sondern ein Programm die Daten versendet. Eine personenbezogene Signatur ist somit nicht möglich. Daher wird in diesem Fall eine Signatur des Rechners, bzw. der absendenden Institution verwendet, um Integrität und Authentizität zu gewährleisten.

Nach der Konvertierung, Signatur und Verschlüsselung der Daten erfolgt der Versand per E-Mail an den Empfänger (s. Abb. 2). Der CHILI-Server schickt die Daten durch eine optionale eigene Firewall über das Internet oder ISDN-Leitungen. Der SMTP-Port der Firewall ist normalerweise für die Übertragung von E-Mails offen.

Die Daten landen zunächst auf dem Kommunikationsserver des Kompetenzzentrums, wo sie temporär zwischengespeichert werden. Dieser steht üblicherweise vor der Firewall im ungeschützten Bereich. Der CHILI-Server im geschützten Bereich des Kompetenzzentrums holt sich ankommende Daten regelmäßig (typischerweise jede Minute) per IMAP-Protokoll ab [11]. Danach werden diese auf dem Kommunikationsserver gelöscht, dekodiert und wieder in DICOM-Files konvertiert und in der Datenbank des CHILI-Servers abgelegt. Der Benutzer wird über akustische und visuelle Alarme über die Ankunft neuer Daten informiert, die dann direkt am Server oder am Client befundet werden können.

Mit weiteren Autorouten können die Daten innerhalb des Kompetenzzentrum wiederum an eine oder mehrere andere Workstations weiter geleitet werden. DICOM-Workstations können die Daten außerdem per Query/Retrieve aktiv holen.

Ergebnisse und andere Informationen können auf einfache Weise per "Antwort" auf einen eingegangenen Datensatz an den Einsender zurückgeschickt werden. Die digitale Unterschrift des absendenden Arztes sichert wiederum Authentizität und Integrität des Befundes, der auf dem selben Weg per verschlüsselter E-Mail über den Kommunikationsserver zum Einsender übertragen wird (s. Abb. 2). Der CHILI-Server des Einsenders fragt sein Postfach auf dem Kommunikationsserver regelmäßig und automatisch ab und integriert die Antworten in die zugehörige Untersuchung. Der Benutzer kann diese dann als Einheit von Bild und Befund abrufen und darstellen.

Die Kontrolle von Vollständigkeit und Korrektheit der Datentransfers ist sehr wichtig und wird automatisch durchgeführt. Aus juristischen Gründen werden alle Datentransfers und deren Erfolg auch auf beiden Seiten in durch Signaturen geschützten Logbüchern protokolliert. Darüber hinaus können Absender und Empfänger den prozentualen Fortschritt des Datentransfers verfolgen. Hierfür wurde ein Meta-Protokoll auf der Basis von SMTP entwickelt und umgesetzt. Über dieses wird die Protokollierung der Datenübertragungen und im Fehlerfall Korrekturmaßnahmen (Wiederholung oder Versand an ein anderes Kompetenzzentrum) gesteuert. Auf diese Weise dienen die Kommunikationsserver gegenseitig als Ausfallsystem.

4 Zusatznutzen

Das realisierte CHILI-System ist nicht nur ein spezialisiertes Notfallsystem. Es basiert auf einer radiologischen Befundungsworkstation, die in der täglichen Routine für andere Zwecke eingesetzt werden kann. Bei Bedarf können weitere Clients an den Server angeschlossen werden. Diese können von Haus aus interaktive Telekonferenzen im lokalen Netz untereinander durchführen, ohne dass die Daten vor der Konferenz explizit ausgetauscht werden müssen. Das "Notfallsystem" kann durch weitere Optionen aus der CHILI-Familie, wie Langzeitarchivierung, Bildverteilung per Web-Technologie, mobile Viewer auf Webpads, persönliche digitale Assistenten (PDAs) oder 3D-Visualisierungen erweitert werden [12,13].

5 Diskussion

Das System wurde, wie oben beschrieben, implementiert. Es ist ein offenes Konzept, basierend auf bereits existierenden Standards, wodurch der Datenaustausch mit anderen Systemen gesichert ist. Bei der Systemrealisierung standen verschiedene Möglichkeiten zur Auswahl. Zur Zeit werden die Daten per OpenPGP verschlüsselt. Eine Alternative dazu war S/MIME [14]. Wir wählten OpenPGP, da es zum gegenwärtigen Zeitpunkt einfacher zu implementieren und ebenso weit verbreitet wie S/MIME war. Es ist geplant das Letztere ebenfalls zu integrieren (siehe unten).

Das Autorouting von Daten beschleunigt die Übertragung von den Modalitäten zu den Kompetenzzentren. Ein einschränkender Faktor ist, dass die Daten von einer Maschine anstatt von einer Person signiert werden. Nach einer Abwägung der Vor- und Nachteile denken wir, dass dies akzeptabel ist.

Ein weiteres Problem tritt auf, wenn viele Personen Empfänger derselben Daten sein können. Aus diesem Grund sollte der Absender den Namen der Person "auf der anderen Seite" kennen. Dies ist jedoch im Falle von großen Abteilungen auf Empfängerseite kaum möglich. Daher werden die Daten nicht an eine Person, sondern an die Institution verschickt.

Gegenwärtig werden alle öffentlichen Signaturen vom CHILI-System selbst verteilt. Die privaten Schlüssel werden auf der Workstation gespeichert und durch eine Passphrase aktiviert. Das System ist für den Einsatz von digitale Signaturen auf Sicherheitskarten, bzw. einen elektronischen Arztausweis, vorbereitet. Bisher wurde im Projekt noch keine Entscheidung über den zukünftigen Kartenlieferanten getroffen. Dabei ist der Preis der Signaturen ein bedeutendes Kriterium, zumal ein Universitätsklinikum ungefähr 20 bis 30 Karten ausschließlich für die radiologische Abteilung benötigt. Bislang ist dafür jedoch kein Budget vorgesehen.

Sphinx ist ein aktuelles Projekt zur Verbesserung der Datensicherheit bei E-Mails, das vom Bundesamt für Sicherheit in der Informationstechnologie (BSI) ins Leben gerufen wurde. Die technologische Basis des Projekts ist das Protokoll TeleTrust e.V. MailTrusT Version 2 einschließlich der Standards S/MIME und X509 [15]. Proprietäre Produkte auf der Basis dieses Standards sind

bereits verfügbar. Ziel des Ägypten-Projektes ist die Realisierung einer freie Softwarelösung, die einfach in populäre Mail-Programme integriert werden kann [16]. Die Verwendung dieser Software in die CHILI-Lösung ist geplant.

Das Ziel des GNU Privacy Projektes ist es, freie Verschlüsselungssoftware für jedermann zu entwickeln [17]. Das Projekt wird vom Bundesministerium für Wirtschaft und Technologie und dem Bundesministerium des Inneren unterstützt. Es ist geplant, das resultierende freie Software-Tool GNU Privacy Guard ebenfalls in unsere bestehende Sicherheitsinfrastruktur zu integrieren, um eine maximale Interoperabilität zu erreichen.

6 Zusammenfassung und Ausblick

Das realisierte Teleradiologie-Netzwerk erfüllt die in den Ausschreibungsbedingungen definierten Anforderungen für das regionale Stroke-Netzwerk Rheinland-Pfalz. Es ist möglich und geplant, das Netzwerk um weitere Institutionen und Anwendungen zu erweitern. Die Redundanz aller kritischen Systemkomponenten ermöglicht eine hohe Ausfallsicherheit. Durch den hohen Sicherheitsstandard und die flexiblen Protokolle können über das realisierte Netzwerk auch andere Daten ausgetauscht werden. Somit ist die Grundlage für ein generelles Telemedizin-Netzwerk geschaffen.

Die Installation im Klinikum Mannheim dient nicht nur der Unterstützung von Schlaganfall-Fragestellungen. Sie ist gleichzeitig auch der Saatpunkt für ein noch weitergehendes, gerade beginnendes Projekt des Sozialministeriums Baden-Württemberg (Teilprojekte A und B der Zukunftsoffensive III). Somit sind wir auf dem Weg eine flächendekkende Kompatibilität auf der Basis offener Standards zumindest in zwei Bundesländern zu realisieren.

Danksagung

Das Pilotprojekt Teleradiologie (Stroke-Unit in Rheinland-Pfalz) wurde vom Ministerium für Arbeit, Soziales, Familie und Gesundheit in Mainz, Rheinland-Pfalz gefördert.

Wir danken allen beteiligen Projektpartnern, insbesondere den Anwendern, für die konstruktive und vertrauensvolle Zusammenarbeit.

Literatur

1 Steinbeis-Transferzentrum Medizinische Informatik. CHILI: Second Generation Teleradiology and Telecardiology. http://www.chili-radiology.com/.

2 Baur HJ, Engelmann U. Saurbier F, Schröter A, Baur U, Meinzer HP. How to deal with Security and Privacy Issues in Teleradiology. Computer Methods and Programs in Biomedicine, 53, 1 (1997) 1-8.

3 NEMA Standards Publication PS 3.1-15. Digital Imaging and Communications in Medicine (DICOM). National Electrical Manufacturers Association, 2101 L Street, N.W., Washington, D.C. 20037, 2000.

4 Resnick P (ed). RFP 2822: Internet Message Format. April 2001. http://www.ietf.org/rfc.html.

5 Wood D. Programming Internet Email. O'Reilly: Sebastopol 1999.

6 Borenstein N, Freed N. RFC 1521: MIME (Multipurpose Internet Mail Extensions) part one: Mechanisms for specifying and describing the format of Internet message bodies, September 1993. http://www.ietf.org/rfc.html.

7 DICOM Standards Committee, Digital Imaging and Communications in Medicine (DICOM). Supplement 54: DICOM MIME Type. http://medical.nema.org/Dicom/supps/sup54_pc.pdf.

8 Galvin J, Murphy S, Crocker S, Freed N. RFC 1847: Security multiparts for MIME: Multipart/signed and multipart/encrypted, October 1995. http://www.ietf.org/.

9 Elkins M, Del Torto D, Levien R, Roessler T. RFC 3156: Mime security with openPGP, August 2001. http://www.ietf.org/rfc.html.

10 Callas J, Donnerhacke L, Finney H, Thayer R. RFC 2440: OpenPGP message format, November 1998. http://www.ietf.org/rfc.html.

11 Mullet D, Mullet K. Managing IMAP . O'Reilly: Sebastopol 2000.

12 Engelmann U, Schröter A, Schwab M, Eisenmann U, Meinzer HP. Openness and Flexibility: From Teleradiology to PACS. In: Lemke HU, Vannier MW, Inamura K, Farman AG (Eds). CARS'99. Amsterdam: Elsevier (1999) 534-538.

13 Engelmann U, Schröter A, Schwab M, Eisenmann U, Bahner ML, Delorme S, Hahne H, Meinzer HP. The Linux-based PACS project at the German Cancer Research Center. Lemke HU, Inamura K, Farman AG, Doi K (Eds). CARS 2000: Computer Assisted Radiology and Surgery. Proceedings of the 14th International Congress and Exhibition. Amsterdam: Elsevier (2000) 419-424.

14 Ramsdell, B. RFC 2633: S/MIME Version 3 Message Specification, June 1999. http://www.ietf.org/rfc.html.

15 Bundesamt für Sicherheit in der Informationstechnik. Sphinx Project. http://www.bsi.de/aufgaben/projekte/sphinx/index.htm.

16 The GNU Privacy Guard. Projekt Ägypten. http://www.gnupg.org/aegypten/tech.en.html.

17 Das GNU Privacy Projekt (GnuPP). http://www.gnupp.de/start.html.