Dieser Artikel ist Teil des

Open Source Jahrbuch 2005

erhältlich unter http://www.opensourcejahrbuch.de.

Das Open Source Jahrbuch 2005 enthält neben vielen weiteren interessanten Artikeln ein Glossar und ein Stichwortverzeichnis.

GENOMatch – Datenschutz für die pharmakogenetische Forschung

Broder Schümann und Denis Petrov

GENOMatch ist ein Projekt der Schering AG, das pharmakogenetische Forschung mit einem hohen Datenschutzniveau ermöglicht. Für die Umsetzung und gerade für die Entscheidung, in diesem kritischen Bereich auf Open–Source-Software zu setzen, hat GENOMatch den „Open Source Best Practice Award" vom Fraunhofer IOA, von der Lightwerk GmbH bzw. vom Linux-Verband gewonnen. In dem Artikel wird das Projekt vorgestellt. Dabei wird zunächst der Datenschutz und der daraus resultierende *Workflow* der doppelten Pseudonymisierung genauer beleuchtet. Bei der Beschreibung der Implementierung wird besonders auf die Gründe für den Einsatz von Open–Source-Software und die dabei gewonnenen Erfahrungen eingegangen.

1. Einleitung – Das GENOMatch-Projekt

> „The GENOMatch project is going to provide the IT-infrastructure necessary for pharmacogenetic analyses." (Luttenberger 2003*a*)

Geschrieben wurde dieser Satz Anfang 2003 in einem ersten Entwurf des Datenschutzkonzepts zum GENOMatch-Projekt der Schering AG. GENOMatch stellt den Datenschutz (die *genetic privacy*) der Probanden durch Pseudonymisierungsverfahren sicher.

Seit diesem vollmundigen Versprechen hat sich viel getan: Das Datenschutzkonzept bekam vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein das Auditsiegel[1] verliehen (Luttenberger 2003*b*), das Projekt wurde mit dem vom Fraunhofer IAO, von der Lightwerk GmbH und vom Linux-Verband initiierten „Open Source Best Practice Award" ausgezeichnet (vgl. Ziegler 2004), und die Software ist inzwischen im produktiven Betrieb.

Diesen Weg – von den ersten Ideen über das Datenschutzkonzept bis hin zur Implementierung mit Open-Source-Software, die für so viel Beachtung gesorgt hat – wollen wir in diesem Artikel noch einmal nachvollziehen.

1 Informationen zum Auditsiegel finden sich unter http://www.datenschutzzentrum.de/audit/index.htm.

Dazu geben wir zunächst eine Einführung in die Pharmakogenetik (Abschnitt 2), beschreiben in Abschnitt 3 die Datenschutzziele, umreißen den GENOMatch-*Workflow* (Abschnitt 4) und untersuchen in Abschnitt 5 kurz die Möglichkeiten des technischen Datenschutzes. Im Hauptteil des Artikels (Abschnitt 6) wenden wir uns dann der technischen Umsetzung und unseren Erfahrungen mit Open-Source-Software zu.

2. Überblick – Pharmakogenetische Forschung

> „Pharmacogenetics (PGx), which is now a central focus of pharmaceutical endeavor and on the near horizon of clinical practice, aims to identify genome-wide polymorphisms or mutation that will reliably predict an individual's response to drugs before they are prescribed. Used clinically, PGx information could identify nonresponders and those likely to suffer adverse drug reactions, and thus save them the burden of unsave or ineffective drugs. In addition, PGx information can identify new drug targets and streamline the drug-testing and approval process." (Robertson 2001)

Wie andere Pharmaunternehmen baut auch die Schering AG eine Probensammlung für die pharmakogenetische Forschung auf. Pharmakogenetik zielt darauf, Beziehungen zwischen dem genetischen Profil von Patienten und Wirkungen von Medikamenten zu erforschen.

Um pharmakogenetische Forschung zu ermöglichen, muss eine Korrelation von klinischen Daten mit genetischen Profilen erfolgen. Klinische Daten fallen im Rahmen von klinischen Studien im Alltagsgeschäft der Schering AG an. Die zusätzlich benötigten genetischen Daten werden in Substudien – Erweiterungen bestehender Studien – erhoben. Dieses Vorgehen entkoppelt die beiden Prozesse, sodass der Patient an der klinischen Studie teilnehmen kann, auch wenn er keine Probe für eine pharmakogenetische Untersuchung abgeben möchte. Da in der Bevölkerung genetische Daten als besonders sensibel angesehen werden, hat sich Schering entschlossen, von Anfang an einen Prozess zu entwickeln und zu implementieren, der über die derzeitigen Erfordernisse hinausgeht und zukünftige Gesetzgebungen, soweit möglich, antizipiert. Dieser in Abschnitt 4 kurz vorgestellte Ablauf wurde in „Norbert Luttenberger: Datenschutzkonzept für den 'Sample and Save'-Teil des GENOMatch-Projektes bei der Schering AG" festgeschrieben und vom Unabhängigen Landeszentrum für Datenschutz des Landes Schleswig-Holstein im Rahmen des behördlichen Datenschutzaudits begutachtet. Mit der Implementierung des Konzeptes wurde im April 2003 bei der Tembit Software GmbH begonnen; Ende des Jahres 2004 nahm das System den produktiven Betrieb auf (Abbildung 1).

3. Datenschutz – Erfordernisse und Datenschutzkonzept

Die Erfordernisse des Datenschutzes stellen besondere Anforderungen an das Design eines Systems zur pharmakogenetischen Forschung. Der Europäische Rat sagt in

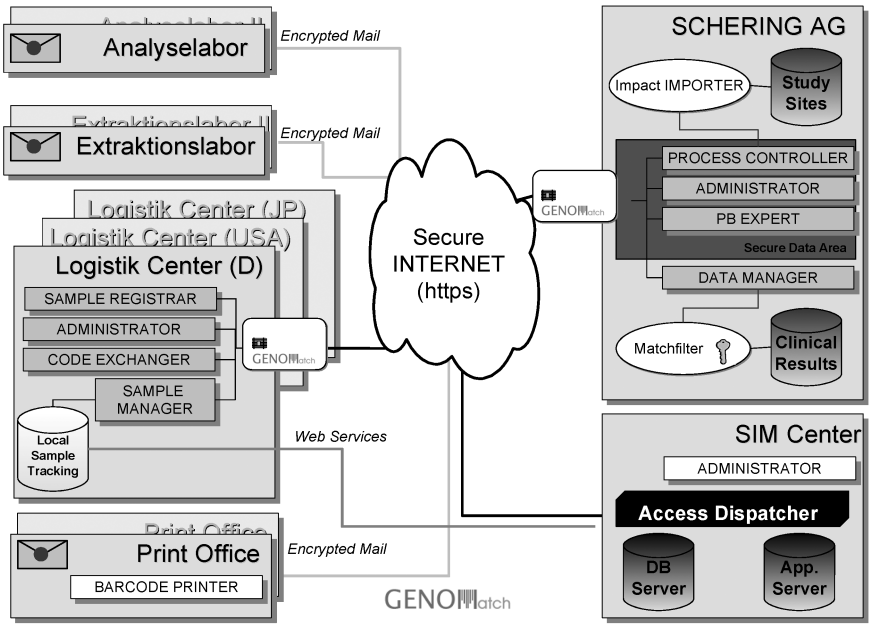

Abbildung 1: GENOMatch-B2B-Interaktionen

Council of Europe (1997) dazu:

> „Die Verarbeitung von Gesundheitsdaten zu Forschungszwecken erfordert zunächst den *Informed Consent* des Patienten und erfolgt am besten vollständig anonymisiert. Können persönliche Daten nicht anonymisiert werden, so sind strikte Datenschutzmaßnahmen nötig."

Eine Anonymisierung würde die Kategorisierung von klinischen Daten vor der Zusammenführung mit den genetischen Datensätzen erfordern und somit den wissenschaftlichen Wert der Proben für die pharmakogenetische Forschung vermindern. Auch die Rücknahme des *Informed Consent* mit der dadurch bedingten Vernichtung von Proben und Datensätzen sowie die Unterrichtung des Patienten über gewonnene Ergebnisse der Studie würden damit unmöglich. Beides widerspricht den Interessen der Forschung und auch den Interessen des teilnehmenden Patienten (Stichwort *Patient Empowerment*). Die *Enquete-Kommission Recht und Ethik in der modernen Medizin* schlägt in Enquete-Kommission (2002) vor,

> „[. . .] ein mehrstufiges Pseudonymisierungsverfahren, möglicherweise mit Verwahrung von Schlüsselbrücken bei Treuhänderinnen bzw. Treuhändern, als Standard für Forschungen mit humangenetischem Material vorzuschreiben."

Hier fordert auch die „Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24.–26. Oktober 2001“,

> „[. . .] die Proben und die genetischen Daten vor der Aufnahme in die Sammlung bei Treuhändern zu pseudonymisieren.“ (Datenschutzbeauftragte 2001)

Aus diesen im Datenschutzkonzept von Luttenberger (2003*a*) ausführlich dargelegten Überlegungen heraus setzt GENOMatch auf eine zweifache Pseudonymisierung des Patientenbezeichners – bestehend aus Patientennummer (PN) und Studiennummer. Die zweifache Pseudonymisierung bewirkt, dass zur Auflösung der Pseudonymisierungskette stets mindestens zwei Personen zusammenwirken müssen. Zusätzlich ist die Auflösung des (PN, SN)-Paares zu einer Person wie auch die Kommunikation mit dem Patienten dem behandelnden Arzt vorbehalten.

4. GENOMatch-*Workflow* – Doppelte Pseudonymisierung

Auch wenn es auf den ersten Blick nicht den Anschein hat, so ist der eigentliche GENOMatch-*Workflow* relativ leicht verständlich.

An dem GENOMatch-Prozess nehmen folgende Institutionen teil:

- Schering AG (SAG)
- Central Sample Repository (CSR): Zentrales Sammellabor, zuständig für Lagerung und Logistik der Proben
- Trial Site: Klinik/Arztpraxis, in der Patienten an einer Studie teilnehmen
- Secure Identity Management Center (SIM-Center): Datentreuhänder. Ein Blackbox-Server-System, extern betrieben bei einer Anstalt des öffentlichen Rechts
- Externe Dienstleister: Analyse- und Extraktionslabore, Barcode-Druckereien usw.

Der grundlegende Ablauf funktioniert so, dass die Trial Site die Proben mit (PN, SN) beschriftet an das CSR sendet. Dort findet die doppelte Pseudonymisierung statt: Für jede Probe wird dort die (PN, SN)-Bezeichnung entfernt und durch das erste Pseudonym (in Form eines Barcodes, BC1) ersetzt. Eine andere Person entfernt diesen BC1 und ersetzt ihn durch das endgültige Pseudonym BC2. Die Verbindung der jeweiligen *Identifier* wird im SIM-Center gespeichert. Erst danach können genetische Daten gewonnen werden, die als einzigen *Identifier* den BC2 der jeweiligen Probe tragen. Zur biostatistischen Auswertung werden in einem speziell abgeschirmten Bereich bei SAG (der sog. *Secure Data Area*, SDA) die genetischen mit den klinischen Daten zusammengeführt. Dazu werden die (PN, SN)-indizierten klinischen Daten an der Grenze zur SDA durch einen sog. *Matchfilter* ebenfalls in zwei Schritten pseudonymisiert, sodass sie schließlich keine personenbezogenen Daten, keine PN oder SN, sondern nur noch das BC2 Pseudonym tragen (Abbildung 2).

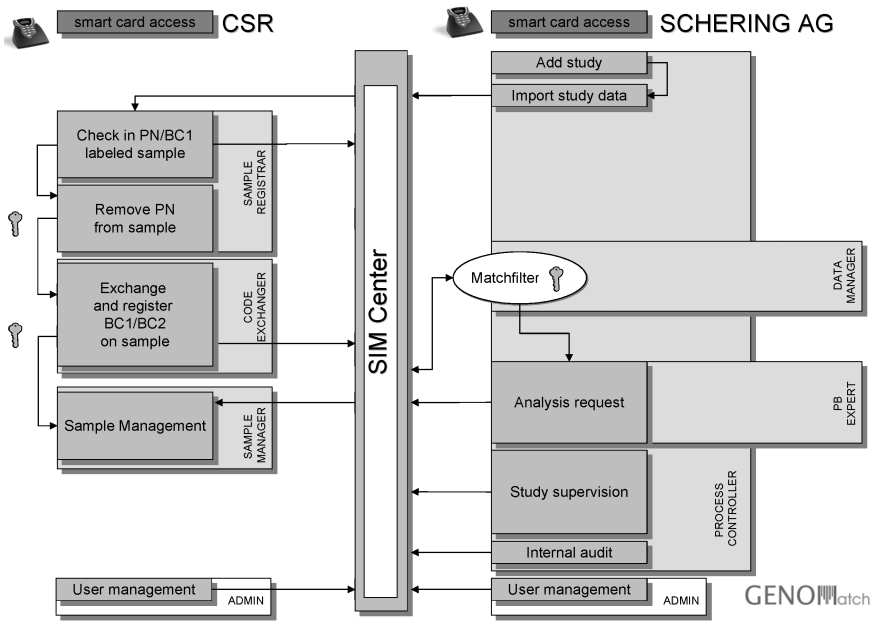

Abbildung 2: GENOMatch-Abläufe

In dieser Beschreibung ausgeblendet wurden viele Details, Sonderfälle, logistische Prozesse sowie Prozeduren zum Feedback von Ergebnissen an den Patienten oder dem Rückzug seines *Informed Consent*. Der GENOMatch-*Workflow* stellt sicher, dass stets folgende Prinzipien gelten:

- Die Identität des teilnehmenden Patienten ist ausschließlich dem Arzt bzw. der Klinik bekannt (Zuordnung PN, SN nach Person).
- Keiner einzelnen Person ist die Auflösung des Pseudonyms BC2 zum (PN, SN)-*Identifier* möglich. Diese Zuordnung ist nur dem SIM-Center bekannt.
- Genetische Daten werden sowohl bei Schering als auch bei externen Dienstleistern nur mit BC2 pseudonymisiert gespeichert und verarbeitet und enthalten keine personenbezogenen Daten.
- Die Zusammenführung der klinischen und genetischen Daten erfolgt in einem abgeschirmten Bereich, nach Löschung aller personenbezogenen Daten und ausschließlich unter dem BC2-Pseudonym.

5. IT-Unterstützung – Technischer Datenschutz

Inwieweit kann und soll ein technisches System diesen *Workflow* unterstützen bzw. durchsetzen? Prof. A. Roßnagel (2004) stellt fest:

> „Außerdem ist technischer Datenschutz viel effektiver als rein rechtlicher Datenschutz. Was technisch verhindert wird oder unterbunden werden kann, muss nicht mehr verboten werden. Gegen Verhaltensregeln kann verstoßen werden, gegen technische Begrenzungen eines Techniksystems nicht."

Ziel des technischen Datenschutzes in GENOMatch ist es also, den Pseudonymisierungsprozess mit technischen Mitteln durchzusetzen, d. h. die beteiligten Personen zu zwingen, von diesem Prozess nicht abzuweichen. Systeme wie GENOMatch erfordern jedoch die Bearbeitung greifbarer Gegenstände durch Menschen (hier z. B. das Entfernen und Anbringen von Etiketten). Solche Systeme müssen darauf vertrauen, dass der Zustand des Gegenstandes dem erwarteten und vorgeschriebenen Zustand entspricht (z. B. „der (PN, SN)-Aufkleber wurde entfernt"). Kontrollieren kann das IT-System diese Annahme nicht. Technische Mittel und verbindliche Verfahrensanweisungen für die beteiligten Personen müssen sich also so ergänzen, dass insgesamt der im Datenschutzkonzept vorgeschriebene *Workflow* sichergestellt wird.

Der technische Datenschutz kann den Prozess allerdings in vielen Bereichen unterstützen. Insbesondere eine strikte rollenbasierte Zugangskontrolle zu Funktionen des Systems und somit auch zu den jeweils verfügbaren Daten gewährleistet eine zuverlässige Pseudonymisierung. Zum Beispiel existiert eine Probe aus Sicht der Mitarbeiter bei Schering überhaupt erst dann, wenn sie vollständig pseudonymisiert wurde. Die Pseudonymisierung dürfen aber nur Mitarbeiter des CSR vornehmen. Somit können nur für pseudonymisierte Proben genetische Daten generiert werden.

6. Open Source – Entscheidung und Erfahrungen

Die Entscheidung, bei der Implementierung auf Open-Source-Produkte zu setzen, stand nicht von vornherein fest. Sie wurde nicht dogmatisch gefällt, vielmehr wurde für jede einzelne Design-Komponente evaluiert, welche Software am besten zur Realisierung der gewünschten Eigenschaften geeignet ist. Dass letztendlich im *GENOMatch Application Layer* fast ausschließlich freie Software zum Einsatz kommt, spricht für die Qualität von Open-Source-Software.

6.1. Architektur

Der grundsätzliche *Workflow* des doppelten Pseudonymisierungsprozesses mit einem Datentreuhänder diktiert große Teile der Systemarchitektur. Der Datentreuhänder – das SIM-Center – verwaltet alle Informationen, stellt die Pseudonymisierung sicher und macht beteiligten Personen stets nur die für sie bestimmten Daten zugänglich. Auf diesen Rechner greifen Nutzer aus mehreren Institutionen über das Internet zu,

Umgebung	Betriebssystem	Server-Software	Programmiersprache
Microsoft	Windows	Internet Information Server (IIS)	.NET (VB, C, C++, C#)
Open Source	Linux	Apache/ mod_ssl/ J2EE-Applikationsserver	Java

Tabelle 1: Betrachtete Standardumgebungen

sodass sowohl eine Standardisierung der Schnittstellen als auch eine Verschlüsselung der Kommunikation erforderlich ist.

Den Nutzern bietet der Server eine Weboberfläche an. Dies erlaubt sowohl die Nutzung von normalen Arbeitsplatz-Rechnern aus als auch die Möglichkeit, ohne großen Aufwand an Punkten, wo kritische Daten anfallen, *Thin Clients* einsetzen zu können. Die Authentifizierung mit *Smartcards* stand weit oben auf der Wunschliste und sollte evaluiert werden, galt zunächst jedoch nicht als zwingende Voraussetzung.

Dienste, die von Programmen (wie dem *Matchfilter* oder der lokalen Lagerverwaltungs-Software des CSR) in Anspruch genommen werden sollen, können mit vielen Techniken realisiert werden: Dateitransfers, *Remote Method Invocation* (RMI), *Common Object Request Broker Architecture* (CORBA) oder *Web Services* kamen hier in Frage. Für *Web Services* sprechen viele Gründe: Standardisierung, Zukunftssicherheit und Plattformneutralität; vor allem aber die Bündelung der kompletten Kommunikation auf ein verbreitetes und sicheres Protokoll (*Hypertext Transfer Protocol over Secure Socket Layer*, HTTPS), das keine Spezialkonfiguration in Firewalls benötigt.

Diese Architektur und diese Schnittstellen standen schon fest, bevor das erste technische Kick-off-Meeting stattfinden sollte. Über Betriebssysteme, Server-Software, Browser, Programmiersprachen und Tools war bis dahin noch kein Wort verloren worden, weshalb diese Besprechung von allen Seiten mit Spannung erwartet wurde (Abbildung 3).

6.2. Server-Seite – SIM-Center

Die wohl grundlegendste Entscheidung betraf die Programmiersprache. Diese bestimmt dann auch die Server-Software und damit praktisch auch das Betriebssystem für das SIM-Center. Um die im vorherigen Abschnitt beschriebene Architektur zu realisieren, gibt es eigentlich nur zwei Standardumgebungen:

Eine Reihe von Gründen sprach für die Open-Source-Lösung. Zu der höheren Sicherheit einer minimalisierten Apache-Installation kam vor allem die Möglichkeit, Anpassungen im Bereich der Verschlüsselung und der Authentifizierungsmechanismen vorzunehmen. Beides sind Faktoren, die durch die Verfügbarkeit des Quellcodes bedingt oder zumindest gefördert werden.

Wie in jedem Projekt entscheiden natürlich auch Entwicklungszeit und -kosten für das eine oder andere System. Mit den genannten Open-Source-Produkten waren um-

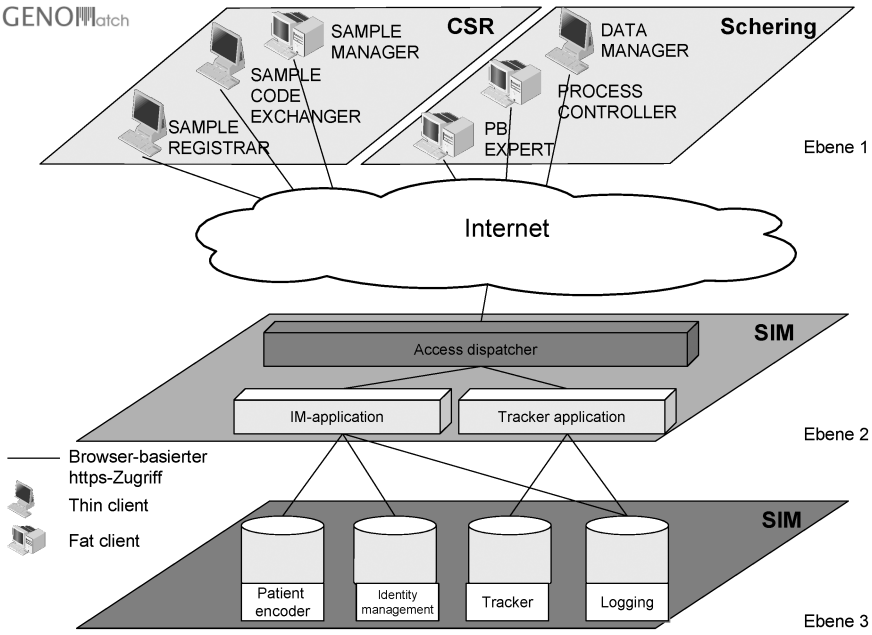

Abbildung 3: GENOMatch-Architektur

fangreiche Erfahrungen vorhanden. Aber auch die Möglichkeit, selbst Fehler zu finden und zu bereinigen oder selbst die nötigen Erweiterungen hinzuzufügen, beschleunigen den Entwicklungsprozess, da die Wartezeiten auf *patches* oder Fehlerdiagnosen des jeweiligen Herstellers entfallen.

Diese Grundsatzentscheidung für Linux/Apache/Java sorgte dann dafür, dass der Rest der Software-Komponenten in diesem Systemumfeld schnell gefunden war. Für den Server boten sich viele der ausgezeichneten Tools der Apache Foundation an:

- Java-Applikationsserver: Tomcat (Apache Jakarta Project)
- *Web Services*: Apache Axis
- *Logging*: log4j
- Weboberfläche: Struts
- *Build/Deployment*: Ant

Ergänzt werden diese Tools durch JavaMail von Sun Microsystems (für den Mailversand) und BouncyCastle Security Provider von BouncyCastle (für die Mailverschlüsselung). Auch Software zur Entwicklung wie Eclipse und CVS sind hervorragende und vielfach erprobte Tools.

Einzig bei der benötigten SQL-Datenbank fiel die Wahl dann wieder auf ein kommerzielles Produkt: Oracle. Oracle ist bei Schering der Standard für Datenbankanwendungen. Weitere Gründe waren vor allem die Stabilität, die Kompatibilität bei Migrationen zwischen Versionen und der Support. Diese waren vor allem deshalb entscheidend, weil die Pseudonymketten für einen Zeitraum von 20 bis 25 Jahren verfügbar bleiben müssen.

Die Wahl der Komponenten hat sich als ausgezeichnet erwiesen und hat es ermöglicht, schnell ein stabiles System mit allen gewünschten Merkmalen zu realisieren.

6.3. Thin Clients

Es gibt mehrere Stellen, an denen im GENOMatch-Prozess sensible Daten anfallen. Dies ist insbesondere bei der eigentlichen Pseudonymisierung im CSR der Fall. Die hier eingegebenen Bezeichnerpaare dürfen niemals außerhalb des SIM-Centers gespeichert werden.

Die Dateneingabe findet deshalb auf *Thin Clients* statt. Diese Geräte verhindern sowohl ein Speichern der Daten als auch jegliche Veränderung am System (wie beispielsweise *Keylogger* oder Screenshot-Programme). Auch Netzwerkverbindungen mit anderen Rechnern als dem SIM-Center müssen unterbunden werden.

Technisch umgesetzt wurden diese Anforderungen mit einem minimierten Linux–System. Dieses System bootet von einer CF-Karte, die ausschließlich lesbar eingebunden wird. Alle Dateien, die veränderbar sein müssen, werden auf RAM-Disks im Arbeitsspeicher gehalten und sind somit durch Ausschalten des Geräts zuverlässig zu löschen. Eine Grundkonfiguration dieser RAM-Disks wird beim Systemstart automatisch aus Konfigurationsimages erzeugt. Ein Paketfilter sorgt dafür, dass die Systeme ausschließlich über die vorgesehenen Protokolle (hier: HTTPS) mit bestimmten Rechnern (hier: SIM-Center) kommunizieren können.

Die Geräte selbst erfordern keine Nutzerauthentifizierung, sondern starten einen X-Server und einen Browser (Mozilla Firefox). Andere Software ist nicht installiert bzw. nicht startbar. Der Nutzer weist sich über das Netzwerk gegenüber dem SIM–Center mit seiner *Smartcard* aus, die mittels eines Browser-*Plugins* das *Secure-Socket–Layer*- (SSL) Client-Zertifikat für die HTTPS-Verbindung bereitstellt.

Der Flexibilität und Einfachheit von Linux ist es zu verdanken, dass ein erstes funktionierendes System innerhalb kürzester Zeit erstellt werden konnte. Die Installation, inklusive aller Anpassungen für den oben beschriebenen *read-only*-Betrieb, nahmen so weniger als zwei Tage in Anspruch. Das ist weniger Zeit, als für die vorher unternommenen Versuche, eine Browser/*Smartcard*-Kombination mit geschlossenen Systemen zu realisieren benötigt wurde. Eine spezialisierte Lösung auf Basis von Open Source zu erstellen, bietet mehr Freiheit, Kontrolle und Eingriffsmöglichkeiten, als der Versuch, eine proprietäre Lösung anzupassen.

6.4. Smartcards

Ein Grundsatz bei GENOMatch ist, dass jegliche Netzwerkkommunikation verschlüsselt erfolgt. Dies betrifft unter anderem folgende Kommunikationskanäle:

- Nutzung des SIM-Centers über die Weboberfläche. Hier kommt HTTPS (SSL–verschlüsseltes *Hypertext Transfer Protocol*) zum Einsatz.
- Zugriffe von externen Programmen oder GENOMatch-Komponenten auf das SIM-Center. Diese sind als *Web Services* realisiert; als Protokoll wird ebenfalls HTTPS genutzt.

Die Verschlüsselung aller Zugriffe auf das SIM-Center verhindert das Abhören der übertragenen Daten durch Dritte. Es bleibt jedoch für einen Angreifer möglich, den Netzverkehr umzuleiten und sich dem Nutzer gegenüber als SIM-Center auszugeben. Dem wird durch die Verwendung von digitalen Zertifikaten begegnet. Das SIM-Center weist sich mit einem solchen Zertifikat aus, wie es auch z. B. beim Homebanking über eine Weboberfläche Stand der Technik ist.

Damit kann der Nutzer sicher sein, mit dem SIM-Center zu kommunizieren. Die Nutzerauthentifizierung wird üblicherweise jedoch immer noch mittels Nutzerkennung und Passwort durchgeführt. Die beiderseitige Identitätsprüfung mittels Zertifikaten verlangt auch vom Nutzer das Vorweisen eines digitalen Ausweises. Dieser wird bei GENOMatch auf einer *Smartcard* gespeichert und ist mit einer PIN geschützt.

Dadurch wird die Sicherheit in mehreren Bereichen verbessert:

- Das Zertifikat verlässt niemals die *Smartcard*, kann also nicht kopiert werden.
- Zugang zum System erfordert nicht nur das Wissen um ein geheimes Passwort / PIN, sondern auch den Besitz einer *Smartcard*.
- Die Eingabe der PIN erfolgt direkt am Kartenleser und ist somit auch an *Fat Clients* vor Mitschneiden geschützt.

Leider werden digitale Zertifikate auf einer *Smartcard* noch nicht in großem Umfang eingesetzt, obwohl das Gesetz zur *Digitalen Signatur* dafür schon länger Rahmenbedingungen vorgibt. Dies bewirkt, dass viele Standardprodukte diese Technik nicht unterstützen und sich ein Markt für proprietäre Nischensysteme gebildet hat.

Die Nutzung von *Thin Clients* stand von Beginn an fest, und es wurde früh überlegt, hier evtl. auf Linux zu setzen. Auf der CeBIT 2003 wurde deshalb bei mehreren Herstellern von Kartenlesern nachgefragt, ob diese ein Browser-*Plugin* und einen Treiber auch für Linux bereitstellen. Viele Hersteller bieten ihre Lösung als *Login*-Mechanismus für Windows oder als komplett proprietäre Lösung an, unterstützen jedoch keine SSL-Client-Zertifikate für Browser. Diejenigen, die diese Möglichkeit vorsehen, liefern jedoch meistens nur *Plugins* für Windows Internet Explorer, auf Nachfragen wurde als Grund oft genannt, dass für die Unterstützung von Netscape/Mozilla und/oder Linux/Unix kein Markt vorhanden sei und es sich somit nicht lohne. Die einzige Firma, die in ihren Geräten Netscape/Mozilla auf mehreren Plattformen unterstützt, ist die Firma Kobil. Hier gibt es gegen Aufpreis Kartenleser mit der benötigten Software sowohl für Windows als auch für Linux und Solaris.

Diese Komponente ist außer der Oracle Datenbank die einzige proprietäre Software, die in GENOMatch zum Einsatz kommt. Zugleich ist dies ein Punkt, an dem

ein benötigtes *Feature* nicht realisiert werden konnte. Nachdem zunächst der Hersteller zugesagt hatte, dieses Merkmal einzubauen, hat man sich nun doch dagegen entschieden. Es bleiben somit nur die Möglichkeiten, den Hersteller dafür in einem gesonderten Auftrag zu bezahlen oder in Verhandlungen die Herausgabe des Quellcodes zu erreichen. Hier sind bisher noch keine Fortschritte erzielt worden. Hätte es sich um offene Software gehandelt, so wäre die Erweiterung mit einer Entwicklungszeit von maximal einer Woche durchführbar gewesen und hätte danach der gesamten Community zur Verfügung gestanden.

7. Fazit

GENOMatch ist nicht nur unter den Aspekten des Datenschutzes und der damit verbundenen Prozeduren ein interessantes Projekt. Auch technisch mussten viele Hürden genommen werden, bei denen uns die Flexibilität, ein Blick in den Quellcode und die hervorragende Dokumentation im Internet – seien es *HOW-TO*s, Erfahrungsberichte oder Foren und Mailinglisten – oftmals weitergeholfen haben.

Dass wir fast ausschließlich Open-Source-Produkte einsetzen, und dass dies nicht aus politischen, sondern allein aus technischen Gründen geschieht, zeigt die Reife und Qualität Freier Software.

Wir glauben, mit diesen Mitteln ein qualitativ hervorragendes Produkt abgeliefert zu haben, das mit anderer Software so vielleicht nicht realisierbar gewesen wäre.

Literatur

Council of Europe (1997), 'RECOMMENDATION No. R (97) 5 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE PROTECTION OF MEDICAL DATA', COUNCIL OF EUROPE COMMITTEE OF MINISTERS, http://cm.coe.int/ta/rec/1997/97r5.html [15. Jan 2005]. Adopted by the Committee of Ministers on 13 February 1997 at the 584th meeting of the Minsters' Deputies.

Datenschutzbeauftragte (2001), 'Anlage zu „Umgang mit genetischen Untersuchungen"', Datenschutz Berlin, http://www.datenschutz-berlin.de/doc/de/konf/62/anlage.htm [15. Jan 2005]. Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24.-26. Oktober.

Enquete-Kommission (2002), 'Schlussbericht der Enquete-Kommission „Recht und Ethik in der modernen Medizin"', Deutscher Bundestag, http://dip.bundestag.de/btd/14/090/1409020.pdf [15. Jan 2005]. Bundestagsdrucksache 14/9020.

Luttenberger, N. (2003*a*), 'Data Protection Concept for the "Sample and Save" Part of the GENOMatch Project at Schering AG', (erhältlich auf Anfrage).

Luttenberger, N. (2003*b*), 'Kurzgutachten zum Datenschutzaudit: Konzept einer Datenverarbeitungsinfrastruktur der Fa. Schering AG für die sichere pseudonyme Einlagerung und Verwahrung von für genetische Analysen genutzten Blut- und Gewebeproben', Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,

http://www.datenschutzzentrum.de/audit/kurzgutachten/a0303/index.htm [15. Jan 2005]. Entwickelt von der AG Kommunikationssysteme am Institut für Informatik und Praktische Mathematik, Prof. Norbert Luttenberger, Christian-Albrechts-Universität zu Kiel.

Robertson, J. A. (2001), Consent and privacy in pharmacogenetic testing, *in* 'nature genetics', Vol. 28, Nature Publishing Group, S. 207–209. zu beziehen unter http://www.nature.com/cgi-bin/doifinder.pl?URL=/doifinder/10.1038/90032 [15. Jan 2005].

Roßnagel, A. (2004), 'Datenschutzrecht in Deutschland', Friedrich-Ebert-Stiftung Korea, http://www.fes.or.kr/Publications/pub/Rossnagel_PSPD-2004.pdf [30. Jan 2005]. Vortrag für den Korean-German Joint Workshop on Privacy Protection der People's Solidarity for Participatory Democracy und der Friedrich-Ebert-Stiftung am 1. November 2004 in Seoul.

Ziegler, P.-M. (2004), 'Sieger des ersten "Open Source Best Practice Award" präsentiert', heise online, http://www.heise.de/newsticker/meldung/51885 [15. Jan 2005].

Weiterführende Informationen

Informationen zur Software der Apache Software Foundation finden sich unter (Tomcat, Apache Axis, log4j, Struts, Apache Ant sind Warenzeichen der *The Apache Software Foundation, USA.*):

- Tomcat: http://jakarta.apache.org
- Apache Axis: http://ws.apache.org/axis
- log4j: http://logging.apache.org/log4j
- Struts: http://struts.apache.org
- Apache Ant: http://ant.apache.org

Detaillierte Informationen zur JavaMail API finden sich auf den Webseiten von Sun Microsystems (Java, J2EE und JavaMail API sind Warenzeichen der *Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054, USA.*):

- Java: http://java.sun.com/
- J2EE: http://java.sun.com/j2ee/index.jsp
- JavaMail API: http://java.sun.com/products/javamail

Weitere Informationen zum BouncyCastle Security Provider sind auf den Internetseiten des Herstellers zu finden (*BouncyCastle Security Provider – Copyright (c) 2000 - 2004 The Legion Of The Bouncy Castle*): http://www.bouncycastle.org