Univ.-Prof. Dr. Klaus Pommerening
Institut für Medizinische Biometrie, Epidemiologie und Informatik
Johannes-Gutenberg-Universität
55101 Mainz

Gutachten zu kryptographischen Fragen

Im Auftrag der
Telematikplattform – Verbund zur Förderung vernetzter Medizinischer Forschung (TMF) e.V.

Mainz, den 29. September 2008

Version 1.1

Inhalt

Einleitung

In der medizinischen Forschung werden sensible persönliche Daten von Patienten oder Probanden verarbeitet. Diese unterliegen starken Datenschutzanforderungen wie z. B. den Regelungen der ärztlichen Schweigepflicht [1].

Hieraus resultiert ein hoher Schutzbedarf, der u. a. durch technische Maßnahmen sichergestellt werden muss und der auch ein hohes Niveau bei den üblichen Sicherheitsanforderungen in offenen und verteilten Systemen – nämlich Vertraulichkeit, Echtheit (Integrität und Authentizität), Verbindlichkeit (Nachweisbarkeit, Unbestreitbarkeit) – erfordert [2]. Diese Anforderungen können zu einem beträchtlichen Teil durch kryptographische Verfahren abgedeckt werden, vorausgesetzt, diese werden nach dem Stand der Technik eingesetzt.

Kryptographie ist die Lehre von der Informationssicherheit in „feindlicher" Umgebung[1]. Kryptographie umfasst Algorithmen, Protokolle, Anwendungssysteme und Infrastruktur. Wirksame Sicherheit in offenen und verteilten Systemen ist nur mit kryptographischen Techniken zu erreichen, die allerdings in eine Vielzahl anderer technischer und organisatorischer Maßnahmen eingebettet sein müssen. Die wesentlichen Schwachpunkte von Systemen sind heutzutage in der Regel nicht in den kryptographischen Algorithmen lokalisiert, sondern in ihrer Einsatz-Umgebung, die bei ungeschickter Konfiguration auch die kryptographischen Verfahren selbst angreifbar machen kann („Seitenkanal-Kryptoanalyse"[2]).

Die kryptographischen Anwendungen, die in medizinischen Forschungsnetzen einzusetzen sind, betreffen im Wesentlichen die Bereiche

- Schutz der Kommunikation (Vertraulichkeit, Integrität),
- Pseudonymisierung zum Schutz der Identität von Patienten und Probanden,
- Authentisierungsverfahren zur Zugriffssteuerung,
- Echtheit (Integrität) von Dokumenten und Daten.

Dieses Gutachten beleuchtet nur die kryptographischen Aspekte von Datenschutz und IT-Sicherheit in medizinischen Forschungsnetzen. Es wird ausdrücklich darauf hingewiesen, dass mit kryptographischen Techniken nur Teile eines umfassenden Datenschutz- und Sicherheitskonzepts abgedeckt werden.

Ein vollständiges Review aller relevanten kryptographischen Systeme, z. B. Netzkomponenten oder PC-Sicherheitssysteme, ist im Rahmen dieses Gutachtens nicht möglich, da der Markt zu unübersichtlich, voller proprietärer Lösungen und in ständigem Fluss ist. Der Schwerpunkt des Gutachtens liegt auf direkt in medizinischen Forschungsnetzen einsetzbaren Verfahren; daneben werden Kriterien formuliert, die zur Beurteilung der kryptographischen Komponenten kommerzieller Produkte dienen.

[1] D. h., man unterstellt, dass Angreifer nicht vor Regelverstößen zurückschrecken, um Informationen auszuspähen oder zu verfälschen, und sucht nach Schutzmaßnahmen, die selbst unter dieser pessimistischen Annahme noch wirksam sind.

[2] http://de.wikipedia.org/wiki/Seitenkanalattacke

1. Algorithmen und deren Sicherheit

1.1 Typen kryptographischer Algorithmen

Bei kryptographischen Algorithmen ist grundsätzlich zu unterscheiden zwischen **symmetrischen** Verfahren und **asymmetrischen** Verfahren (Public-Key-Verfahren). Beide Typen dienen zunächst direkt zum Schutz von Informationen vor unbefugter Einsichtnahme, also zur kryptographischen Verschlüsselung. Die wesentlichen Unterschiede dieser beiden Typen sind:

- **Schlüsselverwendung:** Symmetrische Verfahren verwenden für Verschlüsselung und Entschlüsselung den gleichen Schlüssel; bei asymmetrischen Verfahren unterscheiden sich die Schlüssel für die Verschlüsselung und die Entschlüsselung und sind auch nicht rechnerisch auseinander herzuleiten.
- **Schlüsselmanagement:** Symmetrische Verfahren erfordern die vorherige Vereinbarung eines Schlüssels, der allen Kommunikationsteilnehmern (und nur diesen) bekannt ist. Dagegen beruht die Sicherheit asymmetrischer Verfahren darauf, dass jeder Teilnehmer einen persönlichen, *nur ihm selbst bekannten* „privaten" Schlüssel besitzt, der niemals jemand anderem zur Kenntnis kommen darf.
- **Schlüssellänge:** Asymmetrische Verfahren erfordern eine deutlich größere Schlüssellänge als symmetrische Verfahren; hier muss man bei den gängigsten Verfahren von einem Faktor von etwa 40 ausgehen.
- **Effizienz:** Symmetrische Verfahren sind rechnerisch wesentlich effizienter; der Zeitbedarf asymmetrischer Verschlüsselung ist etwa um den Faktor 10000 höher.
- **Infrastruktur:** Bei der Verwendung asymmetrischer Verfahren muss sichergestellt werden, dass die zur Verschlüsselung verwendeten öffentlichen Schlüssel authentisch sind. Das lässt sich bei breiter Anwendung nur durch eine Public-Key-Infrastruktur (PKI) erreichen, in der öffentliche Schlüssel durch Zertifikate beglaubigt sind.
- **Anwendungsbereich:** Mit asymmetrischen Verfahren lassen sich in vielen Situationen Sicherheitsanforderungen viel unkomplizierter erfüllen als mit symmetrischen; ein Beispiel hierfür ist die digitale Signatur.

Um die Vorteile beider Typen kryptographischer Algorithmen zu verbinden, verwendet man in der Praxis oft **hybride** Verfahren, bei denen die Grundverschlüsselung symmetrisch erfolgt und der dazu verwendete Schlüssel (als „Sitzungsschlüssel" oder „Einmalschlüssel") mit Hilfe eines asymmetrischen Verfahrens übermittlet wird. *Bei der Beurteilung der Sicherheit hybrider Verfahren ist zu beachten, dass beide eingesetzten Verfahren für sich allein genommen sicher sind*, also z. B. über ausreichende Schlüssellängen verfügen. Die Angabe nur einer Schlüssellänge reicht für die Beurteilung der Sicherheit nicht aus.

Neben diesen beiden Typen kryptographischer Verfahren gibt es noch **Einweg-Verfahren** (s. 1.4), speziell **Hash-Verfahren**; zu den kryptographischen Algorithmen gehören ferner **Zufallsgeneratoren** (s. 1.5).

1.2 Symmetrische Verfahren

Gute symmetrische Verschlüsselungsverfahren zeichnen sich dadurch aus, dass kein Angriff auf sie bekannt ist, der effizienter ist als das Durchprobieren aller möglichen Schlüssel („Exhaustion" oder „Brute-Force-Attacke"). Das bedeutet, dass die Schlüssellänge des Verfahrens

(in Anzahl der Bits) ein direktes Maß für die Sicherheit ist. Jedes zusätzliche Bit Schlüssellänge bedeutet eine Verdopplung des Angriffsaufwandes.

Nach dem gegenwärtigen Stand der Technik gilt eine Schlüssellänge oberhalb von 90 Bit als sicher. In der Praxis wird aus Gründen der einfachen technischen Realisierung in der Regel eine Schlüssellänge von 128 Bit verwendet. Für sehr langfristige Sicherheit (über etwa 30 Jahre) werden Verfahren mit 256-Bit-Schlüsseln empfohlen.

Bekannte geeignete Verfahren sind:

- 3DES (= TDES = TripleDES), die dreifache Anwendung des DES-Verfahrens mit zwei oder drei verschiedenen Schlüsseln; die Schlüssellänge ist dabei 112 oder 168 Bit (= 2 × 56 oder 3 × 56).
- AES, das als Standard den DES seit 2001 abgelöst hat; Schlüssellänge 128, 192 oder 256 Bit.
- Die übrigen Endrundenteilnehmer des AES-Wettbewerbs [3]: MARS, RC6, Serpent, Twofish.
- Ältere symmetrische Verfahren, die immer noch als sicher einzustufen sind: IDEA, RC4, RC5, CAST, Blowfish mit Schlüssellängen von mindestens 128 Bit.
- Das NESSIE-Portfolio [4] umfasst die Algorithmen MISTY1, AES, Camellia, SHACAL-2.

Das DES-Verfahren selbst ist nicht mehr sicher, da es eine Schlüssellänge von nur 56-Bit verwendet und der Aufwand zum Brechen inzwischen auch für kleine Organisationen im Bereich weniger Tage liegt.

Die *besonders empfohlenen Verfahren* sind daher:

- **3DES**: Entweder mit zwei DES-Schlüsseln nach dem „EDE-Prinzip“ (Schlüssellänge 112 Bit) oder mit drei DES-Schlüsseln (Schlüssellänge 168 Bit). Beide Varianten dürfen als sicher angenommen werden und sind auf vielen Smartcards implementiert sowie als Software frei verfügbar.
- **AES** (Advanced Encryption Standard, seit 2001 NIST-Standard, Algorithmus Rijndael), Schlüssellänge 128, 192 oder 256 Bit. Es darf als sicher angenommen werden und sollte wo immer möglich zum Einsatz kommen. Erste Implementationen auf Smartcards sind verfügbar; als Software ist es frei erhältlich.

1.3 Asymmetrische Verfahren

Bei asymmetrischen Verfahren sind stets mathematische Ansätze zum Brechen der Verschlüsselung bekannt, die effizienter als das vollständige Durchprobieren aller Schlüssel sind. Daher muss man zur Erzielung einer nach dem Stand der Technik ausreichenden Sicherheit wesentlich größere Schlüssellängen verwenden als bei symmetrischen Verfahren. Mit Ausnahme der ECC-Verfahren (s. u.) *benötigt man für kurzfristige Sicherheit 2048-Bit-Schlüssel und für mittel- bis langfristige Sicherheit 4096-Bit-Schlüssel*.

Asymmetrische Verfahren sind in der Regel unmittelbar zur Verschlüsselung, zur digitalen Signatur und für Authentisierungsverfahren einsetzbar.

Bekannte geeignete asymmetrische Verfahren sind:

- RSA als am weitesten verbreitetes Verfahren, das alle wesentlichen Bedürfnisse an asymmetrische Verfahren alleine abdecken kann. Schlüssellänge beliebig.

- DH, das nur als asymmetrischer Teil eines hybriden Verschlüsselungsverfahrens geeignet ist. Schlüssellänge beliebig.
- DSA, der US-Standard für digitale Signaturen. Die Sicherheit ist wegen der im Standard festgeschriebenen Schlüssellänge von höchstens 1024 Bit zweifelhaft; das Verfahren selbst kann aber auch (außerhalb des Standards) mit längeren Schlüsseln eingesetzt werden.
- ECC, eine Klasse von Verfahren, die mathematisch auf der Theorie der „elliptischen Kurven" beruhen, für alle Zwecke geeignet sind und mit deutlich geringeren Schlüssellängen auskommen. Sie sind damit auch für die Implementation auf Chipkarten gut geeignet. Schlüssellänge beliebig, für mittelfristige Sicherheit empfiehlt das BSI eine Schlüssellänge von mindestens 224 Bit.
- Das NESSIE-Portfolio umfasst neben RSA die ECC-Algorithmen PSEC und ACE und als Signatur-Algorithmen ECDSA und SFLASH (der allerdings Ende 2007 gebrochen wurde). Dazu kommt das asymmetrische Identifikationsschema GPS.

Alle diese Verfahren – mit Ausnahme einiger spezieller ECC-Verfahren – sind als Software frei erhältlich. Zu Verfügbarkeit auf Smartcards s. 3.5. *Besonders empfehlenswert sind* **RSA** *und einige* **ECC***-Verfahren*. Die Implementation der wichtigsten asymmetrischen Verfahren ist in den PKCS[3] (Public Key Cryptography Standards) von den RSA-Laboratorien standardisiert.

1.4 Einweg-Verfahren und Hash-Funktionen

Einweg-Verfahren sind kryptographische Transformationen, deren Umkehrung rechnerisch nicht möglich ist; sie erlauben nur einen Vergleich zweier verschlüsselter Informationen auf Gleichheit oder Ungleichheit. Das wird oft bei der Passwortverwaltung ausgenützt. Andere sinnvolle Anwendungen gibt es im Bereich der Pseudonymisierung. Einweg-Verfahren können „öffentlich" sein, d. h. ohne Anwendung einer geheimen Zusatzinformation anwendbar, oder schlüsselabhängig. Im ersten Fall ist eine naheliegende Angriffsmethode die „Probeverschlüsselung": Wenn man bei Anwendung auf einen gewählten Text ein bereits von anderer Stelle erzeugtes Ergebnis erhält, hat man in diesem Fall die „Verschlüsselung" gebrochen. Bei schlüsselabhängigen Verfahren wird diese Angriffsmöglichkeit auf den Besitzer des Schlüssels beschränkt (der die Verschlüsselung allerdings auch nicht direkt umkehren können soll).

Die wichtigste Klasse von Einweg-Verfahren sind die **Hash-Funktionen**, bei denen man auf die „Injektivität" (Verschiedenheit der Ergebnisse bei unterschiedlichen Eingaben) verzichtet, aber verlangt, dass es rechnerisch unmöglich ist, zwei Klartexte mit gleichem Hash-Wert zu erzeugen („Kollisionsfreiheit" – dadurch unterscheiden sich Hash-Funktionen von gewöhnlichen Prüfsummen wie CRC-Verfahren[4]). Für schlüsselabhängige Hash-Funktionen ist auch die Bezeichnung MAC (Message Authentication Code) im Gebrauch.

Eine der wichtigsten Anwendungen von Hash-Verfahren ist die Vereinfachung der digitalen Signatur: Diese wird wegen der Langsamkeit asymmetrischer Verschlüsselungsverfahren in der Regel über den Zwischenschritt einer Hash-Funktion ausgeführt.

Hash-Werte haben eine feste vorgegebene Länge, unabhängig vom eingespeisten Text. Diese Länge dient als Maß für die Sicherheit des Verfahrens gegen das Finden von Kollisionen. Als

[3] http://www.rsasecurity.com/rsalabs/node.asp?id=2124

[4] cyclic redundancy check; diese Verfahren sichern nur vor zufälligen, nicht vor absichtlichen Verfälschungen einer Nachricht oder eines Dokuments und sind daher für kryptographische Zwecke ungeeignet.

Faustregel sollte sie doppelt so groß sein wie die für symmetrische Verschlüsselung nötige Schlüssellänge, *nach dem Stand der Technik also mindestens 180 Bit*, besser 256 Bit.

Bekannte Hash-Verfahren sind:

- MD2, MD4, MD5, lange Zeit als Standard verwendete Hash-Verfahren mit 128 Bit, mehrfach gebrochen. Für MD2 und MD4 lassen sich Kollisionen mit für Privatpersonen erreichbarem Aufwand finden, für MD5 ist der Aufwand höher.
- RIPEMD-160, ein im Europäischen Rahmenprogramm RACE entwickelter Algorithmus mit 160 Bit; es gibt auch Versionen mit 256 und 320 Bit, die aber nicht als sicherer gelten.
- SHA-1, im Zusammenhang mit dem DSA entwickelter 160-Bit-Algortihmus; da bereits Kollisionen gefunden wurden, kann er nicht mehr als sicher gelten.
- SHA-2, Weiterentwicklung des SHA-1 mit den Varianten SHA-224, SHA-256, SHA-384, SHA-512, wobei der numerische Zusatz die Hash-Länge angibt. Gilt in allen diesen Varianten als sicher.
- Das NESSIE-Portfolio umfasst neben SHA-2 noch Whirlpool, einen 512-Bit-Algorithmus. Dazu kommen die MAC-Algorithmen UMAC, TTMAC, CBC-MAC und HMAC.

*Unter diesen Verfahren ist für die Zukunft **SHA-2** zu empfehlen.* Ein neuer Standard SHA-3 soll 2012 verabschiedet werden; der Wettbewerb[5] dafür läuft bereits seit November 2007.

1.5 Zufallsgeneratoren und Schlüsselerzeugung

Zufall ist ein wichtiges Element vieler kryptographischer Anwendungen: Der „Gegner“ soll keinen statistischen Vorteil beim Erraten bestimmter Informationen finden können. Besonders kritisch ist dieser Aspekt bei der Erzeugung kryptographischer Schlüssel, z. B. privater Schlüssel für asymmetrische Verfahren oder Einmal-Schlüssel für hybride Verfahren; eine andere wichtige Anwendung ist die Erzeugung von „Challenges“ für die starke Authentisierung (s. 2.6).

Ein Prozess der Informationsverarbeitung, der geeignete zufällige oder unvorhersagbare Werte ausgibt, heißt **Zufallsgenerator**. Man unterscheidet zwischen „physikalischen“ (oder „echten“) Zufallsgeneratoren und algorithmischen Zufallsgeneratoren (oder „Pseudozufallsgeneratoren“). Erstere sind langsam, aber gelten als sicher, bei letzteren hängt die Sicherheit davon ab, dass ein geheimer, unvorhersagbarer Startwert gewählt wird und aus keinem bekannten Teil der erzeugten Folge ohne Kenntnis des Startwerts weitere Folgenglieder berechnet werden können. In der Praxis verwendet man auch hier hybride Verfahren, bei denen ein physikalisch erzeugter Zufallswert als Startwert für einen Pseudozufallsgenerator gewählt wird.

Für die Zufallserzeugung gibt es spezielle Chips, z. T. auch in Smartcards. Aber auch die gängigen Betriebssysteme bieten Zufallsgeneratoren[6], bei denen der physikalische Anteil aus mehr oder weniger unvorhersagbaren System-Ereignissen extrahiert wird.

Zur Beurteilung der Sicherheit eines kryptographischen Verfahrens muss unbedingt die Qualität des für die Schlüsselerzeugung verwendeten Zufallsgenerators beachtet werden. Wichtig ist dabei auch, dass der Erzeugungsprozess von einem „Gegner“ nicht beobachtet werden kann; in der Vergangenheit war dies oft der Ansatzpunkt zum Brechen kryptographischer

[5] http://csrc.nist.gov/groups/ST/hash/sha-3/

[6] auf Unix-Systemen (wie Linux) unter `/dev/random` und `/dev/urandom`

Verfahren. Dieser Aspekt spricht gegen die Verwendung der in Standard-Rechner oder -Betriebssysteme eingebauten Zufallsgeneratoren und für die Verwendung speziell gekapselter Chips, wie sie in Smartcards oft vorhanden sind.

Bei NESSIE wurde in dieser Kategorie keine Empfehlung gegeben. Das BSI formuliert in AIS 31 [5] allgemeine Anforderungen an Zufallsgeneratoren.

1.6 Empfehlungen und Perspektiven

Es gibt für die Sicherheit kryptographischer Verfahren Stellungnahmen und Empfehlungen von Behörden (BSI, Bundesnetzagentur, Normierungsbehörden), öffentlich geförderten Projekten und Organisationen (NESSIE[7]) sowie von führenden Wissenschaftlern. Die Empfehlungen der führenden Wissenschaftler sind bisher stets strenger als die der „offiziellen" Stellen und diese wiederum strenger als die Marktverfügbarkeit in kommerziellen Produkten; in der Vergangenheit waren diese Unterschiede z. T. erheblich, wobei die Entwicklung stets den pessimistischen Warnungen der Wissenschaftler recht gegeben hat. Hier gilt der von Bruce Schneier formulierte Grundsatz: Einmal gefundene Angriffe können nur noch effizienter werden, und meist geschieht das recht kurzfristig. Daher sollte man Algorithmen bereits dann ersetzen, wenn erste Angriffe bekannt werden. Andererseits sind von der Wissenschaft gefundene Angriffe auf kryptographische Verfahren oft nicht sofort in praktischen Szenarien anwendbar. Daher gilt die Empfehlung: *Verfahren, bei denen erste Schwächen bekannt geworden sind, sollten in neuen Anwendungssystemen nicht mehr verwendet werden; der Ersatz in existierenden Systemen sollte zügig, aber mit Bedacht erfolgen*. Hier sind vor allem die BSI-Empfehlungen zu beachten.

Die Sicherheit kryptographischer Verfahren nimmt mit wachsender Rechenleistung kontinuierlich, aber ziemlich gut vorhersagbar nach dem Mooreschen Gesetz ab. Schwieriger ist die Voraussage der Steigerung der algorithmischen Leistung, die auf mathematischen Fortschritten beruht.

Besonders große Sicherheitsabstände sind für Langzeitsicherheit vorzusehen. Diese ist nötig bei

- Verschlüsselung – damit einmal kopierte kryptographisch verschlüsselte Daten auch in der Zukunft nicht entschlüsselt werden können,
- Pseudonymen – aus dem gleichen Grund,
- digitaler Signatur – damit signierte Daten ihren Beweiswert über die gesamte Speicherdauer behalten. Hier kann die Sicherheit allerdings vor Ablauf des Algorithmus durch Nachsignieren verlängert werden.

Obwohl die Langfristsicherheit für verschlüsselte Daten und Pseudonyme theoretisch nicht verlängert werden kann, sollte ein Prozess der Umverschlüsselung vorgesehen werden. Durch organisatorische Regelungen wie der Nichtherausgabe von Pseudonymen sollte sichergestellt werden, dass niemand Kopien verschlüsselter Daten zur späteren Entzifferung beiseite schaffen kann.

Langzeitsicherheit ist nicht nötig für

- Authentisierungsverfahren – da hier nach beendetem Anmeldevorgang die dabei ausgetauschten Daten für Angreifer keinen Wert mehr haben.

[7] http://www.cryptonessie.org/

Für das Problem der Langzeitsicherheit verschlüsselter Daten wurde im Auftrag der Bundesärztekammer das Raptis-Verfahren als Lösungsvorschlag entwickelt [6]. Allerdings sind die kryptographischen Verfahren bei den gängigen Vorgehensweisen nicht die wichtigsten Schwachstellen, sondern die Systemumgebung und das organisatorische Umfeld; zur Sicherheit dieser „Randbedingungen" trägt das Raptis-Verfahren nichts bei, sondern erhöht im Gegenteil die Komplexität. Die gängigen empfohlenen Verfahren mit einer ausreichenden, zukunftssicheren Schlüssellänge sollten zumindest für Anwendungen in der medizinischen Forschung ausreichen; die Entwicklung in der Gesundheitstelematik sollte aber beobachtet und gegebenenfalls übernommen werden.

In Deutschland werden empfohlene und zur Erfüllung des Signaturgesetzes zugelassene Verfahren regelmäßig vom BSI vorgeschlagen und von der Bundesnetzagentur[8] veröffentlicht; diese Empfehlungen gelten stets für 7 Jahre im Voraus. Seit Januar 2008 empfiehlt das BSI für die Signaturverfahren RSA und DSA eine Mindestschlüssellänge von 2048 Bit. Konkludent sollte diese Empfehlung auch auf die Verschlüsselung nach RSA angewendet werden. Für die betrachteten ECC-Verfahren ist die empfohlene Mindestschlüssellänge 224 Bit. Als Hash-Funktionen werden die Varianten von SHA-2 empfohlen. Zufallsgeneratoren müssen die Empfehlung AIS 31 erfüllen [5].

Weitere Empfehlungen des BSI sind in den IT-Grundschutz-Katalogen enthalten [7]; hier relevant sind

- Krypto-Konzept[9],
- Auswahl eines geeigneten kryptographischen Verfahrens[10],
- Auswahl eines geeigneten kryptographischen Produktes[11],
- Regelung des Einsatzes von Kryptomodulen[12],
- Datensicherung bei Einsatz kryptographischer Verfahren[13].

NESSIE (New European Schemes for Signatures, Integrity and Encryption) war ein europäisches Forschungsprojekt, das eine Auswahl („Portfolio") an überprüften kryptographischen Verfahren empfehlen sollte (abgeschlossen 2004) [4].

Empfehlungen von Wissenschaftlern werden naturgemäß eher unregelmäßig und sporadisch herausgegeben. Wichtige noch aktuelle Veröffentlichungen waren in der jüngeren Vergangenheit [8; 9].

Aus Gründen der Praktikabilität ist es für medizinische Netze in der Regel nicht sinnvoll, die in der Gesundheitstelematik jeweils zur Zeit üblichen Sicherheitsgrenzen – den BSI-Empfehlungen entsprechenden – zu überbieten, auch wenn diese vielleicht schon angezweifelt werden.

[8] http://www.bundesnetzagentur.de
[9] http://www.bsi.de/gshb/deutsch/baust/b01007.htm
[10] http://www.bsi.de/gshb/deutsch/m/m02164.htm
[11] http://www.bsi.de/gshb/deutsch/m/m02165.htm
[12] http://www.bsi.de/gshb/deutsch/m/m02166.htm
[13] http://www.bsi.de/gshb/deutsch/m/m06056.htm

2. Kryptographische Protokolle und Software

2.1 Datenträgerverschlüsselung

Datenträgerverschlüsselung dient bei Festplatten dem Schutz der gespeicherten Daten und ist unter anderem Teil der Serverhärtung (s. 3.1). Bei mobilen Datenträgern dient die Verschlüsselung der Transportsicherung. Grundsätzlich kann man einzelne Dateien verschlüsseln, was aber in der Regel nur für Transportzwecke – auf mobilen Datenträgern oder als E-Mail-Anlage – zweckmäßig ist. Sonst ist die bessere Alternative, ganze Partitionen (auch „virtuelle Partitionen“) zu verschlüsseln. Unix-Systeme[14] und professionelle Windows-Systeme (die Microsoft-eigenen Verschlüsselungssysteme heißen **EFS**[15] und **BitLocker**[16]) bieten diese Verschlüsselungsmöglichkeit als Leistung des Betriebssystems. Als kostenloses und portables Produkt, das auch für einfachere Systeme geeignet ist, kann man TrueCrypt[17] empfehlen. Wer die kommerzielle Version von PGP[18] nutzt, kann auch das darin enthaltene PGPDisk verwenden. Ferner gibt es eine Reihe kommerzieller Produkte, auch auf Hardware-Basis, was wesentlich höhere Sicherheit, aber wesentlich geringere Flexibilität und Portabilität bietet.

Empfehlung: *Auf Servern in medizinischen Forschungsnetzen sollten mit den im Betriebssystem vorgesehenen Methoden verschlüsselte Partitionen angelegt und zur Speicherung von sensiblen Daten genutzt werden. Arbeitsplatzrechner, auf denen, wenn auch nur kurzfristig, Patientendaten gespeichert werden, sollten mit einer* **TrueCrypt**-*verschlüsselten Partition versehen werden.*

Ein Problem besteht, wenn Server mit verschlüsselten Partitionen nach einem Systemausfall automatisch wieder anlaufen sollen; siehe dazu unten (3.1) unter „Server-Härtung“.

2.2 PKI

Bei der Verwendung von asymmetrischen (oder hybriden) Verschlüsselungsverfahren muss man sich darauf verlassen können, dass öffentliche Schlüssel authentisch sind. Zu diesem Zweck werden die öffentlichen Schlüssel von einem allgemein bekannten **Trustcenter** digital signiert. Ein solcher öffentlicher Schlüssel zusammen mit der Signatur eines Trustcenters heißt **Zertifikat**. Trustcenter werden in einer hierarchischen Struktur angeordnet; der öffentliche Schlüssel der an der Spitze dieser Hierarchie stehenden Instanz, genannt **Root-Zertifikat**, muss jedem Teilnehmer als authentisch bekannt sein. Trustcenter führen einen **Verzeichnisdienst**, aus dem alle ausgestellten Zertifikate bei Bedarf online abgerufen werden können; dazu gehören auch Sperr- und Widerrufslisten, die ebenfalls online nutzbar sein müssen. Die Fachtermini sind **Rückrufliste** (CRL = Certificate Revocation List) und **Online-Verifikation** (OCSP = Online Certificate Status Protocol).

Alle diese Komponenten zusammen machen die **Public-Key-Infrastruktur** (PKI) aus, die notwendige Voraussetzung für die sichere Anwendung asymmetrischer Verfahren „im großen“ ist, und zwar für Verschlüsselung, digitale Signatur und starke Authentisierung.

---

[14] siehe z. B. http://tldp.org/HOWTO/Disk-Encryption-HOWTO/ und http://tldp.org/HOWTO/Encrypted-Root-Filesystem-HOWTO/
[15] http://www.microsoft.com/germany/technet/datenbank/articles/900941.mspx
[16] http://www.microsoft.com/germany/technet/prodtechnol/windowsvista/secprot/bitfaq.mspx
[17] http://www.truecrypt.org/
[18] http://www.pgp.com/

Auf der anderen Seite gehört zur sicheren Anwendung asymmetrischer Verfahren eine persönliche Schlüsselverwaltung in einer gesicherten Umgebung (**Personal Secure Environment**, PSE), die idealerweise durch eine **Smartcard** (Chip-Karte) gegeben ist, aber auch als „Soft-PSE“ in Form einer Datei auf einem sicheren Rechner realisiert werden kann. Diese enthält die privaten Schlüssel ihres Besitzers – aus Sicherheitsgründen je einen separaten für die Anwendungen Verschlüsselung, digitale Signatur und Authentisierung – sowie das Root-Zertifikat.

Eine Smartcard-basierte PKI kann nur mit kommerzieller Unterstützung aufgebaut werden; die bisherigen Versuche dazu im Bereich der medizinischen Forschung haben sich immer noch als zu teuer und viel zu schwerfällig herausgestellt; aus diesem Grund wurde z. B. die im Kompetenznetz Pädiatrische Onkologie und Hämatologie (KPOH) drei Jahre lang betriebene PKI wieder aufgegeben.

2.3 Das Signaturgesetz

Das Signaturgesetz (Gesetz über Rahmenbedingungen für elektronische Signaturen, kurz SigG) vom 16. Mai 2001 definiert Rahmenbedingungen für die digitale Signatur. Geregelt werden als rechtssichere Zertifizierungsdienste die Ausstellung von qualifizierten **Zertifikaten** und qualifizierten **Zeitstempeln**. Das Signaturgesetz regelt ausschließlich diese Zertifizierungsdienste; andere kryptographische Verfahren sind davon nur indirekt betroffen. Das Signaturgesetz definiert drei Typen der digitalen Signatur mit wachsendem Sicherheitsanspruch:

1. die (einfache) elektronische Signatur, die nur eine einfache Kennzeichnung der Urheberschaft oder Verantwortlichkeit ohne nachprüfbare Sicherheitseigenschaften ist,
2. die fortgeschrittene elektronische Signatur, die Basis-Anforderungen an die Sicherheit genügen muss[19],
3. die qualifizierte elektronische Signatur, eine fortgeschrittene elektronische Signatur, die auf einem qualifizierten Zertifikat beruht und mit einer sicheren **Signaturerstellungseinheit** (SSEE)[20] erstellt wurde.

Nur die letztere hat einen festgelegten Beweiswert und genügt den sonst für kryptographische Verfahren üblichen Sicherheitsvorstellungen. Ein Anbieter von qualifizierten Zertifikaten (ZDA) oder qualifizierten Zeitstempeln muss die folgenden Anforderungen erfüllen:

- Zuverlässige Identifikation von Antragstellern für Zertifikate.
- Sicherstellung der Schlüsselerzeugung in einer geeigneten SSEE, die bereits im Besitz des Antragstellers ist oder ihm bei dieser Gelegenheit übergeben wird.
- Unterweisung der Zertifikatsinhaber.
- Aufnahme der Zertifikate in ein Verzeichnis (öffentlich, sofern der Inhaber dem zustimmt).
- Vorkehrungen gegen Fälschung von Zertifikaten.
- Vorkehrungen zum Sperren von Zertifikaten.

[19] Hierunter fallen „selbstgestrickte“ Lösungen, z. B. mit PGP, sofern geeignete Sicherheitsmaßnahmen getroffen werden.
[20] in der Regel eine Smartcard zusammen mit einem sicheren Kartenterminal

- Dokumentation der Ausstellung von qualifizierten Zertifikaten und qualifizierten Zeitstempeln.
- Einhaltung von Datenschutzbestimmungen.
- Fachkunde und Zuverlässigkeit des eingesetzten Personals.
- Definierte und überprüfte IT-Sicherheit.
- Haftpflicht-Versicherung für Schäden durch Pflichtverletzung.

Für medizinische Forschungsnetze ergibt sich daraus zwingend, dass zur Nutzung von qualifizierten Signaturen ein kommerzieller geprüfter Dienstleister hinzugezogen werden muss. Daher ist zu empfehlen, hier keine eigenen Strukturen für medizinische Forschungsnetze zu schaffen, sondern *auf die Mitnutzung der PKI der künftigen Gesundheitstelematik zu setzen*. Lösungen für Forschungsnetz-Mitarbeiter, die keine Zertifikate aus der Gesundheitstelematik erhalten, sind ergänzend zu erarbeiten. Bis zur Etablierung der Gesundheitstelematik sollte die Rechtssicherheit von Dokumenten, so weit nötig, durch fortgeschrittene Signaturen und ordnungsgemäße Datenverarbeitung sichergestellt werden; für Authentisierungsvorgänge können statt einer qualifizierten Signatur auch einfachere ad-hoc-Lösungen verwendet werden (s. 2.6).

2.4 PGP

Die bekannte Software PGP ist als **OpenPGP**[21] im RFC 4880[22] standardisiert. Hauptanwendungsbereiche sind E-Mail und die Verschlüsselung einzelner Dateien. PGP benutzt ein hybrides Verschlüsselungsverfahren, bei dem jeweils mehrere Algorithmen zur Auswahl stehen. Das „originale“ PGP ist kommerziell, aber auch in abgespeckter freier Version erhältlich[23]. Daneben gibt es als freie Implementierung GnuPG[24], das auch in dem für MS-Windows vorkompilierten Paket gpg4win[25] enthalten ist.

> Das für E-Mail ebenfalls weit verbreite **S/MIME**-Protokoll verwendet ein anderes Schlüsselformat (X.509-Zertifikate) und ist deshalb grundsätzlich nicht kompatibel zu OpenPGP. Allerdings gibt es Werkzeuge zur Umformatierung von Schlüsseln von PGP nach X.509.

Bei der Verwendung von PGP wird in der Regel keine PKI aufgebaut – obwohl auch das möglich ist –, sondern statt dessen ein „Web of Trust“.

Empfehlung: *Für E-Mail und Datei-Transport sollte in einem medizinischen Forschungsnetz PGP/ GnuPG verwendet werden, solange keine PKI verfügbar ist; das Web of Trust sollte durch eine zentrale Stelle im Netz repräsentiert werden, die öffentliche Schlüssel beglaubigt*.

2.5 SSL/TLS

SSL (Secure Sockets Layer) oder TLS (Transport Layer Security)[26] bildet eine kryptographische Zwischenschicht im Internet-Protocol-Stack zwischen Netz- und Anwendungsschicht (OSI-Schichten 4 und 5) und dient zur **sicheren Datenübertragung im Internet** auf der Ba-

[21] http://www.openpgp.org/
[22] http://tools.ietf.org/html/rfc4880
[23] http://www.pgpi.org/
[24] http://www.gnupg.org/, http://www.gnupp.de/
[25] http://www.gpg4win.org/
[26] http://www.ietf.org/html.charters/tls-charter.html

sis hybrider Verschlüsselungsverfahren. Hauptanwendungsbereich ist die sichere Client-Server-Kommunikation im WWW. Die Nutzung dafür ist relativ leicht, da SSL in allen gängigen Web-Browsern und Web-Servern als Komponente enthalten ist; für die Einrichtung gibt [10] eine einfache Anleitung.

SSL basiert auf einer PKI (s. 2.2), die mit X.509-Zertifikaten arbeitet. Diese kann mit geringem Aufwand selbst erstellt und gepflegt werden. Sicherer ist eine Smartcard-basierte PKI, die jedoch mit den in 2.2 aufgeführten Problemen behaftet ist.

SSL wird auch in anderen Anwendungen genutzt, so z. B. zum Aufbau von VPNs (s. 2.7), für E-Mail oder für sicheren Datentransfer mit dem Protokoll sFTP; z. B. in dem freien Software-Produkt FileZilla[27]. Da über **OpenSSL**[28] auch der gesamte Quellcode in Form von Programm-Bibliotheken zur Verfügung steht, ist SSL mit relativ geringem Aufwand in selbst entwickelten Anwendungen nutzbar.

Empfehlung: *Web-basierte Anwendungen* (z. B. RDE-Systeme) *sollten mit SSL aufgesetzt werden*, bevorzugt mit Client-Zertifikaten; eine Passwort-Lösung, die nur ein Serverzertifikat benötigt, ist aber auch akzeptabel. Im letzteren Fall ist keine PKI nötig, sondern es reicht ein selbstsigniertes Server-Zertifikat; damit kann bereits eine verschlüsselte Verbindung aufgebaut und insbesondere Passwörter verschlüsselt übertragen werden. Diese Empfehlung gilt bis zur Etablierung einer nutzbaren PKI im Gesundheitswesen.

2.6 Starke Authentisierung[29]

Das herkömmliche Authentisierungsverfahren per **Passwortabfrage** gilt als schwach; besonders schwach ist es, wenn Passwörter unverschlüsselt über das Netz übertragen werden, wie es z. B. bei der „Basic Authentication“ im http-Protokoll geschieht.

Unter **starker Authentisierung** versteht man ein Verfahren (**Challenge-Response**), bei dem die über das Netz transportierten Informationen nicht wiederverwendbar sind. Der prinzipielle Ablauf sieht so aus, dass der Server dem Clienten eine zufällige Zeichenfolge („Challenge“) zuschickt, die dieser digital signiert zurückschickt („Response“); mit einer weiteren digitalen Signatur ist sogar eine wechselseitige Authentisierung möglich („Drei-Wege-Verfahren“). Voraussetzung für die Sicherheit der starken Authentisierung ist die Einbettung in eine PKI.

SSL bringt die Voraussetzungen mit, um für Web-basierte Anwendungen eine starke Authentisierung einzurichten. In diesem Kontext ist auch leicht das **Single-Sign-On**-Prinzip (SSO) umzusetzen: Der Nutzer authentisiert sich einmal gegenüber seinem Browser per PIN oder Passwort, wobei im Hintergrund sein privater Schlüssel freigeschaltet und von da an für Authentisierungsvorgänge gegenüber Servern benützt wird. Wird im Netz eine Smartcard-basierte PKI eingesetzt, sollte diese auch hierfür genutzt werden.

2.7 VPN

Ein **virtuelles privates Netz** (VPN) wird in einem anderen Netz (in der Regel im Internet) betrieben, aber mit einer logisch getrennten Netzstruktur. Diese logische Trennung wird durch kryptographische Verfahren abgesichert, so dass das VPN sicher vor Zugriffen aus dem um-

[27] http://www.filezilla.de/
[28] http://www.openssl.org/
[29] Die im Deutschen gelegentlich getroffene, im englischen Sprachgebrauch nicht übliche Unterscheidung zwischen „Authentisierung“ und „Authentifizierung“ wird hier nicht verwendet.

gebenden Netz geschützt ist. Eine Möglichkeit zum Aufbau eines VPN bietet SSL/TLS, indem zwischen geeigneten Knoten- oder Endpunkten „Tunnel“ aufgebaut werden, in denen das gesamte Internet-Protokoll virtuell abgewickelt wird. Als frei verfügbares Produkt zu diesem Zweck ist vor allem OpenSSL geeignet.

Auf einer niedrigeren Netzschicht, der Vermittlungsschicht (Schicht 3) des OSI-Referenzmodells, setzt IPsec (Kurzform für Internet Protocol Security) auf, das eine Sicherheitsarchitektur für den Aufbau eines VPN über IP-Rechnernetze zur Verfügung stellt. Der RFC 2401[30] beschreibt die Architektur von IPsec.

Andere Möglichkeiten zum Aufbau von VPNs bieten PPTP[31] und L2TP[32].

Mit Ausnahme des oft wegen mangelnder Sicherheit kritisierten[33] PPTP sind *alle diese Methoden zum Aufbau von VPNs geeignet, wobei die offenen Standards* **OpenSSL** *und* **IPsec** *besonders zu empfehlen sind*.

2.8 Sonstige kryptographische Sicherheitsdienste

Es gibt viele weitere solche Dienste, die prinzipiell für den Einsatz in medizinischen Forschungsnetzen geeignet sind. Einige werden hier kurz summarisch erwähnt.

Kerberos ist ein Authentisierungs- und Rechteverwaltungsdienst, der auf dem Internet-Protokoll basiert und nur symmetrische Verschlüsselung verwendet. Kerberos bietet auf dieser Basis auch Integrität und Vertraulichkeit der Kommunikation im Netz sowie ein Single-Sign-On. Statt einer PKI wird eine verteilte Serverstruktur aufgebaut mit Servern, die TTP-Dienste anbieten, die ihrerseits hohe Ansprüche an Sicherheit und Vertrauenswürdigkeit stellen.

Microsoft verwendet Kerberos als Standardprotokoll für die Authentisierung in Netzen unter Windows/2000/XP/2003. Hier werden die Kerberos-Schlüssel im Active Directory gespeichert. Für selbstgestrickte Anwendungen ist Kerberos nur umständlich nutzbar; es spricht aber nichts gegen den Einsatz von fertigen Software-Lösungen, die mit Kerberos arbeiten, solange die kryptographischen Grundforderungen hinsichtlich der verwendeten Verfahren erfüllt werden.

MyProxy ist ein Netzdienst, der asymmetrische Schlüsselpaare für Nutzer erzeugt und speichert, so dass sie online abgerufen werden können. Ein MyProxy-Server dient also unter anderem zur Ablage privater Schlüssel, die aber niemals übers Netz transportiert werden müssen, und stellt somit für jeden Nutzer das PSE (Personal Secure Environment) dar. MyProxy erhöht die Mobilität von Nutzern, da die Schlüssel nicht an ein bestimmtes Endgerät gebunden sind und ihre Verwendbarkeit auch nicht vom Vorhandensein eines passenden Chipkartenlesers abhängt oder durch Herumtragen auf einem transportablen Speichermedium sichergestellt werden muss. Andererseits wird dadurch das Prinzip „privater Schlüssel nur auf einem nichtauslesbaren Speicher unter persönlicher Kontrolle“ abgeschwächt und somit das Sicherheitsniveau deutlich erniedrigt. Daran ändert auch die Tatsache nichts, dass die privaten Schlüssel auf dem MyProxy-Server verschlüsselt abgelegt sind, da der Schlüsseleingabe- und Entschlüsselungsprozess die vom Nutzer kontrollierbare Umgebung verlassen.

[30] http://tools.ietf.org/html/rfc2401
[31] http://tools.ietf.org/html/rfc2637
[32] http://tools.ietf.org/html/rfc2661
[33] z. B. Bruce Schneier auf http://www.schneier.com/pptp-faq.html

Shibboleth ist eine Sammlung von Diensten, die lokalen Authentisierungs- und Autorisierungsdiensten ermöglicht, fremden Diensten die nötigen Informationen für Zugriffsentscheidungen zur Verfügung zu stellen. Es fördert also die verteilte Authentisierung und Autorisierung für Personen und Dienste und das SSO in einer sehr heterogenen Netzlandschaft. Insbesondere lassen sich völlig unterschiedliche lokale Authentisierungsverfahren einbinden.

MyProxy und Shibboleth werden hauptsächlich im Grid-Computing eingesetzt; ansonsten ist ihre Nutzung in einem medizinischen Forschungsnetz zwar denkbar, aber bei einer vorhandenen PKI redundant und somit überflüssig.

Zeitstempel werden im Signaturgesetz geregelt (s. 2.3). Qualifizierte Zeitstempel bescheinigen, dass bestimmte Daten zu einem angegebenen Zeitpunkt vorgelegen haben. Obwohl ein Einsatz in medizinischen Forschungsnetzen – wie überall, wo es auf die Verbindlichkeit von Informationen ankommt – durchaus sinnvoll wäre, sollte wegen des damit verbundenen Aufwands die Einführung nur im Rahmen der Gesundheitstelematik-Infrastruktur erfolgen.

Pseudonymisierungsdienste werden in 6.6-6.11 behandelt.

2.9 Der TMF-Sicherheitsproxy

Zur Nutzung der geplanten Smartcard-basierten PKI wurde in der ersten Phase der TMF ein Sicherheitsproxy vom Fraunhofer SIT entwickelt[34]. Er stellt eine Middleware dar, die die PKI mit (nicht nur Web-basierten) Anwendungen verbindet und insbesondere mit Kartenlesern kommuniziert. In Teilen ist dieses Werkzeug speziell auf die damals favorisierte Smartcard- und Trustcenter-Lösung von CCI (später Schlumberger-Sema, danach Atos Origin) sowie die Kartenlesegeräte Chipdrive Pinpad 532 von SCM zugeschnitten und unabhängig davon nicht unmittelbar zu nutzen.

2.10 Remote-Desktop-Verbindungen

Remote-Desktop- oder Terminalserver-Protokolle dienen dazu, Anwendungen und ihre Benutzungsoberfläche voneinander zu trennen, indem diese auf verschiedenen Rechnern laufen können. Anwendungen laufen dabei auf einem **Applikationsserver**, die Nutzungsoberfläche auf einem – irgendwo im Netz befindlichen – Client-Rechner. Der Applikationsserver kann selbst als **Terminalserver** fungieren; es ist aber möglich, diese beiden Funktionen nochmals zu separieren. Der Terminalserver erzeugt Bildschirmausgaben auf dem Terminal (-Client). Außerdem kann er Benutzereingaben vom Client entgegennehmen.

Grundsätzliche Vorteile dieser Architektur sind:

- Anwendungen müssen nur einmal installiert werden und sind ohne großen Aufwand zu aktualisieren.
- Eine sichere Anwendungsumgebung ist kaum von möglicherweise zweifelhafter Sicherheit auf den Client-Rechnern betroffen.

Die Vorteile für die Systemverwaltung sind also beträchtlich. Auf der anderen Seite stehen natürlich hohe Performanz-Ansprüche der Server, insbesondere bei Mehrbenutzerbetrieb.

[34] Programmcode, Dokumentation und Manuale liegen der TMF-Geschäftsstelle vor.

Beispiele für solche Protokolle sind das **Remote Desktop Protocol**[35] (RDP) von Microsoft, **ICA** (Independent Computing Architecture) von Citrix[36] sowie das in der Unix-Welt seit jeher verwendete **X-Window-System**[37].

Wichtig für die Anwendung in medizinischen Forschungsnetzen ist die kryptographische Datenübertragung. RDP benutzt den RC4-Chiffrieralgorithmus (s. 1.2), der für die Verschlüsselung von Datenströmen in Netzwerken konzipiert ist. Unter Windows 2000 kann ein Administrator zwischen einer Schlüssellänge von 56 oder 128 Bit auswählen. Auf der niedrigsten Sicherheitsstufe wird allerdings nur der Verkehr vom Client zum Server verschlüsselt; dadurch wird im wesentlichen die Passwortübertragung geschützt. In der Standardeinstellung werden beide Richtungen mit einem Schlüssel von 56 Bit Länge verschlüsselt. 128-Bit-Verschlüsselung kann erst nach der Installation des Windows 2000 High Encryption Pack[38] eingestellt werden. *Dies ist dringend zu empfehlen*.

Das X-Protokoll der Unix-Welt kann über **SSH**[39], ein kryptographisches Remote-Login-Protokoll verschlüsselt werden; dieses bietet ähnliche kryptographische Optionen wie SSL, kann also insbesondere auf hoher Sicherheitsstufe und mit starker Authentisierung betrieben werden.

2.11 Kryptographische Protokolle und Firewall-Technik

Medizinische Forschungsnetze sind einrichtungsübergreifende Strukturen. Das bedeutet, dass die Teilnehmer am Forschungsnetz Einrichtungen (z. B. Kliniken) angehören, die als Ganzes mit dem Forschungsnetz nichts zu tun haben und deren Sicherheitsvorkehrungen mit denen des Forschungsnetzes kollidieren können[40]. Das betrifft jede Art von verschlüsselter Datenübertragung, sei es per E-Mail, Dateitransfer, VPN-Technik, verschlüsselter Kommunikation zwischen Anwendungen oder auch Remote-Desktop-Diensten. In vielen Einrichtungen gehört die Kontrolle des ein- und ausgehenden Datenverkehrs auf Zulässigkeit zu den Grundaufgaben der eingesetzten Firewall-Technik; kryptographische Verschlüsselung verhindert diese Kontrolle, durch kryptographische Tunnel wird der Firewall-Schutz ausgehebelt. Daher ist es nötig, dass das Forschungsnetz dem Firewall-Administrator genaue Informationen über die Anforderungen der Kommunikation, die übermittelten Inhalte sowie die eingesetzte Technik gibt; dazu gehören insbesondere freizuschaltende Ports und anzusprechende externe Rechner und Netzadressen.

Keinesfalls sollte ein medizinisches Forschungsnetz seine kryptographischen Maßnahmen zugunsten der Kontrollierbarkeit durch lokale Systemadministratoren abschwächen.

---

[35] http://support.microsoft.com/kb/186607
[36] http://www.citrix.com/English/ps2/products/product.asp?contentID=163057
[37] Hier ist zu beachten, dass die Bezeichnungen umgekehrt verwendet werden: Das Terminal, das seinen „Präsentationsdienst“ anbietet, heißt X-Server, die Anwendung, die diesen Dienst nutzt, X-Client.
[38] http://www.microsoft.com/downloads/details.aspx?FamilyID=c10925a0-ac66-4c44-b5c3-9dcab4da1c63&DisplayLang=en
[39] http://openssh.org/de/
[40] Typisch ist die Verschlüsselung beim Export von Patientendaten aus einem Kliniksystem in die Datenbank eines Forschungsnetzes.

3. Hardware-Unterstützung

In Gegensatz zu den kryptographischen Algorithmen und Protokollen und der kryptographischen Software ist der Markt bei der Hardware, die zur Unterstützung kryptographischer Techniken benötigt wird, sehr stark im Fluss, so dass nur der momentane Stand mit Perspektiven für die nahe Zukunft beschrieben werden kann. Insbesondere im Hinblick auf die weitere Entwicklung der Gesundheitstelematik sind noch viele Änderungen bei den angebotenen Produkten zu erwarten.

3.1 Server-Härtung (kryptographische Aspekte)

Server-Härtung bedeutet, dass Server, die vom Internet aus zugänglich sind, besonders gründlich gegen unbefugte Zugriffe geschützt sind. Dazu gehört, dass auf Anwendungsebene *nur die benötigten Dienste* angeboten und auf Netzebene *alle Ports und Kommunikationswege*, die nicht ausdrücklich benötigt werden, *konsequent abgeschaltet* werden. Dieses muss ein aktives Vorgehen sein, da Server „von der Stange“, egal mit welchem Betriebssystem[41], viele Netzdienste freigeschaltet haben. Für die Details sei auf die **IT-Grundschutzkataloge** [7] des BSI verwiesen. Zur Sicherheit von Servern gehören ferner Richtlinien zur Sicherheit von Rechnerräumen, Firewall-Regelungen und manches andere.

Im Rahmen dieses Gutachtens sind vor allem die kryptographischen Aspekte von Bedeutung. Hier sind die Forderungen nach *verschlüsselter Speicherung*, siehe 2.5, und *verschlüsselter Kommunikation*, siehe 2.5, 2.6, 2.7 und 2.10, zu erfüllen. Ein Problem dabei ist die Handhabung der notwendigen Schlüssel, insbesondere der zu den Serverzertifikaten gehörigen „privaten“ Schlüssel, etwa für SSL, sowie der Schlüssel für die eigene Festplattenverschlüsselung. Diese dürfen nicht in fremde Hände fallen, müssen aber – da die Server medizinischer Forschungsnetze in der Regel unterbrechungsfrei zur Verfügung stehen sollen, aber nicht rund um die Uhr bewacht werden können – auch bei einem automatischen Wiederanlauf nach einer Störung zur Verfügung stehen. Oft werden dazu die Schlüssel in einer verschlüsselten Datei abgelegt, deren Passphrase beim Bootvorgang aus einer speziellen, sonst nicht zugreifbaren Datei ausgelesen wird. *Eine sicherere Lösung ist nur dann möglich, wenn der Wiederanlauf nur in Anwesenheit eines Administrators ermöglicht wird, der die Passphrase an der Konsole eingeben kann oder, noch besser, den Schlüssel auf einer Smartcard dem System verfügbar macht*. Diese muss nicht den Anforderungen des Signaturgesetzes genügen, es kann sich also um eine programmierbare Chipkarte (s. 3.4) handeln, auf die ein extern erzeugter Schlüssel geladen wird. Eine mögliche kurzfristige Lösung für Linux (ohne Chipkarte) wird auch in [11] beschrieben; für den Einsatz des MS-Windows-eigenen Programms BitLocker siehe [12].

3.2 Grundsätzliches zu Smartcards (Prozessor-Chipkarten)

Smartcards sind Plastikkarten in Scheckkarten-Größe, die einen eingebauten Mikroprozessor und Speicher besitzen („Computer im Scheckkarten-Format“)[42]. Sie besitzen ein spezifisches Betriebssystem und kommunizieren mit der Außenwelt über acht auf der Oberfläche angebrachte Kontakte. Smartcards sind gesichert vor Ausspähung gespeicherter Geheimnisse (z. B. kryptographischer Schlüssel), und Manipulation. Technische Sicherheitsvorkehrungen dafür sind

[41] Mit Ausnahme von OpenBSD, das aber wegen etwas schwerfälliger Administration und geringer Performanz selten eingesetzt wird.

[42] Andere Typen von Chipkarten werden hier nicht betrachtet.

- nicht direkt lesbare Speicher,
- Zugriff nur über I/O-Port, CPU und Sicherheitsmodul,
- manipulationssichere Verschweißung mit Selbstzerstörungsmechanismen,
- „mehrstöckiges“ Design, das physikalische Angriffe durch Auseinandernehmen der Karte oder Abätzen von Schichten verhindern soll,
- PIN-Schutz mit Sperrung nach (meist drei) Fehlversuchen; auch Fingerabdruck-Sensoren sind möglich, aber bisher noch nicht mit ausreichender Sicherheitsstufe auf dem Markt[43].

Dadurch sind Smartcards als persönliche Ausweiskarten prädestiniert, insbesondere als PSE und SSEE (s. 2.2): falls sie die nötigen Schlüssel enthalten, können Sie im Zusammenspiel mit einem geeigneten Kartenterminal (s. 3.3) zur starken Authentisierung sowie zur qualifizierten digitalen Signatur und für andere kryptographische Funktionen verwendet werden. Diese Funktionen werden im Gesundheitswesen künftig ganz oder teilweise mit dem HBA und der eGK genutzt, s. 3.5. Schlüssel, die den Anforderungen des Signaturgesetzes an eine qualifizierte Signatur genügen sollen, müssen auf der Karte selbst erzeugt werden und dürfen diese niemals verlassen; insbesondere müssen die damit ausgeführten kryptographischen Funktionen auf der Karte selbst ausgeführt werden.

Für den sicheren Einsatz von Smartcards ist eine passende Infrastruktur sowie eine vertrauenswürdige Systemumgebung nötig; hierzu gehört unbedingt ein **Kartenterminal** (Kartenleser) mit ausreichender Sicherheitsstufe. Die Schlüsselerzeugung für eine PKI sollte auf der Karte selbst stattfinden (nach dem Signaturgesetz ist das sogar obligatorisch, wenn eine qualifizierte Signatur verwendet werden soll). Diese Anforderung gilt aber nicht notwendig für Spezialanwendungen wie z. B. verschlüsselte Datenspeicherung (s. 2.1) oder den Pseudonymisierungsdienst (s. 6.9). Ein besonderes Problem stellt die Erzeugung einer Backup-Karte, also einer Karte mit identischen Schlüsseln dar. Da für einen geheimen Signaturschlüssel ein solches Backup nicht nötig ist, ist dieses Problem im Signaturgesetz nicht adressiert. Ein Auslesen eines Schlüssels, um ein Backup anzulegen, ist mit den dort definierten Sicherheitsanforderungen nicht vereinbar. Davon abgesehen ist *die beste Lösung für das Problem eine programmierbare Smartcard* (s. 3.4).

Trotz der Bemühungen um ein hohes Sicherheitsniveau von Smartcards gibt es gravierende Sicherheitsprobleme[44], die nur schwer in den Griff zu bekommen sind. Es gibt nichtinvasive Angriffe, die etwa aus der Reaktion der Karte auf provozierte Fehler Informationen über die gespeicherten Schlüssel gewinnen. Am weitesten gehen die invasiven (und gar nicht besonders aufwendigen) Angriffe, die Anderson und Kuhn demonstriert haben: Hier wird der Chip Schicht für Schicht abgetragen und analysiert; benötigt wird dazu nur eine Standard-Elektroniklabor-Ausrüstung.

Die wichtigsten Normen und Standards für Chipkarten-Funktionen (außerhalb der Spezifikationen in der Gesundheitstelematik) sind ISO 7816, PKCS #11, PKCS #15, siehe 4.1 und 4.7.

---

[43] http://www.heise.de/newsticker/meldung/103207

[44] Ross Anderson, Markus Kuhn: Tamper Resistance – a Cautionary Note. The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, November 18-21, 1996, pp 1-11, online: http://www.cl.cam.ac.uk/users/rja14/tamper.html

3.3 Kartenterminals

Die Fähigkeiten von Chipkartenlesern gehen meist über das reine Auslesen der Informationen hinaus – und müssen dies bei höheren Sicherheitsanforderungen sogar. Daher ist die Bezeichnung „Terminal“ üblich und angemessen. Es gibt vier Sicherheitsklassen:

- Geräte der Klasse 1 sind reine Kontaktgeräte, die eine Schnittstelle zu einem angeschlossenen Rechner herstellen.
- Geräte der Klasse 2 erlauben die Eingabe einer PIN über eine eigene Tastatur, die also vor Schadsoftware auf dem angeschlossenen Rechner geschützt ist.
- Geräte der Klasse 3 haben darüber hinaus ein eigenes Display und sind daher von der manipulierbaren Anzeige des angeschlossenen Rechners unabhängig. Geräte dieser Klasse sind geeignet, die Anforderungen des Signaturgesetzes zu erfüllen.
- Geräte der Klasse 4 besitzen einen weiteren Kartensteckplatz, der ein sogenanntes Authentifizierungsmodul (SAM) aufnehmen kann, mit dem sich das Terminal gegenüber der Karte ausweist. Die Hauptanwendung sind „Point-of-Sale“-Terminals zur bargeldlosen Zahlung.

Als Secure Interoperable Chip Card Terminal (**SICC-Terminal**) werden Kartenlesegeräte mit generischer Systemarchitektur und verschiedenen Anschlussmöglichkeiten bezeichnet. Dazu gehört auch eine vertrauenswürdige Anzeige der zu signierenden Daten (Trusted Viewer). Die relevante Definition ist die SICCT-Spezifikation[45]. Diese wurde vom TeleTrusT e.V. erarbeitet und liegt inzwischen in der Version 1.20 vor.

3.4 Programmierbare Smartcards

Es gibt eine Reihe programmierbarer Smartcards unterschiedlicher Technik. Am einfachsten zu handhaben (und inzwischen wohl auch am weitesten verbreitet) sind Javakarten (Java Card), Smartcards mit einem Java-basierten Betriebssystem und einer Java-Programmierschnittstelle. Sie erlauben, extern erstellte Java-Anwendungen auf die Karte zu laden. Mit dieser Technik können Karten für Spezialanwendungen günstig hergestellt werden. Die **Java-Card-Spezifikation**[46] sieht unter anderem aktuelle kryptographische Algorithmen vor. Zur Anwendlungsentwicklung steht das OpenCard Framework[47] zur Verfügung.

Ähnlich funktionieren .NET-Karten für die von Microsoft entwickelte (proprietäre, aber weit verbreitete) .NET-Plattform. Daneben gibt es natürlich auch noch in Maschinensprache bzw. dem zugehörigen Assembler programmierbare Karten.

Programmierbare Smartcards sind dann angebracht, wenn für Spezialanwendungen Karten mit identischen Schlüsseln (als Backup) erstellt werden müssen. Hier ist es sogar denkbar, die Schlüssel außerhalb der Karte in einer gesicherten Umgebung zu erzeugen – und auch aufzubewahren – und dann auf die Karte zu laden. Expertise im Umgang mit programmierbaren Karten ist beim Fraunhofer-Institut für sichere Informationstechnik (SIT) vorhanden[48] und wurde in der ersten Phase der TMF auch schon genutzt.

---

[45] http://www.teletrust.de/index.php?id=530
[46] http://java.sun.com/javacard/specs.html
[47] http://www.openscdp.org/
[48] http://www.sit.fraunhofer.de/

3.5 Smartcards in der Gesundheitstelematik

In der Gesundheitstelematik ist die Einführung der elektronischen Gesundheitskarte (eGK) für Patienten und des elektronischen Heilberufeausweises (HBA) für Ärzte, Apotheker und Pflegekräfte vorgesehen.

Die Spezifikation „eHealth-Terminal auf der Basis SICCT für das deutsche Gesundheitswesen“, die z. Z. für die Telematik-Infrastruktur der elektronischen Gesundheitskarte erstellt wird, beruft sich auf die SICCT-Spezifikation (s. 3.3).

Die als eGK geplante erste Chipkartengeneration (ab 2008) wird mit den Verfahren RSA (2048 Bit Schlüssellänge) (s. 1.3), 3DES (s. 1.2) und SHA-256 (s. 1.4) versehen, die zweite Generation ab 2011 mit ECC (s. 1.3), AES (s. 1.2) und SHA-256. Die Kartenleser werden mit einem „Security Access Module“ (SAM) ausgestattet, das mit Karten verschiedener Generationen umgehen kann.

Der elektronische Heilberufe-Ausweis (HBA) dient zur Identifizierung mittels starker Authentisierung und damit indirekt zur Zugriffsregelung auf die über die eGK zugänglichen Patientendaten. Er wird auch die digitale Signatur ermöglichen. Die aktuelle Spezifikation (V2.1.1) ist über die Webseiten der Bundesärztekammer[49] erhältlich.

3.6 RFID-Technik

RFID (Radio Frequency Identification) beruht auf Chips (Transpondern), die berührungslos und ohne eigene Stromversorgung gespeicherte Daten im Nahbereich übertragen können. Mögliche Anwendungen, die auch im Bereich der medizinischen Forschung von Bedeutung sein können, sind der Ersatz von Barcodes zur Markierung von Gegenständen sowie der Ersatz der PIN- oder Passworteingabe bei Authentisierungsverfahren. Ein RFID-System besteht aus einem Transponder sowie einem Lesegerät zum Auslesen der gespeicherten Daten [13].

Aufgrund ihrer geringen Leistungsfähigkeit sind in gängigen RFID-Systemen keine kryptographischen Mechanismen implementierbar[50], so dass man die Sicherheitstechnik als noch nicht ausgereift bezeichnen muss. *Daher ist die RFID-Technik für sicherheitskritische Anwendungen bis auf weiteres nicht geeignet*.

3.7 TPM

Das „Trusted Platform Module“ (TPM) ist ein Chip, der als Teil der TCG-Spezifikation[51] Computer sicherer machen soll. Der Chip enthält eine eindeutige Kennung (und dient damit zur Identifizierung des Rechners) sowie kryptographische Schlüssel in nicht manipulierbarer Weise und *kann somit wesentlich zur Vertrauenswürdigkeit des Rechners beitragen*; geeignet ist diese Technik z. B. zur sicheren Verwahrung und Verwendung von Server-Schlüsseln (s. 3.1). Die TCG-Spezifikation garantiert außerdem einen sicheren Zufallsgenerator auf dem TPM.

---

[49] http://www.bundesaerztekammer.de/page.asp?his=1.134.3421.4132

[50] Insbesondere müssten für eine wirksame Sicherheit die für eine PKI nötigen kryptographischen Mechanismen zur Verfügung stehen.

[51] Trusted Computing Group, https://www.trustedcomputinggroup.org/

Für einen konkreten Einsatz in medizinischen Forschungsnetzen ist es noch zu früh; das BSI beobachtet die Entwicklung[52].

[52] http://www.bsi.bund.de/sichere_plattformen/trustcomp/

4. Normen, Standards, Richtlinien

Es folgt eine weitgehend unkommentierte Liste von einschlägigen Normen, Standards und Richtlinien, auf die z. T. im übrigen Text an geeigneten Stellen Bezug genommen wird. Zu bemerken ist, dass die Dokumente der offiziellen Normierungsgremien ISO, CEN und DIN nicht frei, sondern nur gegen relativ hohe Gebühren verfügbar sind.

4.1 ISO

Die ISO[53] ist die internationale Normierungsorganisation. Für die Telematik in medizinischen Forschungsnetzen einschlägige Committees sind:

- JTC 1 Information Technology, insbesondere SC 17 Cards and personal identification, SC 27 IT Security techniques
- TC 215 Health Informatics, insbesondere WG 4 Security

Einschlägige Normen:

ISO/IEC 2382: Information technology – Vocabulary – Part 8: Security
ISO/IEC 7816: Integrated circuit cards – Part 15: Cryptographic information application
ISO/IEC 9594: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
ISO/IEC 9796: Information technology – Security techniques – Digital signature schemes giving message recovery (Parts 1-3)
ISO/IEC 9797: Information technology – Security techniques – Message Authentication Codes (MACS) (Parts 1-2)
ISO/IEC 9798: Information technology – Security techniques – Entity Authentication (Parts 1-6)
ISO/IEC 10116: Information technology – Security techniques – Modes of operation for an n-bit block cipher
ISO/IEC 10118: Information technology – Security techniques – Hash functions (Parts 1-4)
ISO/IEC 10181: Information technology – Open Systems Interconnection – Security frameworks for open systems
ISO/IEC 10745: Information technology – Open Systems Interconnection – Upper layers security model
ISO/NP TR 11636: Health Informatics – Dynamic on-demand virtual private network for health information infrastructure
ISO/IEC 11770: Information technology – Security techniques – Key management (Parts 1-4)
ISO/IEC 11889: Trusted Platform Module (Parts 1-4)
ISO/IEC 13888: Information technology – Security techniques – Non-repudiation (Parts 1-3)
ISO/IEC TR 14516: Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services
ISO/IEC 14888: Information technology – Security techniques – Digital signatures with appendix (Parts 1-3)
ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves (Parts 1-5)
ISO 17090: Health Informatics – Public key infrastructure (Parts 1-3)

[53] http://www.iso.org/

ISO/IEC 18014: Information technology – Security techniques – Time-stamping services (Parts 1-3)
ISO/IEC 18028: Information technology – Security techniques – IT network security (Parts 1-5)
ISO/IEC 18031: Information technology – Security techniques – Random bit generation
ISO/IEC 18032: Information technology – Security techniques – Prime number generation
ISO/IEC 18033: Information technology – Security techniques – Encryption algorithms (Parts 1-4)
ISO/IEC FCD 19772: Information technology – Security techniques – Authenticated encryption
ISO/IEC 19790: Information technology – Security techniques – Security requirements for cryptographic modules
ISO/TR 21089: Health Informatics – Trusted end-to-end information flows
ISO/TS 21091: Health Informatics – Directory services for security, communications and identification of professionals and patients
ISO/TS 22600: Health Informatics – Privilege management and access control (Parts 1-3)
ISO/IEC FDIS 24759: Information technology – Security techniques – Test requirements for cryptographic modules
ISO/TS 25237: Health Informatics – Pseudonymisation (Publikation 2008 in Vorbereitung)
ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements
ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security management
ISO/IEC 27005: Information technology – Security techniques – Information security risk management
ISO/IEC WD 29100: Information technology – Security techniques – A privacy famework

4.2 CEN

Das CEN[54] ist verantwortlich für europäische Normen in allen technischen Bereichen außer der Elektrotechnik und der Telekommunikation. Für diese Bereiche sind die beiden Institutionen CENELEC[55] und ETSI[56] zuständig.

Einschlägige Arbeitsgruppen (Technical Committees) bei CEN sind:

- CEN/TC 224: Personal identification, electronic signature and cards and their related systems and operations
- CEN/TC 251: Health Informatics

Die CEN/ISSS (Information Society Standardization System) eHealth Standardization Focus Group[57] untersucht die Standardisierungsanforderungen im Bereich „eHealth“.

Einschlägige Normen:

CEN/NP Health Informatics – Patient Identification …
CEN ENV 13729 Secure user identification – Strong authentification using microprocessor cards

[54] http://www.cenorm.be/
[55] Europäisches Komitee für elektrotechnische Normung, http://www.cenelec.org/
[56] Europäisches Institut für Telekommunikationsnormen, http://www.etsi.org/
[57] http://www.cen.eu/CENORM/businessdomains/businessdomains/isss/activity/ehealth_fg.asp

CEN TR 13694 Safety and security related software quality standards for healthcare

4.3 DIN

DIN[58] (Deutsches Institut für Normung e. V.) ist die nationale Normungsorganisation der Bundesrepublik Deutschland mit Sitz in Berlin.

Einschlägige Arbeitsgruppe:

- NA 063 Normenausschuss Medizin (NAMed)

Einschlägige Normen:

DIN EN 12251 (Norm) Medizinische Informatik - Sichere Nutzeridentifikation im Gesundheitswesen - Management und Sicherheit für die Authentifizierung durch Passwörter; Englische Fassung EN 12251:2004

DIN V ENV 12388 (Vornorm) Medizinische Informatik - Algorithmen für digitale Unterschriftsdienste im Gesundheitswesen; Englische Fassung ENV 12388:1996

DIN V ENV 12924 (Vornorm) Medizinische Informatik - Sicherheitskategorisierung und Schutz für Informationssysteme im Gesundheitswesen; Englische Fassung ENV 12924:1997

DIN EN 13606-4 (Norm) Medizinische Informatik - Kommunikation von Patientendaten in elektronischer Form - Teil 4: Sicherheit; Englische Fassung EN 13606-4:2007

DIN EN 14484 (Norm) Medizinische Informatik - Internationaler Austausch von unter die EU-Datenschutzrichtlinie fallenden persönlichen Gesundheitsdaten - Generelle Sicherheits-Statements; Deutsche Fassung EN 14484:2003, Text Englisch

DIN EN 14485 (Norm) Medizinische Informatik - Anleitung zur Verwendung von persönlichen Gesundheitsdaten in internationalen Anwendungen vor dem Hintergrund der EU-Datenschutzrichtlinie; Deutsche Fassung EN 14485:2003, Text English

DIN CEN/TS 15260 (Vornorm) Medizinische Informatik - Klassifikation von Sicherheitsrisiken bei der Benutzung von Medizininformatikprodukten; Deutsche und Englische Fassung CEN/TS 15260:2006

DIN EN ISO 27799 (Norm-Entwurf) Medizinische Informatik - Sicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 17799 (ISO/DIS 27799:2006); Englische Fassung prEN ISO 27799:2006

Ferner gibt es eine Reihe von deutschen Fassungen von ISO-Normen und Dokumenten:

ISO 17090 (Norm) Medizinische Informatik - Public-Key-Infrastruktur

ISO/TR 21089 (Norm) Health informatics - Trusted end-to-end information flows

ISO/TS 21091 (Vornorm) Medizinische Informatik - Verzeichnisdienste für Sicherheit, Kommunikation und Identifikation von Heilberuflern und Patienten

ISO/TS 22600 (Vornorm) Medizinische Informatik - Privilegienmanagement und Zugriffssteuerung

ISO 22857 (Norm) Health informatics - Guidelines on data protection to facilitate transborder flows of personal health information

ISO/TS 25238 (Vornorm) Medizinische Informatik - Klassifikation der Sicherheitsrisiken von Software aus dem Bereich Gesundheitswesen

ISO/FDIS 27799 (Norm-Entwurf) Medizinische Informatik - Sicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002

[58] http://www.din.de/

ISO/TR 27809 (Norm) Medizinische Informatik - Sicherstellung von Patientensicherheit bei Software im Gesundheitswesen

4.4 NIST

Das NIST[59] (National Institute of Standards and Technology) ist eine US-amerikanische Behörde, die zum Handelsministerium gehört. FIPS (Federal Information Processing Standard) ist die Bezeichnung für technische Standards, die das Institute of Computer Sciences and Technology (ICST) in den USA herausgibt[60]. Das ICST gehört zum NIST. Kryptographisch relevant sind u. a. folgende FIPS-PUBs:

- 140-2[61] Security Requirements for Cryptographic Modules
- 180-2[62] SHS (Secure Hash Standard)
- 186-2[63] DSS (Digital Signature Standard)
- 196[64] Entity Authentication Using Public Key Cryptography
- 197[65] Advanced Encryption Standard (AES)
- 198[66] The Keyed-Hash Message Authentication Code (HMAC)

4.5 IETF

Die IETF[67] (Internet Engineering Task Force) ist zwar keine offizielle Normierungsbehörde, definiert aber die de facto gültigen Standards für das Internet. RFCs[68] (Requests for Comments**)** sind technische und organisatorische Dokumenten zum Internet. Sie behalten auch dann ihren Namen RFCnnnn, wenn sie sich durch allgemeine Akzeptanz und Gebrauch zum Standard entwickelt haben. Hier relevant ist u. a. der IETF-Standard ERS („Evidence Record Syntax“), verabschiedet im August 2007 als RFC 4998[69], der sich am ArchiSig-Projekt[70] orientiert.

4.6 BSI

Das Bundesamt für Sicherheit in der Informationstechnik[71] (BSI) ist eine in Bonn ansässige obere Bundesbehörde im Geschäftsbereich des Bundesministerium des Innern (BMI), die für Fragen der IT-Sicherheit zuständig ist. Hier relevant sind die Grundschutzkataloge [7] sowie die folgenden technischen Richtlinien:

---

[59] http://csrc.nist.gov/
[60] http://www.itl.nist.gov/fipspubs/
[61] http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
[62] http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf
[63] http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf
[64] http://csrc.nist.gov/publications/fips/fips196/fips196.pdf
[65] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[66] http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf
[67] http://www.ietf.org/
[68] http://www.ietf.org/rfc.html
[69] http://www.ietf.org/rfc/rfc4998.txt
[70] http://www.archisig.de/
[71] http://www.bsi.de/

- Technische Richtlinie für die Stapelsignatur mit dem Heilberufsausweis (BSI-TR-03114)[72]. Sie „beschreibt technische und organisatorische Sicherheitsmaßnahmen für die zeitlich zusammenhängende Erstellung einer begrenzten Anzahl qualifizierter elektronischer Signaturen nach einer einmaligen Authentisierung des Signaturschlüssel-Inhabers gegenüber der Signaturerstellungseinheit (Heilberufsausweis – HBA) in einer gesicherten Einsatzumgebung (Stapelsignaturen). Die Sicherheitsmaßnahmen beziehen sich auf den Heilberufsausweis als sichere Signaturerstellungseinheit und den Konnektor und die eHealth-Kartenterminals als Signaturanwendungskomponente in der gesicherten Einsatzumgebung dezentraler Komponenten der Telematikinfrastruktur."
- Elliptische-Kurven-Kryptographie (ECC) (BSI-TR-03111)[73] mit dem Ziel, „durch Beschreibung der mathematischen Grundlagen Elliptischer Kurven und der Formulierung von Algorithmen basierend auf Elliptischen Kurven in einem Dokument, den Einsatz Elliptischer-Kurven-Kryptographie zu unterstützen."
- Technische Richtlinie für die eCard-Projekte der Bundesregierung (BSI-TR-03116)[74]

Aus den Grundschutzkatalogen ist noch der Baustein „Kryptokonzept"[75] zu erwähnen, in dem beschrieben wird, „wie ein Kryptokonzept erstellt werden kann. Beginnend mit der Bedarfsermittlung und der Erhebung der Einflussfaktoren geht es über die Auswahl geeigneter kryptographischer Lösungen und Produkte bis hin zur Sensibilisierung und Schulung der Anwender und zur Krypto-Notfallvorsorge."

4.7 RSA – PKCS

PKCS steht für Public Key Cryptography Standards und bezeichnet eine Reihe von kryptographischen Spezifikationen, die unter Federführung der RSA-Laboratorien ab 1991 entwickelt[76] wurden. Diese Standardisierung hatte das Ziel, die Verbreitung der asymmetrischen Kryptographie zu erleichtern und zu beschleunigen. Die zur Zeit aktuellen Standards sind:

PKCS #1: RSA Cryptography Standard
PKCS #3: Diffie-Hellman Key Agreement Standard
PKCS #5: Password-Based Cryptography Standard
PKCS #6: Extended-Certificate Syntax Standard
PKCS #7: Cryptographic Message Syntax Standard
PKCS #8: Private-Key Information Syntax Standard
PKCS #9: Selected Attribute Types
PKCS #10: Certification Request Syntax Standard
PKCS #11: Cryptographic Token Interface Standard
PKCS #12: Personal Information Exchange Syntax Standard
PKCS #13: Elliptic Curve Cryptography Standard
PKCS #15: Cryptographic Token Information Format Standard

[72] http://www.bsi.de/literat/tr/tr03114/
[73] [http://www.bsi.de/literat/tr/tr03111/
[74] http://www.bsi.de/literat/tr/tr03116/
[75] http://www.bsi.de/gshb/deutsch/baust/b01007.htm
[76] http://www.rsa.com/rsalabs/node.asp?id=2124

4.8 Sonstige

Es folgt noch eine etwas unsystematische Liste weiterer im Zusammenhang mit Kryptographie in medizinischen Anwendungen relevanter Texte.

ANSI[77] (American National Standards Institute) ist die US-amerikanische Normierungsorganisation, vergleichbar dem DIN in Deutschland. Die relevante Arbeitsgruppe ist das „Standards Committee X9 - Financial Services". Relevante Normen[78] sind u. a.:

- ANSI X9.30 ff., Public Key Cryptography
- ANSI X9.62ff., die Übertragung des DSA auf elliptische Kurven, als ECDSA (Elliptic Curve Digital Signature Algorithm) bezeichnet.

ASTM[79] International (ursprünglich American Society for Testing and Materials) ist eine internationale Standardisierungsorganisation mit Sitz in den USA. Sie veröffentlicht technische Standards. Das ASTM Committee E31[80] (Healthcare Informatics) entwickelt Standards zu Architektur, Sicherheit, Funktionalität und Kommunikation von Informationen im Gesundheitswesen. Hier relevant sind u. a.:

- ASTM E 1714-00 Standard guide for properties of a Universal Healthcare identifier
- ASTM E 1987-98 Standard guide for individual rights regarding health information
- ASTM E 2085-00a Standard Guide on Security Framework for Healthcare Information
- ASTM E 2086-00 Standard Guide for Internet and Intranet Healthcare Security

IEEE[81] (Institute of Electrical and Electronics Engineers) ist ein weltweiter Berufsverband von Ingenieuren aus den Bereichen Elektrotechnik und Informatik, der unter anderem Arbeitsgruppen zur Erstellung von Standards unterhält. Eine Norm für Datenträgerverschlüsselung wird zur Zeit von der Arbeitsgruppe SISWG[82] (Security in Storage Working Group) im Projekt P 1619 entwickelt (IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices).

ITU[83] (International Telecommunication Union, Internationale Fernmeldeunion) ist eine Unterorganisation der Vereinten Nationen und beschäftigt sich offiziell und weltweit mit technischen Aspekten der Telekommunikation. Relevant ist hier der ITU-T (Telecommunication Standardization Sector), der unter anderem folgenden Standard herausgegeben hat:

- X.509[84], der wichtigste Standard für digitale Zertifikate. Die aktuelle Version ist X.509v3.

Für Smartcards und Terminals hat eine Gruppe aus Vertretern der IT-Industrie, die PCSC Working Group[85], den acht Teile umfassenden Standard „Interoperability Specification for

---

[77] http://www.ansi.org/
[78] Auch ANSI-Normen sind nur gegen Gebühr erhältlich; außerhalb der USA haben sie natürlich keinen Norm-Charakter, werden aber oft als de-facto-Standard akzeptiert.
[79] http://www.astm.org/
[80] http://www.astm.org/COMMIT/SCOPES/E31.htm
[81] http://www.ieee.org/
[82] https://siswg.net/
[83] http://www.itu.int/
[84] Nur gegen Gebühr zugänglich

ICCs and Personal Computer Systems“ – der Kurzname PC/SC (Personal Computer/ Smart Card) wurde von einer früheren Version beibehalten – herausgegeben, der auf der ISO-Norm 7816 beruht und die Einbindung von Kartenlesern in Betriebssysteme beschreibt. Ein konkurrierender Standard CT-API („CardTerminal Application Programming Interface“) wurde von Teletrust im Rahmen der MKT-Spezifikation („Multifunktionales Kartenterminal“) herausgegeben; dieser ist nur im deutschsprachigen Raum verbreitet.

CSP (Cryptographic Service Provider) ist eine proprietärer Standard von Microsoft in Konkurrenz zu PKCS #11, der kryptografische Funktionen im Rahmen von Microsofts Cryptographic Application Programming Interface (CAPI[86]) zur Verfügung stellt. Hier muss bei internationalen Versionen (außerhalb den USA) dringend auf die implementierte Verschlüsselungsstärke geachtet werden.

Diese Übersicht erhabt keinen Anspruch auf Vollständigkeit. Für eine z. Z. ständig aktualisierte und – zumindest dem Anspruch nach – vollständige Übersicht[87] für den Bereich des Gesundheitswesens und der biomedizinischen Forschung sei auf das Projekt BioHealth[88] verwiesen.

[85] http://www.pcscworkgroup.com/
[86] http://msdn.microsoft.com/en-us/library/ms884377.aspx
[87] http://biohealth.helmholtz-muenchen.de/index.php?option=com_bookmarks&Itemid=219&mode=0&catid=1&navstart=0&search=*
[88] http://biohealth.helmholtz-muenchen.de/

5 Kommerzielle Angebote

Der Markt für kommerzielle kryptographische Produkte ist unübersichtlich und sehr wenig stabil, so dass hier nur ein unvollkommener Überblick über aktuelle Angebote gegeben werden kann, der voraussichtlich schnell veraltet. Ziel ist lediglich, die wesentlichen Möglichkeiten, die der Markt bietet, vorzustellen.

Zu beachten ist, dass Werbeaussagen gerade im Bereich der Sicherheit mit großer Skepsis zu betrachten sind; siehe dazu auch den Abschnitt 5.6 „Snake-Oil-Cryptography“. Darüber hinaus ist die zuverlässige Beurteilung der Sicherheit eines Produkts nur im Rahmen eines Gesamtsystems möglich, das auch die Einbettung in die Anwendungsumgebung umfasst. Diese Beurteilung muss auch die Möglichkeiten der Seitenkanal-Kryptoanalyse, siehe Fußnote 2, so vollständig wie möglich berücksichtigen. Ganz allgemein gilt der Grundsatz, dass Sicherheit nicht ein Produkt ist, sondern durch Produkte nur unterstützt werden kann.

5.1 PC-Sicherheitssysteme mit Verschlüsselung

Utimaco Safeware AG[89]: Marktführer im Bereich der PC-Sicherheit, wofür die SafeGuard-Produkte angeboten werden. Neben Software-basierten Produkten gibt es unter der Bezeichnung SafeGuard CryptoServer auch Hardware-Lösungen. Die aktuellen kryptographischen Verfahren werden unterstützt.

CE Infosys[90]: bietet ebenfalls Hardware- und Software-basierte Sicherheitslösungen an und ist (oder war zumindest in der Vergangenheit) für besonders solide Produkte bekannt. Die Produktlinie im Bereich PC-Sicherheit heißt CompuSec und wird für Windows- und Linux-Systeme angeboten.

Glück & Kanja Technology AG[91]: Angeboten werden Leistungen rund um die IT-Sicherheit, speziell in einer Microsoft-Infrastruktur, u. a. Datei- und Ordnerverschlüsselung für Arbeitsgruppen in Unternehmensnetzen. Das CryptoEx-Portfolio mit Smartcard-Unterstützung und AES-Verschlüsselung und mit Komponenten zur E-Mail-, Daten-, Festplatten- und PDA-Verschlüsselung ist allerdings schon wieder vom Markt verschwunden[92].

Crypto AG[93]: Diese renommierte Schweizer Firma bietet Hochsicherheitsprodukte, vor allem für Politik und Militär, an. Es werden vor allem proprietäre Algorithmen an Stelle von offenen Standards verwendet, was angesichts des Renommés dieser Firma ausnahmsweise nicht als Nachteil zu werten ist.

COMCITY GmbH[94]: Angeboten wird ein verschlüsselter Server (COMCITY Secured Data Server), der mit dem Gütesiegel[95] des ULD Schleswig-Holstein ausgezeichnet wurde[96].

---

[89] http://www.utimaco.de/
[90] http://www.ce-infosys.com/
[91] http://www.glueckkanja.com/
[92] http://www.cryptoex.com/
[93] http://www.crypto.ch/
[94] http://www.comcity.de/
[95] https://www.datenschutzzentrum.de/guetesiegel/
[96] https://www.datenschutzzentrum.de/guetesiegel/kurzgutachten/g0310006/

5.2 Chipkarten

Hauptanbieter in Deutschland ist Gieseke & Devrient[97] (G&D); angeboten werden u. a. eine Java-Card-Lösung mit zugehörigem Entwicklungs-Toolkit sowie das für die Gesundheitstelematik vorgesehene Karten-Applikations-Management-System KV-KAMS.

Hauptanbieter weltweit ist die niederländische Gemalto nv[98], die aus Gemplus und Axalto hervorgegangen ist. Produkte: Javacard und JCardManager zur Entwicklung und Nutzung, .NET Smartcard für die .NET-Umgebung von Microsoft mit den entsprechenden Entwicklungswerkzeugen, Kartenterminals aller Sicherheitsklassen. Unterstützt werden alle aktuellen kryptographischen Funktionen (RSA allerdings z. Z. nur bis 2048 Bit).

Sagem Orga[99] ist ein Smartcard-Anbieter, der durch eGK-Lösungen bekannt ist, aber auch eine Java-Card mit Entwicklungsumgebung in der Produktpalette hat.

Siemens[100] stellt Smartcards selbst her und bietet dafür ein eigenes Betriebssystem CardOS sowie eine Programmier-Schnittstelle an.

5.3 Kartenleser

SCM Microsystems[101] entwickelt und vertreibt Chipkartenlesegeräte aller Arten. Im KPOH wurde das Chipdrive Pinpad 532 eingesetzt, wobei es allerdings nicht gelang, die externe Pineingabe zu nutzen.

Das Verfahren zur Zulassung von Kartenterminals für die Gesundheitskarte durch die Gematik ist im Internet zugänglich[102]. Die ersten zugelassenen Terminals sind MedCompact von Hypercom[103] und eHealth 200 BCS von SCM Microsystems[98].

Andere bekannte Anbieter sind Kobil[104], Celectronic[105], Becker & Partner[106], Cherry[107], Reiner SCT[108], Sagem Monétel[109], Advanced Card Systems[110], gemalto[95], Omnikey[111] und german telematics[112].

5.4 Trustcenter

Nach dem Signaturgesetz in Deutschland **akkreditierte Zertifizierungsstellen** sind:

- D-Trust[113] (Bundesdruckerei)

---

[97] http://www.gi-de.com/
[98] http://www.gemalto.com/
[99] http://www.sagem-orga.com/
[100] http://www.siemens.com/
[101] http://www.scmmicro.com/
[102] http://www.gematik.de/(S(1yiusiiztpsm4ti5d0b4ulmc))/Zulassungsverfahren_Kartenterminal_BCS.Gematik
[103] https://www.medline-online.com/
[104] http://www.kobil.de/
[105] http://www.celectronic.de/
[106] http://www.becker-partner.de/
[107] http://www.cherry.de/
[108] http://www.reiner-sct.com/
[109] http://www.sagem-monetel.de/
[110] http://www.advancedcardsystems.com/
[111] http://www.omnikey.com/
[112] http://germantelematics.com/

- Signtrust[114] (Deutsche Post)
- Telesec[115] (Deutsche Telekom)
- TC Trustcenter GmbH[116]
- DGN Deutsches Gesundheitsnetz Service GmbH[117]
- DATEV Zertifizierungsstelle[118]
- Bundesnotarkammer[119]
- S-Trust[120] (Deutscher Sparkassen Verlag)

Darüber hinaus gibt es weitere kommerzielle Angebote wie etwa

- Authentidate International[121]
- ATOS Origin[122]
- Verisign[123]
- u. v. a.

ATOS Origin ist ein breit gefächerter IT-Dienstleister, der unter anderem auch die von Schlumberger Sema (und dort wiederum von CCI) übernommenen Trustcenter-Dienste anbietet, und daher in der Vergangenheit als Trustcenter für das KPOH wirkte. Probleme gab es u. a. mit der zeitnahen Ausstellung von Zertifikaten sowie der Verfügbarkeit von Sperrlisten (CRL/OCSP), so dass die Zusammenarbeit insgesamt als unbefriedigend beurteilt wurde.

5.5 Sonstiges

Eine kryptographische Dienstleistung, die auch für die medizinische Forschung von prinzipiellem Interesse ist, ist die **externe verschlüsselte Speicherung** (Hosting); dies ist dann datenschutzrechtlich unproblematisch, wenn die Ver- und Entschlüsselung nur beim „Kunden" stattfinden kann und der Dienstleister selbst keine Möglichkeit zur Einsicht in die gespeicherten Daten hat. Exemplarisch seien die folgenden Angebote genannt:

- Telepaxx Software GmbH[124] mit dem e-pacs-Speicherdienst (Archivierung von Röntgenbildern und anderen medizinischen Daten) das mit einem Gütesiegel des ULD[125] ausgezeichnet wurde.
- Swiss Tresor[126].

---

[113] http:// www.d-trust.net/
[114] http://www.signtrust.de/
[115] http://www.telesec.de/
[116] http://www.trustcenter.de/
[117] http://www.dgn-service.de/
[118] http://www.zs.datev.de/
[119] http://dir.bnotk.de/
[120] http://www.s-trust.de/
[121] http://www.authentidate.de/
[122] http://www.de.atosorigin.com/
[123] http://www.verisign.de/
[124] http://www.telepaxx.de/
[125] https://www.datenschutzzentrum.de/guetesiegel/kurzgutachten/g030503/
[126] http://www.swiss-tresor.ch/

- ClearMedia Backup[127] (als Backup-Angebot).

Verschlüsselnde Handys sind für medizinische Forschungsnetze eher nicht nötig, könnten aber bei entsprechender Entwicklung des Marktes im Bereich der Krankenversorgung durchaus eine interessante Option bilden; interessant ist insbesondere im Zusammenhang mit mobiler Datenerfassung die Möglichkeit, SMS zu verschlüsseln. Hier gibt es eine Reihe von Angeboten (KRYPTEXT, MultiTasker), deren kryptographische Seriosität vor einem eventuellen Einsatz erst noch geprüft werden müsste.

5.6 „Snake-Oil"-Kryptographie

Auf dem Markt für kryptographische Produkte werden nach wie vor viele ungeeignete Produkte angeboten. Dafür hat sich der Begriff „Snake-Oil-Kryptographie" eingebürgert, der durch die danach benannte FAQ[128] populär wurde (ein passender, aber unüblicher, deutscher Begriff wäre „Quacksalber-Kryptographie"). Diese FAQ stellt typische Anzeichen zusammen, an denen man recht deutlich erkennt, ob ein Anbieter (egal ob kommerziell oder nicht) im Bereich der Kryptographie kompetent ist. Sie sollte in Zweifelsfällen zu Rate gezogen werden. Trotz Ihres Alters ist sie immer noch relevant.

[127] http://www.clearmedia.ch/dienstleistungen/clearmedia_backup/
[128] http://www.faqs.org/faqs/cryptography-faq/snake-oil/

6. Einsatz für medizinische Forschungsnetze

Abschließend werden die kryptographischen Verfahren und Produkte im Hinblick auf die möglichen Einsatzszenarien in medizinischen Forschungsnetzen, wie sie im TMF-Datenschutzkonzept definiert sind, beurteilt.[129]

6.1 Komponenten und Prozesse des generischen Datenschutzkonzepts

Komponenten und Prozesse des generischen Datenschutzkonzepts (einschließlich des Datenschutzkonzepts für Biomaterialbanken) mit kryptographischen Anforderungen sind:

- Server und Datenbanken: s. 6.2
    - Klinische Datenbank
    - Studiendatenbank
    - Forschungsdatenbank
    - Bilddatenbank
    - Biomaterialbanken: Befunddatenbank
    - Qualitätssicherungsdatenbank
    - Applikationsserver
- Dokumente: s. 6.3
- Kommunikation: s. 6.4-6.5
    - Client-Server-Kommunikation
    - Mail
    - Remote-Desktop-Verbindungen
    - Drahtlos-Techniken, s. 6.5
    - Sonstige Kommunikationswege
- Identitätsmanagement für Patienten, s. 6.6-6.11
    - PID-Dienst, s. 6.7
    - Biomaterialbanken: Erzeugung von LabID und $LabID_{tr}$, s. 6.8
    - Andere pseudonyme Kennzeichen, s. 6.9
    - Pseudonymisierungsdienst, s. 6.10
    - Export-Pseudonymisierung, s. 6.11
- Nutzerverwaltung und Administration, s. 6.12-6.14
    - Authentisierung, s. 6.12
    - Verzeichnis- und Rechtedienst, s. 6.13
    - Fernadministration, s. 6.14

Die jeweiligen kryptographischen Anforderungen werden in den folgenden Abschnitten beschrieben.

[129] Hier werden sowohl das bisherige generische Datenschutzkonzept [1] und das Datenschutzkonzept für Biomaterialbanken (noch unveröffentlicht) als auch – soweit das bereits möglich scheint – das revidierte generische Datenschutzkonzept der TMF berücksichtigt.

6.2 Sicherheit von Servern und Datenbanken

Für alle Datenbanken in einem medizinischen Forschungsnetz ist grundsätzlich verschlüsselte Datenspeicherung anzustreben, um bei einer Kompromittierung des Servers eine zusätzliche Sicherheitsschicht zur Verfügung zu haben. Dies sollte durch Ablage der Datenbankdateien auf einer verschlüsselten Partititon oder einem verschlüsselten Laufwerk realisiert werden. Die technischen Einzelheiten sind in 2.1 und 3.1 beschrieben; dort werden auch weitere Sicherheitsmaßnahmen benannt wie sichere Aufstellung und Server-Härtung.

6.3 Dokumentenorientierte Sicherheit

Für die Verschlüsselung einzelner Dateien oder Dokumente, sei es zur Speicherung oder zum Versand, wird vorläufig PGP/ GnuPG empfohlen, siehe 2.4; dieses Verfahren ist auch für die fortgeschrittene digitale Signatur geeignet, sofern nicht die Anforderungen des Signaturgesetzes (qualifizierte Signatur) erfüllt werden müssen. Für Anforderungen an qualifizierte Signaturen, die dem Signaturgesetz genügen sollen, sollte auf die Nutzbarkeit der Gesundheitstelematik-Infrastruktur gewartet werden. Eine eigene Infrastruktur für diesen Zweck aufzubauen, sollte auf besondere Fälle beschränkt bleiben, von denen dem Gutachter bisher keine bekannt sind.

6.4 Kommunikation in medizinischen Forschungsnetzen

Für die Client-Server-Kommunikation bei webbasierten oder anderen Anwendungen wird bis auf weiteres die Nutzung von SSL, zunächst mit (selbsterzeugten) Serverzertifikaten empfohlen, dazu Nutzerzertifikate oder Passwort-geschützter Zugang, siehe 2.5. Für die Mail-Nutzung ist PGP/ GnuPG die zu empfehlende Methode, siehe 2.4. Für Remote-Desktop-Anwendungen siehe 6.12. Alle sonstigen Kommunikationswege (zwischen Anwendungen/ Inter-Prozess-Kommunikation) sind mit SSL oder VPN-Technik zu sichern.

6.5 Drahtlos-Techniken

- RFID ist bisher nicht für sicherheitskritische Anwendungen geeignet, s. 3.6.
- WLAN-Techniken sind mit entsprechenden (inzwischen üblichen) Sicherheitsmaßnahmen, insbesondere starker Verschlüsselung nach WPA oder WPA2, in lokalen Netzen geeignet.
- Drahtlose Telefonie (Datenübertragung per Handy) ist nur mit Ende-zu-Ende-Verschlüsselung sicher genug; die angebotenen Lösungen, s. 5.5, sind für Forschungsnetze in der Regel zu teuer, so dass dieser Ansatz zur Datenübertragung nicht empfohlen werden kann.

6.6 Kryptographische Anforderungen an pseudonyme Kennzeichen

In Forschungsnetzen werden in verschiedenen Szenarien pseudonyme Kennzeichen verwendet. Diese sollen eindeutig für die zu kennzeichnende Entität (Patient, Probe, Bild, …) sein, aber keine Information über deren Identität preisgeben. Hier sind verschiedene Arten von zusätzlichen Anforderungen relevant:

- Handhabungsalternative:
    - Das Kennzeichen soll nur maschinell verarbeitet werden.
    - Das Kennzeichen soll auch von menschlichen Bearbeitern mit möglichst geringer Fehleranfälligkeit gelesen, kommuniziert und geschrieben werden können, z. B. manuell in Formulare und Eingabemasken übertragen werden.
- Sicherheit: Hier ist der Aufwand für die unbefugte Entschlüsselung zu beurteilen unter Berücksichtigung des Nutzens eines solchen Angriffs.

Diese Anforderungen werden von vier verschiedenen Typen solcher Kennzeichen unterschiedlich erfüllt:

1. laufende Nummer,
2. Zufallszahl (oder zufällige Zeichenkette),
3. verschlüsselte laufende Nummer mit für menschliche Bearbeiter handhabbarem Ergebnis,
4. verschlüsselte laufende Nummer mit nur maschinell zu verarbeitendem Ergebnis.

Typ 3 (je nach Weiterverarbeitung auch Typ 2) erfordert insbesondere eine Prüfzeichentechnik. Dabei ist die Länge und der Zeichenvorrat beschränkt; die im TMF-PID-Generator verwendeten Parameter – acht Zeichen aus einem Vorrat von 32 Ziffern und Buchstaben – erscheinen unter diesen Randbedingungen als gerade noch vertretbar. Eine unter diesen Vorgaben optimale Codierung wurde in [14] entwickelt; sie besteht aus 6 nutzbaren Zeichen und 2 Prüfzeichen. Mit diesen sechs nutzbaren Zeichen plus 2 Prüfzeichen lassen sich $32^6 = 2^{30} \approx 1$ Milliarde verschiedene Kennzeichen der Länge 8 erzeugen und neben einzelnen Zeichenfehlern auch Vertauschungen von Nachbarzeichen korrigieren.

Die Verschlüsselung bei Typ 4 sollte mit dem AES-Verfahren erfolgen, die entstehende 128-Bit-Zeichenkette ist nur maschinenlesbar.

Der kryptographische Verschlüsselungsalgorithmus für Typ 3 muss einschränkende Randbedingungen berücksichtigen:

1. Er soll bijektiv auf einem Raum von 2^{30} möglichen Klartexten operieren und 30-Bit-Chiffretexte liefern (die sich dann durch 6 Zeichen des gewählten Vorrats ausdrücken lassen).
2. Für die gesamte Lebensdauer des Forschungsnetzes darf sich der Algorithmus nicht ändern, insbesondere dürfen die Schlüssel hierfür nicht gewechselt werden. Andernfalls wäre die Eindeutigkeit der PIDs nicht mehr gewährleistet.

Durch diese Randbedingungen werden starke Verschlüsselungsalgorithmen ausgeschlossen, insbesondere AES, das 128-Bit-Ergebnisse liefert; eine Verkürzung der Ergebnisse auf 30 Bit würde die Eindeutigkeit gefährden und wegen des Geburtstagsphänomens eine „Kollision“ schon nach etwa $2^{15} \approx 32000$ Fällen mit Wahrscheinlichkeit ½ erwarten lassen [15, p. 53]. Daher ist ein kryptographisches Verfahren von bescheidener Stärke, das aber keinesfalls trivial sein soll, ausreichend für den Schutzzweck, da bei unbefugter Entschlüsselung nur eine laufende Nummer entsteht, die immer noch nicht unmittelbar auf die eigentliche Information schließen lässt. Ein solches ist im TMF-PID-Generator implementiert.

Eine Alternative für die Verschlüsselung bei den Typen 3 und 4 ist stets die Verwendung zufälliger Kennzeichen (also Typ 2), die dann aber die Führung einer Zuordnungsliste verlangt; andernfalls handelt es sich nicht um eine Pseudonymisierung, sondern um eine Anonymisierung.

Da Schlüssel langfristig verwendet werden müssen, sollten alle durch kryptographische Transformation erzeugten pseudonymen Kennzeichen nur strikt im Rahmen ihrer Zweckbestimmung verwendet und nicht an Dritte herausgegeben werden, siehe 1.6.

6.7 PID-Erzeugung

Ein PID (Patientenidentifikator) soll ein pseudonymes, aber in einem Forschungsnetz eindeutiges Kennzeichen für einen Patienten sein. Zur Erzeugung ist eines der Verfahren aus 6.6 zu verwenden; der PID-Generator der TMF bietet das Verfahren nach Typ 3 an, wobei trotzdem, um Eingabefehler bei den Identitätsdaten abfangen zu können, eine Zuordnungsliste („Patientenliste“) mitgeführt wird, die ein umfassendes Identitätsmanagement für Patienten ermöglicht. Eine Zusatzmöglichkeit, die bisher nur im KPOH genutzt wird, ist die Möglichkeit, die Zuordnungsliste Einweg-verschlüsselt zu führen. Dies könnte u. U. bei der Abwägung der Verhältnismäßigkeit von organisatorischen Schutzmaßnahmen eine Rolle spielen, bringt aber Abstriche bei der fehlertoleranten Zuordnung von Identitätsdaten mit sich.

6.8 Kennzeichnung von Proben

Im generischen Datenschutzkonzept für Biomaterialbanken werden Proben durch eine LabID und Referenzen zu Proben in der Forschungsdatenbank durch eine $LabID_{tr}$ gekennzeichnet. Die LabID entsteht nach einem der Verfahren aus 6.6; die $LabID_{tr}$ entsteht durch kryptographische Transformation aus der LabID; alternativ kann eine Zuordnungsliste eingesetzt werden, die am besten in einer separaten Datei aufbewahrt wird.

6.9 Andere pseudonyme Kennzeichen

Als SIC (Study Identification Code) und BildID werden Kennzeichnungen eines Patienten in einer Studien- bzw. Bilddatenbank bezeichnet. Sie werden am besten durch kryptographische Transformation aus dem zugehörigen PID erzeugt. Alternativ wäre eine Zufallserzeugung mit Speicherung in der Patientenliste denkbar.

6.10 Kryptographische Anforderungen an den Pseudonymisierungsdienst

Das Pseudonym ist das Kennzeichen, das nach dem TMF-Datenschutzkonzept in der Forschungsdatenbank verwendet wird und bei einem separaten Dienst durch Transformation aus dem PID erzeugt wird. Auch hier sind wieder die Varianten „Pseudonymisierung mit symmetrischer Verschlüsselung“ oder Führung einer Zuordnungsliste möglich. Letzteres ist technisch einfacher umzusetzen, aber in der Handhabung im Dauerbetrieb aufwendiger. Die Verschlüsselungslösung ermöglicht einen „schlanken“ Betrieb, da nur der Schlüssel sicher gespeichert werden muss, nicht eine stetig wachsende Datei, und somit als Instrument eine Chipkarte eingesetzt werden kann.

Für das Problem des Backup bei der Chipkartenlösung (Erzeugung identischer Karten) siehe 3.4.

6.11 Pseudonymisierung beim Datenexport

Hier reichen laufende Nummern oder Zufallszahlen, die aber in jedem Fall in einer Zuordnungsliste gespeichert werden müssen (sonst handelt es sich um eine Anonymisierung). Diese Liste soll unabhängig von der Datenbank aufbewahrt werden; als Format reicht eine einfache Datei.

6.12 Authentisierung

Für die Authentisierung in medizinischen Forschungsnetzen ist vorläufig der Passwortschutz über eine SSL-gesicherte Verbindung ausreichend.

Mittelfristig wird die Mitnutzung der Gesundheitstelematik-Infrastruktur in Form von Chipkarten, PKI, kryptographischen Funktionen und Schnittstellen empfohlen, siehe 2.6.

6.13 Verzeichnisdienst und Rechteverwaltung

Als Werkzeug wird hierfür ein LDAP-Server empfohlen. Für seine Sicherheit gelten die Anforderungen an Datenbanken und Kommunikation, wie sie in 2.1 und 2.5 beschrieben wurden.

6.14 Fernadministration

Zur Administration von Servern ist der bevorzugte Zugang der direkte physische Zugang zur Konsole. Ist die Administration über eine Netzverbindung nötig – was in realistischen Szenarien kaum zu vermeiden ist – ist der Zugang über SSH oder gesicherte Remote-Desktop-Verbindung, siehe 2.10, zu schalten.

Abkürzungsverzeichnis

AES	Advanced Encryption Standard
AIS	Anwendungshinweise und Interpretationen zu ITSEC vom BSI
ANSI	American National Standards Institute
ASTM	American Society for Testing and Materials
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAPI	Cryptographic Application Programming Interface
CAST	Verschlüsselungsverfahren von Carlisle Adams und Stafford Tavares
CBC-MAC	Cipher Block Chaining MAC
CCI	Competence Center Informatik
CEN	Comité Européen de Normalisation
CENELEC	Europäisches Komitee für elektrotechnische Normung
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
CT-API	Card Terminal Application Programming Interface
DES	Data Encryption Standard
DH	Schlüsselvereinbarungsverfahren nach Diffie und Hellman
DIN	Deutsches Institut für Normung
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EDE	Encrypt, Decrypt, Encrypt
EFS	Encrypting File System
eGK	elektronische Gesundheitskarte
ETSI	Europäisches Institut für Telekommunikationsnormen
FAQ	Frequently Asked Questions – im Internet gepflegte Listen von immer wieder auftretenden Fragen mit Antworten
FTP	File Transfer Protocol
HBA	Heilberufe-Ausweis
HMAC	Hash Message Authentication Code
http	HyperText Transfer Protocol
ICA	Independent Computing Architecture
IDEA	International Data Encryption Algorithm
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IPsec	Internet Protocol Security
ISO	International Organisation for Standardisation
ISSS	Information Society Standardization System
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunication Union
KPOH	Kompetenznetz Pädiatrische Onkologie und Hämatologie
L2TP	Layer 2 Tunneling Protocol
MAC	Message Authentication Code
MD2, MD4,MD5	Message Digest
MISTY1	Verschlüsselungsverfahren Mitsubishi Improved Security Technology oder nach den Erfindern Matsui, Ichikawa, Sorimachi, Tokita und Yamagishi

MKT	Multifunktionales Kartenterminal
NESSIE	New European Schemes for Signatures, Integrity and Encryption
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OSI	Open Systems Interconnection
PC/SC	Personal Computer/ Smart Card
PGP	Pretty Good Privacy
PID	Patientenidentifikator
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standards
PPTP	Point-to-Point Tunneling Protocol
PSE	Personal Secure Environment
RACE	Research and Technology Development in Advanced Communications Technologies in Europe
RC4, RC5, RC6	Verschlüsselungsverfahren „Ron's Cipher"
RDP	Remote Desktop Protocol
RDE	Remote Data Entry
RFC	Request for comments
RFID	Radio Frequency IDentification
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RSA	Verschlüsselungsverfahren nach Rivest, Shamir und Adleman
SAM	Security Access Module
SCM	Smart Card Microsystems
sFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SHACAL-2	SHA based Cryptographic Algorithm
SHS	Secure Hash Standard
SIC	Study Identification Code
SICCT	Secure Interoperable ChipCard Terminal
SigG	Signaturgesetz
SIT	Fraunhofer-Institut für sichere Informationstechnologie
S/MIME	Secure Multipurpose Internet Mail Extensions
SSEE	sichere Signaturerstellungseinheit
SSH	Secure SHell
SSL	Secure Sockets Layer
SSO	Single-Sign-On
TCG	Trusted Computing Group
TDES	Triple-DES
TLS	Transport Layer Security
TPM	Trusted Platform Module
TTMAC	Two-Track-MAC
TTP	Trusted Third Party
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UMAC	Message Authentication Code based on Universal hashing
VPN	Virtual Private Network
ZDA	Zertifizierungsdiensteanbieter

Quellen und Literatur

1 Reng, C.-M. et al. (2006). Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin: Im Auftrag des Koordinierungsrates der Telematikplattform für Medizinische Forschungsnetze. (1. Aufl.), Berlin: Medizinisch Wissenschaftliche Verlagsgesellschaft.

2 Pommerening, K. und Sergl, M. Vorlesung Datenschutz und Datensicherheit. *http://www.staff.uni-mainz.de/pommeren/DSVorlesung*

3 NIST. AES – Advanced Encryption Standard. *http://csrc.nist.gov/CryptoToolkit/aes/*

4 New European Schemes for Signatures, Integrity, and Encryption (2003). Portfolio of recommended cryptographic primitives. https://*www.cosic.esat.kuleuven.be/nessie/* Letzter Zugang: 2012-08-09.

5 Bundesamt für Sicherheit in der Informationstechnik (1999). AIS 20 - Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren. https://*www.bsi.bund.de/cae/servlet/contentblob/478150/publicationFile/30276/ais20pdf.pdf* Letzter Zugang: 2012-08-09.

6 Raptis, G. (2007). Ein Verfahren zur Lösung des Problems der kryptographischen Langzeitsicherheit medizinischer Daten, die in einer Infrastruktur gespeichert werden. Bundesärztekammer *http://www.baek.de/page.asp?his=1.134.135.5554* Letzter Zugang: 2012-08-09.

7 BSI. Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzkataloge. *http://www.bsi.de/gshb/*

8 Blaze, M. et al. (1996). Minimal key lengths for symmetric ciphers to provide adequate commercial security. A Report by an Ad Hoc Group of Cryptographers and Computer Scientists. Information Assurance Technology Analysis Center *http://people.csail.mit.edu/rivest/pubs/BDRSx96.pdf* Letzter Zugang: 2013-12-11.

9 Lenstra, A. K. und Verheul, E. R. (2001). Selecting Cryptographic Key Sizes. *Journal of Cryptology* **14** (4): S. 255 - 293.

10 Pommerening, K. und Wagner, M. (2000). Die Einrichtung sicherer HTTP-Server. KKS Mainz, Kompetenznetz POH *http://mi.imsd.uni-mainz.de/prjb/ServerSSL.html* Letzter Zugang:

11 Neuhaus, S. und Rütten, C. (2008). Fernverschlüsselt - Verschlüsselte Root-Partitionen für Linux-Systeme. *c't* **12/2008** S. 188 - 191.

12 Fraunhofer SIT und BSI (2007). BitLocker Drive Encryption im mobilen und stationären Unternehmenseinsatz. *http://testlab.sit.fraunhofer.de/content/output/project_results/bitlocker/*

13 Projektträger Mikrosystemtechnik VDI/VDE Innovation + Technik GmbH (2007). RFID-Studie 2007. Technologieintegrierte Datensicherheit bei RFID-Systemen. *http://www.informatik.uni-bremen.de/~sohr/papers/RFIDStudie07.pdf* Letzter Zugang: 2014-10-21.

14 Faldum, A. und Pommerening, K. (2005). An optimal code for patient identifiers. *Computer methods and programs in biomedicine* **79** (1): S. 81 - 88.

15 Menezes, A. J. et al. (1997). *Handbook of Applied Cryptography.* Boca Raton: CRC Press.

Anmerkung. Definitionen und Erläuterungen aus der Wikipedia [http://de.wikipedia.org/] wurden an einigen Stellen ohne ausdrücklichen Verweis, aber nach inhaltlicher Prüfung auf Richtigkeit frei übernommen.

Webseiten

ANSI	http://www.ansi.org/
ASTM	http://www.astm.org/
BSI	http://www.bsi.de/
Bundesärztekammer	http://www.bundesaerztekammer.de/
CEN	http://www.cenorm.be/
DIN	http://www.din.de/
GnuPG	http://www.gnupg.org/
IEEE-SISWG	https://siswg.net/
IETF	http://www.ietf.org/
ISO	http://www.iso.org/
ITU	http://www.itu.int/
NESSIE	http://www.cryptonessie.org/
NIST	http://csrc.nist.gov/
PGP	http://www.pgp.com/
SIT	http://www.sit.fraunhofer.de/
TeleTrusT	http://www.teletrust.de/