# Was leisten die aktuellen kryptographischen Verfahren für die Medizin?

K. Pommerening
Institut für Medizinische Biometrie, Epidemiologie und Informatik
Johannes-Gutenberg-Universität Mainz

**Schlüsselwörter:** Kryptographie – IT-Sicherheit – Infrastruktur – Authentisierung – Pseudonyme – Web-Dienste

**Zusammenfassung:** Kryptographie ist die Grundlage für wirksame Datensicherheit in offenen und verteilten Systemen. Sie kann das Arztgeheimnis, die Integrität und Verbindlichkeit von Dokumenten sowie die Authentizität von Netzteilnehmern sichern. Auf kryptographischen Basisfunktionen bauen kryptographische Protokolle auf, die über eine geeignete Infrastruktur zu sicheren Anwendungs- und Kommunikationssystemen führen. Als Beispiele für den Einsatz kryptographischer Verfahren in der Medizin wird die Pseudonymiserung in medizinischen Forschungsnetzen sowie der Betrieb von sicheren Web-Diensten, etwa für Befundserver, vorgestellt. Kryptographische Verfahren werden im medizinischen Umfeld bereits an vielen Stellen eingesetzt, oft ohne dass der Nutzer das explizit merkt. Viele weitere Vorgänge lassen sich leicht kryptographisch absichern. Für viele Anwendungen allerdings besteht auf Seiten der Systemhersteller noch erheblicher Handlungsbedarf zur Integration kryptographischer Verfahren und Infrastruktur.

**Title:** What can the Current Cryptographic Procedures do for Medical Information Processing?

**Key words:** Cryptography – IT security – infrastructure – authentication – pseudonyms – web sevices

**Summary:** Cryptography is the basis for effective IT security in open and distributed systems. Cryptography, if properly used, can protect the professional discretion, the integrity and liability of documents, as well as the authenticity of network participants. Basic cryptographic procedures are the building blocks for cryptographic protocols that in turn, via a standardized infrastructure, are essential elements of secure and dependable application and communication systems. The paper describes some examples for the use of cryptographic procedures in a medical context, such as a pseudonymisation service for medical research networks and the setup of secure web services for medical reports. Cryptographic procedures are presently being used in medicine in many places, often without explicit awareness of the user. Some more processes can easily protected by cryptographic means. For many applications however there remains considerable need for action by the system providers.

## Der Nutzen der Kryptographie

Wer an Kryptographie denkt, denkt in erster Linie wohl zunächst an Verschlüsselung (Chiffrierung) von Nachrichten, an Militär, Geheimdienste, Diplomatie. Informationen können verschlüsselt in »feindlicher Umgebung« aufbewahrt oder durch feindliche Umgebung transportiert werden, ohne ihre Vertraulichkeit zu gefährden.

Diese Art der Geheimhaltung von Informationen betrifft aber auch die Medizin: Nach den strengen Vorgaben der ärztlichen Schweigepflicht gehört jeder, der nicht direkt mit der Behandlung eines bestimmten Patienten befasst ist, zur »feindlichen Umgebung«, vor der die Informationen über Diagnose und Therapie dieses Patienten unbedingt geheim zu halten sind. Solange diese Informationen nur im Kopf des Arztes oder in seinen handschriftlichen Notizen existieren, ist die Geheimhaltung nur eine Frage der Disziplin und der Organisation. Sobald die Informationen aber in die elektronische Welt gelangen, ist die Kontrolle über ihre Sichtbarkeit verloren – nicht einmal auf dem eigenen Rechner, der für Systemadministratoren oder gar fremde Wartungsfirmen offen ist, geschweige denn im Netz, das immer mehr zum zentralen Kommunikationsmedium in der medizinischen Versorgung wird, sind die Informationen vor fremden Augen sicher. Für den Arzt ist das besonders brisant, denn für eine Verletzung der Schweigepflicht haftet er persönlich: strafrechtlich, standesrechtlich und zivilrechtlich.

Kryptographie ist also auch für den Arzt ein wichtiges Thema. Natürlich muss er für ihren sinnvollen Einsatz nicht die – sehr komplizierten – mathematischen Verfahren einer sicheren Verschlüsselungstechnik verstehen, aber eine Vorstellung davon, was kryptographische Verfahren leisten, wie sie eingesetzt werden können und wie sie zu beurteilen sind, hilft in ähnlicher Weise, wie es für die bildgebenden Verfahren in Bezug auf ihre physikalischen Grundlagen gilt.

Bemerkenswert ist, dass die Kryptographie in der elektronischen Welt nicht nur die Mittel zur Wahrung der Vertraulichkeit (durch kryptographische Verschlüsselung) bietet, sondern in Form der digitalen Signatur auch zur Wahrung der Echtheit (Authentizität, Integrität) und Verbindlichkeit von Dokumenten. Zusammengefasst ist festzustellen: *Wirksame Datensicherheit in offenen und verteilten Systemen ist nur mit kryptographischen Methoden zu erreichen.*

Als allgemeine aktuelle Referenz zum Thema sei auf [1] verwiesen, speziell für das medizinische Umfeld auf [2].

## Die Themen der angewandten Kryptographie

Angewandte Kryptographie besteht aus mehreren Stufen von der Grundlagenforschung bis zur sicheren Anwendung:

*Kryptographische Basisfunktionen*, das sind die mathematischen Algorithmen, die zur sicheren Transformation von Zeichenketten oder Binärdaten eingesetzt werden.

*Kryptographische Protokolle*, die die Ablaufsteuerung der Kommunikation regeln, wenn kryptographische Funktionen eingesetzt werden.

*Kryptographische Infrastruktur*, das ist der organisatorische und technische Rahmen, in dem der flächendeckende – über das persönliche Engagement einzelner hinausgehende – Einsatz kryptographischer Verfahren erst praktikabel wird.

*Kryptographische Software*, die die kryptographischen Funktionen und Protokolle sowie die Anbindung der Infrastruktur in eine für jeden handhabbare, bequeme und verständliche Form bringt.

*Sichere Anwendungs- und Kommunikationssysteme*, die unter Verwendung der kryptographischen Software und der Infrastruktur weitgehend automatisch für sichere Datenspeicherung und Übertragung im Anwendungsumfeld, z. B. dem Intranet eines Klinikums oder einem Praxisnetz, sorgen.

Die für den Anwender aktuellsten Gebiete der Kryptographie sind einmal auf der Grundlagenebene das Wettrennen um die Schlüssellängen, zum anderen auf der Anwendungsebene der Kampf um den praktischen Einsatz kryptographischer Infrastruktur, Software und Anwendungssysteme in der Fläche, die mit dem Aufbau medizinischer Telematik-Plattformen vorangetrieben werden sollen.

Zu Befürchtungen, der Einsatz von Kryptographie könne die Informationsverarbeitung schwerfällig und unhandlich machen, besteht kein Anlass: Verschlüsselung ist vergleichbar mit Datenkompression, kryptographische Protokolle sind vergleichbar mit gewöhnlichen Kommunikationsprotokollen bezüglich Komplexität und Performanz; für eine moderne CPU ist das kein Thema – mit einer Ausnahme: Web-Server, die bei schwerer Belastung ihre Kommunikation mit SSL kryptographisch sichern, können durch Hardware-Unterstützung der CPU Performanz gewinnen. Was die Handlichkeit für den Anwender angeht, sehen die modernen Konzepte – die leider immer noch im Pilotprojektstadium dümpeln – den Einsatz von Chipkarten, z. B. dem elektronischen Arztausweis, vor, der die Kryptographie für den Nutzer darauf reduziert, seine Karte in ein Lesegerät zu stecken und ihre Funktionen mit der PIN freizuschalten; für digitale Signaturvorgänge kommt aus rechtlichen Gründen noch jeweils eine Extra-Bestätigung dazu.

**Kryptographische Basisfunktionen**

Die grundlegenden Verfahren der Kryptographie sind

Symmetrische Verschlüsselung.
Asymmetrische Verschlüsselung.
Einweg-Verschlüsselung und Hash-Funktionen, z. B. für Passwort-Speicherung.
Zufallserzeugung, z. B. zur Erzeugung sicherer Schlüssel oder im Rahmen der Pseudonymisierung.
Steganographie, das Verstecken von Informationen, das auch bei Kopierschutzverfahren wie elektronischen Wasserzeichen eine wichtige Rolle spielt.

Zu den ersten beiden Verfahren folgen hier weitere Informationen; diese sind insoweit wichtig, als die Namen der Verfahren und insbesondere die Anforderungen an die Schlüssellängen zu dem Wissen gehören, mit dem man bei der Beschaffung und Installation von kryptographisch gesicherten Systemen immer wieder konfrontiert wird, z. T. in Gestalt abstruser Werbeaussagen.

*Symmetrische Verschlüsselung*

Von symmetrischer Verschlüsselung spricht man, wenn Urheber und Adressat der Information – das kann durchaus auch dieselbe Person sein, z. B. bei verschlüsselter Speicherung – denselben Schlüssel (Kennwort zur Ver- und Entschlüsselung) benötigen. Für die symmetrische Verschlüsselung gibt es schnelle Verfahren für große Datenmengen; 1 Megabit bis 1 Gigabit pro Sekunde und mehr, je nach Plattform, sind die Regel. Das in den letzten zwanzig Jahren meist verwendete Verfahren DES (»Data Encryption Standard«) ist veraltet: Es verwendet Schlüssel der Länge 56 Bit (8 Sieben-Bit-Zeichen mit Paritäts-Check-Bits) und kann durch vollständiges Durchsuchen des Schlüsselraums routinemäßig gebrochen werden. Als Ersatz wird zur Zeit meist das Triple-DES-Verfahren angewendet: dreimal hintereinander DES mit zwei oder drei verschiedenen Schlüsseln, also effektiv mit einem 112- oder 168-Bit-Schlüssel; dieses Verfahren ist brauchbar, aber etwas langsam.

Seit vorigem Jahr heißt der Stand der Technik AES (Advanced Encryption Standard) mit 128-Bit-Schlüssel; auch 192 oder 256 Bit sind möglich. Dieser Algorithmus wurde in einem internationalen Wettbewerb unter Beteiligung der kryptographischen Fachleute aus aller Welt von der US-amerikanischen Standardisierungsorganisation NIST ausgewählt. Die »Sieger« waren zwei junge belgische Wissenschaftler, Joan Daemen und Vincent Rijmen, mit ihrem Algorithmus, den sie nach ihren Namen und im Bewusstsein, dass die Aussprache im internationalen Bereich eine Herausforderung darstellt, »Rijndael« nannten. Er ist trotz höherer Sicherheit sogar schneller als der DES. In mancher kryptographischen Software wird er schon verwendet.

Was hat es nun mit der Wahl der Schlüssellängen auf sich? Solange ein Algorithmus nicht aufgrund einer Designschwäche mit schnelleren Methoden gebrochen werden kann, ist die Schlüssellänge das Maß für die Sicherheit; ein Bit mehr bedeutet eine Verdoppelung des Aufwandes für die vollständige Schlüsselsuche. Ein 64-Bit-Schlüssel wurde im Sommer 2002, wenn auch mit riesigem Aufwand, öffentlich gebrochen. 90 Bit gilt unter Fachleuten als Sicherheitsschwelle zur mittelfristigen Sicherheit, etwa für 20 Jahre. 128 Bit sind auch langfristig unangreifbar – immer vorausgesetzt, bei dem Verschlüsselungsverfahren wird keine anderweitige Schwäche entdeckt. Nach oben hin gibt es physikalische Grenzen: Selbst wenn jedes Elementarteilchen im Universum eine mit Lichtgeschwindigkeit rechnende CPU wäre, könnte ein solcher Rechner 475-Bit-Schlüssel in der angenommenen Zeitdauer des Universums nicht finden. Aber schon ein sehr viel kleinerer Rechner würde zu einem schwarzen Loch kollabieren; egal was er berechnet, er könnte es nicht von sich geben. Als realistische physikalische Grenze in diesem Universum werden ca. 200 Bit angesehen.

*Asymmetrische Verschlüsselung*

Eine ganz andere Art von Verschlüsselungsverfahren, sowohl in der Anwendung als auch in der zugrundeliegenden Theorie, sind die asymmetrischen. Hier sind Verschlüsselung und Entschlüsselung insofern entkoppelt, als man dazu verschiedene Schlüssel braucht; der Kerngedanke dabei ist, dass es mathematische Funktionen gibt, deren Umkehrfunktion nicht effizient berechenbar ist. Ein analoges Bild dafür ist ein Briefkasten: Jeder kann eine Nachricht für

den Besitzer hineinwerfen – das entspricht der Anwendung von dessen »öffentlichen« Schlüssel –, aber herausholen kann sie nur dieser mit seinem passenden – »privaten« – Schlüssel. Man spricht daher auch von »adressierter Vertraulichkeit« – eine im medizinischen Umfeld wichtige Eigenschaft dieser Verfahren.

Leider sind die bekannten asymmetrischen Verfahren sehr langsam, also nur für kleine Datenmengen geeignet; in Software auf schnellen Rechnern schaffen sie ca. 2 Kbit/sec. Man macht aus der Not eine Tugend durch die »hybride Verschlüsselung«: Die eigentliche Verschlüsselung großer Datenmengen wird symmetrisch mit einem zufälligen Einmalschlüssel (»Sitzungsschlüssel«) durchgeführt, der dazu nötige Schlüssel wird seinerseits asymmetrisch verschlüsselt und mit der Nachricht mitgeschickt. Die weiter unten erwähnten Verfahren PGP, S/MIME und SSL machen genau dieses. Für den Anwender präsentiert sich das hybride Verfahren wie ein asymmetrisches. Die besondere Bedeutung der asymmetrischen Verfahren liegt aber in ihrer Verwendung für kryptographische Protokolle wie z. B. die digitale Signatur, siehe unten.

Stand der Technik sind die Verfahren RSA oder DH mit 2048-Bit-Schlüsseln (benannt nach ihren Erfindern Rivest/Shamir/Adleman bzw. Diffie/Hellman). Zu beachten ist die im Vergleich zu symmetrischen Verfahren völlig andere Anforderung an die Schlüssellänge – die asymmetrischen Verfahren sind mit mathematischen Methoden wesentlich schneller zu brechen als durch vollständige Schlüsselsuche, erst die genannte Schlüssellänge verhindert das. Auf Chipkarten werden meist noch 1024-Bit-Schlüssel verwendet, das ist nur ganz kurzfristig tolerierbar, mittelfristig aber zu schwach. Zu beachten ist auch, dass bei hybriden Verschlüsselungsverfahren *beide* Schlüssellängen stimmen müssen – Merkregel also: »2048 und 128«.

Bemerkt werden sollen noch zwei Besonderheiten: Für die asymmetrische Kryptographie gibt es auch Verfahren, die auf der mathematischen Theorie der elliptische Kurven beruhen und zwar nicht schneller sind, aber mit deutlich kürzeren Schlüsseln auskommen. Ferner machen in letzter Zeit Fortschritte in der Quantenkryptographie von sich reden; diese dient allerdings nur zur sicheren Übermittlung von Sitzungsschlüsseln und ist daher kaum von praktischer Relevanz – die hybriden Verfahren erledigen diese Aufgabe bis auf weiteres wesentlich einfacher.

**Kryptographische Protokolle**

Kryptographische Protokolle sind Kommunikationsprotokolle und Verfahrensabläufe, die kryptographische Funktionen einsetzen. Als Beispiele seien hier genannt:

hybride Verschlüsselung,
digitale Signatur,
starke Authentisierung,
Pseudonymisierung.

Grundlage vieler kryptographischer Protokolle sind die asymmetrischen Verschlüsselungsverfahren.

*Digitale Signatur*

Die digitale Signatur ist in erster Näherung einfach die Umkehrung der asymmetrischen Verschlüsselung: Ärztin A signiert ein Dokument, z. B. einen Arztbrief, indem sie es mit ihrem privaten Schlüssel verschlüsselt. Die Umkehrfunktion, die Anwendung des öffentlichen Schlüssels, kann jeder durchführen und sich dabei überzeugen, dass das Dokument nur von A unterzeichnet sein kann – nur A kann ja ihren privaten Schlüssel anwenden –, und darüberhinaus, dass kein einziges Bit dieses Dokuments seit der Unterzeichnung verändert wurde. Es sind also Urheberschaft und Echtheit prüfbar. (Eine »erste Näherung« ist dies insofern, als in der Praxis aus Effizienzgründen nur ein Hash-Wert signiert wird.)

*Starke Authentisierung*

Authentisierung bedeutet Nachweis einer Identität. Eine Benutzerin A meldet sich z. B. in einem Netz an und sagt dabei, wer sie ist (»Benutzername«). Da damit jeder Täuschungsversuch möglich wäre, wird sie nach einem Beweis dafür gefragt, in der bisherigen Praxis so gut wie immer nach einem Passwort, also nach der Kenntnis eines persönlichen Geheimnisses. Dieses Verfahren ist mangelhaft und entspricht längst nicht mehr dem Stand der Technik. Dieser verlangt nämlich nach einer »starken« Authentisierung. Diese ist eine direkte Anwendung der digitalen Signatur: Statt der Aufforderung zur Passworteingabe bekommt der sich anmeldende Benutzer einen einmaligen Zufallsstring (als »Challenge«) vorgelgt und muss diesen digital signieren. Da nur er im Besitz seines privaten Schlüssels ist, ist das Verfahren fälschungs- und abhörsicher. Es wird auch »Challenge-Response-Verfahren« genannt. Auf diese Weise wird der private Schlüssel zur digitalen Identität und der öffentliche Schlüssel zu einem Ausweis, den jeder überprüfen kann.

*Pseudonymisierung*

Pseudonyme stellen einen Kompromiss zwischen Anonymität und Personenbezug dar: sie können zu faktischer Anonymität führen, ohne die Datenverwertung wesentlich einzuschränken – die Datenzusammenführung aus verschiedenen Quellen bleibt möglich, unter Umständen bleibt sogar der Weg zurück möglich, etwa um für eine epidemiologische Studie Daten nachzuerheben oder wichtige Ergebnisse aus einem Forschungsprojekt an einen Patienten rückzumelden [3]. Daher ist die Pseudonymisierung ein wichtiges Instrument, um medizinische Forschungs- und Qualitätssicherungsprojekte datenschutzgerecht zu gestalten [6]. Als Faustregel kann gelten:

Im klinischen oder Behandlungs-Kontext sind die Identitätsdaten des Patienten nötig und erlaubt, im Forschungs- oder Qualitätssicherungs-Kontext sind die Daten wo immer möglich zu anonymisieren, sonst zu pseudonymisieren.

Ist ein Pseudonym auf irgendeine Weise auf die Identitätsdaten rückführbar, ist für die Verwendung eine Einwilligung des Betroffenen nötig; kann dagegen niemand diese Verbindung herstellen, so gelten die Daten als faktisch anonymisiert. Die Aufgabe, verschiedene Modelle der Pseudonymisierung organisatorisch und technisch auszugestalten, ist ein Kernprojekt der TMF (= Telematikplattform für die medizinischen Forschungsnetze des BMBF) [www.tmf-net.de]. Eines

dieser Modelle (die genauere Beschreibung wird als Veröffentlichung vorbereitet) ist das Treuhänder-Modell, in dem verschiedene kryptographische Transformationen von Bedeutung sind:

Im *Behandlungszusammenhang* wird ein für die Studie einheitlicher Patientenidentifikator (PID) generiert. Dieser PID wird zusammen mit den für die Studie relevanten medizinischen Daten einem Datentreuhänder übergeben. Dazu werden die medizinischen Daten mit dem öffentlichen Schlüssel der Forschungsdatenbank der Studie (asymmetrisch) verschlüsselt.

Ein *Datentreuhänder* wandelt den PID durch (sysmmetrische) kryptographische Verschlüsselung in ein Pseudonym um. Der Schlüssel dazu ist sein Geheimnis, so dass eine Reidentifizierung nur über den Datentreuhänder möglich ist. Die medizinischen Daten können hier nicht gelesen werden; sie werden verschlüsselt durchgeschleust.

Auf der Seite der *Forschungsdatenbank* können die medizinischen Daten entschlüsselt und zusammen mit dem Pseudonym verwendet werden. Die Identitätsdaten einschließlich des PID sind hier unbekannt und können auch nicht hergeleitet werden.

Natürlich muss ein so kompliziertes Modell durch entsprechende Kommunikations- und Anwendungssysteme nutzerfreundlich umgesetzt werden. Das Treuhänder-Modell ist eine Modifikation des bekannten Krebsregister-Modells [4], das in den neunziger Jahren ja sogar in Gesetzen festgeschrieben wurde und ebenfalls wesentlichen Gebrauch von kryptographischen Verfahren macht. Pseudonymisierung ist inzwischen auch in verschiedenen anderen Gesetzen vorgesehen, so etwa dem Bundesdatenschutzgesetz (§§3 und 3a) [www.datenschutz.de].

**Kryptographische Infrastruktur**

Unter kryptographischer Infrastruktur versteht man in erster Linie die sogenannte PKI (Public Key Infrastructure), die sicherstellt, dass öffentliche Schlüssel authentisch sind, d. h., dass der Besitzer nicht verwechselt wird. Dies geschieht durch die Ausstellung eines Zertifikats, die nichts anderes ist als die digitale Signierung eines »Dokuments«, das aus öffentlichen Schlüssel und dem Namen plus eventuell weiteren Attributen des Besitzers besteht. Dafür werden Trustcenter oder Certification Authorities (CA) eingerichtet, wie im Signaturgesetz beschrieben. Zu den Leistungen eines Trustcenters gehört auch die Führung eines Verzeichnisdienstes, aus dem öffentliche Schlüssel abgerufen werden können, sowie einer Zertifikats-Widerrufliste (CRL) für abgelaufene oder gesperrte Zertifikate. Der hiermit verbundene organisatorische und finanzielle Aufwand ist der Hauptgrund, dass sich kryptographische Infrastruktur trotz des dringenden Bedarfs immer noch nicht flächendeckend durchgesetzt hat; insbesondere verzögert sich die Einführung des elektronischen Arztausweises (HPC = Health Professional Card) schon seit vielen Jahren, vgl. [5].

Auf der Nutzerseite gehört zur kryptographischen Infrastruktur eine Möglichkeit, die Schlüssel bequem und sicher aufzubewahren. Hierfür sind Chipkarten wie die HPC optimal geeignet. Eine solche nützt aber nur, wenn sie in konkreten vorhandenen Anwendungen auch eingesetzt werden kann, und dazu benötigt man einen weiteren wesentlichen Teil der kryptographischen Infrastruktur: Schnittstellen und Standards zur Integration.

**Kryptographische Software**

Für einige Anwendungsfälle gibt es sehr gute kryptographische Software, die jeder sofort einsetzen kann und sollte und die im nichtkommerziellen Bereich oft sogar kostenlos ist:

E-Mail-Verschlüsselung mit PGP [www.pgpi.com] oder S/MIME,
Verschlüsselung von Festplatten-Partitionen mit den im Betriebssystem vorgesehenen Varfahren von Linux oder Win2000 (wobei letzteres eine Hintertür für den Administrator offen lässt) oder mit Produkten wie ScramDisk oder PGPdisk.

Der Aufbau kryptographisch geschützter Internet-Verbindungen wird mit SSL erreicht. Dieser Zusatz zum TCP/IP-Protokoll ist in aktuellen Web-Servern und Browsern vorhanden; ob er genutzt wird, hängt von der Konfiguration des Servers ab.

Eine Stufe tiefer setzt die VPN-Technik an (Virtual Private Network). Sie sorgt für Verschlüsselung und Integrität auf Netzebene – unter der Kontrolle des Netzbetreibers. Damit ist eine virtuelle Erweiterung eines lokalen Netzes über das offene Internet möglich; zu beachten sind allerdings einige Schwächen dieser Technik:

Beide Enden der Verbindung müssen in sicherer Umgebung liegen, denn sie bilden zusammen ein lokales Netz. Insbesondere muss jedes so angebundene System vertrauenswürdig sein. Der PC eines von zu Hause aus arbeitenden Klinikarztes ist in diesem Sinne für die Klinik nicht vertrauenswürdig, wenn er zu anderen Zeiten von Familienmitgliedern genutzt wird.
Eine VPN-Verbindung ersetzt nicht die Nutzer-Authentisierung für ein Anwendungsprogramm, sie authentisiert nur den Rechner. Ebensowenig erübrigt sie die Rechteverwaltung in Anwendungen (wer darf was?).
Sie sorgt nicht für die im medizinischen Umfeld nötige Ende-zu-Ende-Vertraulichkeit zwischen Arzt und Arzt oder zwischen Arzt und Anwendungsprogramm.

Geeignet und unbedingt zu empfehlen ist die VPN-Technik zur Sicherung eines Funk-LAN.

Ausführliche Informationen über alle diese Software findet man im WWW mühelos [www.google.de].

**Sichere Anwendungssysteme**

Schwieriger ist die Situation bei kompletten Anwendungssystemen. Hier ist der Endnutzer darauf angewiesen, dass der Hersteller die kryptographische Infrastruktur nach dem Stand der Technik und standardgemäß integriert. Am leichtesten ist die Sicherheit in Webdienste einzubinden, also in Anwendungssysteme, bei denen über das http-Protokoll Clients in Form von Web-Browsern mit Servern kommunizieren; das kann auch im Intranet einer Klinik mit Vorteil verwendet werden. Solche Anwendungssysteme sind besonders leicht aufzusetzen und profitieren unmittelbar von einer vorhandenen PKI, indem sie einfach über SSL wie oben beschrieben abgewickelt werden. Hier gibt es drei Stufen, die sich im Anspruch an die vorhandene Infrastruktur deutlich

unterscheiden:

*Stufe 1,* einfach umzusetzen: Es werden nur Serverzertifikate verwendet. Das reicht schon, um für verschlüsselte Verbindungen zu sorgen. Authentisiert wird mit einer Passwortabfrage, was hier – über die verschlüsselte Verbindung – akzeptabel ist.

*Stufe 2,* mittlerer Aufwand: Auch Nutzerzertifikate werden verwendet, allerdings nicht auf Chipkarten, sondern als Dateien in den Browser importiert. Hierdurch erreicht man bereits die starke Authentisierung über das Netz und kann ein Single-Logon verwirklichen – der Nutzer schaltet einmal im Browser sein Zertifikat durch Eingabe seines (lokalen) Passworts frei; die Anmeldung an allen beteiligten Servern übernimmt der Browser dann für ihn im Hintergrund ohne weitere Intervention. Allein dieser Gewinn an Bequemlichkeit rechtfertigt schon die Mühe, Nutzerzertifikate einzuführen.

*Stufe 3,* hoher Aufwand: Die Nutzerzertifikate werden auf Chipkarten gespeichert. Das gewährleistet erhöhte Sicherheit und kann bei geeigneter Zusatz-Software sogar Signaturgesetz-konform gestaltet werden. Es ist aber unbedingt darauf zu achten, dass die Chipkarten mit den für die Einbindung in die verwendeten Browser nötigen Treibern ausgeliefert wird (CSP bzw. PKCS#11-Schnittstelle).

Als Beispiel für ein auf diese Weise mit kryptographischen Mitteln gesichertes Anwendungssystem sei ein Befundserver, z. B. für Röntgenaufnahmen, beschrieben:

Der Nutzer hat auf seinem Arbeitsplatzrechner einen Web-Browser laufen. Dieser kann auf ein Nutzer-Zertifikat direkt zugreifen oder mit einer kryptographischen Chipkarte (wie HPC) kommunizieren.

Der Nutzer aktiviert seinen privaten Schlüssel bzw. seine Chipkarte für den Browser durch Eingabe seines Passworts bzw. seiner PIN.

Der Nutzer wählt eine geeignete Webseite auf dem Befundserver. Im Hintergrund wird eine wechselseitige Authentisierung zwischen Browser und Server durchgeführt sowie ein kryptographischer Kommunikationskanal aufgebaut. Der Befundserver ist sich jetzt über die Identität des Nutzers sicher und kann bei Anfragen und Nutzeraktionen zuverlässig die Berechtigung prüfen. Auf diese Weise wird ein Röntgenbefund nur demjenigen präsentiert, der das Recht hat, ihn zu sehen. Auch ein unbefugter Lauscher im Netz hat keine Chance.

Tritt der Nutzer auf diese Weise mit weiteren Servern in Kontakt, verläuft der Vorgang genauso, ohne dass er jedes Mal neu Passwort oder PIN eingeben muss.

*Anwendungen lassen sich als Web-Dienste nicht nur besonders einfach implementieren, sondern auch besonders einfach datenschutzgerecht absichern*.

**Resumé**

Kryptographische Verfahren werden also im medizinischen Umfeld bereits an vielen Stellen eingesetzt, oft ohne dass der Nutzer das explizit merkt. Viele weitere Vorgänge lassen sich leicht – oft sogar in Eigenregie – kryptographisch absichern. Für viele Anwendungen allerdings besteht auf Seiten der Systemhersteller noch erheblicher Handlungsbedarf zur Integration kryptographischer

Verfahren und Infrastruktur.

**Literatur**


[1] Eckert, C. IT-Sicherheit – Konzepte – Verfahren – Protokolle. Oldenbourg, München 2001.

[2] The ISHTAR Consortium (Hrsg.). Implementing Secure Healthcare Telematics Applications in Europe. IOS Press, Amsterdam 2001.

[3] Pommerening K. Pseudonyme – ein Kompromiß zwischen Anonymisierung und Personenbezug. In: Trampisch HJ, Lange S (Hrsg.). Medizinische Forschung – Ärztliches Handeln. MMV Medizin Verlag, München 1995, 329-333.

[4] Pommerening K, Miller M, Schmidtmann I, Michaelis J. Pseudonyms for cancer registry. Meth Inf Med 1996; 35: 112-121.

[5] Pommerening K. IT-Sicherheit in medizinischen Netzen – aktuelle Probleme und Lösungsansätze. Zentralbl Gynakol 2000; 122: 658-662.

[6] Wichmann HE et al. Epidemiologie und Datenschutz. Online im WWW unter http:// www.datenschutz-bayern.de/verwaltung/epidem.htm.



**Korrespondenzanschrift:**
Univ.-Prof. Dr. Klaus Pommerening
Institut für medizinische Biometrie, Epidemiologie und Informatik
Johannes-Gutenberg-Universität
D-55101 Mainz
E-Mail: pommerening@imsd.uni-mainz.de