

**Protokoll**  
**der 4. Sitzung der GMDS-Arbeitsgruppe**  
***Datenschutz in Krankenhausinformationssystemen***  
**am 18. und 19. Mai 1995 in Bremen**

Die Sitzung fand im neuen Institut MeVis (Institut für Medizinische Visualisierungs- und Diagnosesysteme) an der Universität Bremen statt, in dem Herr Hortmann einer der wissenschaftlichen Leiter und Geschäftsführer ist.

Anwesend:

- G. Bleumer (Hildesheim)
- Dr. B. Blobel (Magdeburg)
- Dr. M. Hortmann (Bremen)
- M. Pöll (Innsbruck)
- Prof. Dr. K. Pommerening (Mainz)
- Dr. H. Ruelius (Göttingen)
- M. Schnabel (München)
- M. Schunter (Hildesheim)
- W. Thoben (Oldenburg)

Entschuldigt:

- S. Brings (Troisdorf)
- Dr. K.-H. Elsässer (Heidelberg)
- Dr. H. Lautenbacher (Tübingen)
- V. Lieder (Dresden)
- P. Messerer (Ludwigshafen)
- Prof. Dr. K. Sauter (Kiel)
- Dr. K.-H. Schicketanz (Mainz)
- Dr. W. Schoner (Innsbruck)

Tagesordnung:

1. Festlegung der Tagesordnung
2. Protokoll der vorigen Sitzung
3. Mitteilungen und Berichte
4. Pseudonyme Abrechnung im Gesundheitswesen
5. Firewall-Konzept der Universitätsklinik Mainz
6. PGP signing party
7. Demonstration von "Secure Talk"
8. "Threats to the System, Information System Security and Data Protection" - Video der NHS Management Executive Information Management Group
9. Musterkonzept für ein sicheres KIS
10. Verschiedenes

Der Vorsitzende begrüßt die neuen Teilnehmer und dankt Herrn Hortmann für die Organisation der Sitzung. Die Teilnehmer stellen sich kurz vor.

## **TOP 1. Festlegung der Tagesordnung**

Die mit der Einladung verschickte vorläufige Tagesordnung wird um die Punkte "1. Festlegung der Tagesordnung", "2. Protokoll der vorigen Sitzung" und "7. Demonstration von "Secure Talk" ergänzt.

## **TOP 2. Protokoll der vorigen Sitzung**

Das Protokoll der 3. Sitzung der Arbeitsgruppe wird in der vorliegenden Form angenommen.

## **TOP 3. Mitteilungen und Berichte**

a) Herr Pommerening weist noch einmal auf den WWW- und den anonymen FTP-Server der Arbeitsgruppe hin. Der WWW-Server ist unter

- <http://www.uni-mainz.de/FB/Medizin/IMSD/AGDatenschutz/AGDS.html>

zu erreichen (oder von <http://www.uni-mainz.de/> aus durch mehrmaliges Klicken). Er enthält Protokolle und Berichte sowie eine Ressourcenliste mit Literaturverzeichnis und weiteren relevanten Verweisen ins Internet. Der FTP-Server ist unter

- <ftp://ftp.uni-mainz.de/pub/FB/04/imsd/pom>

zu finden. Dort liegen Dokumente zum Datenschutz und zur Informationssicherheit sowie kryptografische Sicherheitssoftware. Die Arbeitsgruppe ist mit dem Angebot dieser Informationen im Internet einverstanden.

b) In Zusammenarbeit mit der Arbeitsgruppe organisierte Herr Dr. Blobel am 13. und 14. Februar 1995 in Magdeburg einen internationalen Workshop über Datenschutz in medizinischen Informationssystemen, der wichtige Vertreter aus Politik, Rechtspflege, Medizin und Medizinischer Informatik zusammenführte und einen sehr fruchtbaren Gedankenaustausch, insbesondere mit einigen anwesenden Landesdatenschutzbeauftragten, brachte. Unter anderem stieß die Idee der Pseudonyme auf Interesse. Der Tagungsband wird von Herrn Blobel redigiert und herausgegeben und erscheint voraussichtlich Ende Juli im Vieweg-Verlag.

c) Herr Pommerening hielt einen eingeladenen Vortrag zum Thema "Datenschutz in Krankenhausinformationssystemen" auf der Tagung der Fachgruppe "Verlässliche Informationssysteme" (VIS '95) der Gesellschaft für Informatik (GI), 5.-7. April 1995 in Rostock. Von besonderem Interesse auf dieser Tagung war auch ein Vortrag von B. Pfitzmann (Hildesheim), die sich sehr ausführlich mit der benutzergerechten Gestaltung von kryptographischen Geräten beschäftigt hat.

d) Herr Hortmann berichtet von der Tagung "Toward an Electronic Patient Record", die im März in Orlando (Florida) stattfand. Die Ansätze zum Datenschutz waren eher enttäuschend; kryptografische Verfahren wurden kaum erwähnt. Der Tagungsband liegt vor; Herausgeber C. P. Waegemann, erschienen beim Medical Records Institute.

e) Am 4. IT-Sicherheitskongress des BSI, 8. - 11. Mai 1995 in Bonn-Bad Godesberg, konnte leider kein Mitglied der Arbeitsgruppe teilnehmen.

f) Weitere Veranstaltungen im Jahre 1995 sind:

- GMDS-Jahrestagung in Bochum, 10. - 14. September 1995. Herr Blobel wird einen Vortrag über "Modellierung und Realisierung sicherer offener medizinischer Informationssysteme" und Herr Pommerening einen über "Pseudonyme - ein Kompromiss zwischen Anonymisierung und Personenbezug" halten.
- "Trust Center", veranstaltet von VIS und TeleTrusT am 27. und 28.9.1995 in Siegen. Herr Hortmann und Herr Schunter nehmen teil.
- IMIA WG 4 Security Working Conference "Communicating Health Information" in Helsinki vom 30. September bis 3. Oktober. Herr Bleumer wird einen Vortrag über kryptografische Mechanismen halten. Herr Blobel ist Mitglied des Programmkomitees und plant, als Repräsentant der GMDS teilzunehmen.
- HEALTH CARDS '95 am 23.-26. Oktober in Frankfurt am Main. Die Teilnahme ist bisher von keinem Mitglied der Arbeitsgruppe geplant.
- Jahrestagung der DGkDK (Deutsche Gesellschaft für klinische Datenverarbeitung und Kommunikation) am 25./26.11.95 in Kreischa bei Dresden. Herr Blobel wird einen Vortrag halten.
- Seminar "Datenschutz in verteilten und offenen Systemen" an der Akademie Medizinische Informatik, Heidelberg, am 29. November unter der Leitung von Herrn Pommerening. Herr Blobel erklärt sich bereit, als weiterer Referent teilzunehmen.

g) Herr Hortmann berät die belgische Ärztekammer in der Frage der Einrichtung eines "Trust Centers" mit "Key Escrow"-Funktion.

h) Herr Schunter weist darauf hin, dass nach dem neuen Entwurf zum Fernmeldeanlagen-gesetz Betreiber verpflichtet sein sollen, das Abhören *aller* digitalen Kommunikation zu ermöglichen. Er verteilt eine Kopie des Entwurfs.

#### **TOP 4. Pseudonyme Abrechnung im Gesundheitswesen**

Herr Bleumer und Herr Schunter legen einen Entwurf "Datenschutzorientierte Abrechnung medizinischer Leistungen" vor; Herr Schunter stellt den Entwurf vor. Gleichzeitig verteilt Herr Pommerening einen Vorschlag zur pseudonymen Abrechnung. Dieser enthält eine Minimallösung, die nur die Pseudonymisierung der Versichertenkarte vorsieht.

In der Diskussion ergibt sich als Standpunkt der Arbeitsgruppe, dass man den Maximalvorschlag weiter verfolgen sollte, der allen Beteiligten konsequent Datenschutz garantiert; Herr Blobel weist darauf hin, dass dies auch im Sinne der Ärzte ist, die den Überwachungsmöglichkeiten durch Weiterentwicklung der Technik misstrauisch gegenüberstehen. Er nennt aber auch einige Argumente, die einen solchen Vorstoß erschweren können: 10% der abgerechneten Leistungen werden von den Kassen im Detail kontrolliert. Die Kassen haben den Auftrag, die medizinische Versorgung trotz Kostendämpfung zu sichern und treten auch als Anwalt des Patienten auf, um diesem die optimale bezahlbare Behandlung zu gewährleisten.

Die Herren Bleumer und Schunter erklären sich bereit, den vorgelegten Vorschlag weiter auszuarbeiten.

## **TOP 5. Firewall-Konzept der Universitätsklinik Mainz**

Das Konzept ist noch in der Vorbereitung. Herr Pommerening will eine Marktübersicht auf dem WWW-Server zur Verfügung stellen. Eine eingehendere Behandlung des Themas wird vertagt.

## **TOP 6. PGP signing party**

Herr Pommerening erstellt ein neues Schlüsselpaar speziell für den Gebrauch in der Arbeitsgruppe; die Kennung des öffentlichen Teils ist

- pub 1024/6147CD 1995/05/18 Pommerening(GMDS)
- Key fingerprint = 5E F9 3A 49 AF 03 65 0F 89 FD 70 6B 00 EF 79 E3

Die anderen Gruppenmitglieder erhalten diesen und lassen ihre öffentlichen Schlüssel mit dem zugehörigen geheimen Schlüssel zertifizieren; die Schlüssel der Gruppenmitglieder wurden entweder mitgebracht oder aktuell neu erzeugt. Diese Schlüssel sollen ab sofort zum Sammeln von Erfahrungen mit sicherer Kommunikation in der Arbeitsgruppe verwendet werden. Die Arbeitsgruppe kommt überein, vorerst bei der PGP-Version 2.3a zu bleiben.

Herr Hortmann kündigt ein Programm "PGP Helper" an, das in wenigen Wochen verfügbar sein wird und den Umgang mit PGP, insbesondere die Gruppenverschlüsselung, vereinfachen soll. Herr Pommerening weist auf drei neu erschienene Bücher zu PGP hin, die auch für kryptografische Laien verständlich sind. Die Autoren sind Bruce Schneier, Simson Garfinkel und Philip Zimmermann. Genauere Angaben finden sich in der Ressourcen-Liste der Arbeitsgruppe.

## **TOP 7. Demonstration von "Secure Talk"**

Herr Bleumer und Herr Schunter führen das Programm "Secure Talk" vor, das im Rahmen von SEISMED am Institut für Informatik der Universität Hildesheim entwickelt wurde. Es ist ein Prototyp zum sicheren Datentransfer in Apple-Talk-Netzen und enthält mehrere kryptografische Mechanismen (RSA, DES, IDEA) zum Verschlüsseln und elektronischen Signieren sowie Schlüsselmanagement-Funktionen. Eine portable, auf C++ basierende Version, wird angestrebt.

## **TOP 8. "Threats to the System, Information System Security and Data Protection" - Video der NHS Management Executive Information Management Group**

Herr Bleumer und Herr Schunter führen das Video vor. Es ist eine sehr elementare Darstellung von Sicherheitsproblemen in Krankenhausinformationssystemen, die sich an Mediziner und Verwaltungsfachleute wendet. Dazu gibt es eine Broschüre "Basic Information Systems Security". Beides ist erhältlich bei

- Kate Woodward
- NHS Information Management Centre
- 15 Frederick Road
- Edgbaston, Birmingham, B15 1JD
- Fax 021 625 1999

Die Arbeitsgruppe ist sich einig, dass ein solches Video auf deutsche Verhältnisse zugeschnitten, wünschenswert, aber nicht mit angemessenem Aufwand herstellbar wäre. Die entsprechende Übertragung der Broschüre ist aber sinnvoll und soll im Rahmen des Muster-sicherheitskonzepts berücksichtigt werden; Zielgruppe: Verwaltungsdirektoren, ärztliche Direktoren und Klinikchefs.

### **TOP 9. Musterkonzept für ein sicheres KIS**

Herr Pommerening hat einen ersten, noch sehr groben Entwurf vorgelegt. Herr Blobel hat einige Ergänzungen verfasst, die den Gruppenmitgliedern aber noch nicht vorliegen. Ferner hat Herr Sauter in einem Schreiben eine Reihe von Verbesserungsvorschlägen, Literaturhinweisen und Anregungen mitgeteilt.

Als weitere zu berücksichtigende Punkte werden in der Diskussion genannt: Eine Erläuterung der Gesetzeslage unter besonderer Berücksichtigung der Schweigepflicht; die derzeitige Umstrukturierung des Gesundheitswesens; die Zuweisung und Delegation von Rollen; die Einbeziehung der Patientenrechte; der Zielkonflikt bei der Auswertung von Audit-Daten; die Anonymisierung von Daten für Forschungszwecke; das "Outsourcing" von Datenverarbeitungsleistungen.

In einem nächsten Schritt wird Herr Blobel ein überarbeitetes Dokument erstellen, das den Gruppenmitgliedern zugestellt wird. Weitere Vorschläge zur Formulierung sollen rechtzeitig vor der nächsten Sitzung der Arbeitsgruppe beim Vorsitzenden eingereicht werden. Das Ziel ist, auf der nächsten Sitzung eine Version zu verabschieden, die auch zur Diskussion in einem breiteren Kreis außerhalb der Arbeitsgruppe geeignet ist.

### **TOP 10. Verschiedenes**

Das nächste Treffen der Arbeitsgruppe soll am 7. und 8. Dezember 1995 in Hildesheim stattfinden.

---

Protokoll: (Prof. Dr. K. Pommerening)

email: [Pommerening@imsd.uni-mainz.de](mailto:Pommerening@imsd.uni-mainz.de)