Das TMF-Datenschutzkonzept für Biomaterialbanken

DGKL 2005 – Jena, 8. Oktober 2005

Klaus Pommerening, IMBEI Universität Mainz

Coautoren: Peter Debold, Regina Becker

Anforderung an die TMF

Aufgabe: *Erstellung eines umfassenden Datenschutzkonzepts für den Betrieb von Biomaterialbanken*.
Konsensfindung mit den Datenschutzbeauftragten des Bundes und der Länder
[repräsentiert durch den AK Wissenschaft].

Ziele:

Möglichst wenig Einschränkung für die wissenschaftliche Nutzung.

- Essenzielles Interesse der medizinischen Forschung.

Möglichst geringe Beeinträchtigung von Persönlichkeitsrechten der Probanden.

- Ausbalancieren der Grundrechte „Forschungsfreiheit“ und „informationelle Selbstbestimmung“.

Zielgröße: Minimierung des Rückidentifizierungsrisikos [= Risiko der unbefugten Zuordnung zum Probanden].

Vorarbeiten

Stellungnahme des NER zu Biobanken –

- relativ liberal zugunsten der Forschung,
- aber z. T. geforderte rechtliche Voraussetzungen (Forschungsgeheimnis) nicht gegeben (und nicht in Sicht).
- Als konkrete Handlungsanleitung zu allgemein.

Generisches Datenschutzkonzept der TMF –

- Konkretes Organisations- und Prozessmodell.
- 2003 verabschiedet mit Votum der Datenschutzbeauftragten.
- Buchveröffentlichung im Druck.
- Erste Revision in Arbeit.
- Übertragung auf BMB als Ansatz sinnvoll.

Musterszenarien für BMB

1. Integration in eine Klinik.
   - Proben aus Behandlungszusammenhang.
   - Nutzung zur Forschung? Weitergabe?
2. BMB als eigenständige Organisation.
   - Zentrale Probensammlung und -verwaltung.
   - Auch kooperative Formen möglich.
3. BMB als Teil eines Forschungsnetzes (krankheitsbezogen).
   - Zentrale Probensammlung
   - oder dezentrale Sammlung mit zentraler Verwaltung
   - oder Verweisliste, zentrale Forschungsdatenbank.

Wie lassen sich die Informationsflüsse jeweils so steuern, dass das Rückidentifizierungsrisiko minimiert wird?

Informatische Werkzeuge zur Lösung

- Informationstrennung – umgesetzt durch die Telematik-Architektur des Netzes –
  - Kontrolle des Rückidentifizierungspotenzials.
  - Verhältnismäßigkeit (je nach Größe und Brisanz der BMB).
- Pseudonymisierung – *„ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.“* [BDSG]
  - Auch mehrstufig.
  - Vorläufig auch noch Anonymisierung.
- Technische Schutzmaßnahmen.
  - Z. B. verschlüsselte Datenübertragung,
  - z. B. Sicherung und Härtung von Servern.

Pseudonymisierung: Das Basismodell

Proben- und Daten-quelle

MDAT

PID

Datenbank oder Auswertung

IDAT

PID

Patientenliste (Identitäts-management)

Datenleck

L85FD23S

Angreifer

IDAT	PID
...	...
Maier, Johannes	6AZCB661
Maier, Josef	KY2P96WA
Maier, Jupp	L85FD23S
...	...

Pseudonymisierung: Das Basismodell (Fortsetzung)

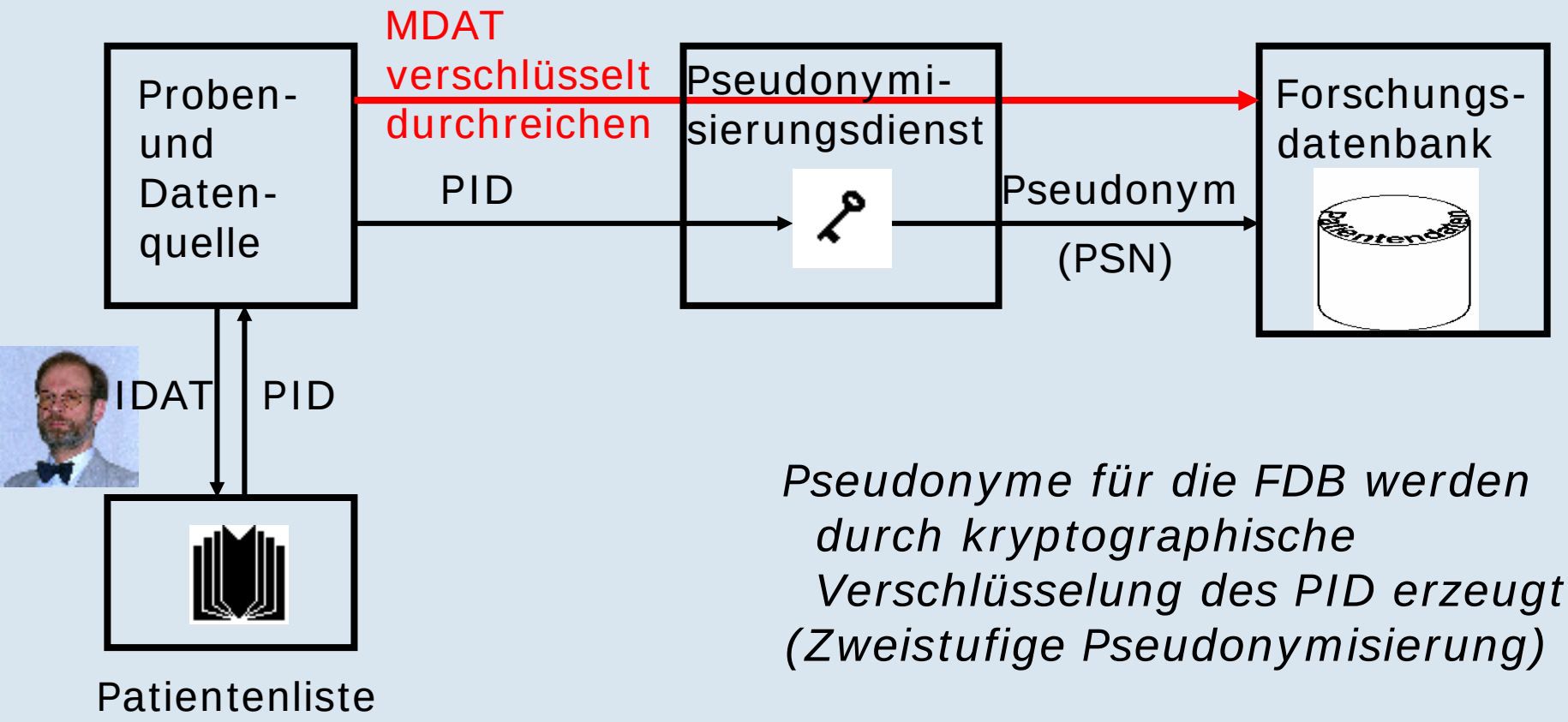
PID-Erzeugung = 1. Stufe der Pseudonymisierung

- *Trennung von IDAT und MDAT,*
  - ausreichend für getrennte Speicherung von identifizierenden Merkmalen nach BDSG;
- *pseudonyme Übermittlung zur Auswertung,*
  - ausreichend für klinische Studien nach AMG
  - und für „kleine“ BMB.

Durch Pseudonymisierung wird die Rückidentifizierung unter kontrollierten Umständen ermöglicht.

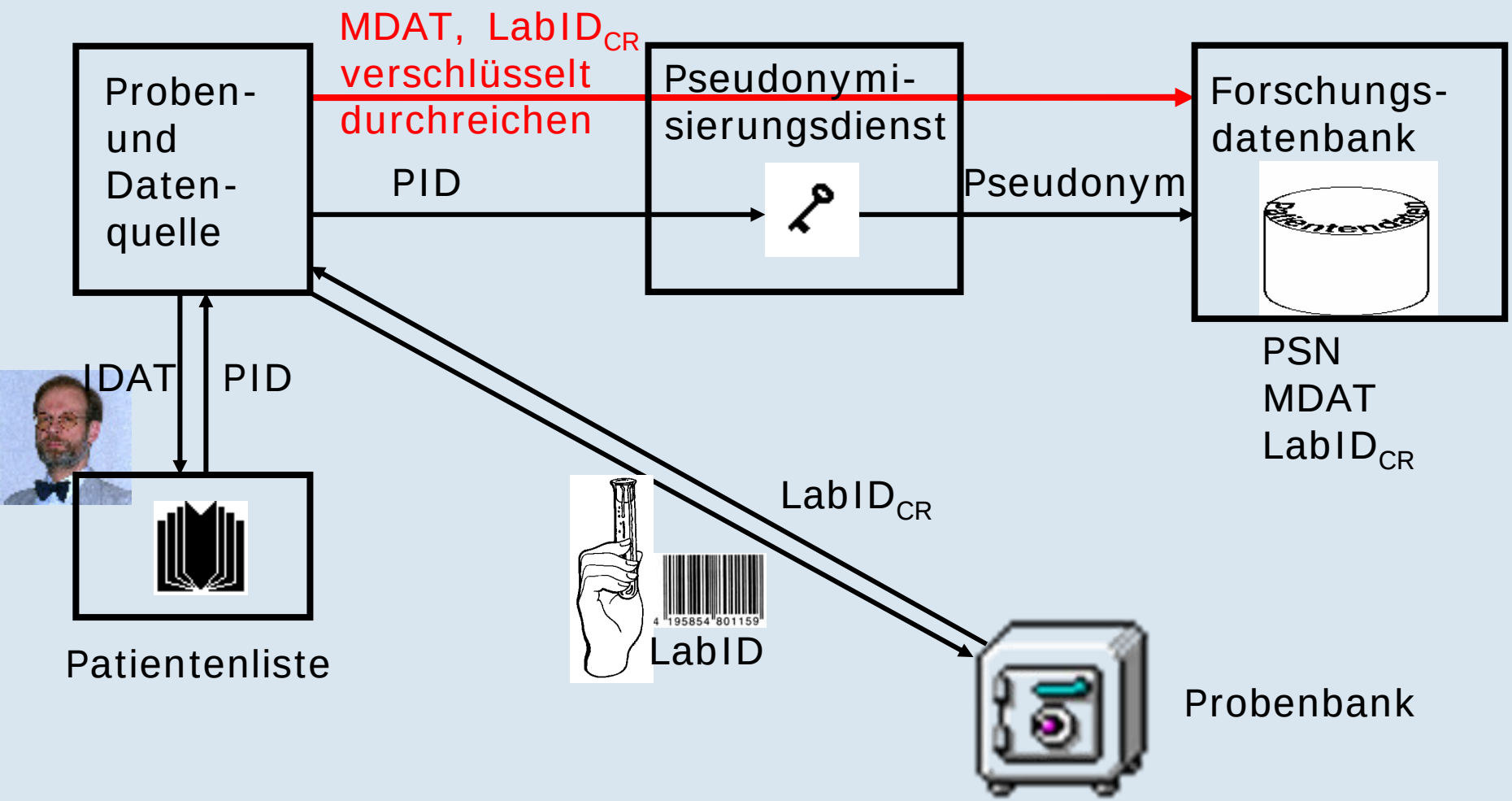
Der Umgang mit pseudonymisierten Daten ist einwilligungspflichtig.

Pseudonymisierung: Modell für Forschungsnetze (nach TMF-Modell B)

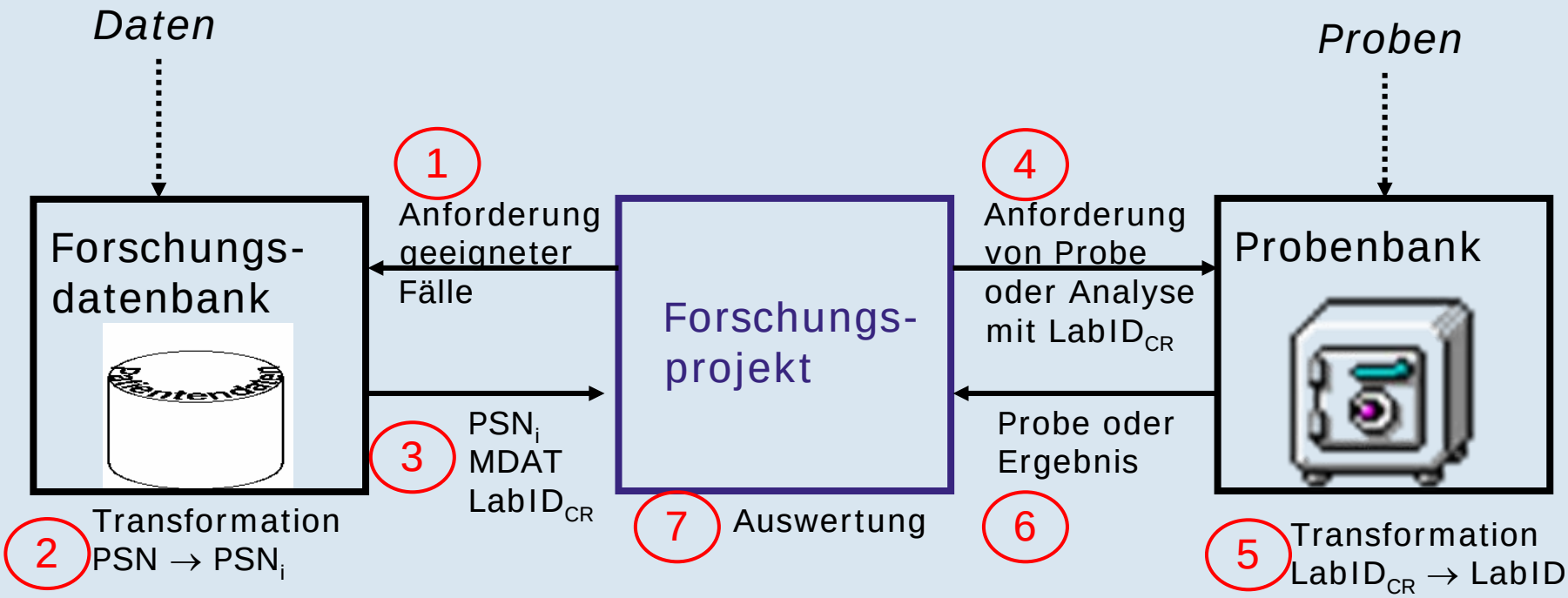


Pseudonyme für die FDB werden durch kryptographische Verschlüsselung des PID erzeugt. (Zweistufige Pseudonymisierung)

Pseudonymisierung: Modell für Forschungsnetze mit Biomaterialbank



Übermittlung von Daten und Proben an Forschungsprojekte



PSN$_i$ = ad-hoc-Pseudonym
(3. Stufe der Pseudonymisierung –
Sinn: *verschiedene Projekte können nicht unabhängig Daten zusammenführen*)

Weitere Elemente des Konzepts

Organisatorische Regelungen

Trennung von Verantwortlichkeiten

Vertragswerke und Nutzungsregelungen (Muster).

- Policies, SOPs.

Entscheidungs- und Überwachungsgremien –

- z. B. „Ausschuss Datenschutz“.

Gestaltung der Einwilligungserklärung.

Diskussion

- Unbestimmtheit der Einwilligungserklärung durch ordnungsgemäßen Betrieb der BMB „kompensiert“.
- Verhältnismäßigkeit des Aufwands,
  z. B. Abstufung der „Treuhänderschaft“ für Identitätsmanagement:
  - getrennte Datenbanktabelle,
  - getrennte Datenhaltung,
  - Notariatsdienst.
- Modulares und skalierbares Konzept.
- Lösungsvorschlag für „Altproben“.
  - Bis auf weiteres anonyme Weitergabe zulässig.
- Workshop mit AK Wissenschaft (Datenschutzbeauftragte) am 17. Oktober 2005.