Institut
für Informatik
Arbeitsgruppe
Kommunikationssysteme

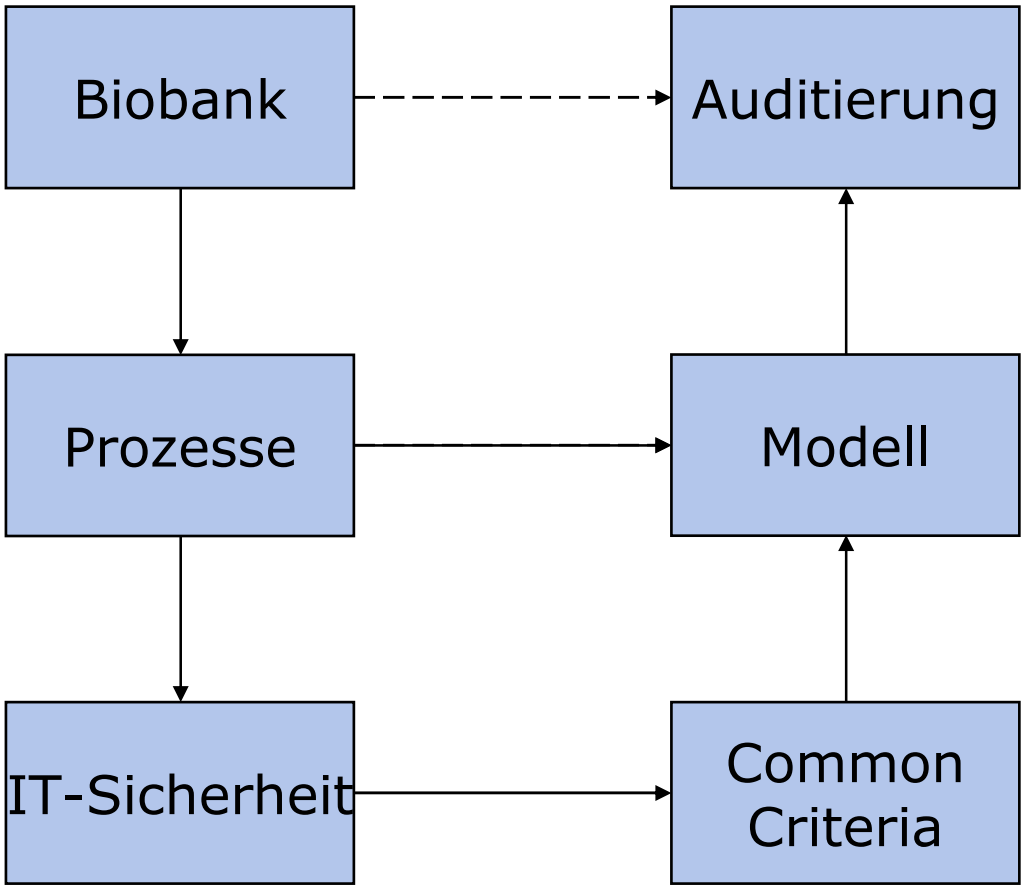
IT-Sicherheit in Biobankprozessen durch Schutzprofile und bewertete De-Identifizierungsverfahren

Ralph Herkenhöner

Arbeitsgruppe Kommunikationssysteme
Institut für Informatik
Christian-Albrechts-Universität zu Kiel

Übersicht

Institut
für Informatik
Arbeitsgruppe
Kommunikationssysteme



Common Criteria

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

Nutzergruppe

Geschäftsmann Hr. G

stellt Sicherheits-Anforderungen

IT-Produkt z.B. DBMS

mein Produkt erfüllt diese Anforderungen

prüft das Produkt

Gutachter

- Idee: Einheitliche Systematik zur Beschreibung und Evaluierung

Common Criteria

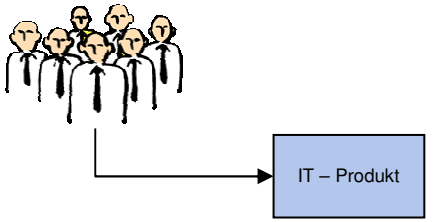
Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

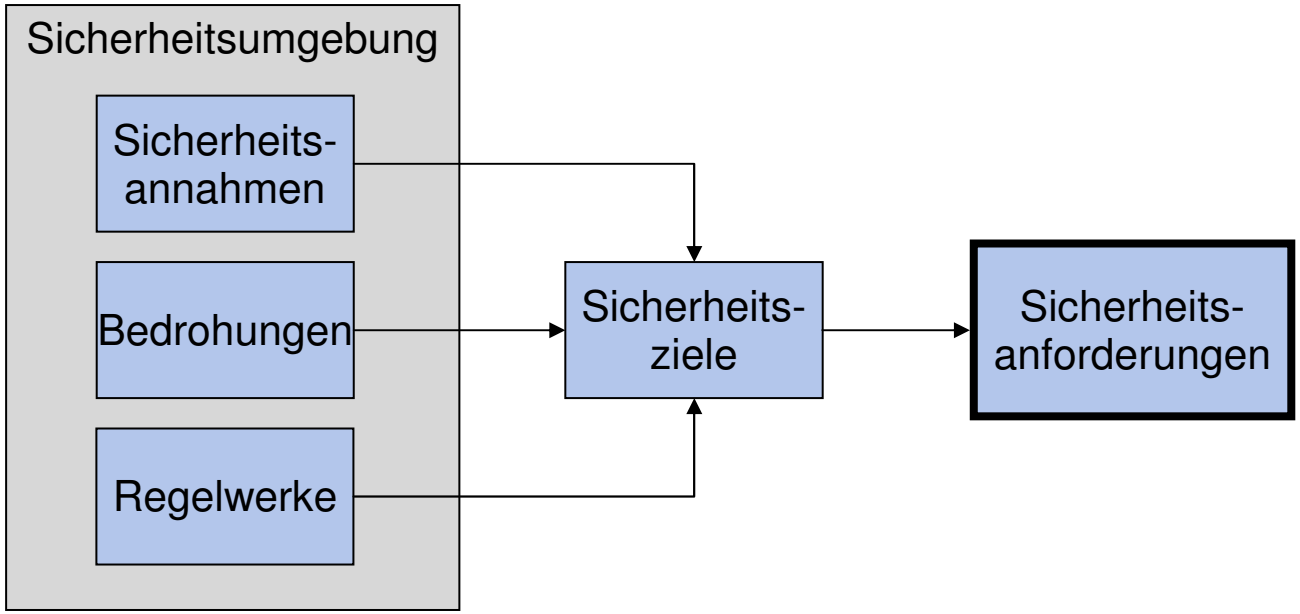
- Bereitstellung von standardisierter Methodik, Dokumentenstruktur und Sprache zum
  - Erstellen von implementierungsunabhängigen Schutzprofilen (*Protection Profiles, PPs*)
  - Erstellen von spezifischen, produktabhängigen Schutzzielen (*Security Targets, STs*)
  - Prüfen von Gegenständen gegen PPs bzw. STs (*Evaluation*)
- nachvollziehbare Evaluationsvorgänge
- ausschließlich textuelle Beschreibungsmethodik
- stark Technik-bezogen

Common Criteria – Protection Profile

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

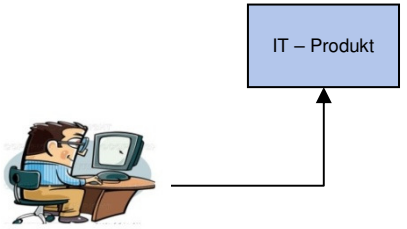
- adressiert eine Gruppe von evaluierbaren IT-Produkten (z.B. Datenbanksysteme)





Common Criteria – Evaluation

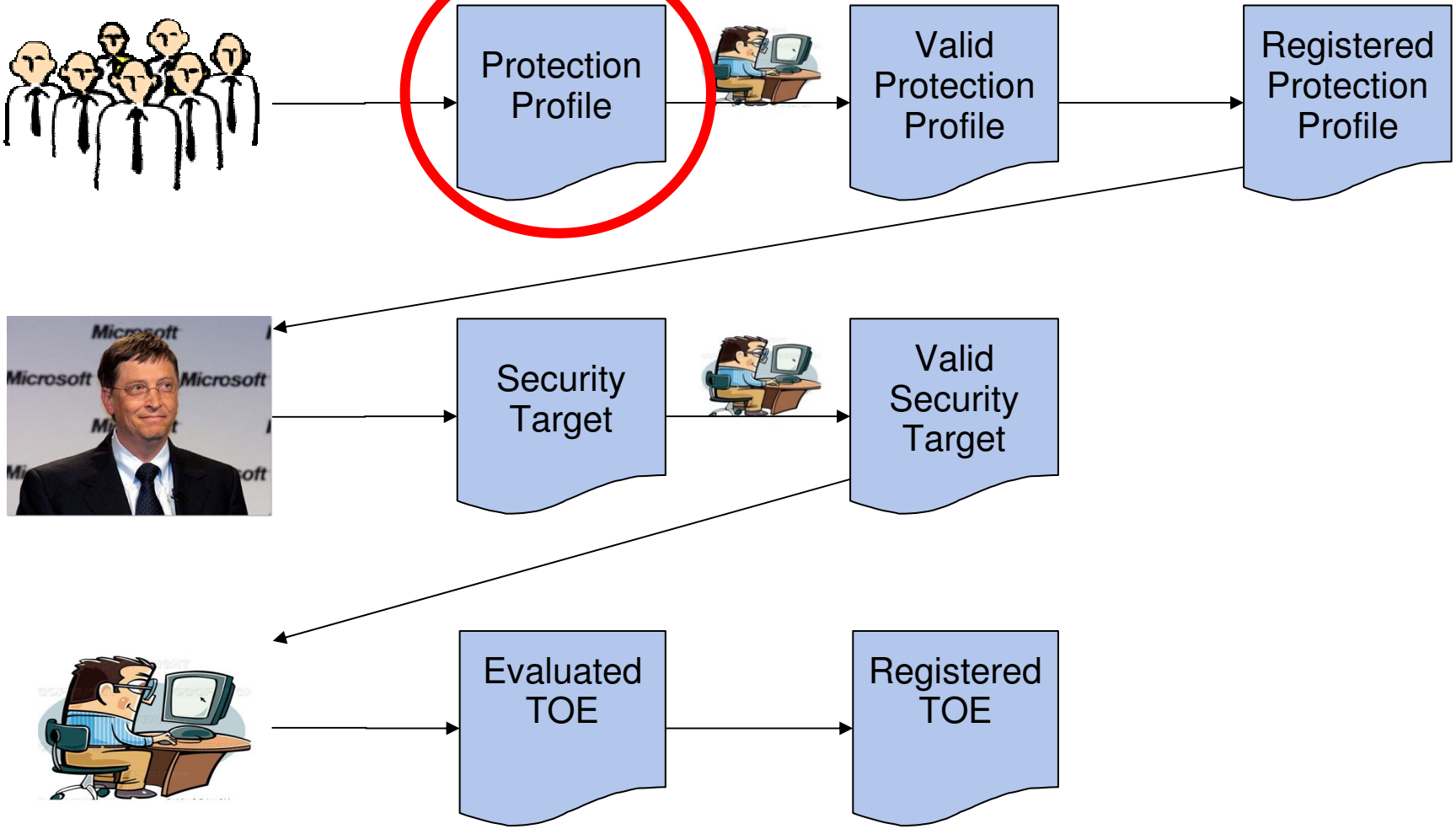
Institut für Informatik
Arbeitsgruppe Kommunikationssysteme



- formale Prüfung eines Evaluierungsgegenstandes (*Target of Evaluation*) gegen PP bzw. ST
- nur durch akkreditierte Stellen (z.B. BSI)
- Methodik und Umfang der Prüfung
  - bereits durch Protection Profile bzw. Security Target festgelegt
  - erfolgt in einer von 7 Vertrauenswürdigkeitsstufen (*Evaluation Assurance Level*)
    - Stufe 1: "functionally tested"
    - Stufe 2: "structurally tested"
    - Stufe 3: "methodically tested and checked"
    - Stufe 4: "methodically designed, tested and reviewed"
    - Stufe 5: "semiformally designed and tested"
    - Stufe 6: "semiformally verified design and tested"
    - Stufe 7: "formally verified design and tested"
  - Stufe wird im Zertifikat genannt, z.B. EAL4

Common Criteria – Evaluierungsprozess

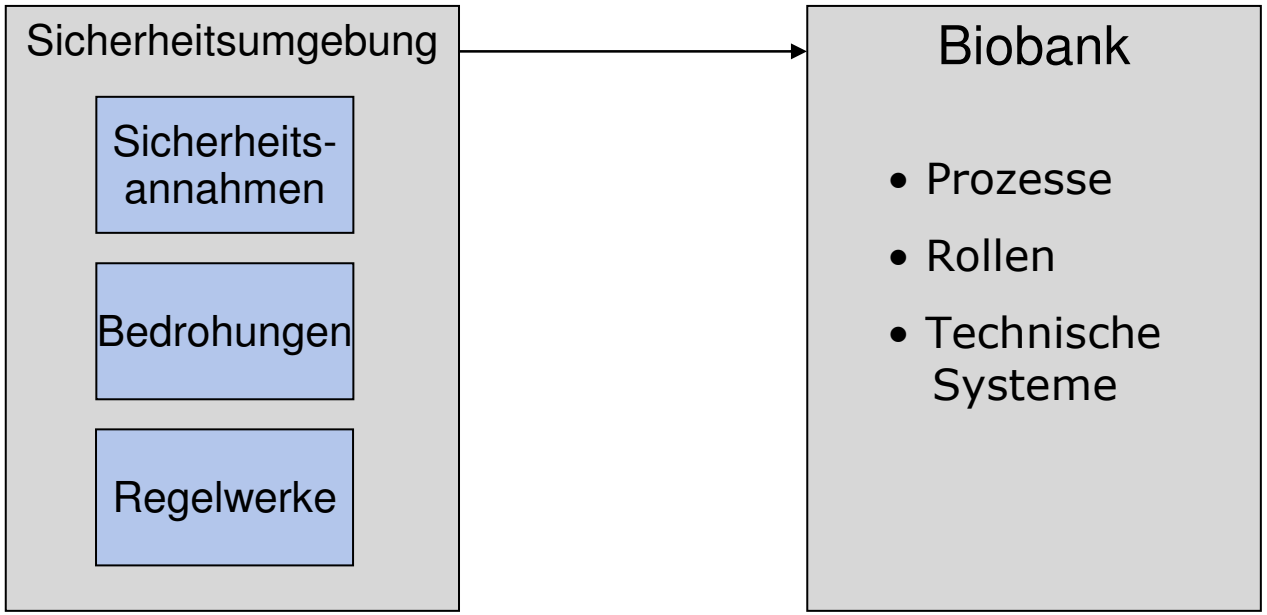
Institut für Informatik
Arbeitsgruppe Kommunikationssysteme



TOE=Target of Evaluation

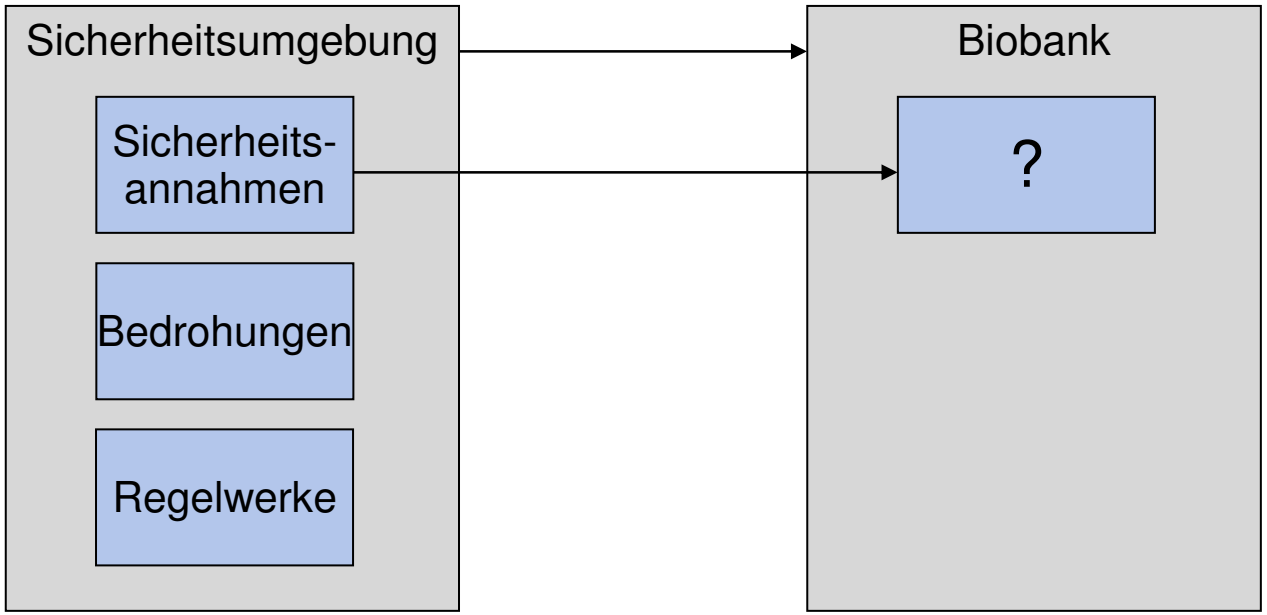
Schutzprofil einer Biobank (1)

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme



Schutzprofil einer Biobank (2)

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme



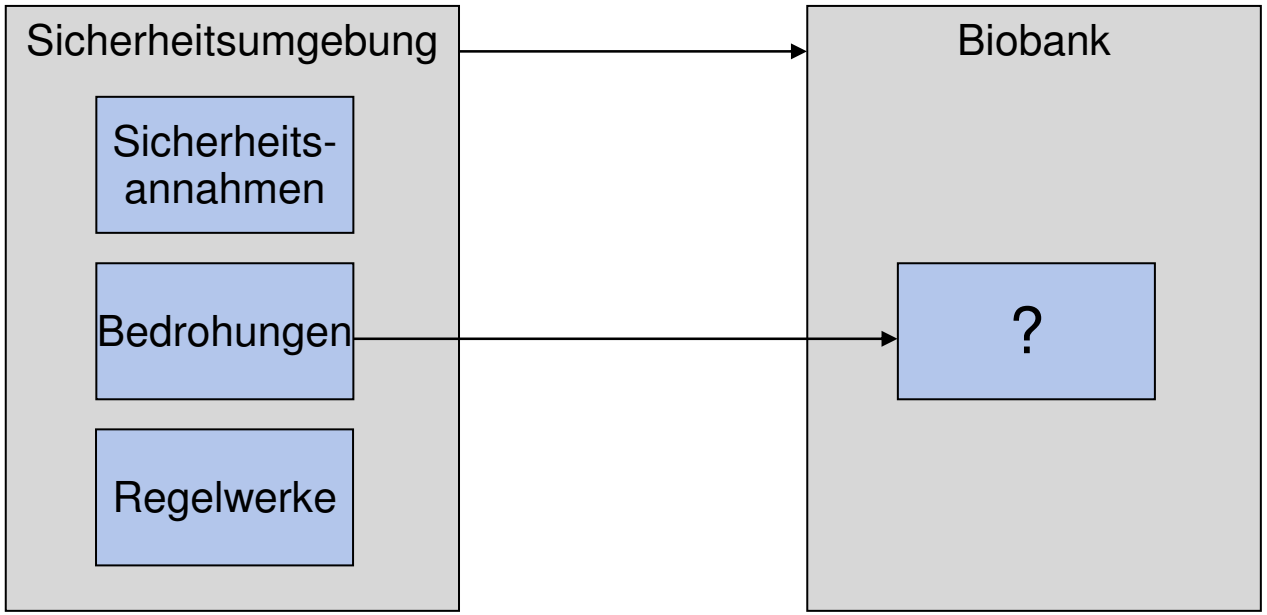
Schutzprofil einer Biobank (3)

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

- Sicherheitsannahmen
  - Zutrittskontrolle
  - Materielle Sicherheit
  - Umsetzen und Durchsetzen der SOPs und Policys

Schutzprofil einer Biobank (4)

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme



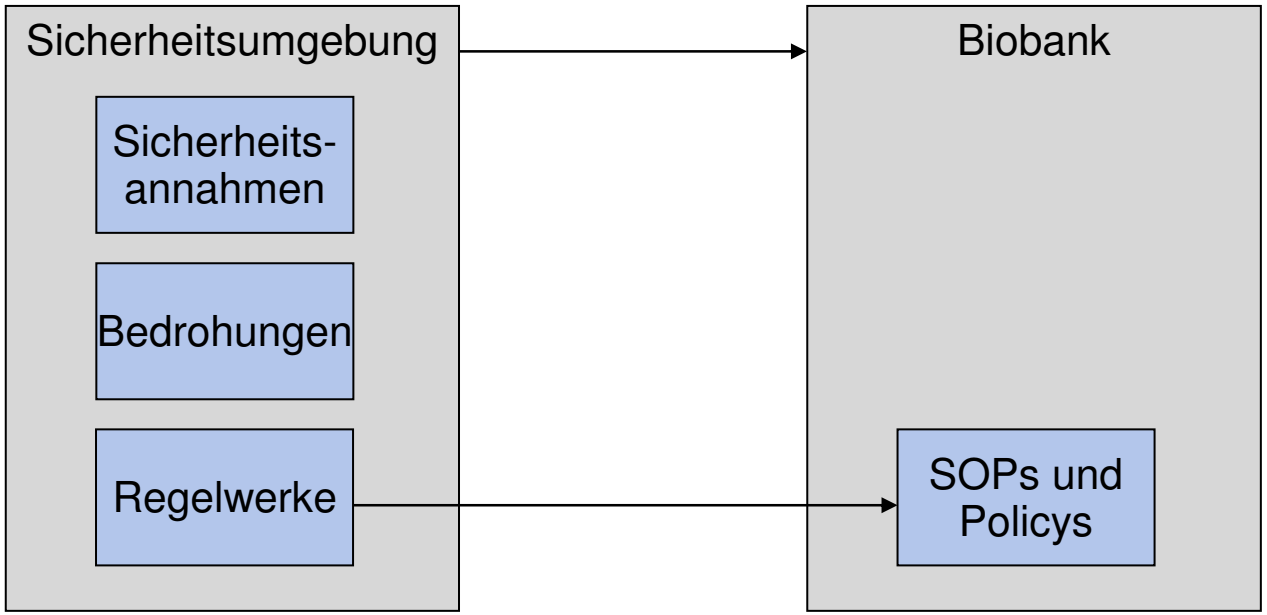
Schutzprofil einer Biobank (5)

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

- Bedrohungen
  - Unbefugter Zutritt/Zugang/Zugriff
  - Systemfehler, Systemabsturz, Nicht-Verfügbarkeit
  - Fehlerhafte oder unzureichende Protokollierung
  - Manipulation oder Fehlbedienung
  - Wiederherstellung von zu löschenden Daten
  - Unbefugte Re-Identifizierung

Schutzprofil einer Biobank (4)

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme



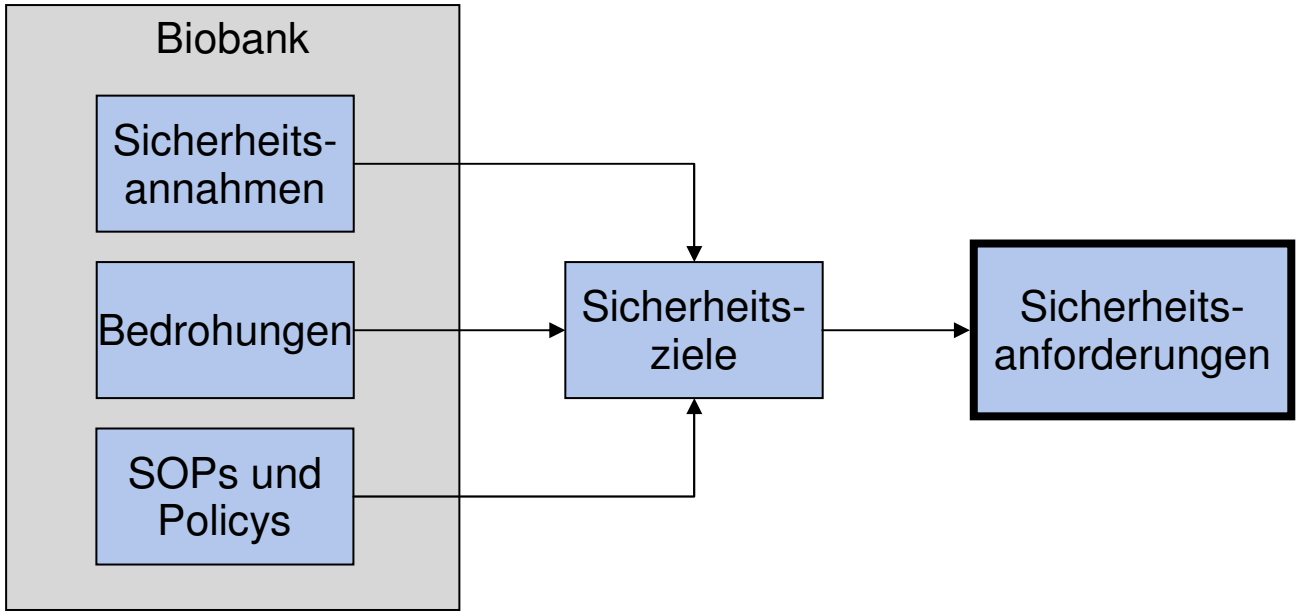
Schutzprofil einer Biobank (5)

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

- SOPs und Policys
  - IT-Sicherheit und Datenschutz als
    - Managementaufgabe
    - Teilprozesse
  - Gesetzeskonformes Handeln
    - Datensparsamkeit und De-Identifizierung
    - Umsetzen der materiellen Datentreuhänderschaft
  - Schutz von Daten und Ressourcen durch
    - Verantwortungsbereiche
    - Festschreibung von Notfallregeln
    - Anpassung und Weiterführung der SOPs und Policys

Schutzprofil einer Biobank (6)

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme



Schutzprofil einer Biobank (7)

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

- Sicherheitsanforderungen
  - Sicherheitsprotokollierung (FAU)
  - Nachweisbarkeit der Kommunikation (FCO)
  - Kryptographische Unterstützung (FCS)
  - Schutz der Spenderdaten (FDP)
  - Identifizierung und Authentisierung (FIA)
  - Sicherheitsmanagement (FMT)
  - Schutz vor Re-Identifizierung (FPR)
  - Schutz der Sicherheitsfunktionen (FPT)
  - Zugriffskontrolle (ZTA)
  - Vertrauenswürdiger Pfad/Kanal (FTP)

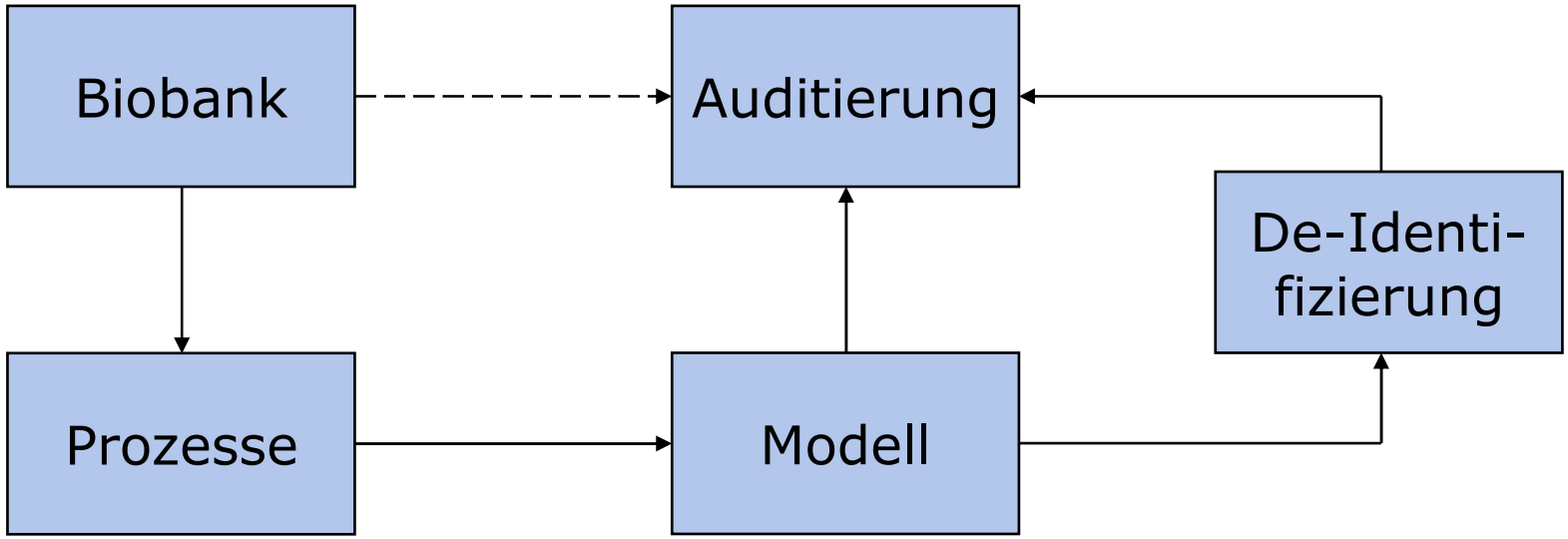
Schutzprofil einer Biobank (7)

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

- Vertrauenswürdigkeitsstufe: EAL 4
  - methodisch entwickelt, getestet und durchgesehen
  - Architekturentwurf (ADV_INT)
    → Selbstbeschreibung der Biobank (z.B. in UML/UMLsec)
  - Integrierte Fehlerbehebung (ALC_FLR)

Übersicht

Institut
für Informatik
Arbeitsgruppe
Kommunikationssysteme



Risiko der Identifizierung

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

- Bei Anonymisierung
  - Größe der Anonymitätsmenge
  - Grad der Anonymisierung
    - Identifizierende Eigenschaft
    - (Zusatz-)Wissen der Beteiligten
- Bei Pseudonymisierung
  - wie Anonymisierung, aber zusätzlich:
    - Qualität der Pseudonyme
    - Verarbeitung der Verkettungsregeln

Größe der Anonymitätsmenge

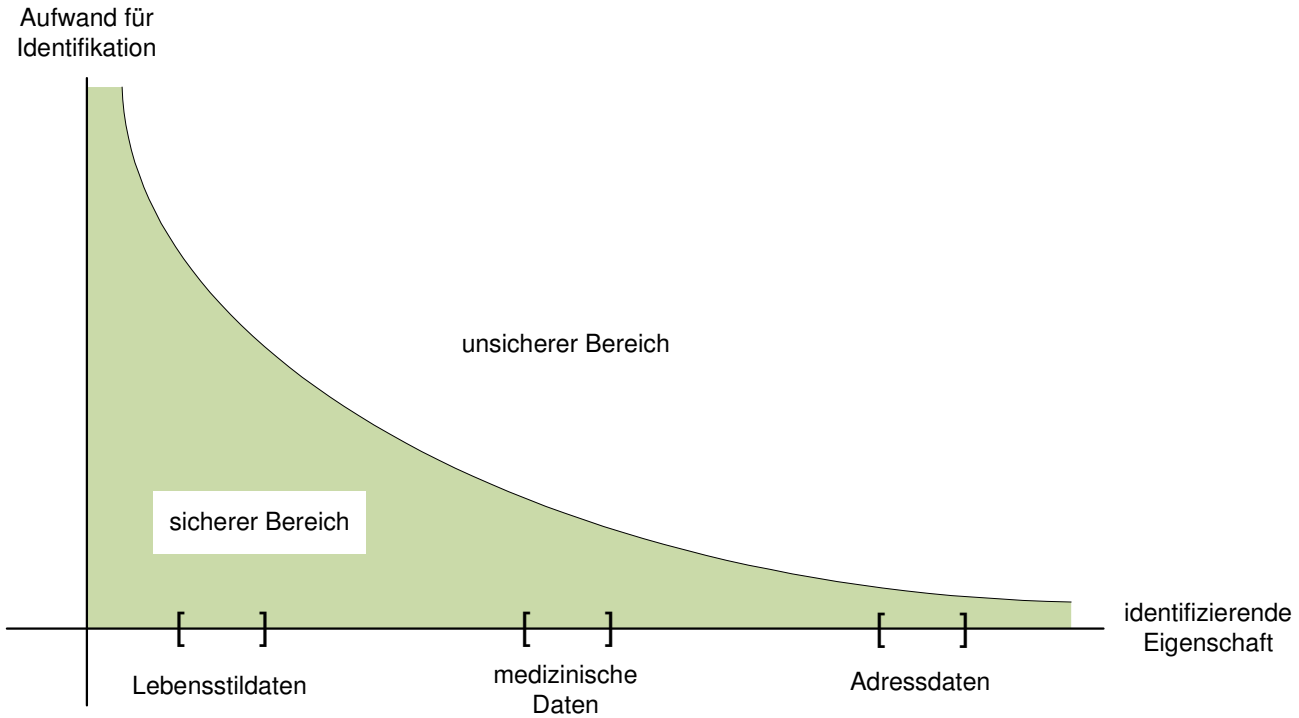
Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

- Maximal: Anzahl der Spender oder Spendefälle
- Herausgabefall: Anzahl der herausgegebenen Datensätze (bzw. Proben)
- Risiko: kleine Herausgabemenge
- Gegenmaßnahme: mindest Herausgabemenge

Grad der Anonymisierung – Identifizierende Eigenschaften

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

- Risiko: schwer abschätzbar
- Gegenmaßnahme: datensparsame Weitergabe



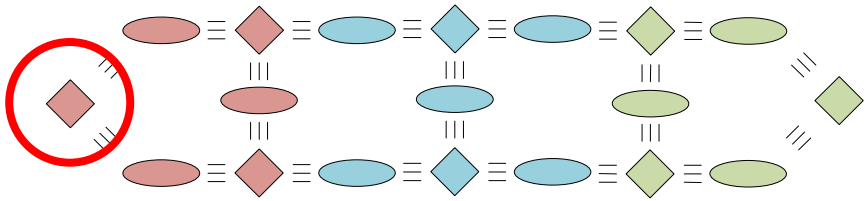
Grad der Anonymisierung – (Zusatz)-Wissen der Beteiligten (1)

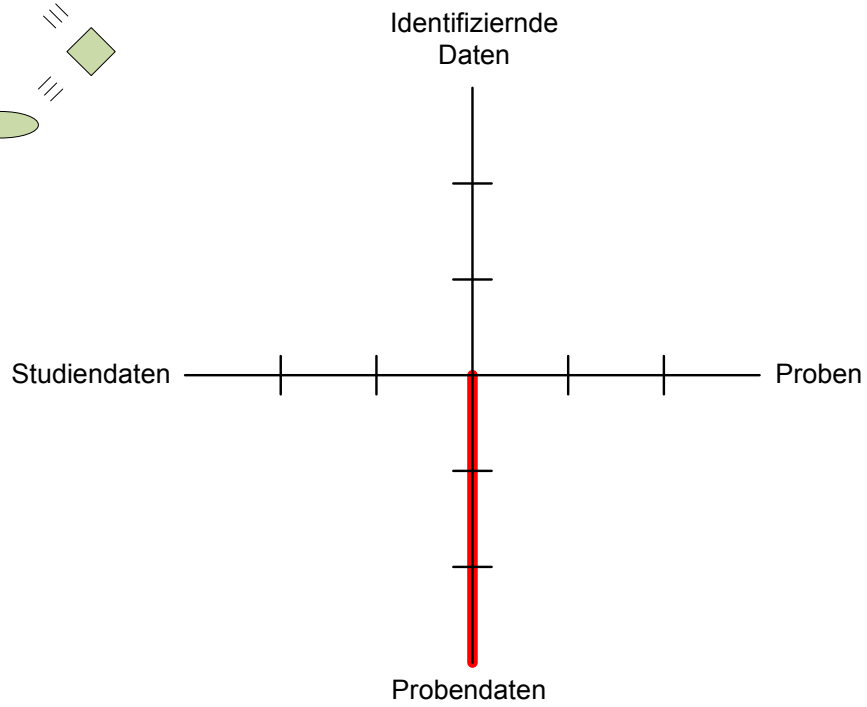
Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

- 5 Wissensquellen:
  - Identifizierende Daten
  - Studiendaten
  - Proben
  - Probendaten (insbes.: genetische Daten)
  - Verkettungsregeln

Grad der Anonymisierung – (Zusatz)-Wissen der Beteiligten (2)

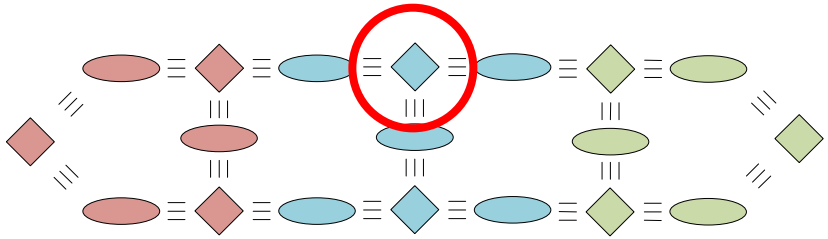
Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

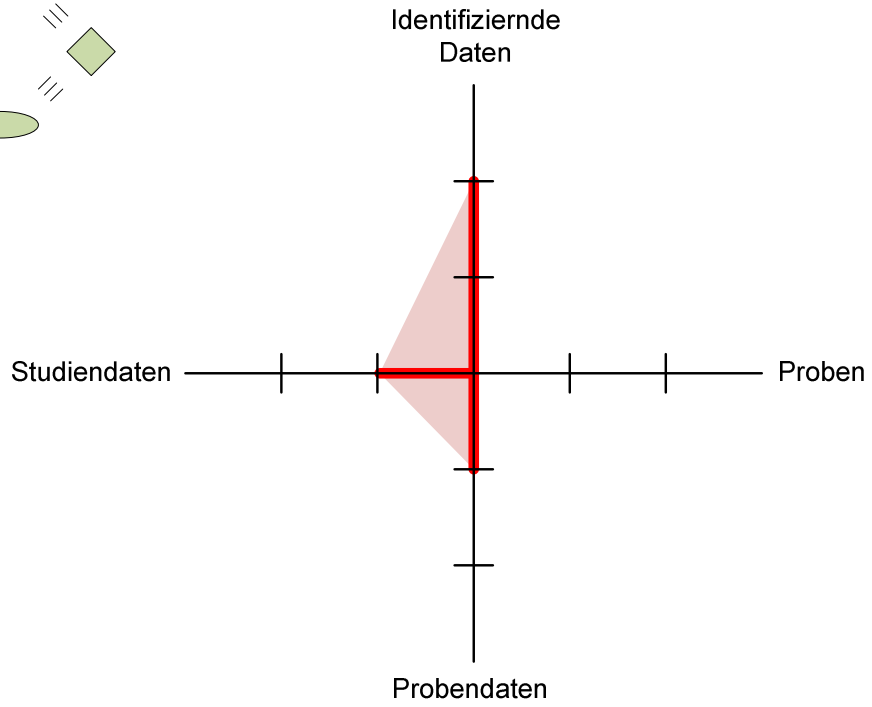




Grad der Anonymisierung – (Zusatz)-Wissen der Beteiligten (3)

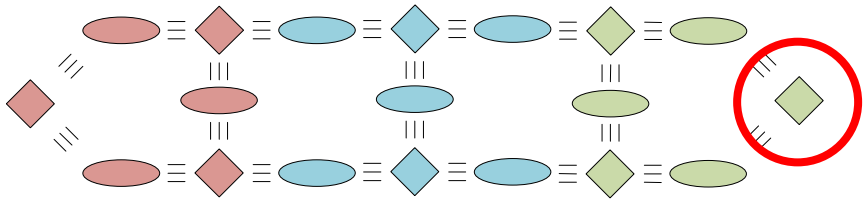
Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

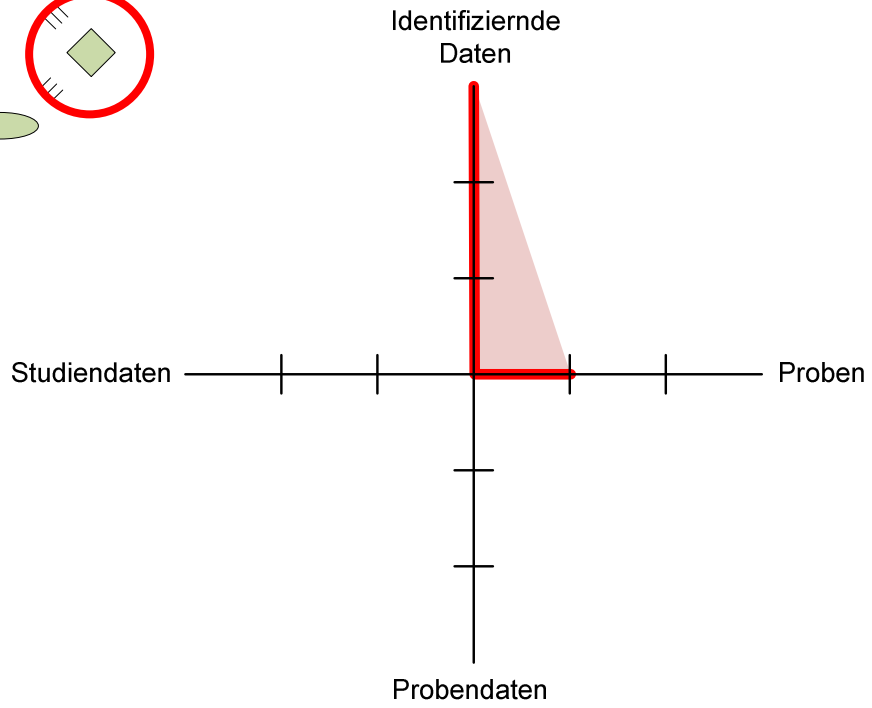




Grad der Anonymisierung – (Zusatz)-Wissen der Beteiligten (4)

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme





Pseudonymisierung – Qualität der Pseudonyme

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

- Risiko: Pseudonym enthält Hinweise auf die Verkettungsregel
  - Bildungsregel basiert auf identifizierenden Daten
    - z.B. Sozialversicherungsnummer
  - Bildungsregel basiert auf der Verarbeitung
    - z.B. Rechnungsnummer
- Gegenmaßnahme: Zufallsbasierte Bildungsvorschrift

Pseudonymisierung – Verarbeitung der Verkettungsregeln

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

- Risiko: Existenz der Verkettungsregel
- Gegenmaßnahme:
  - Speicherung der Verkettungsregel vermeiden
  - Verkettungsregeln an unabhängiger Stelle verwalten (nicht bei der Proben-/Daten-verarbeitenden Stelle)
  - Kontrolliertes Abrufen der Verkettung

Fazit

- Evaluation der IT-Sicherheit nach Common Criteria
  - Schutzprofil einer Biobank (EAL 4)
  - anschlussfähig zur Selbstbeschreibung in UML/UMLsec
- Bewertung von De-Identifizierung
  - Größe der Anonymitätsmenge
  - Grad der Anonymität
  - Pseudonymbildungsvorschrift
  - Verkettungsregeln