

› Datentreuhänder

GECKO Institut – Hochschule Heilbronn

Datentreuhänder Heilbronn

- GECKO Institut für Medizin, Informatik und Ökonomie
 - Projekte mit Universitäts- und anderen Kliniken, wissenschaftlichen Einrichtungen und der Industrie
- Datentreuhänder Heilbronn
 - Historie: Pseudonymisierungsdienst entwickelt für Research Data Warehouse der Abteilung Kardiologie, Angiologie und Pneumologie am Universitätsklinikum Heidelberg (2012).
 - Aktuell: Beratung in externen Projekten, Datentreuhänder für standortübergreifende Abfragen im MII HiGHmed Konsortium.

Pseudonymisierungsdienst

Übersicht

- Typischer Anwendungsfall
 - Nutzung von Behandlungsdaten mit Hilfe von Data Repositories in der klinischen Forschung
 - RecordLinkage Problem gelöst mittels zentraler IDs (ISH Patientenummer), MPI, Mainzliste, etc.
 - Datenfluss (Datenquellen:Datensenken): 1:1, 1:n, m:1, m:n
 - Unterschiedliche Pseudonyme je Anwendungsfall / Studie / Datensenke
 - Keine Übertragung der medizinischen Daten an den Datentreuhänder
 - Keine persistente Speicherung von IDs und Pseudonymen

Pseudonymisierungsdienst - Demo

Versorgung

ID	Gewicht	Temperatur	Syst. Blutdruck	Diast. Blutdruck
3678403	58	37,8	177	80
3678404	104	36,2	173	97
3678405	74	36,5	159	101
3678406	97	36,8	160	87
3678407	60	36,7	162	104
3678408	47	37	155	96

Forschung



Datentreuhänder (PS)

1 - Start

Identifizierte Daten im Versorgungskontext
IDAT + MDAT

Pseudonymisierungsdienst - Demo

Versorgung

Gewicht	Temperatur	Syst. Blutdruck	Diast. Blutdruck
58	37,8	177	80
104	36,2	173	97
74	36,5	159	101
97	36,8	160	87
60	36,7	162	104
47	37	155	96

Forschung



ID
3678403
3678404
3678405
3678406
3678407
3678408



Datentreuhänder (PS)

2

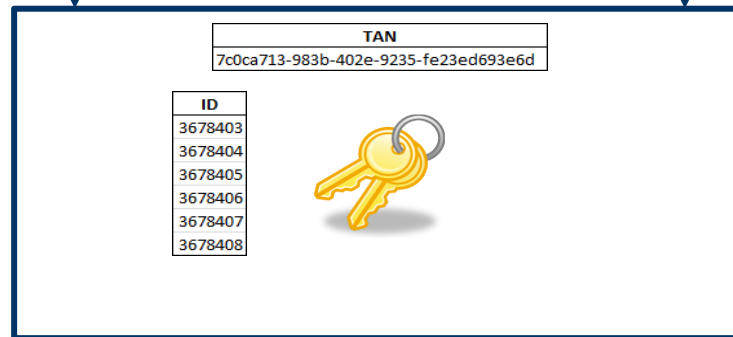
Übermittlung IDAT zum Datentreuhänder

Pseudonymisierungsdienst - Demo

Versorgung

Gewicht	Temperatur	Syst. Blutdruck	Diast. Blutdruck
58	37,8	177	80
104	36,2	173	97
74	36,5	159	101
97	36,8	160	87
60	36,7	162	104
47	37	155	96

Forschung



Datentreuhänder (PS)

3

Empfang IDAT
Generierung einer Transaktionsnummer (TAN)

Pseudonymisierungsdienst - Demo

Versorgung

Gewicht	Temperatur	Syst. Blutdruck	Diast. Blutdruck
58	37,8	177	80
104	36,2	173	97
74	36,5	159	101
97	36,8	160	87
60	36,7	162	104
47	37	155	96


Forschung



TAN

7c0ca713-983b-402e-9235-fe23ed693e6d

ID
3678403
3678404
3678405
3678406
3678407
3678408



PSN
AF6421B307
54CBDE34AA
1498A563D4
A7B3CD23D1
143AB49E12
FF12A43921

Datentreuhänder (PS)

4

*Pseudonymisierung der IDAT
Verschlüsselung mit Projekt-Schlüssel*

Pseudonymisierungsdienst - Demo


Versorgung

Gewicht	Temperatur	Syst. Blutdruck	Diast. Blutdruck
58	37,8	177	80
104	36,2	173	97
74	36,5	159	101
97	36,8	160	87
60	36,7	162	104
47	37	155	96

Forschung



TAN
7c0ca713-983b-402e-9235-fe23ed693e6d



PSN
Af6421B307
54CBDE34AA
1498A563D4
A7B3CD23D1
143AB49E12
FF12A43921

Datentreuhänder (PS)

5

Löschen der IDAT

Temporäre Speicherung der PSN (nicht persistent)

Pseudonymisierungsdienst - Demo


Versorgung

Gewicht	Temperatur	Syst. Blutdruck	Diast. Blutdruck
58	37,8	177	80
104	36,2	173	97
74	36,5	159	101
97	36,8	160	87
60	36,7	162	104
47	37	155	96

Forschung



TAN
7c0ca713-983b-402e-9235-fe23ed693e6d



PSN
AF6421B307
54CBDE34AA
1498A563D4
A7B3CD23D1
143AB49E12
FF12A43921

Datentreuhänder (PS)

6

Antwort des Datentreuhänders
Transaktionsnummer (TAN)

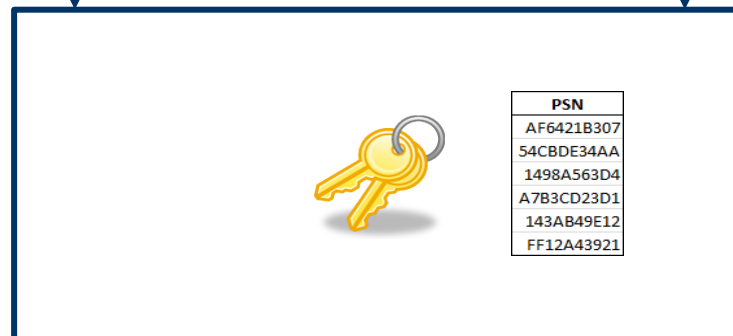
Pseudonymisierungsdienst - Demo

Versorgung

Gewicht	Temperatur	Syst. Blutdruck	Diast. Blutdruck
58	37,8	177	80
104	36,2	173	97
74	36,5	159	101
97	36,8	160	87
60	36,7	162	104
47	37	155	96

TAN
7c0ca713-983b-402e-9235-fe23ed693e6d

Forschung



Datentreuhänder (PS)

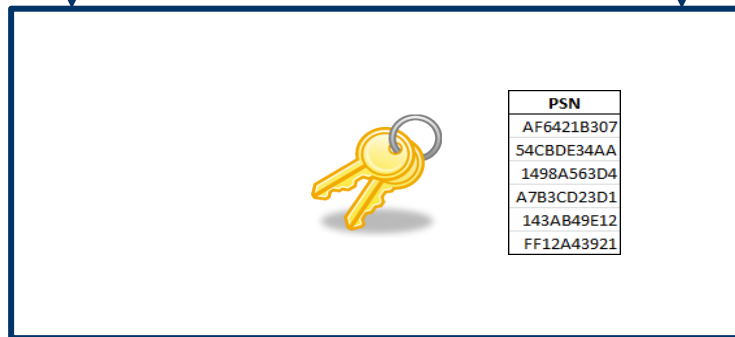
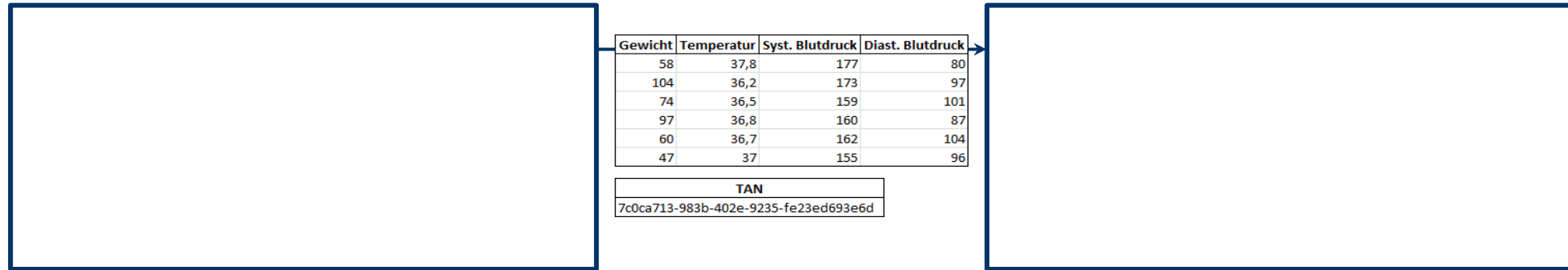
7

Empfang TAN

Pseudonymisierungsdienst - Demo

Versorgung

Forschung



Datentreuhänder (PS)

8

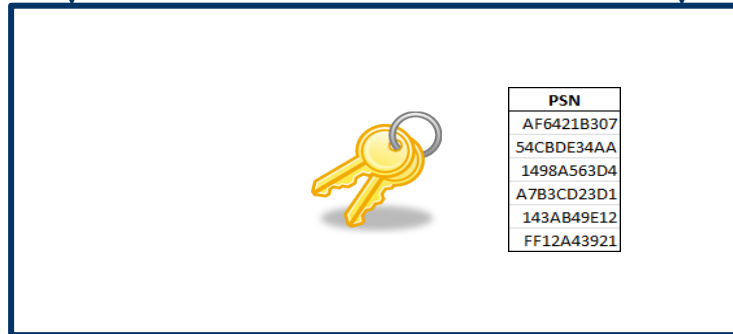
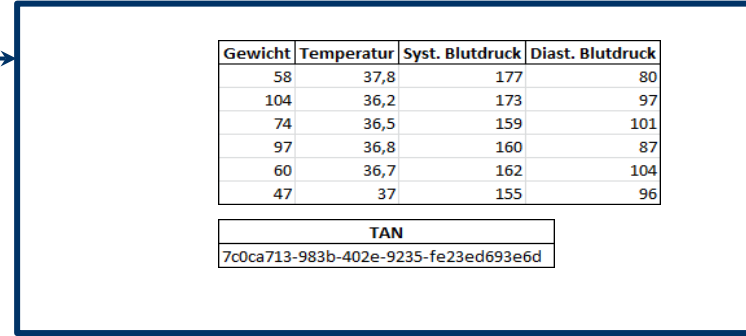
Übermittlung von MDAT und TAN in Richtung Forschungskontext

Pseudonymisierungsdienst - Demo

Versorgung



Forschung



Datentreuhänder (PS)

9

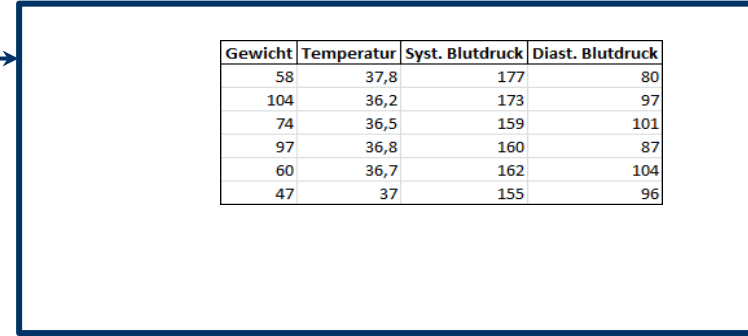
Empfang MDAT und TAN

Pseudonymisierungsdienst - Demo

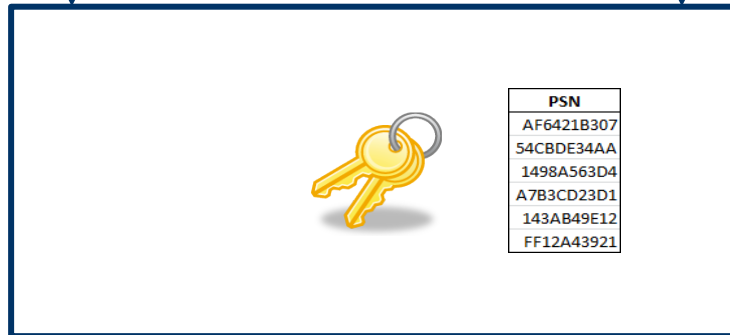
Versorgung



Forschung



TAN
7c0ca713-983b-402e-9235-fe23ed693e6d



Datentreuhänder (PS)

10

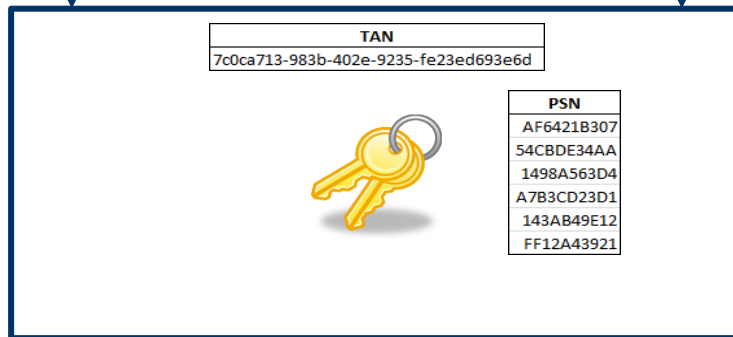
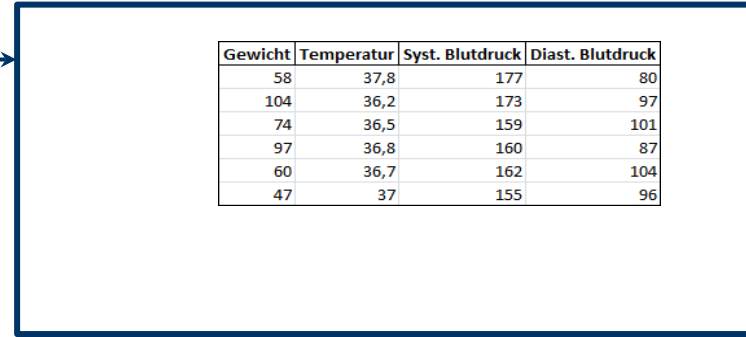
Abruf der Pseudonyme (PSN) mit TAN

Pseudonymisierungsdienst - Demo

Versorgung



Forschung



Datentreuhänder (PS)

11

Empfang TAN

Pseudonymisierungsdienst - Demo

Versorgung



Forschung

Gewicht	Temperatur	Syst. Blutdruck	Diast. Blutdruck
58	37,8	177	80
104	36,2	173	97
74	36,5	159	101
97	36,8	160	87
60	36,7	162	104
47	37	155	96

PSN
AF6421B307
54CBDE34AA
1498A563D4
A7B3CD23D1
143AB49E12
FF12A43921



Datentreuhänder (PS)

12

Antwort des Datentreuhänders
Pseudonyme (PSN)

Pseudonymisierungsdienst - Demo

Versorgung



Forschung

PSN	Gewicht	Temperatur	Syst. Blutdruck	Diast. Blutdruck
AF6421B307	58	37,8	177	80
54CBDE34AA	104	36,2	173	97
1498A563D4	74	36,5	159	101
A7B3CD23D1	97	36,8	160	87
143AB49E12	60	36,7	162	104
FF12A43921	47	37	155	96



Datentreuhänder (PS)

13 - Ende

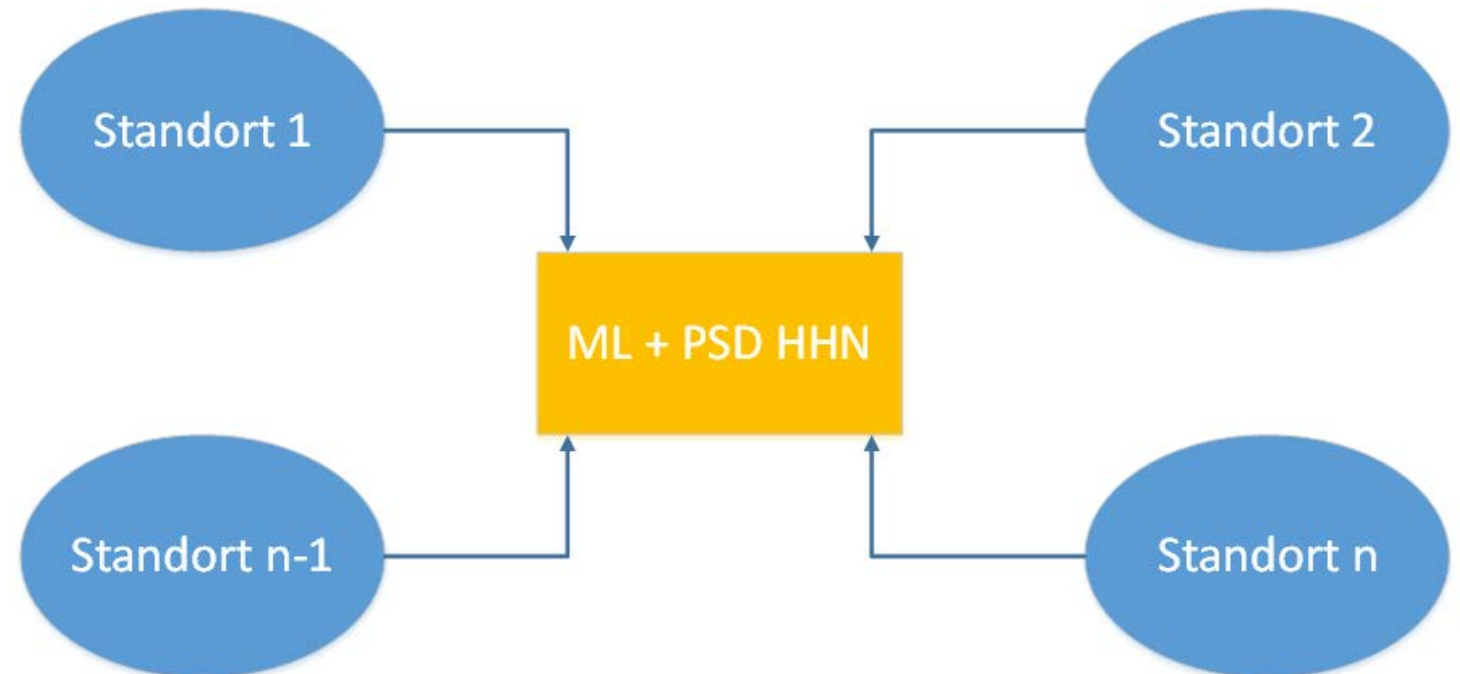
Pseudonymisierte Daten im Forschungskontext

Pseudonymisierungsdienst Technik

- Pseudonymisierung mittels symetrischer Verschlüsselung
 - AES-256, CBC
 - Schlüssel und statischer Initialisierungsvektor pro Anwendungsfall
- Kommunikation
 - Rest-Interface, HTTP über TLS 1.2 / 1.3
 - Authentifikation: Client und Server Zertifikate, Eigene Root-CA, Cert.Pining.
- Daten
 - Keine persistente Speicherung der IDAT, MDAT und PSN beim Datentreuhänder
- Alle Aktionen durch Audit-Logs nachvollziehbar

HiGHmed: Diskussionsstand Mainzelliste + PSD Heilbronn

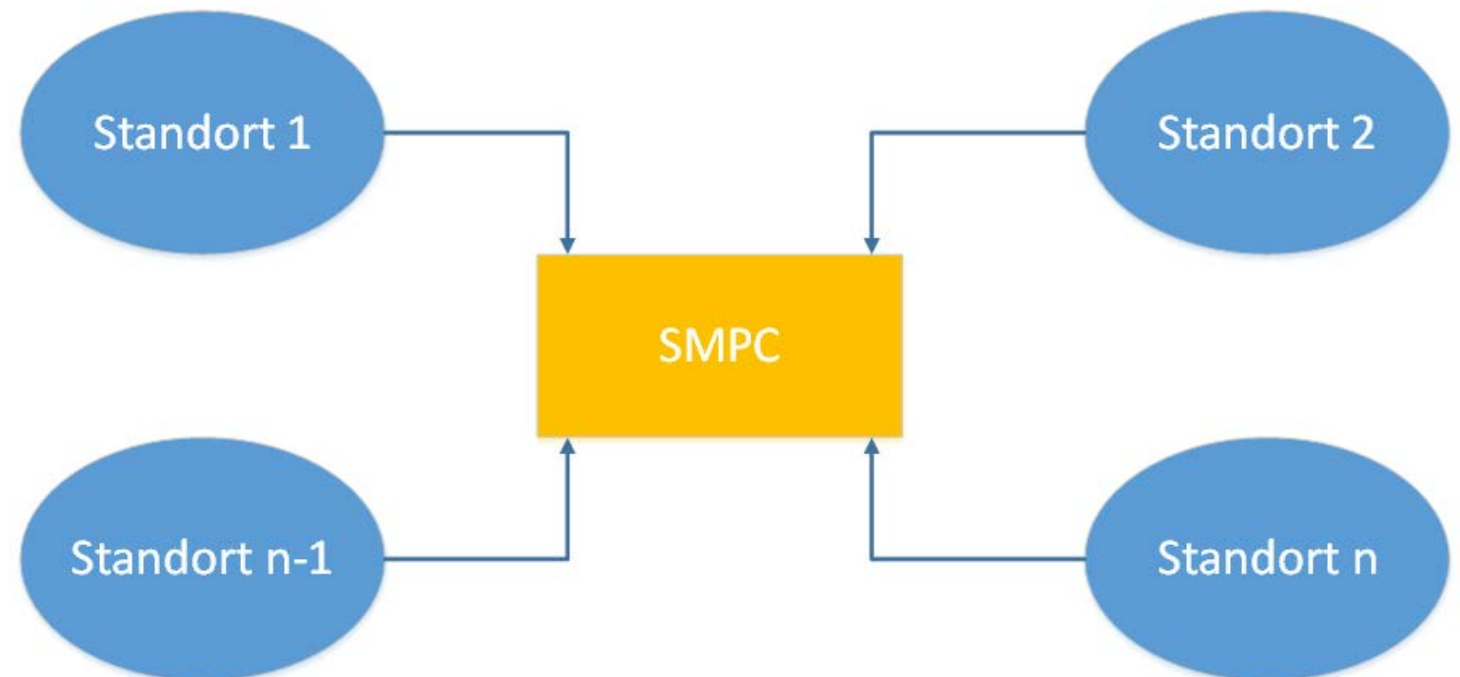
- Datentreuhänder für standortübergreifende Abfragen
- On Demand Pseudonymisierung pro Projekt
- RecordLinkage: Mainzelliste
- Projektspezifische Pseudonyme: PSD HHN



Für die HiGHmed AG Datenschutz
M.Lablans, P.Werner, H.Hund

HiGHmed: Diskussionsstand Secure Multiparty Computation

- RecordLinkage mittels Secure Multiparty Computation
- Forschungsfrage in HiGHmed
- Offene Frage: N-Standorte



Für die HiGHmed AG Datenschutz
M.Lablans, P.Werner, H.Hund