
Pseudonymisierungskonzept der QuaSi-Niere gGmbH

Henrik Fahlke, QuaSi-Niere gGmbH

Aufteilung des Vortrags

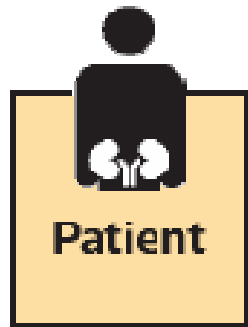
Pseudonymisierungskonzept

1. **Beteiligte und deren Aktivitäten**
2. **Pseudonymisierung beim Datentreuhänder**
3. **Chipkarteneinsatz**

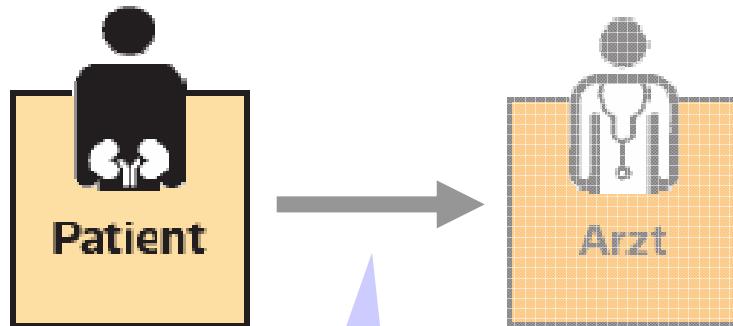
Teil 1

Beteiligte und deren Aktivitäten

Beteiligte am QuaSi-Niere-Verfahren



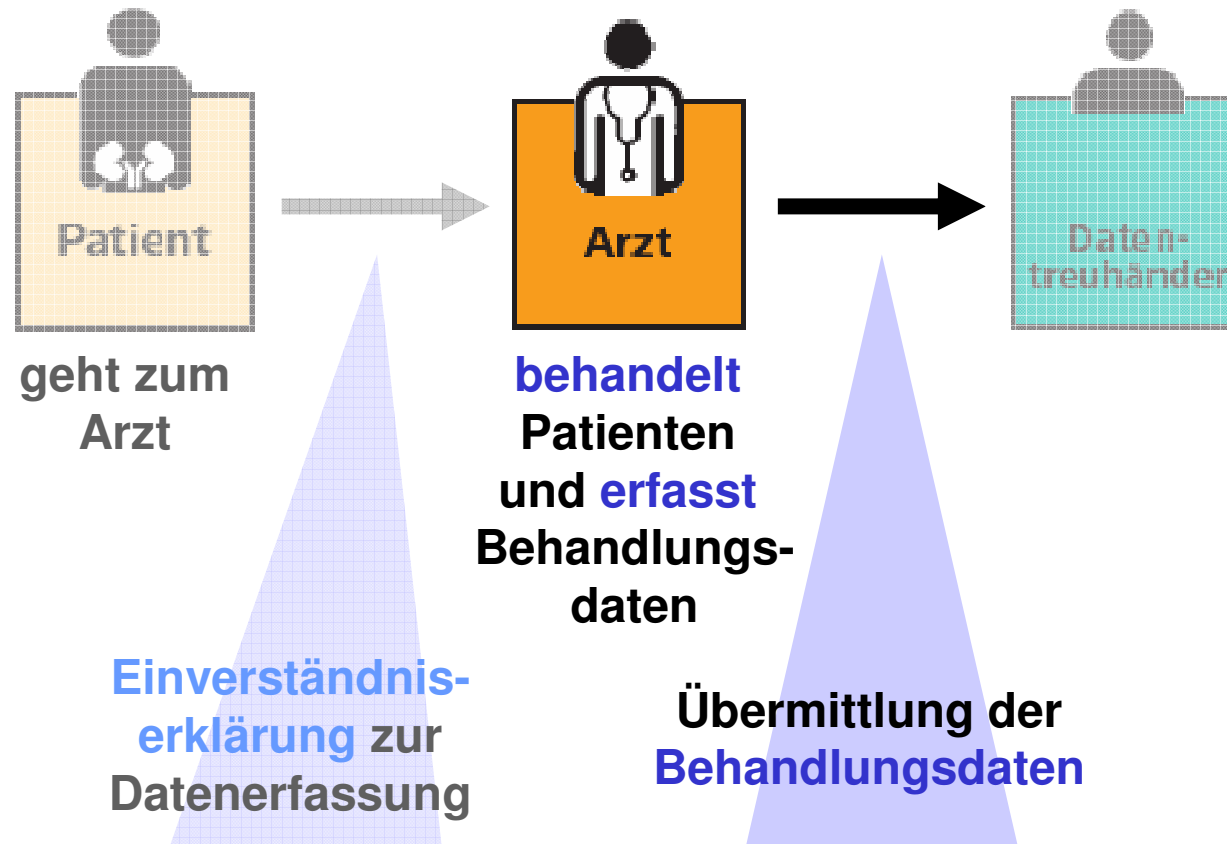
Aktivität des Patienten



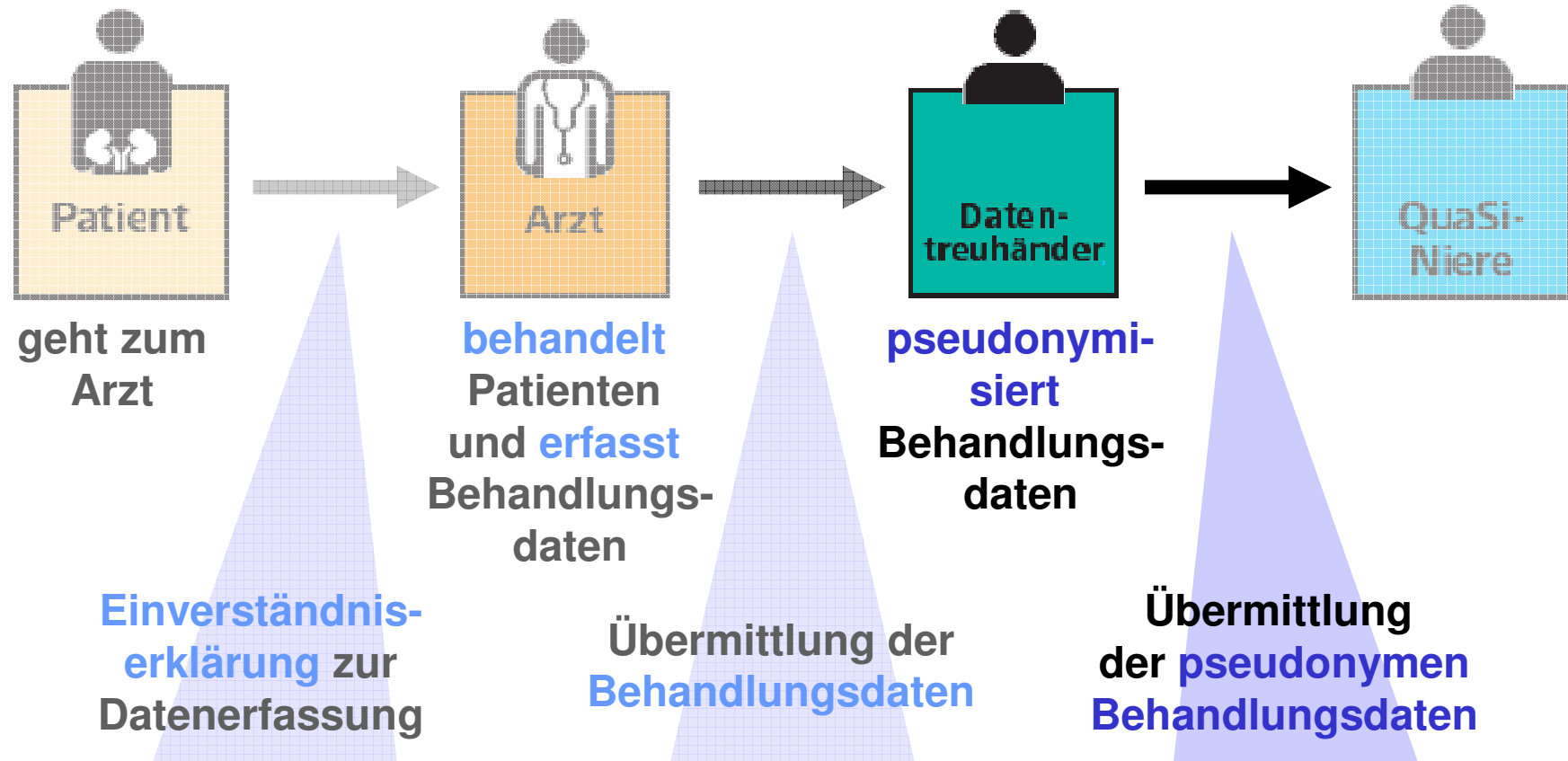
geht zum
Arzt

Einverständnis-
erklärung zur
Datenerfassung

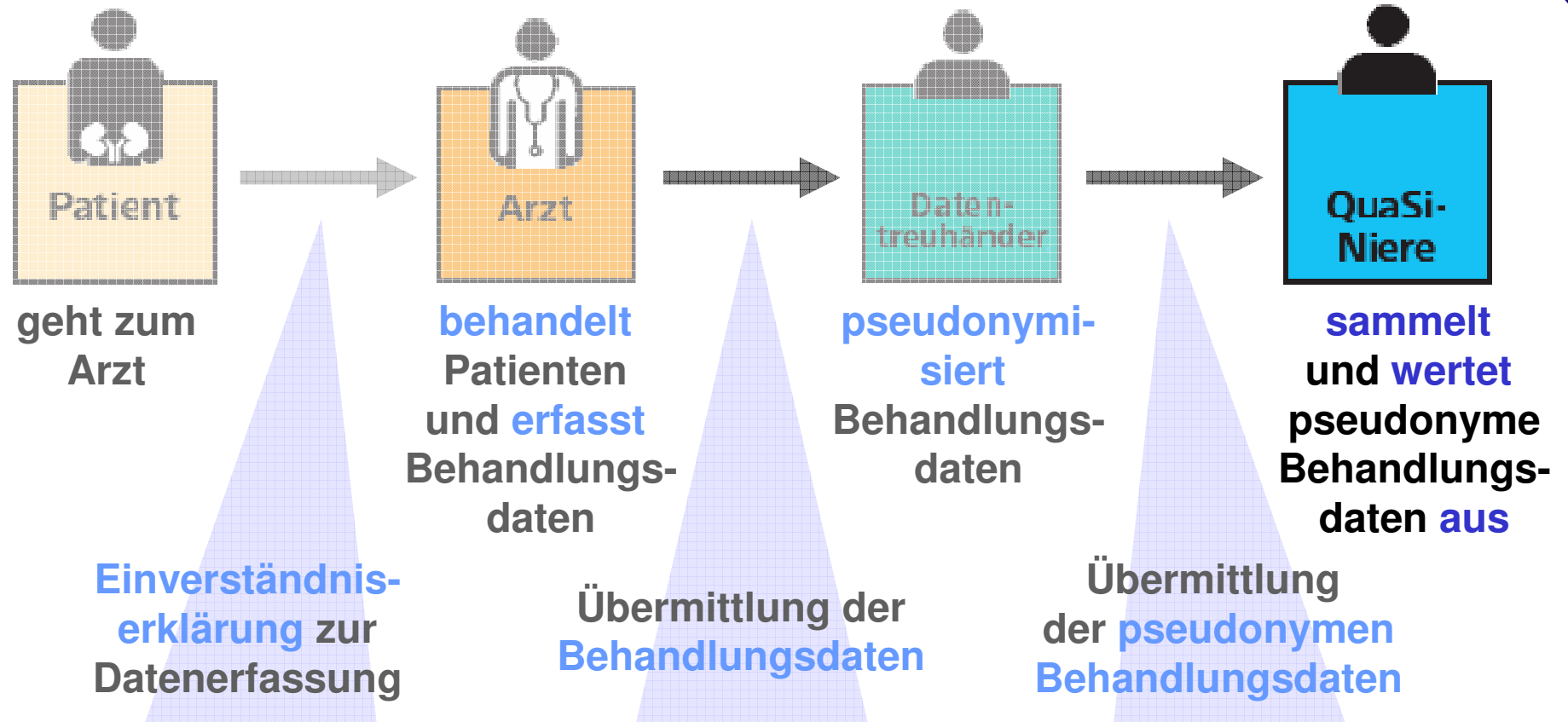
Aktivität des Arztes



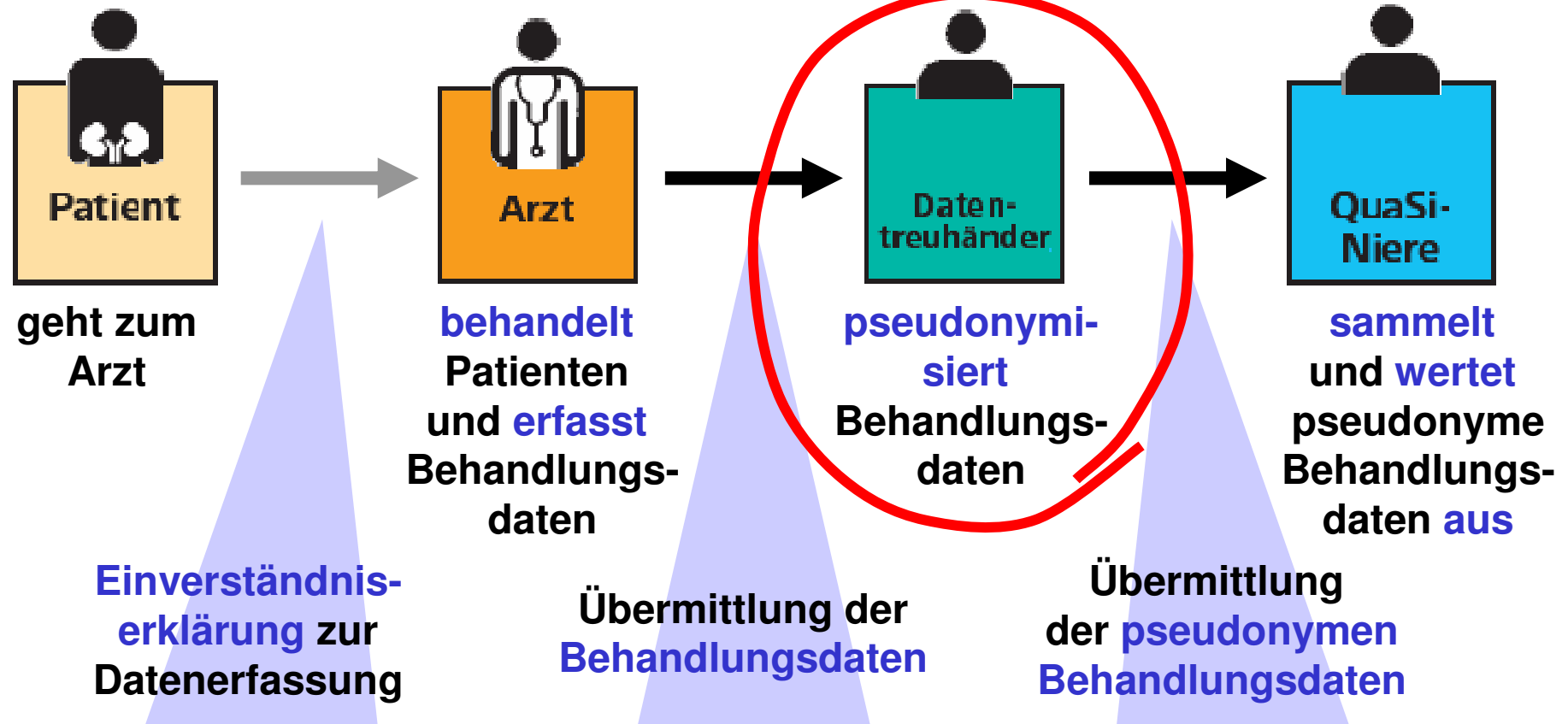
Aktivität des Datentreuhänder



Aktivität der QuaSi-Niere



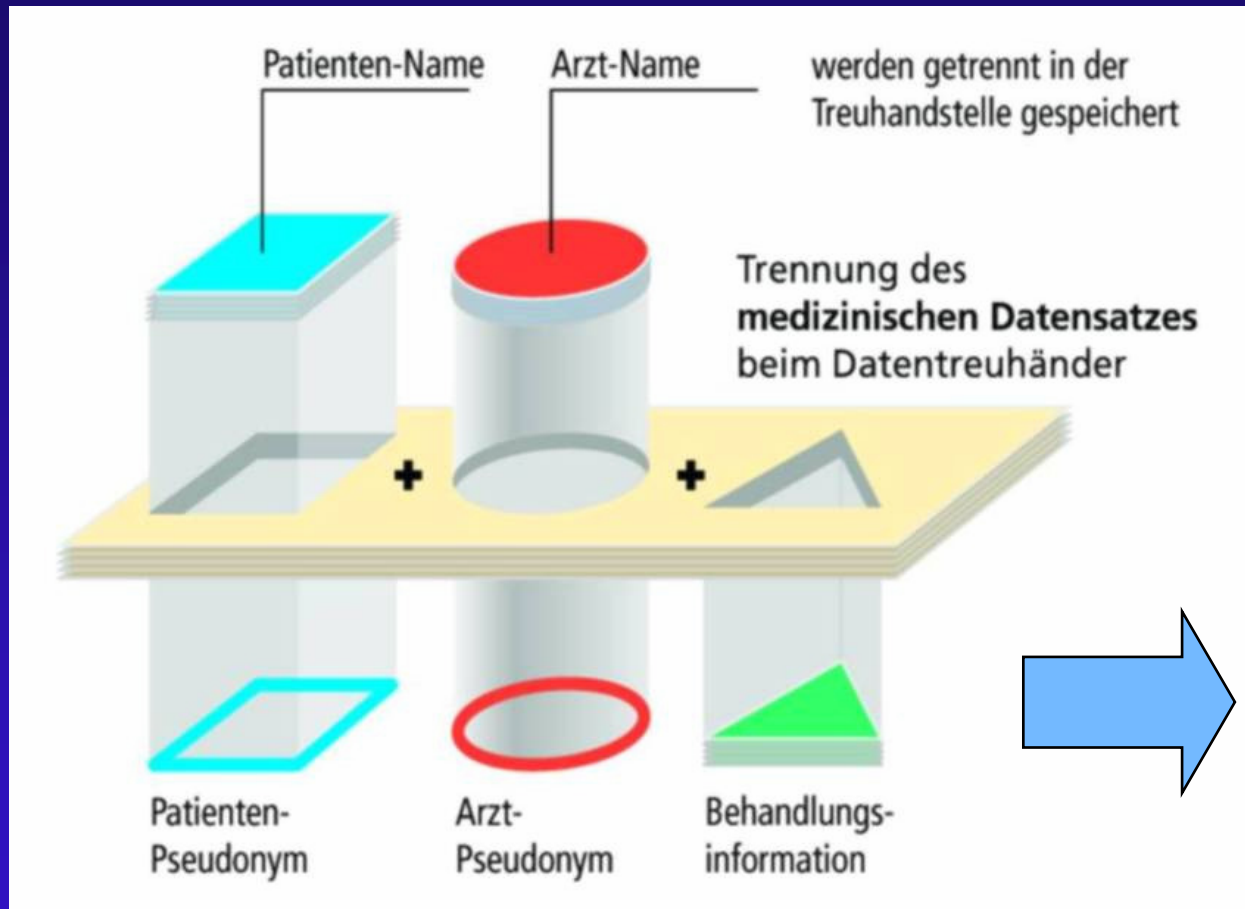
Übersicht des QuaSi-Niere-Verfahrens



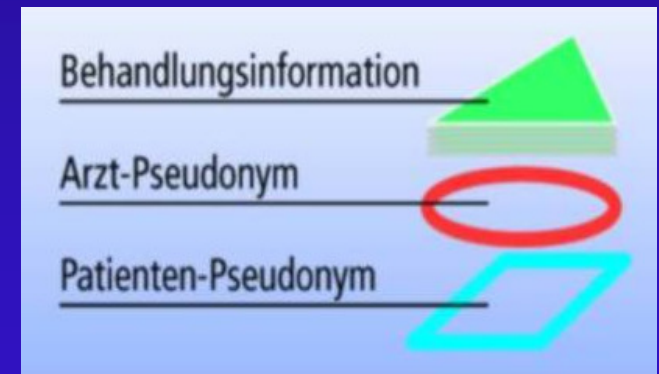
Teil 2

Pseudonymisierung beim Datentreuhänder

Trennung der Daten beim Datentreuhänder



Auswertung des pseudonymen medizinischen Datensatzes bei **QuaSi-Niere**:



Identifikationslisten beim Datentreuhänder

Patientenliste

ID	Name	Vorname	...
A6B728	Müller	Lieschen	...
25C79A	Maier	Peter	...
D56FAA	Schuster	Franz	...
...

- Neuanmeldungen werden mit Listen überprüft
- Folgemeldungen werden über ID identifiziert

Arztliste

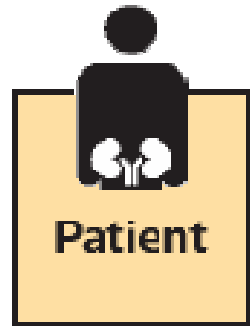
ID	Name	Vorname	...
...

eindeutige Identifikation
über die ID

Teil 3

Chipkarteneinsatz

Verwendete Chipkarten



Patient

60.000
Patientenkarten
PDC



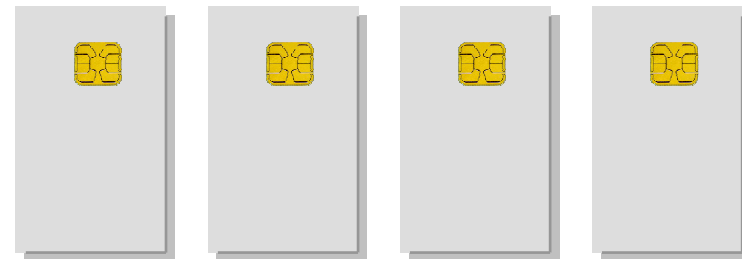
Arzt

400
Arztkarten
HPC

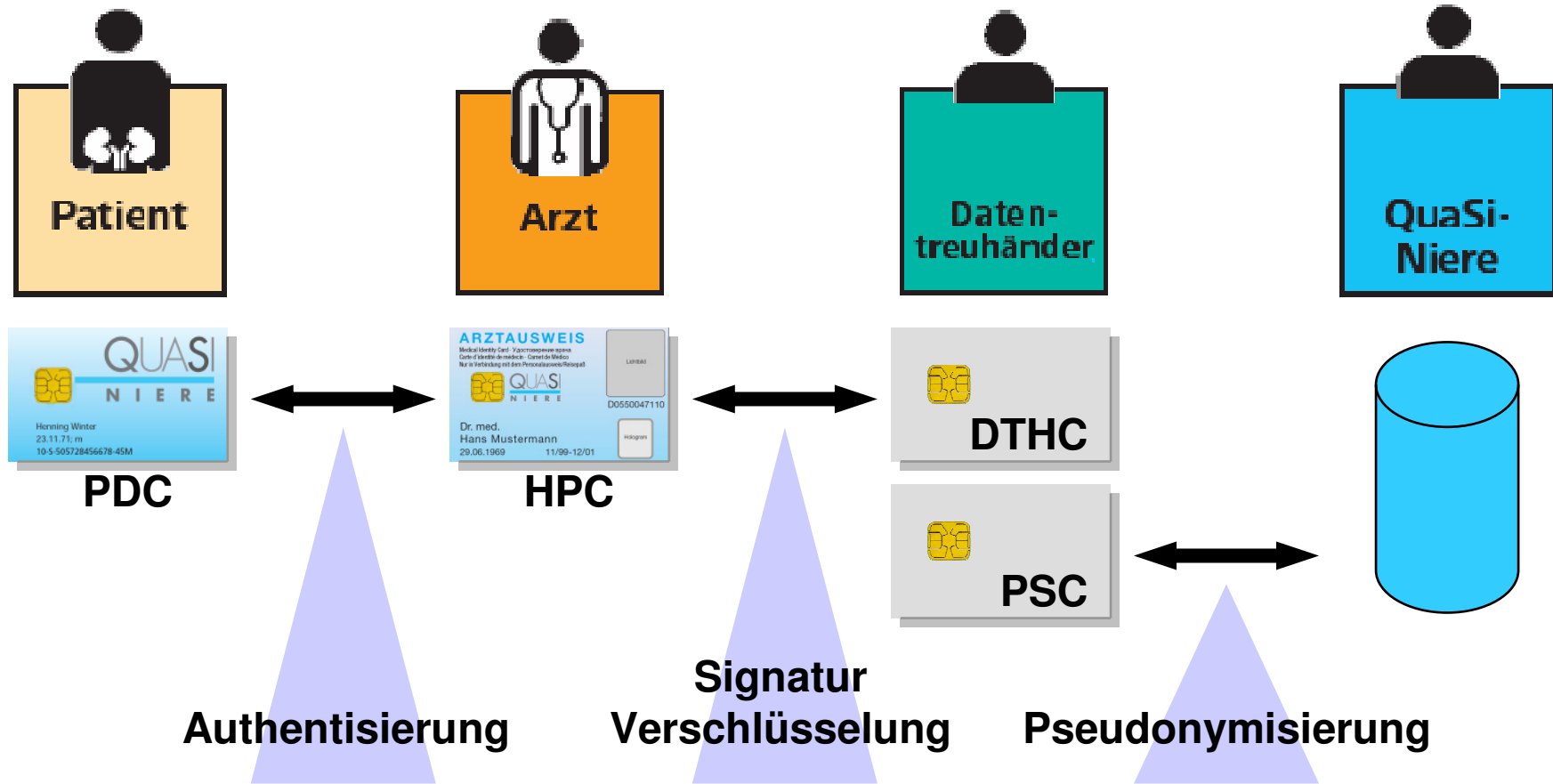


Daten-
treuhänder

Datentreuhänderkarte DTHC
Pseudonymisierungskarte PSC
Masterkey-Karte MSC
Patienten-Personalisierungskarte PPC



Funktionalitäten der Chipkarten



Patientenkarte PDC

Hauptfunktionen der Prozessorkarte:

1. Eindeutige Identifizierung des Patienten im Gesamtsystem
2. Zustimmung des Patienten zur Datenverwertung durch die QuaSi-Niere
3. Speicherung von Behandlungsdaten (z.B. Quartalsbericht) auf der PDC, sobald eine Authentisierung durch den Patienten und den Arzt erfolgt ist
4. Protokollierung der letzten 64 Zugriffe auf die PDC



Arztkarte HPC

Kryptoprozessorkarte STARCOS SPK 2.3:

1. Nachweis gegenüber dem Patienten, dass der Arzt mit QuaSi-Niere zusammenarbeitet
2. Symmetrische Authentisierung zwischen HPC und PDC (Challenge/Response) -> gestattet Schreib- und Lesezugriff auf erweiterten Speicherbereich der PDC
3. Signieren der Patientendaten (SHA-1, RSA)
4. Verschlüsseln der Patientendaten vor der Datenfernübertragung (Hybridverfahren)
5. Entschlüsseln von Institutions- bzw. Individualberichten



Datentreuhänderkarte DTHC

Unterstütz den Datenaustausch mit dem Arzt durch:

- 1. Signieren von Institutions- bzw. Individualberichten**
- 2. Verschlüsseln von Berichten (Hybridverfahren)**
- 3. Entschlüsselung des mit dem Public Key verschlüsselten 3DES Session Key (Hybridverfahren)**

Pseudonymisierungskarte PSC

PSC unterstützt symmetrische Verschlüsselung zur:

- 1. Berechnung der Pseudonyme anhand der Patienten- und Arzt-IDs zur datenschutzkonformen Trennung der medizinischen Daten von den identifizierenden**
- 2. Berechnung der IDs anhand der Pseudonyme**

Ende