NEC Empowered by Innovation

aneurIST

Integrated biomedical informatics for the management of cerebral aneurysms

ID-Management im EU-Grid-Projekt @neurIST

Luigi Lo Iacono (ルイジ・ロ・イアコノ)

NEC Laboratories Europe, NEC Europe Ltd.

TMF Workshop ID-Management

15. Dezember 2008, Berlin

The financial support of the European Commission is gratefully acknowledged. Material in this presentation reflects only the author's views and the Commission is not liable for any use that may be made of the information contained herein.

Der Fahrplan

- Das @neurIST-Projekt
- Pseudonymisierung in @neurIST
  - ID-Management Fokus auf den Patienten
- Authentifizierung in @neurIST
  - ID-Management Fokus auf die Heilberufler

Das @neurIST-Projekt

Ziele

Entwicklung einer generischen IT Infrastruktur zum Management und Verarbeiten heterogener Daten, die mit der Diagnose und der Behandlung von zerebralen Aneurysmen assoziiert sind

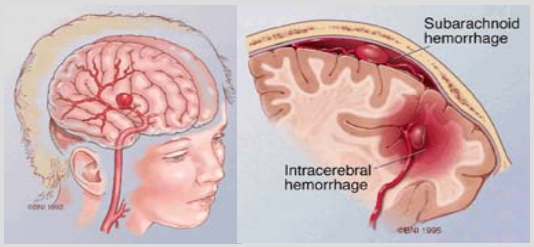
Projekt in Zahlen

- Start: 1. Januar 2006
- Dauer: 4 Jahre
- Budget: > 17 Millionen Euro
- Partner: 30 aus 12 Ländern

http://www.aneurist.org/

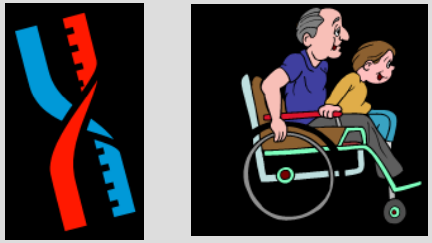
@neurIST Forschungsschwerpunkt

Operatives Entfernen oder endovaskulare Behandlung?



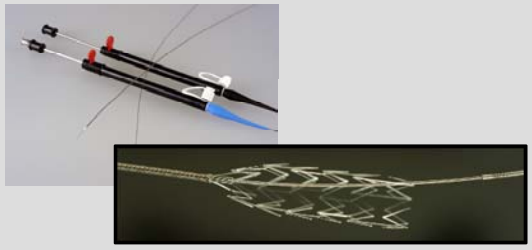
- Eruptionsrisiko muss feststellbar sein
- Können Modelle und Simulation für die individuelle Risikobestimmung herangezogen werden?

Untersuchen der Gründe für das Auftreten von Aneurysmen



- Genetische Veranlagung?
- Bedingt ausgiebiger Untersuchung der Familienhistorie und damit einen großen Patientenpool

Verbessern der endovaskularen Behandlungsmöglichkeiten

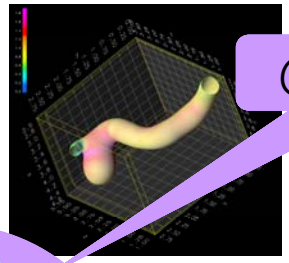


- Simulation der verfügbaren Behandlungsmöglichkeiten für individuelle Fälle
- Verbesserung medizinischer Behandlungsmöglich-keiten (Stent-Design) auf Basis reeller Patientendaten

@neurIST Applikationen und Middleware

@neurIST

@neuRisk
Anwendung zur Daten-erfassung, Risikoanalyse und Behandlungsplanung

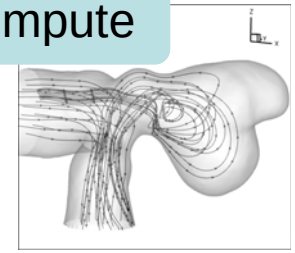


@neuFuse
Anwendung zur Visualisierung und Manipulation medizinischer Bilder

@neuLink
Forschungstool zur Analyse der Beziehung zwischen Genom und Krankheit

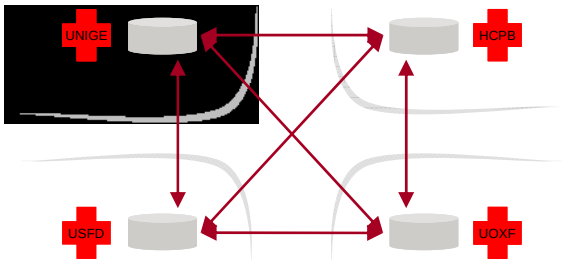
@neuEndo
Anwendung zur Simulation und Planung von Stent Platzierungen

@neuCompute
Compute-Dienstleistungen zur Simulation auf Basis medizinischer Bilder oder Risikoanalyseberechnungen



@neuInfo
Datenzugriff und Datentransfer Middleware

Sicherheitsanforderungen



- **Schutz der Privatheit der Patientendaten**
  - Pseudonymisierung
  - Filtering
- **Zugriffsschutz auf föderierte Daten and Ressourcen in verteilten Umgebungen**
  - Verteiltes Zugriffskontrolsystem
- **Monitoring und Logging**
- **Kommunikationssicherheit**
  - Verschlüsselter Transport der Datenanfragen und -antworten
  - Ende-zu-Ende Sicherheit auf Web Service Schicht

Szenario

Patient

DE

CH

UK

ES

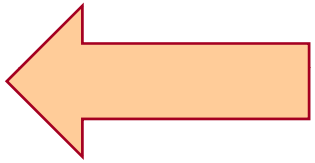
Föderierte und Pseudonymisierte Forschungs-DB

Angestrebte minimal Population

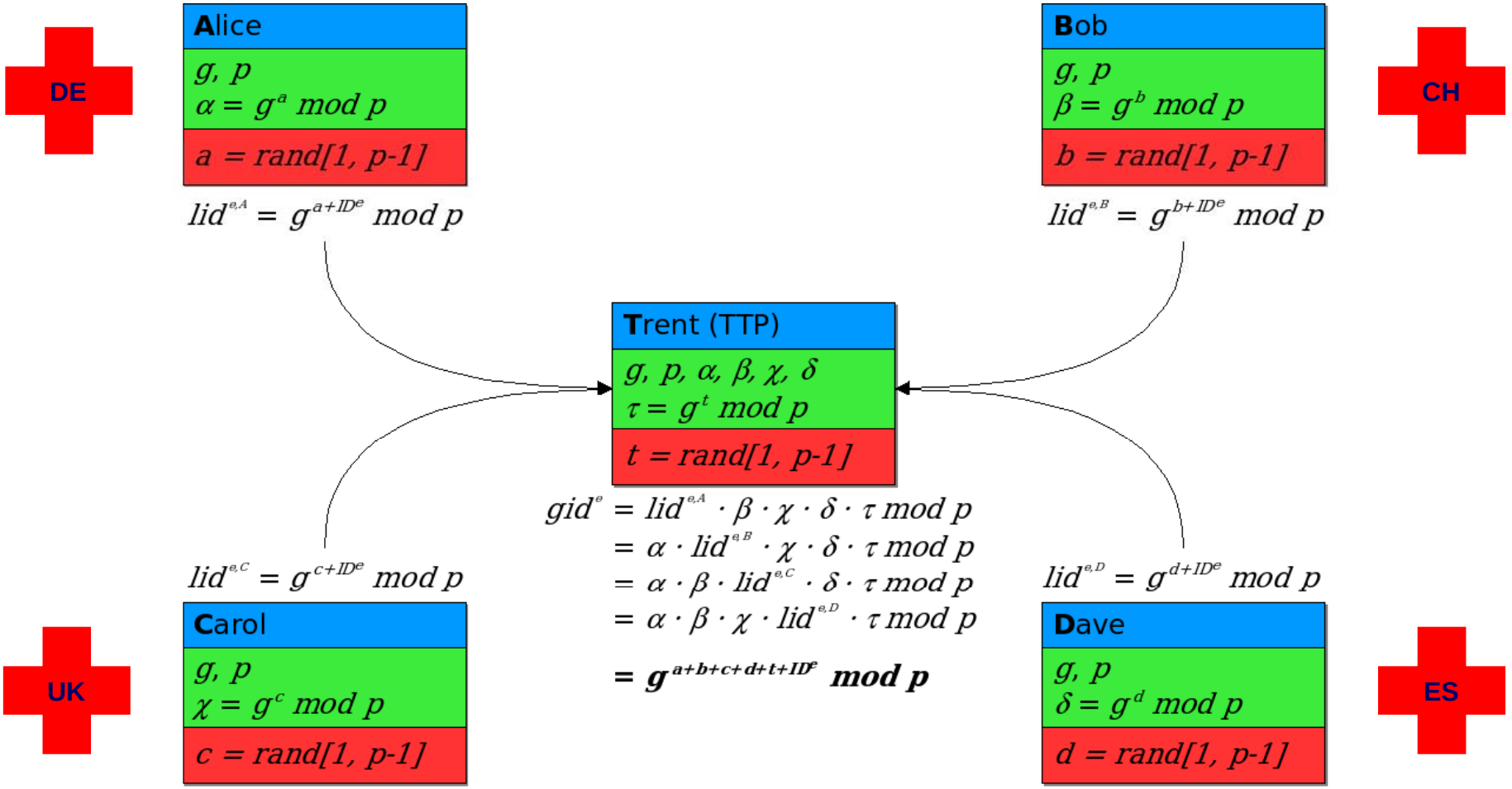
- 400 Patienten mit Aneurysma
- 400 Patienten mit gerissenem Aneurysma
- 400 Kontrollfälle

Der Fahrplan

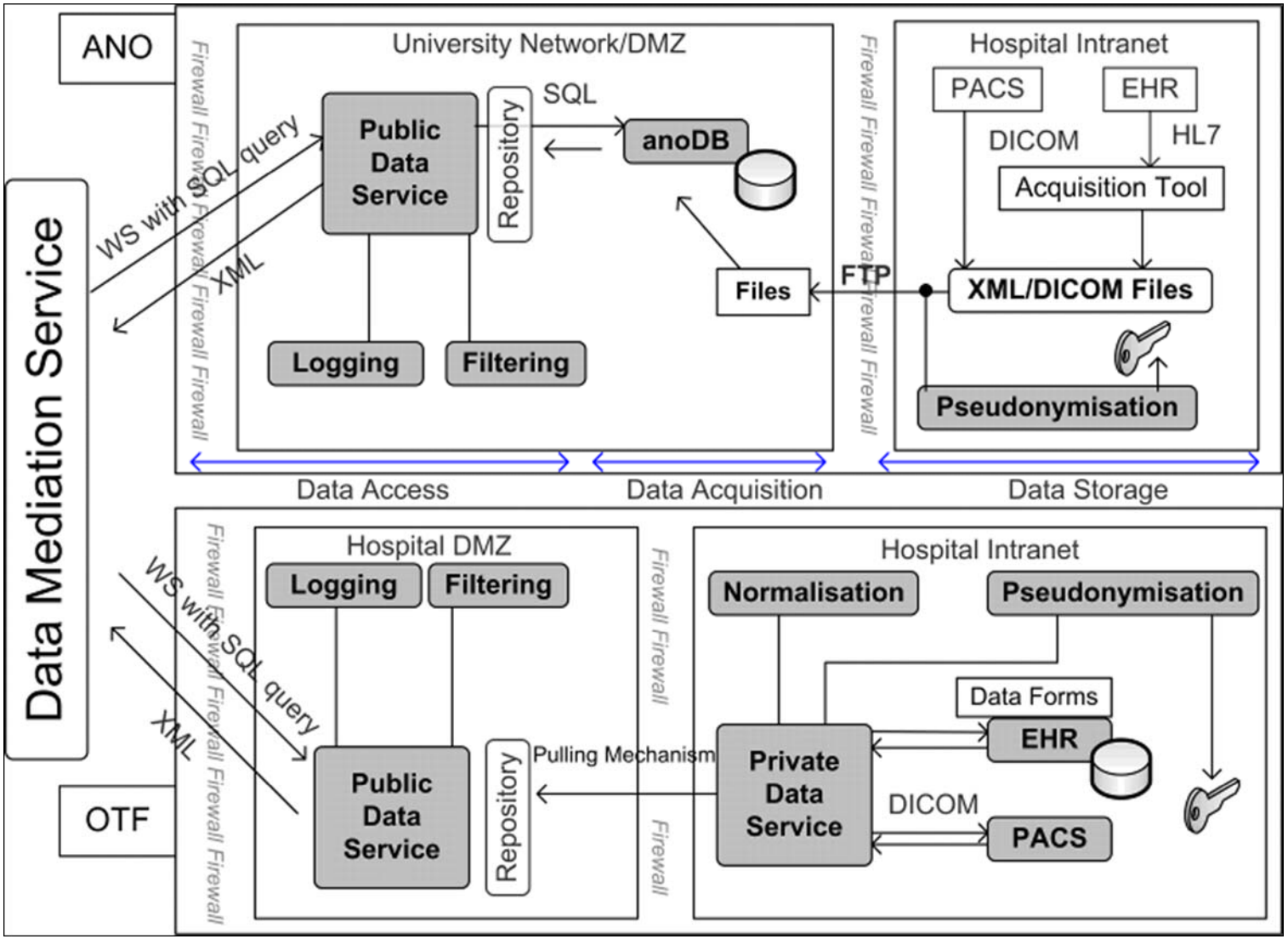
- Das @neurIST-Projekt
- Pseudonymisierung in @neurIST
  - ID-Management Fokus auf den Patienten
- Authentifizierung in @neurIST
  - ID-Management Fokus auf die Heilberufler



Dezentrale Globale Pseudonymisierung



Datenbereitstellungsmodelle



Pseudonymisierung in @neurIST

- **Verschlüsselung der Patienten-ID (PID)**
  - **Keine Mapping-Tabelle zur Re-Identifizierung notwendig**
  - **PID kann aus dem Pseudonym durch Entschlüsselung gewonnen werden**
  - **Ausschließlich der geheime/private Schlüssel muss vor unbefugtem Zugriff geschützt werden**
- **Patienten-ID**

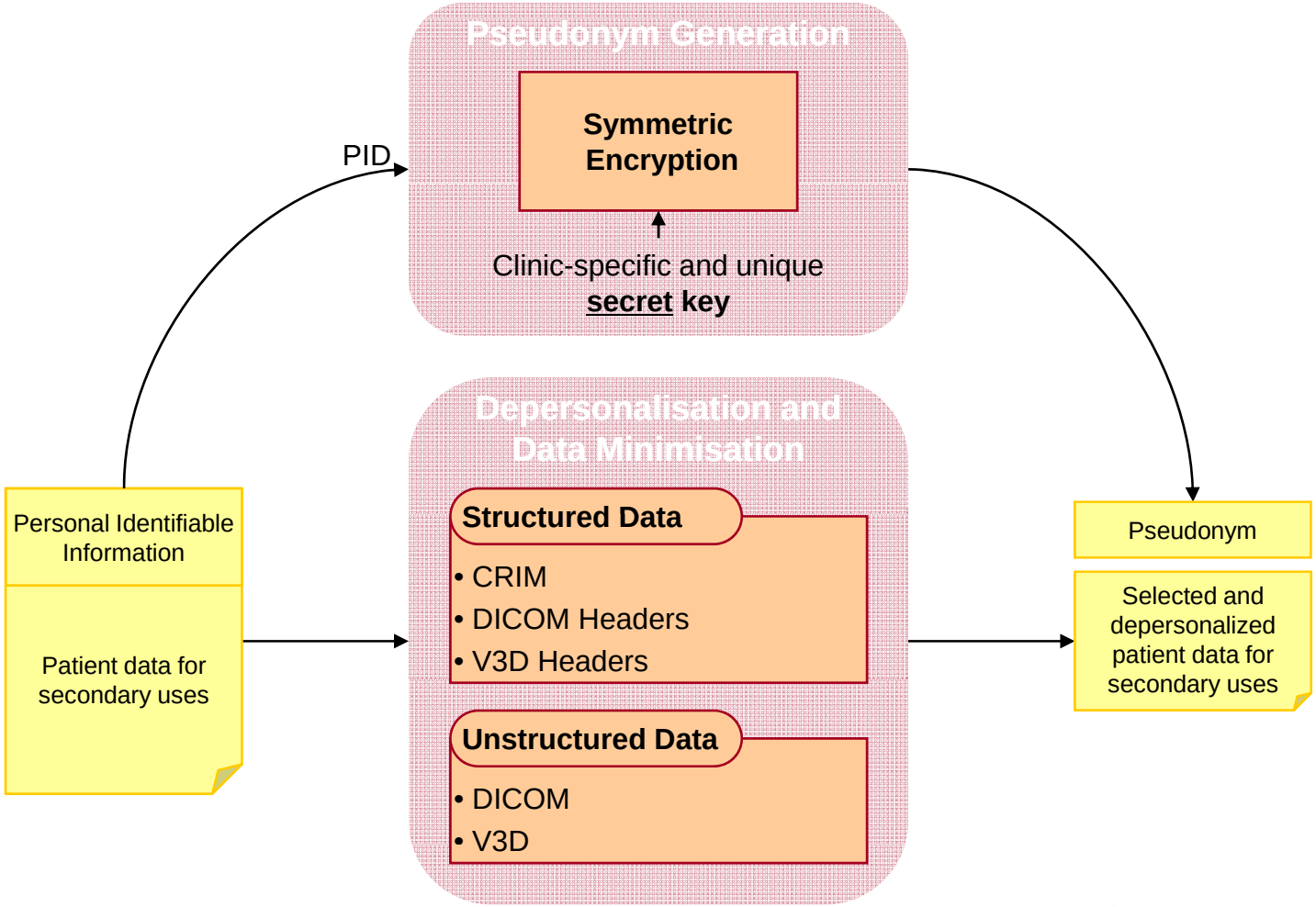
Klinik	Format	Länge	Beispiel
UNIGE	Numerisch	6-8	01234567
USFD	Numerisch	10	0123456789
UOXF	Numerisch	10	01234567890
HCPB	Heute: Numerisch Zukunft: Alphanumerisch	8 14	01234567 0123456789WXYZ

- **Anforderungen an die Generierung von Pseudonymen**

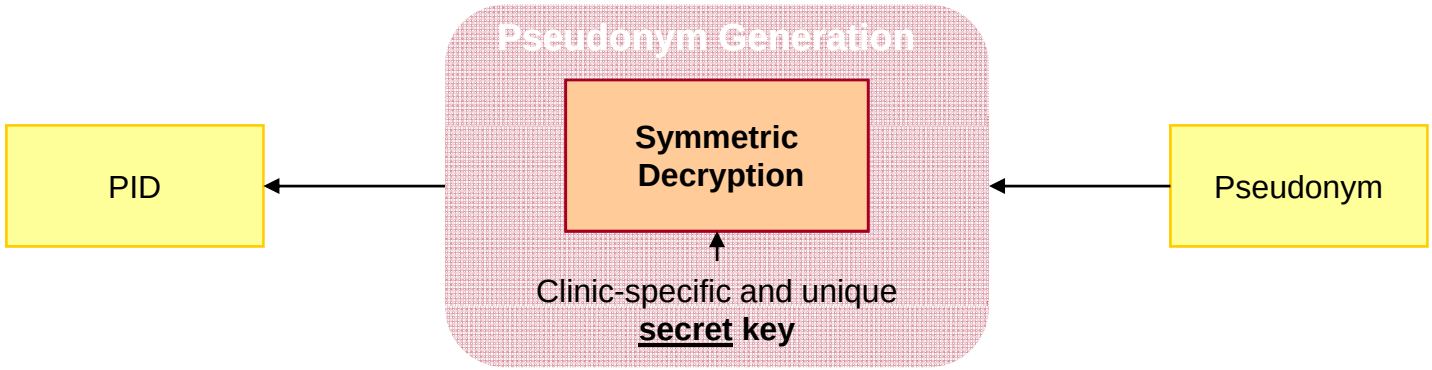
- **Gleiche PID erzeugt gleiches Pseudonym**
- **PID-Länge: 6-14 Byte**
- **Rahmenbedingungen aus dem DICOM-Standard (PID-Feld)**
  - **Längenbeschränkung auf 64 Zeichen**
  - **Ohne '\' Zeichen**
- **Nicht nur Verschlüsselung, sondern auch Integritätsschutz**
  - **Wenn das Pseudonym „geöffnet" wird (entschlüsselt) kann die Integrität zuvor geprüft werden**

➔ **Symmetrische Verschlüsselung und MAC-Berechnung**
  - **Keine deterministische asymmetrische Verschlüsselung bekannt, die die Längenbeschränkung erfüllt**

Pseudonymisierungsarchitektur – De-Identifizierung

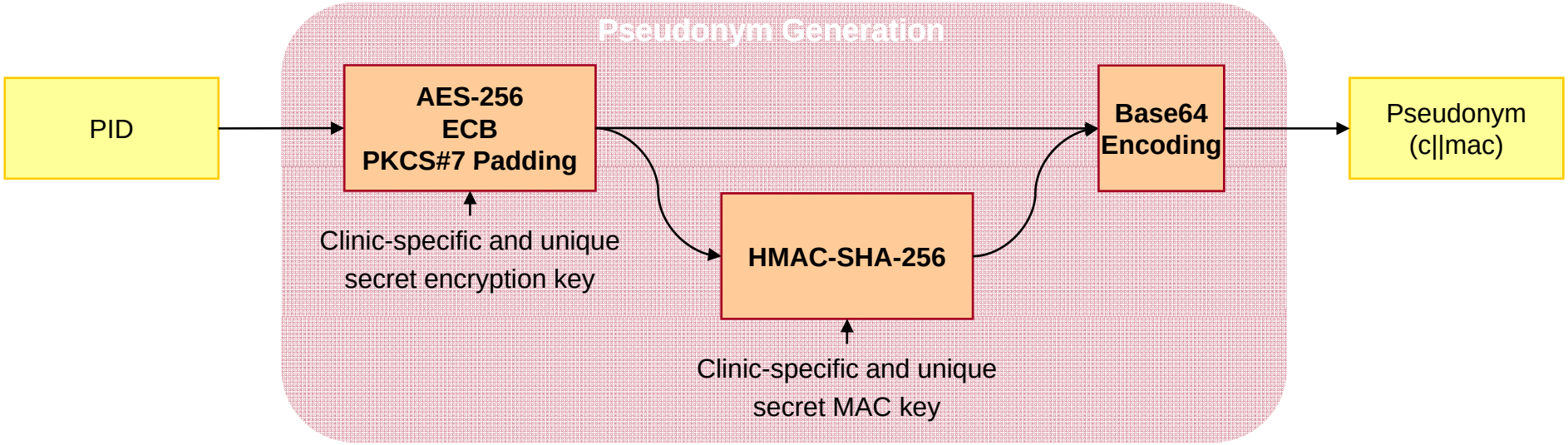


Pseudonymisierungsarchitektur – Re-Identifizierung



Dieser Prozess steht unter der Kontrolle des “Clinic and Ethical Board” und muss von diesem autorisiert sein

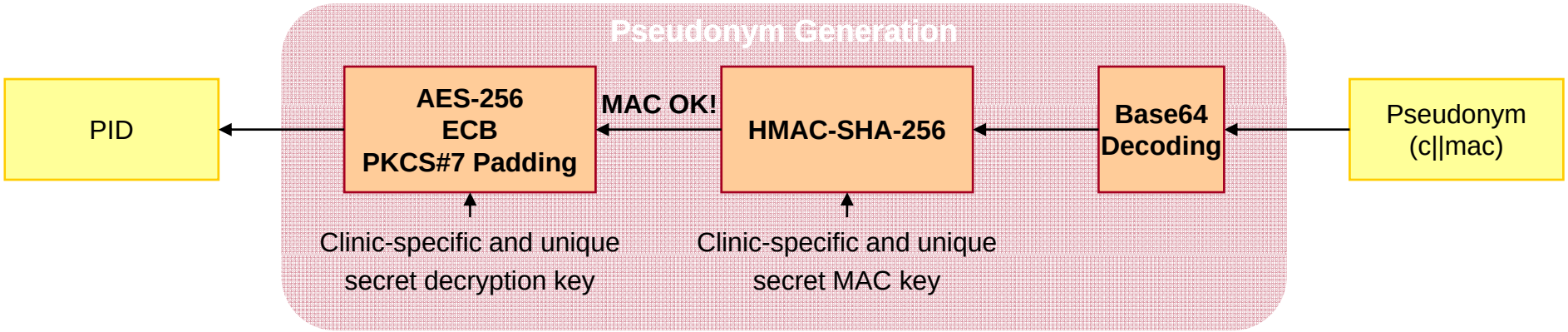
Algorithmus zur Generierung von Pseudonymen



Pseudonym

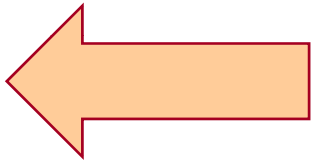
- Konkatenation von Chiffrat und MAC (c||mac) ➔ 48 Byte
- Kodierung: base64
  - Größte 2er Potenz, die mit darstellbaren ASCII-Zeichen kodiert werden kann: ‘A-Z’, ‘a-z’, ‘0-9’, ‘+’, ‘/’ (RFC 3548)
  - 3 Byte werden zu 4 Byte ➔ 64 Byte (passt in das DICOM PID-Feld!)
  - Beispiel: `ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/`

Algorithmus zur Re-Identifizierung

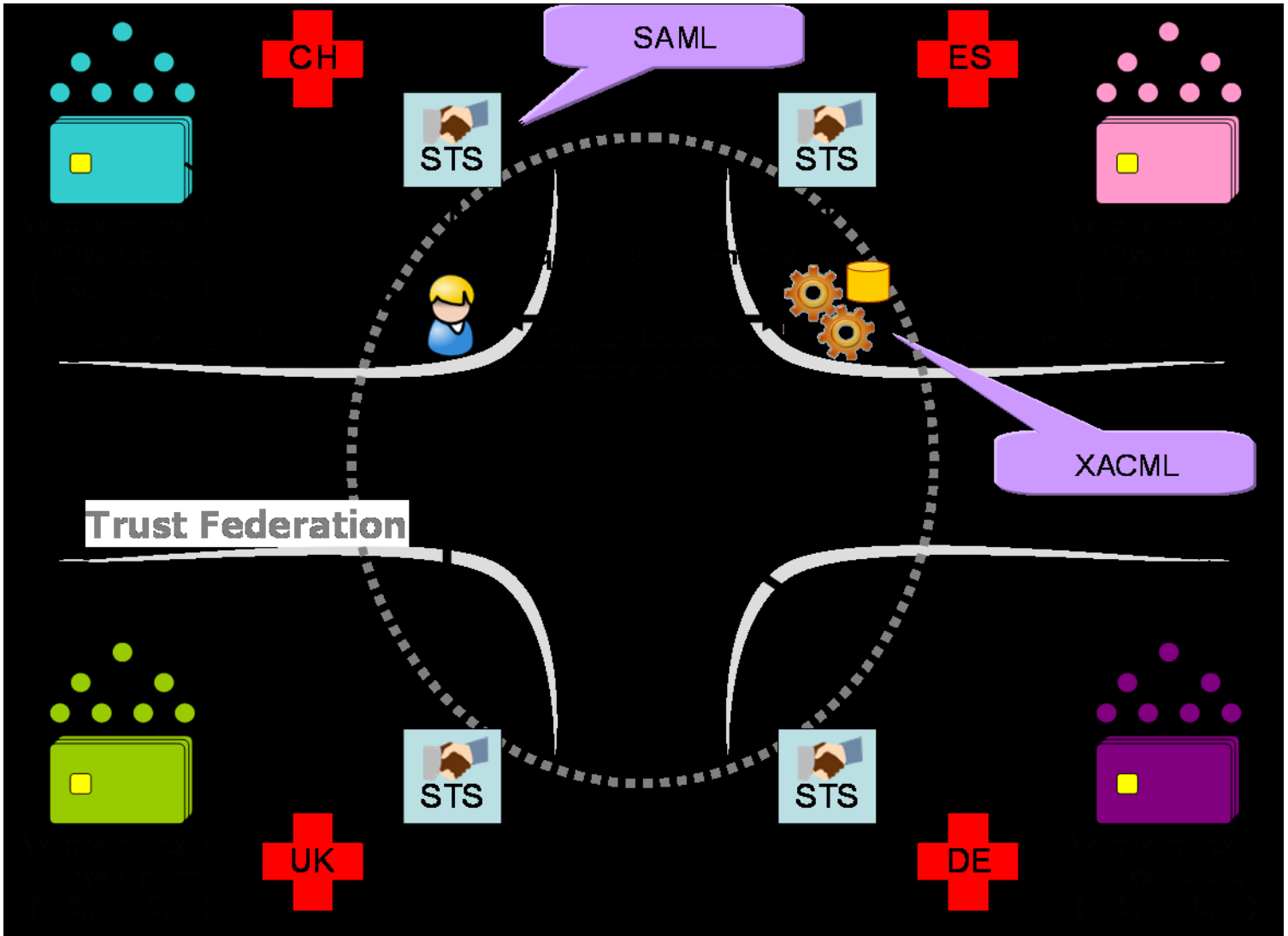


Der Fahrplan

- Das @neurIST-Projekt
- Pseudonymisierung in @neurIST
  - ID-Management Fokus auf den Patienten
- Authentifizierung in @neurIST
  - ID-Management Fokus auf die Heilberufler

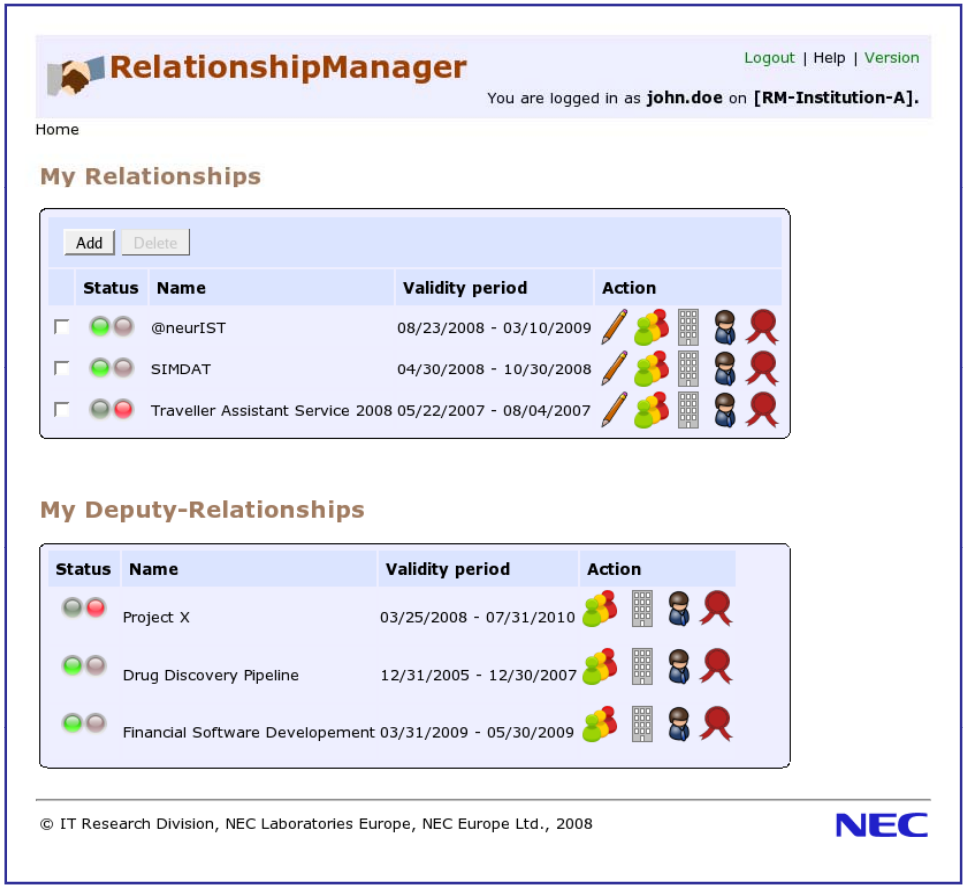


ID und Zugriffsmanagement in @neurIST



NEC RelationshipManager

- Anlegen und Verwaltung von Kollaborationsbeziehungen
- Hinzufügen von externen Partnern zu einer Kollaboration
- Hinzufügen von lokalen Benutzern zu einer Kollaboration
- Festlegen von Kollaborations-spezifischen Attributen (z.B. Rollen oder Klassifikationen)
- Zuweisung von Attributen an lokale Benutzer
- Angabe eines Stellvertreters



- **Wir haben das Ziel erreicht**

Fragen?