Telematikplattform für
Medizinische Forschungsnetze e. V.

Workshop ID-Management
15. Dezember 2008, Berlin

Internationale IT-Standards für ID-Management und Pseudonymisierung

Bernd Blobel PhD, Associate Professor
eHealth Competence Center
Universitätsklinikum Regensburg
Past-Chair and Chair-Elect, HL7 Germany
Deputy Chair, German Health Informatics Standards Mirror Group
Deputy Head, German Delegation to ISO TC 215 and CEN TC 251
Chair, EFMI WGs “EHR“ and “Security, Safety and Ethics“

eHealth Competence Center
eHCC
REGENSBURG

Der Autor dankt den Kollegen des ISO TC 215, CEN TC 251, ETSI, OASIS, OMG/CORBA, HL7, der EFMI WG Security, Safety and Ethics, aber auch dem BioHealth Consortium, Dr. Christoph Goetz (Ärztekammer und KV Bayern), der gematik und dem bIT4health-Consortium für die freundliche Unterstützung.

Problemstellung

ID-Management und bezogene Dienste wie Policy-Management, Rollenmanagement, Privilegmanagement, Zugriffskontrolle, Zugangskontrolle, Verzeichnisdienste, etc. sind grundlegende Erfordernisse für die Etablierung einer Gesundheitstelematik / eHealth /Personal Health.

Dazu müssen die inhaltlichen, organisatorischen, rechtlichen ethischen, sozialen und technischen Aspekte der entsprechenden Lösungsarchitekturen beherrscht werden.

Im Folgenden werden Grundlagen, Standards, Lösungsbeispiele sowie die Situation zum ID-Management im Gesundheitswesen in Deutschland im Vergleich zu in der Thematik fortgeschrittenen Ländern diskutiert.

Bernd Blobel, PhD, Asssociate Professor
eHealth Competence Center, Regensburg
Email: bernd.blobel@klinik.uni-regensburg.de

Authentifizierung einer vorgegebenen Identität

- Durch spezielles Wissen (z.B. Passwort, andere Geheimnisse)

- Durch Besitz (z.B. eines speziellen Tokens wie Smartcard, RFID Tag, etc.)

- Durch Eigenschaften (biologische, genetische oder Verhaltenseigenschaften)

Probleme

- Authentifizierung durch Identifikation vs. Verifikation

- Authentifizierung als Diskriminanzproblem

Bernd Blobel, PhD, Asssociate Professor
eHealth Competence Center, Regensburg
Email: bernd.blobel@klinik.uni-regensburg.de

ID- und ID-Managementstandards (Auswahl) 1/4

- prCEN/TR 15872 Health informatics — Guidance on patient identification and crossreferencing of identities
- EN 14484:2003 Health Informatics – International Transfer of Personal Health Data covered by the EU Data Protection Directive – High Level Security Policy
- EN 14485:2003 Health Informatics – Guidance for Handling Personal Health Data in International applications in the context of the EU Data Protection Directive
- EN 13606, Health informatics – Electronic health record communication
- EN 12967 Health informatics – Service architecture (HISA)
- General and detailed specifications for patient's identification, 2001-2002, GIP GMSIH (France): Principles of Patient Identification (2vol)
- CEN 13729: Health informatics - Secure user identification - Strong authentication using microprocessor cards

ID- und ID-Managementstandards (Auswahl) 2/4

- ISO/TS 22220 Health informatics – Identification of subjects of healthcare
- ISO TS 27527 Health informatics – Provider identification
- ISO TS 21298 Health informatics – Functional and structural roles
- ISO 21091 Health informatics - Directory services for security, communications and identification of professionals and patients
- ISO TS 22600 Health informatics – Privilege management and access control
- ISO 17090 Health informatics - Public key infrastructure
- ISO/TS 25237:2008 Health informatics – Pseudonymisation Practices for the Protection of Personal Health Information and Health Related Services

ID- und ID-Managementstandards (Auswahl) 3/4

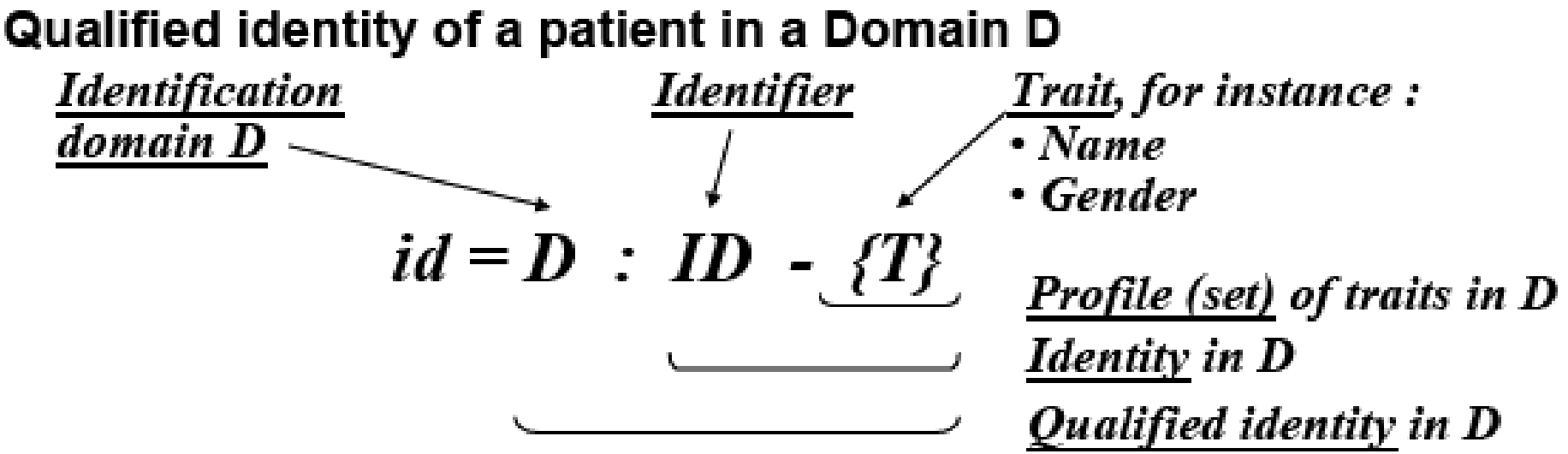
- Service Functional Model Specification - Entity Identification Service (EIS), HSSP (joint endeavour between HL7 and OMG), Version 0.997 July 17, 2006
- Person Identification Service (PIDS), (a.k.a. Patient Identification Service), Final Submission - Revision 7, OMG CORBAmed DTF, 98-01-09
- ASTM E1714-07 Standard Guide for Properties of a Universal Healthcare Identifier (UHID)
- ASTM E1762-95(2003) Standard Guide for Electronic Authentication of Health Care Information
- ASTM E1869-04 Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records
- ASTM E1985-98(2005) Standard Guide for User Authentication and Authorization
- ASTM E1986-98(2005) Standard Guide for Information Access Privileges to Health Information
- ASTM E2017-99(2005) Standard Guide for Amendments to Health Information
- ASTM E2084-00 Standard Specification for Authentication of Healthcare Information Using Digital Signatures See also WK8017 proposed revision
- ASTM E2212-02a Standard Practice for Healthcare Certificate Policy
- ASTM E2595-07 Standard Guide for Privilege Management Infrastructure

ID- und ID-Managementstandards (Auswahl) 4/4

- Guideline for elaboration of the patient identification policy
- Guideline for elaboration of the cross reference patient identification policy
- Patient identification services
- Cross Reference Patient identification services
- Good practices referential for healthcare patient's identification; BP S97-723, AFNOR (France)
- Strategic Short Study - Names and Numbers as Identifiers (Final report version 2.0); Robin Hopkins, CEN/TC 251/N98-083
- Analysis of unique Patient Identifier Options, Final report, Soloman I. Appavu, November 24, 1997, DHHS
- Foundations for the future, Priorities for health informatics standardisation in Australia, 2005–2008,
- Information and Communications Technology Standards Committee (ICTSC) 2004
- IHE IT Infrastructure Technical Framework, Volume 1, (ITI TF-1) Integration Profiles, Revision 4.0 – Final Text, August 22, 2007, ACC/HIMSS/RSNA
- IHE IT Infrastructure Technical Framework, Volume 2, (ITI TF-2) Transactions, Revision 4.0 – Final text, August 22, 2007, ACC/HIMSS/RSNA

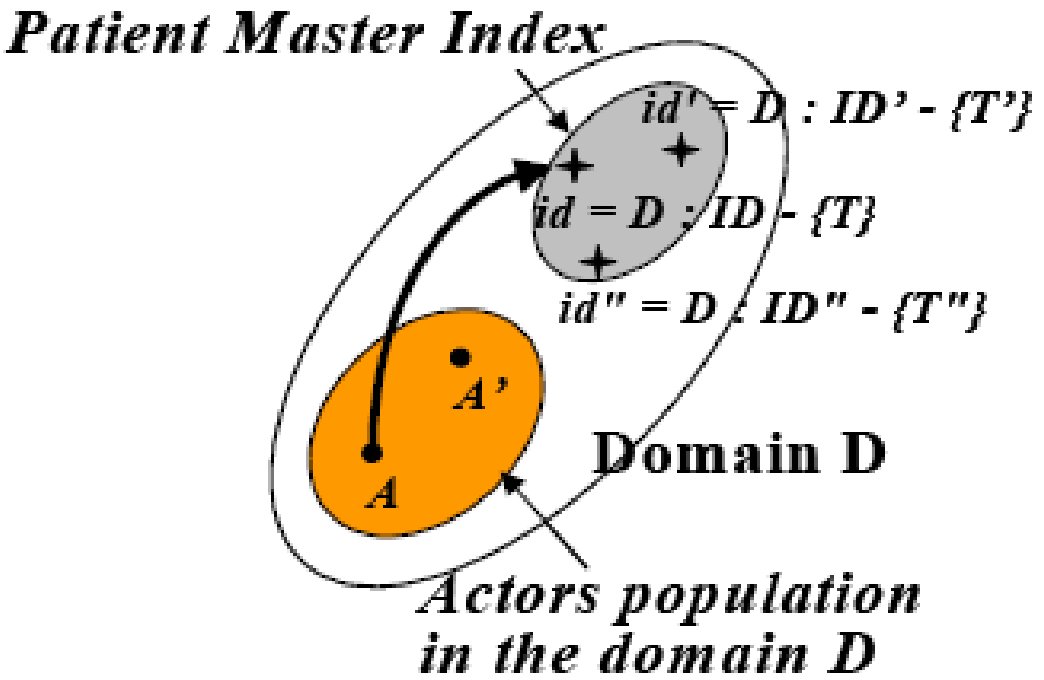
CEN TR Health informatics — Guidance on patient identification and crossreferencing of identities

Definition einer qualifizierten Identität



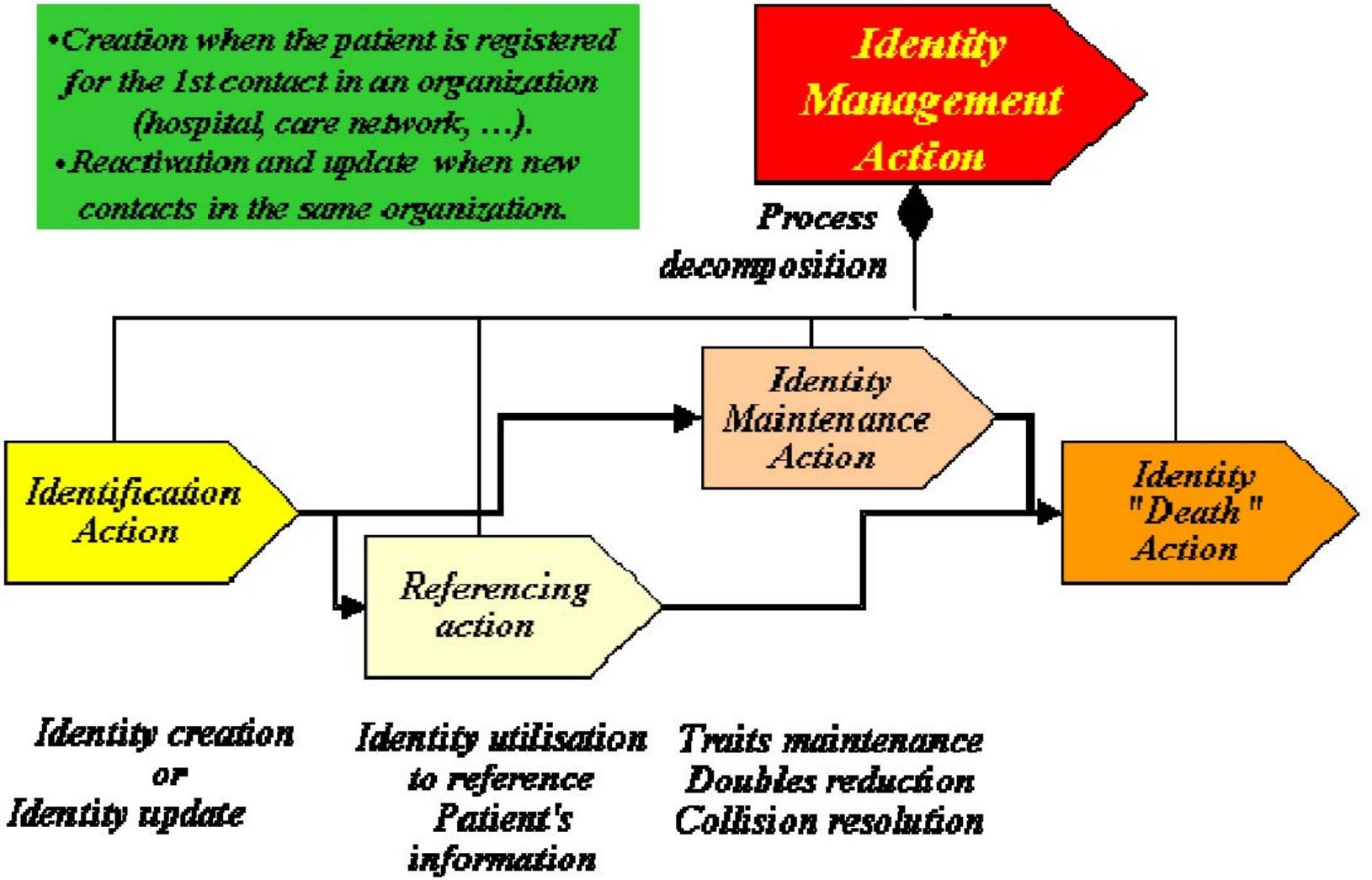
Bernd Blobel, PhD, Asssociate Professor
eHealth Competence Center, Regensburg
Email: bernd.blobel@klinik.uni-regensburg.de

Master Patient Index (MPI)



Bernd Blobel, PhD, Asssociate Professor
eHealth Competence Center, Regensburg
Email: bernd.blobel@klinik.uni-regensburg.de

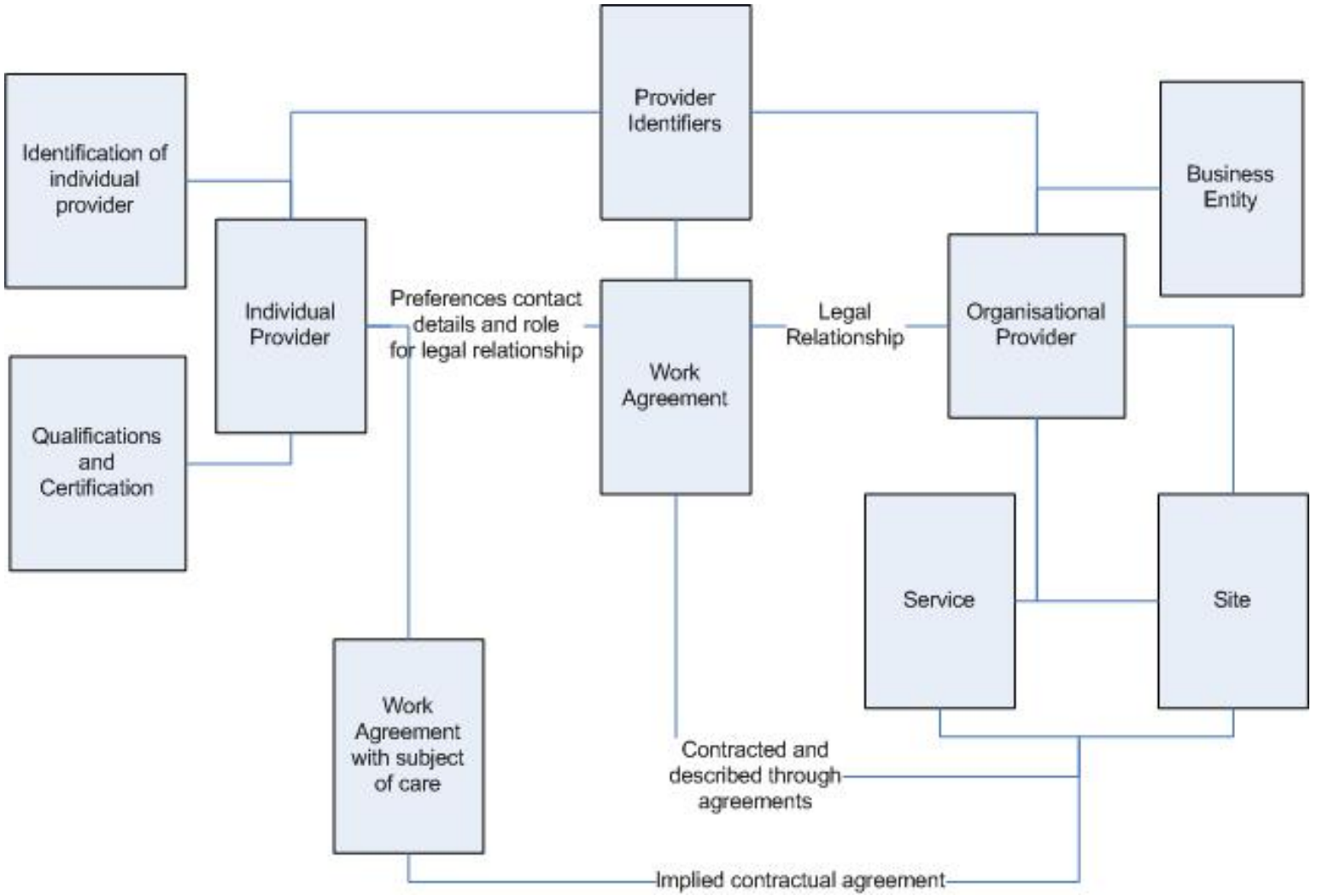
Patientenmanagement-Prozess



Bernd Blobel, PhD, Asssociate Professor
eHealth Competence Center, Regensburg
Email: bernd.blobel@klinik.uni-regensburg.de

ISO TS 27527 Health informatics – Provider identification

Typische Komponenten eines Leistungserbringer-Registers



Bernd Blobel, PhD, Asssociate Professor
eHealth Competence Center, Regensburg
Email: bernd.blobel@klinik.uni-regensburg.de

Identifikatorenzuweisung an Leistungserbringer

Die folgenden Kriterien und Charakteristika für Leistungserbringer-Identifikatoren wurden vom ASTM E1714-95 *Guide for Properties of a Universal Identifier (UHID)* adaptiert.

Atomar – der Leistungserbringer-Identifikator sollte ein einzelnes Data Item sein. Es sollte keine Subelemente enthalten, die eine Bedeutung außerhalb des Kontextes des gesamten Identifikators haben. Noch sollte die Identifikatorenzuweisung aus mehreren Items bestehen, die gemeinsam benutzt werden müssen, um einen Identifikator darzustellen.

Inhaltsfrei – der Leistungserbringer-Identifikator sollte nicht von möglicherweise veränderlichen oder unbekannten Informationen im Zusammenhang mit dem Leistungserbringer abhängen. Die Einbeziehung solcher Inhalte in den Identifikator wird es unmöglich machen, den korrekten Identifikator zuzuweisen, wenn diese Information nicht bekannt ist. Es würde auch zu ungültigen Situationen führen, wenn die Information sich ändert: Was würde z.B. passieren, wenn ein Identifikator auf dem Geschlecht basiert und das Subjekt eine Geschlechtsumwandlung vornehmen lässt.

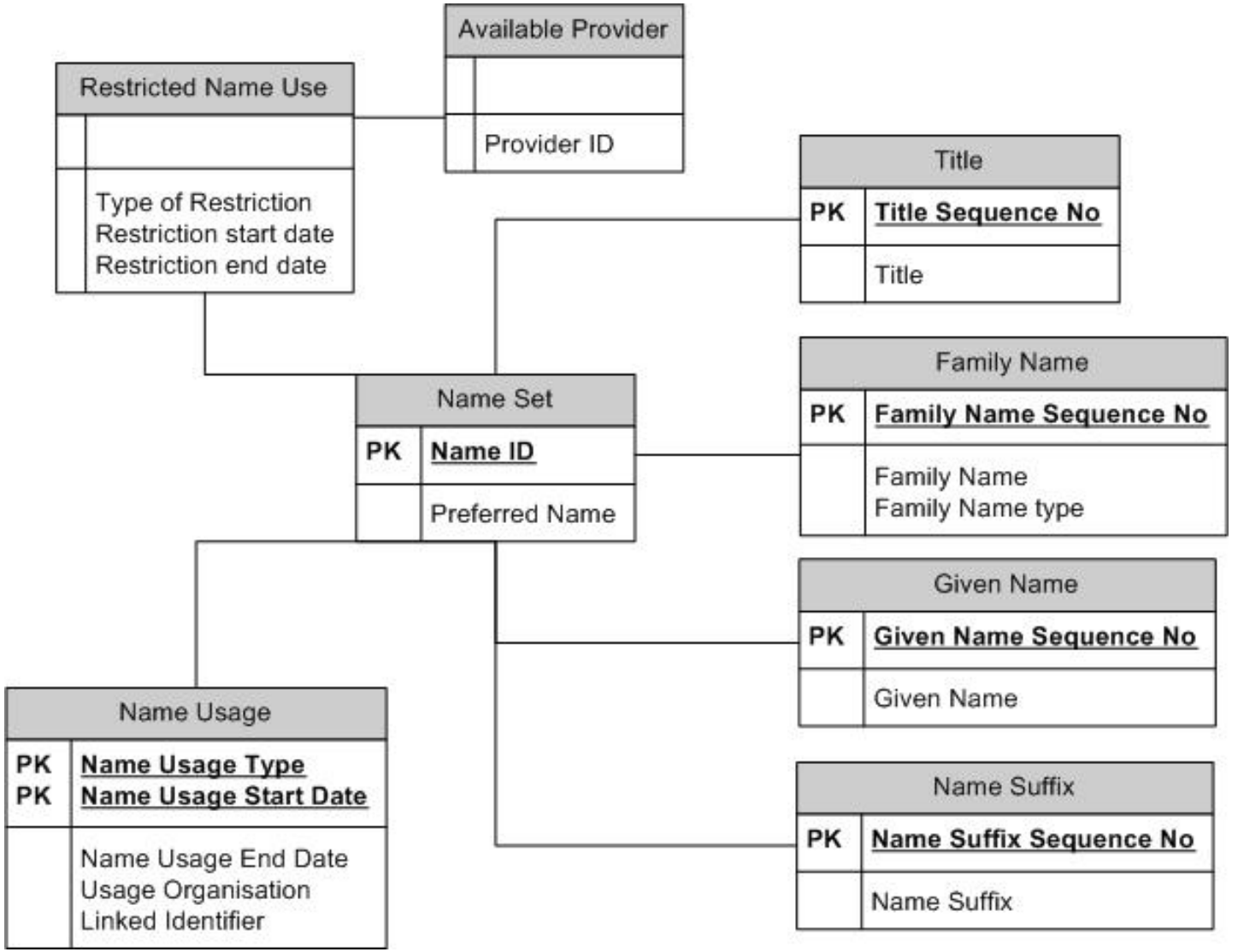
Langlebigkeit – das Leistungserbringer-Identifikationssystem sollte für die vorhersehbare Zukunft gestaltet werden. Es sollte keine bekannten Limitierungen enthalten, die das System zu einer radikalen Umstrukturierung oder Revision zwingen würden.

Permanent – wenn einmal zugewiesen, sollte ein Leistungserbringer-Identifikator bei dem individuellen Leistungserbringer erhalten bleiben. Er sollte nie einem anderen Subjekt zugewiesen werden, nicht einmal nach dem Tod des Subjekts.

Unzweideutig – gleich ob in einer automatisierten oder handschriftlichen Form dargeboten, sollte ein Leistungserbringer-Identifikator das Risiko einer Fehlinterpretation minimieren. Wo Zeichenketten-Identifikatoren benutzt werden, sollte man sich möglicher Konfusionen mit der Zahl 0 und dem Buchstaben O sowie der Zahl 1 und dem Buchstaben l bewusst sein.

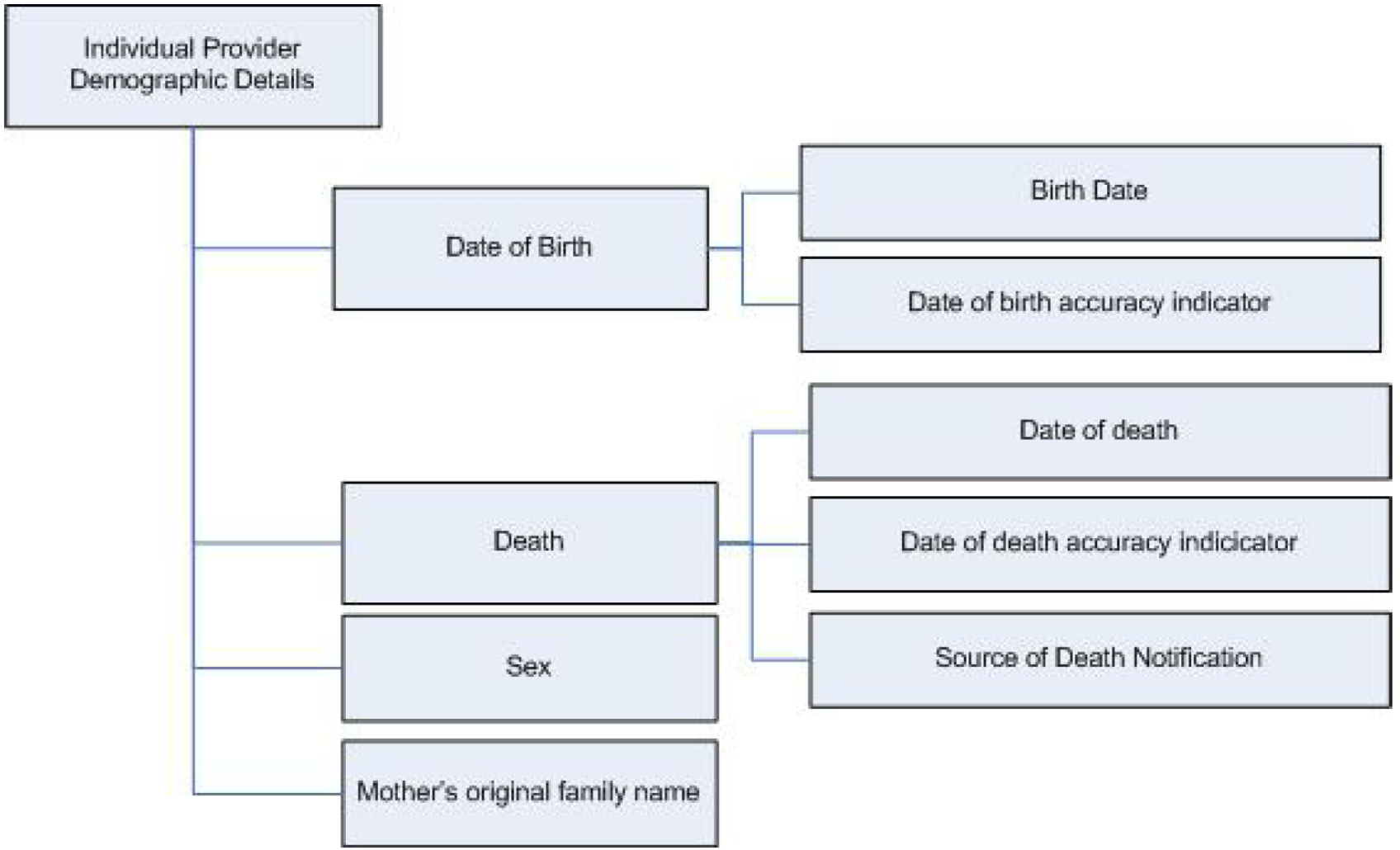
Einzigartig – eine gültige Leistungserbringer-Identifikatorzuweisung sollte einen und nur einen Leistungserbringer identifizieren.

Beziehungen zwischen Namens-Datenelementen



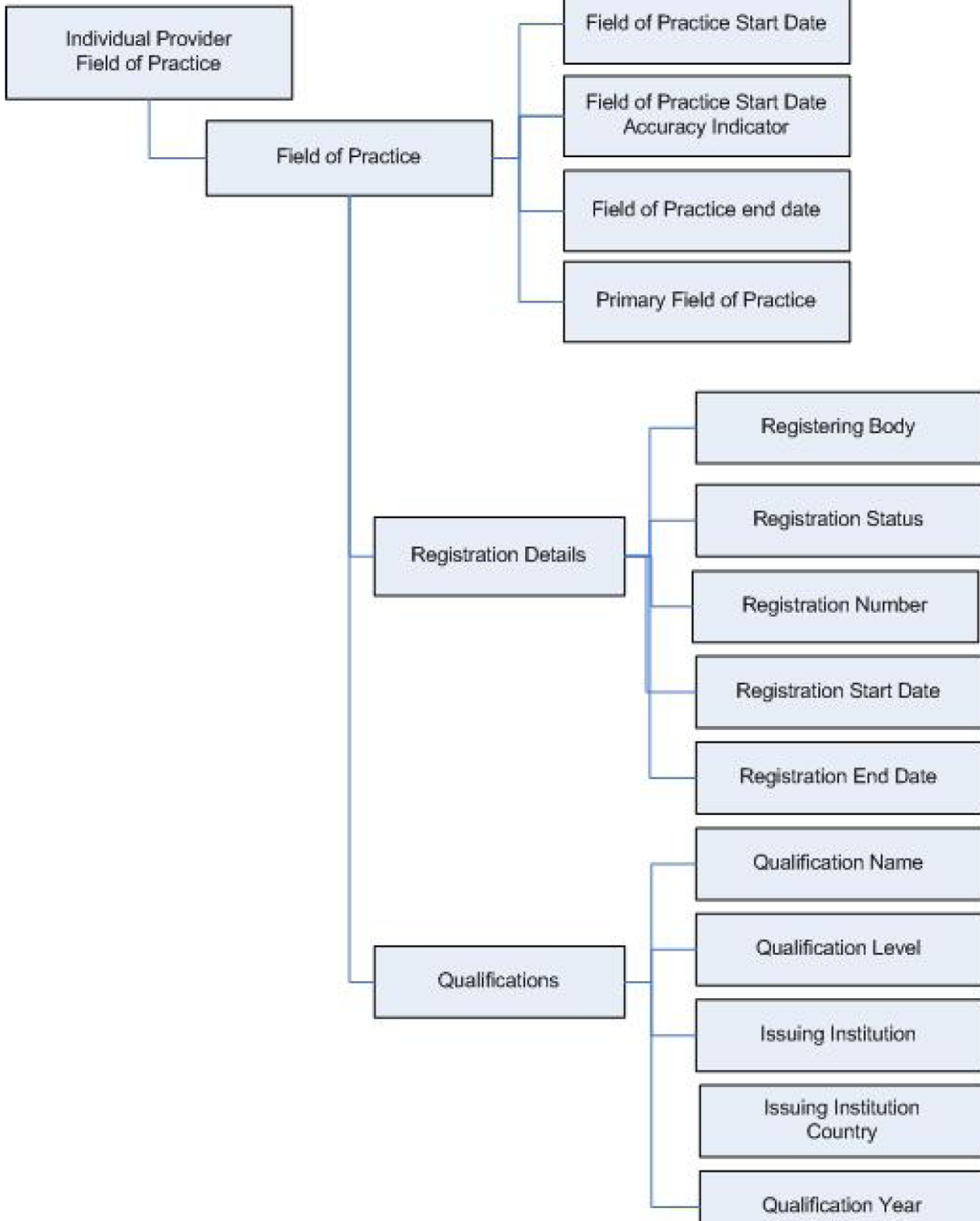
Bernd Blobel, PhD, Asssociate Professor
eHealth Competence Center, Regensburg
Email: bernd.blobel@klinik.uni-regensburg.de

Struktur der demographischen Details individueller Leistungserbringer



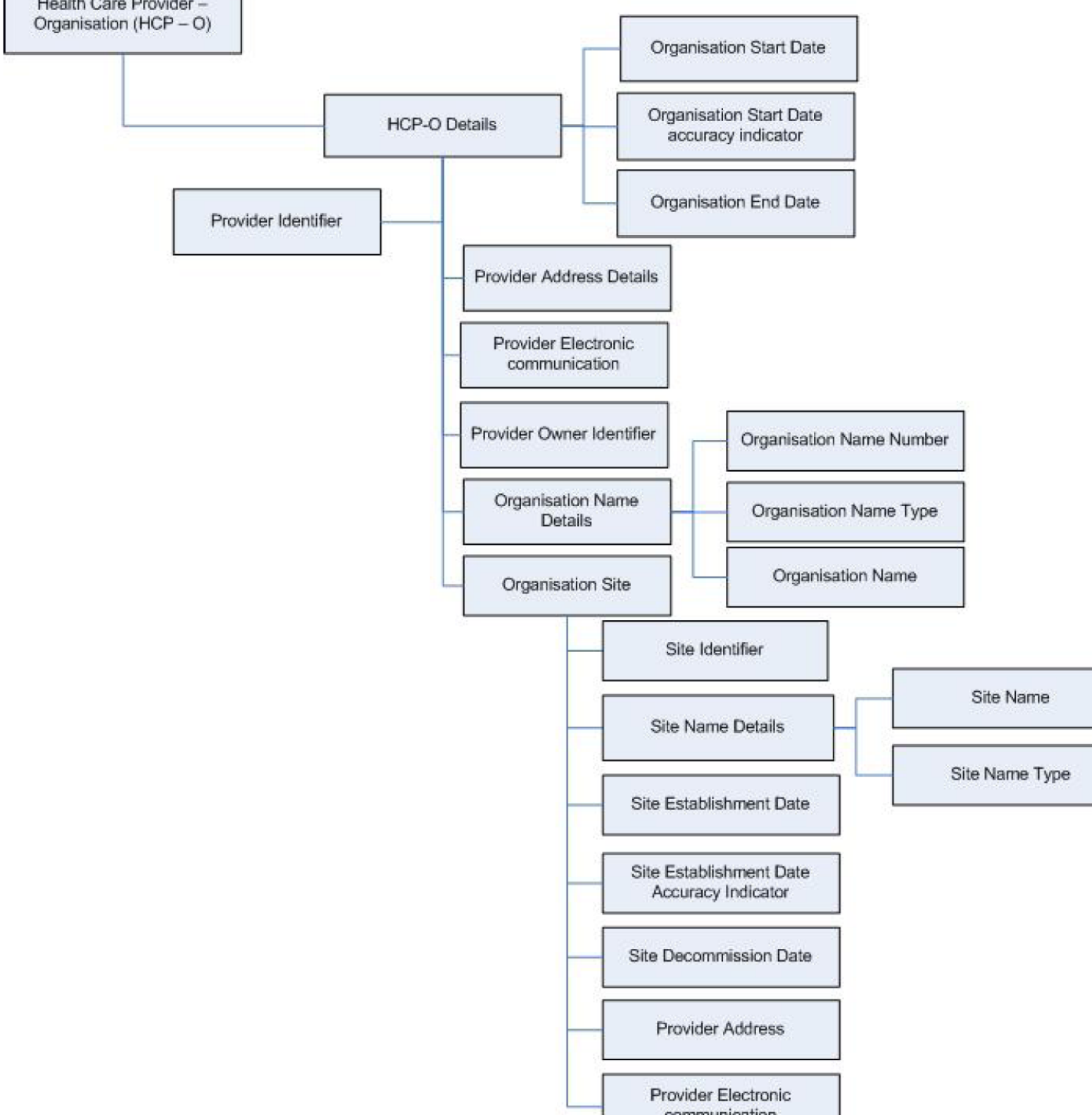
Bernd Blobel, PhD, Asssociate Professor
eHealth Competence Center, Regensburg
Email: bernd.blobel@klinik.uni-regensburg.de

Struktur und Komponenten von individuellen Tätigkeits-feldern



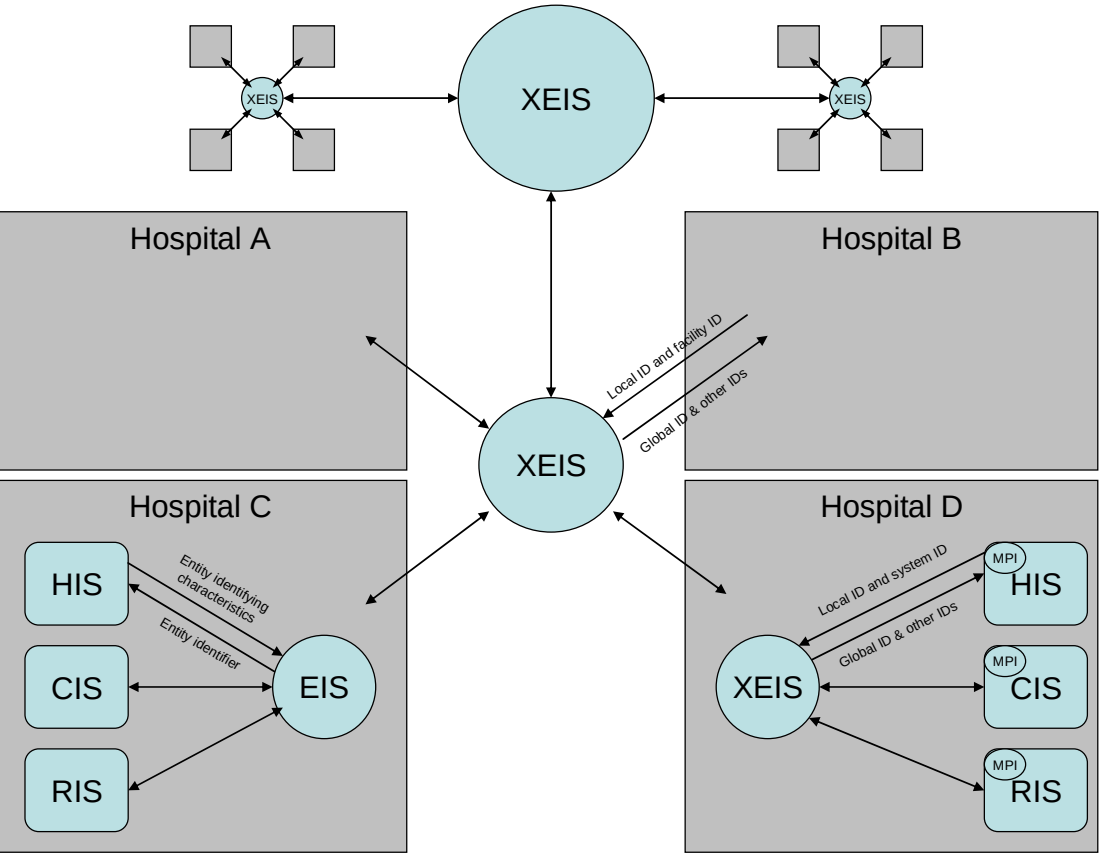
Bernd Blobel, PhD, Asssociate Profe
eHealth Competence Center, Regen
Email: bernd.blobel@klinik.uni-reger

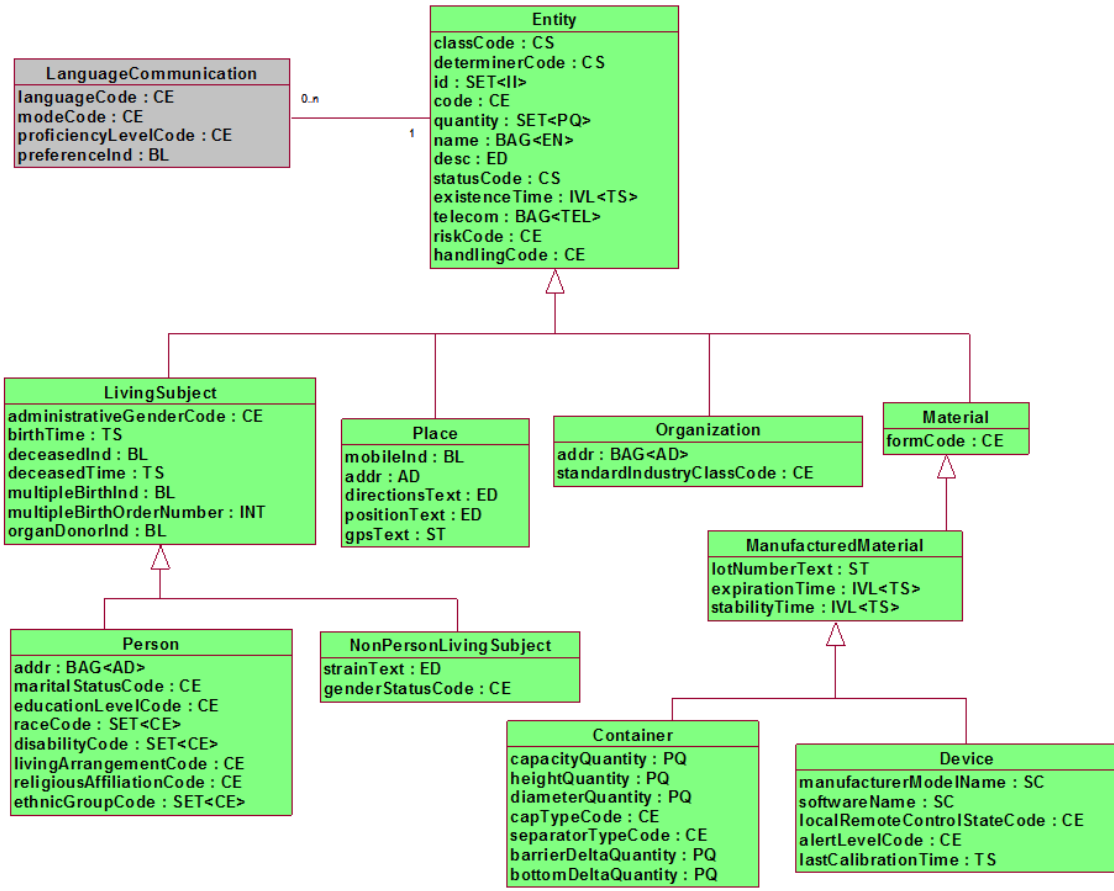
Struktur und Komponenten von Identifikatoren für die Leistungserbringer-Organisation



Bernd Blobel, PhD,
eHealth Competenc
Email: bernd.blobel

SOA4HL7 Entity Identification Services Spezifikation



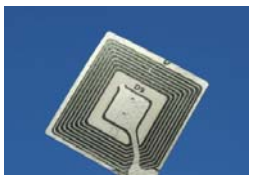


Bernd Blobel, PhD, Asssociate Professor
eHealth Competence Center, Regensburg
Email: bernd.blobel@klinik.uni-regensburg.de

Biometrie und RFID für ID-Management

Handgeometrie

Iris scan



RFID

Finger-print

Bernd Blobel, PhD, Asssociate Professor
eHealth Competence Center, Regensburg
Email: bernd.blobel@klinik.uni-regensburg.de

Biometrische Technologien

Erkennen von

- Fingerprint
- Handgeometrie
- Iris
- Gesicht
- Gefäßstrukturen
- Handschrift
- Stimme

Bernd Blobel, PhD, Asssociate Professor
eHealth Competence Center, Regensburg
Email: bernd.blobel@klinik.uni-regensburg.de

Biometrie (Biometrics) Definitionen

- Biometrics ist eine Kombination von Biologie, Elektronik und Genetik, die den Körper in ein “Passwort” konvertiert, welches nicht verändert oder reproduziert werden kann (Aldo Agostini, President – Security Studio System s.r.l., Presentation of annual report 2002)

- Biometrische Daten können stets als Information bezogen auf eine natürliche Person betrachtet werden, die infolge ihrer Natur Informationen über eine gegebene Person liefert. (EC, Working document on Biometrics, paragraph 3.1)

Biometrics Standards

- ISO/IEC 11694-6:2006 Identification cards -- Optical memory cards -- Linear recording method -- Part 6: Use of biometrics on an optical memory card
- ISO/IEC 18013-1:2005 Information technology -- Personal identification -- ISO-compliant driving licence -- Part 1: Physical characteristics and basic data set
- ISO/IEC 24713-2:2008 Information technology -- Biometric profiles for interoperability and data interchange -- Part 2: Physical access control for employees at airports
- ISO/IEC TR 24714-1:2008 Information technology -- Biometrics -- Jurisdictional and societal considerations for commercial applications -- Part 1: General guidance
- ISO/IEC 19785-1:2006, Information technology -- Common Biometric Exchange Formats Framework -- Part 1: Data element specification
- ISO/IEC 19785-2:2006, Information technology -- Common Biometric Exchange Formats Framework -- Part 2: Procedures for the operation of the Biometric Registration Authority

- Cooperation between ISO/IEC JTC1, SC31, SC 6, ITU-T, & NFC Forum

Einige JTC1 Subcommittees / SC 37 Working Groups

- ….
- SC 17 - CARDS AND PERSONAL IDENTIFICATION
- SC 27 - IT SECURITY TECHNIQUES
- SC 31 - AUTOMATIC IDENTIFICATION AND DATA CAPTURE TECHNIQUES
- SC 32 - DATA MANAGEMENT AND INTERCHANGE
- SC 35 - USER INTERFACES
- SC 37 – BIOMETRICS

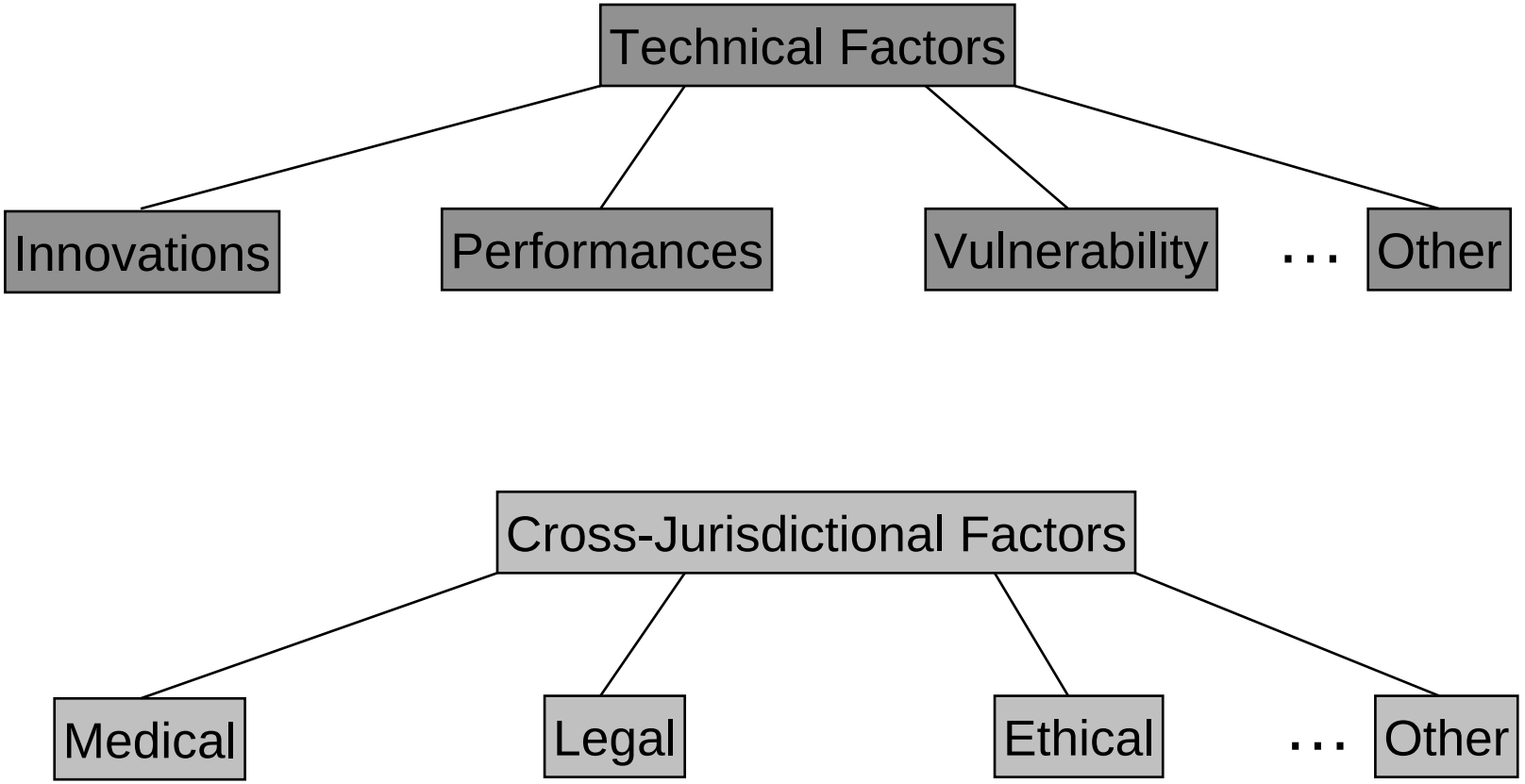
- WG 1 - WORKING GROUP ON HARMONIZED BIOMETRIC VOCABULARY AND DEFINITIONS
- WG 2 - WORKING GROUP ON BIOMETRIC TECHNICAL INTERFACES
- WG 3 – WORKING GROUP ON BIOMETRIC DATA INTERCHANGE FORMATS
- WG 4 - WORKING GROUP ON PROFILES FOR BIOMETRIC APPLICATIONS (US)
- WG 5 - WORKING GROUP ON BIOMETRIC TESTING & REPORTING
- WG 6 – WORKING GROUP ON CROSS-JURISDICTIONAL AND SOCIETAL ASPECTS OF BIOMETRICS

Hauptanwendungen von Biometrie im Gesundheitsbereich

- Physikalische Zugangskontrolle:
  - Zu Sicherheitszonen in Krankenhäusern
  - U.a. zu Bereichen, in denen die Gefahr der Entführung von Kleinkindern besteht
- Logische Zugangskontrolle
  - Sichere Anmeldeverfahren für Ärzte und Krankenschwestern beim Zugang zu elektronischen Krankenakten

Bernd Blobel, PhD, Asssociate Professor
eHealth Competence Center, Regensburg
Email: bernd.blobel@klinik.uni-regensburg.de

Einige technische und gerichtsbarkeitsbezogene Faktoren biometrischer Verfahren (nach Savastano)



Bernd Blobel, PhD, Asssociate Professor
eHealth Competence Center, Regensburg
Email: bernd.blobel@klinik.uni-regensburg.de

Zusammenfassung und Schlussfolgerungen

- ID-Management ist die Grundlage einer ganzen Reihe von Anwendungs- und Infrastrukturdiensten (hier insbesondere Security, Safety und Privacy Services).
- In mobilen, pervasiven und autonomen eHealth-Anwendungen betrifft ID-Management alle Principals (Personen, Organisationen, Systeme, Geräte, Applikationen, etc.).
- ID-Management beinhaltet neben den technischen auch rechtliche, organisatorische und soziale Aspekte.
- ID-Management nimmt inzwischen eine zentrale Stellung in der internationalen Standardisierung ein. So gibt es neben den “klassischen” ID-Management Standards eine ganze Serie von Health Informatics Standards und NWI zur Thematik.

- **Weitere Informationen finden sich auf der Webseite des BioHealth-Projektes http://www.bio-health.eu**

eHealth Competence Center
eHCC
Bernd Blobel, PhD, Asssociate Professor
eHealth Competence Center, Regensburg
Email: bernd.blobel@klinik.uni-regensburg.de

Fragen und Hinweise

Kontakt:
Priv.-Doz. Dr. habil. Bernd Blobel
Leiter eHealth Competence Center
Klinikum der Universität Regensburg
Franz-Josef-Strauss-Allee 11
93053 Regensburg
Email: bernd.blobel@klinik.uni-regensburg.de
Tel.: 0941-944 6769
Fax: 0941-944 6766