TMF-Workshop am 11. Dezember 2006, Berlin
Sicherheitskonzepte in der vernetzten medizinischen Forschung

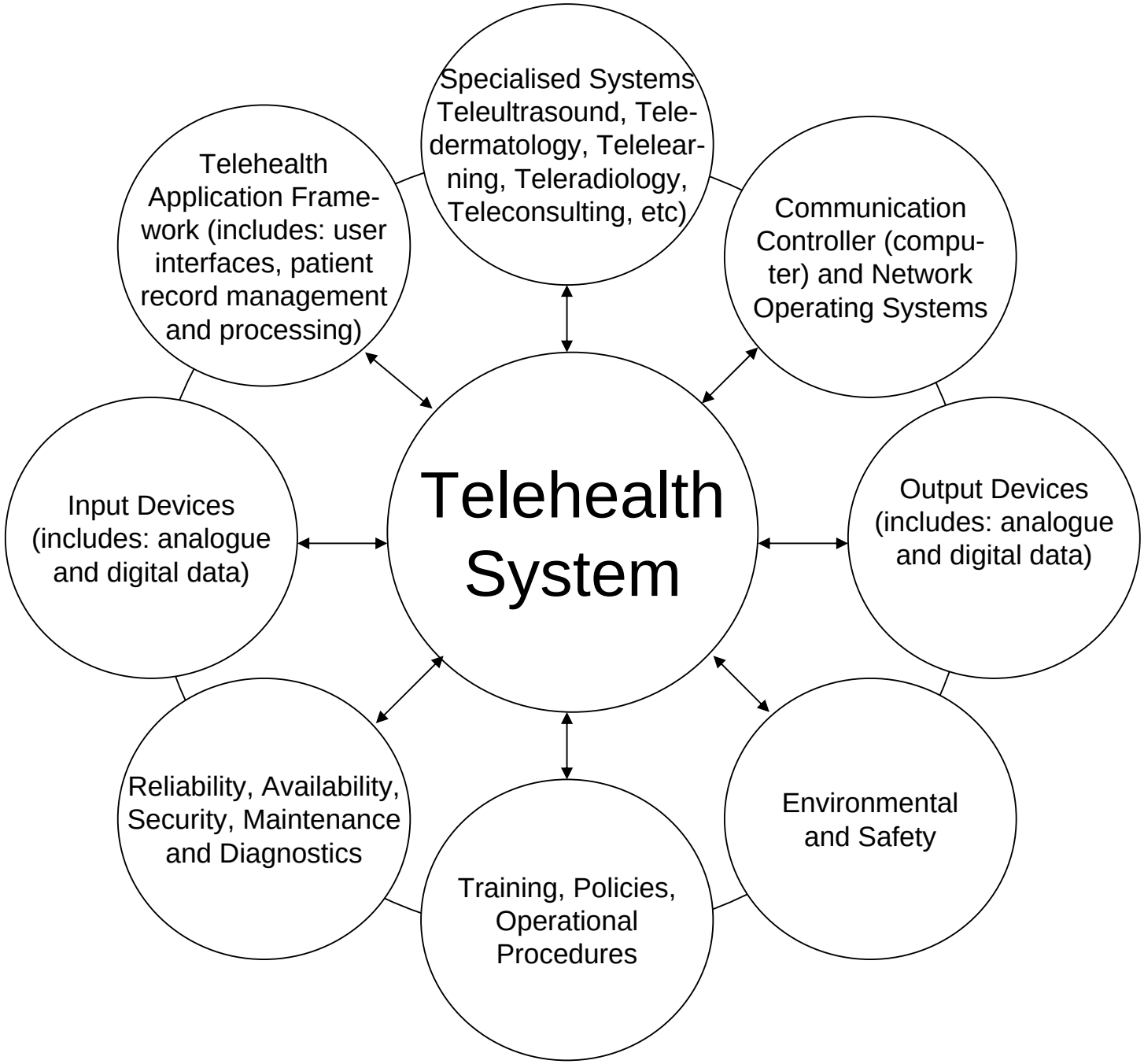
Sicherheitskonzepte für zukünftige Systemarchitekturen in der medizinischen Forschung

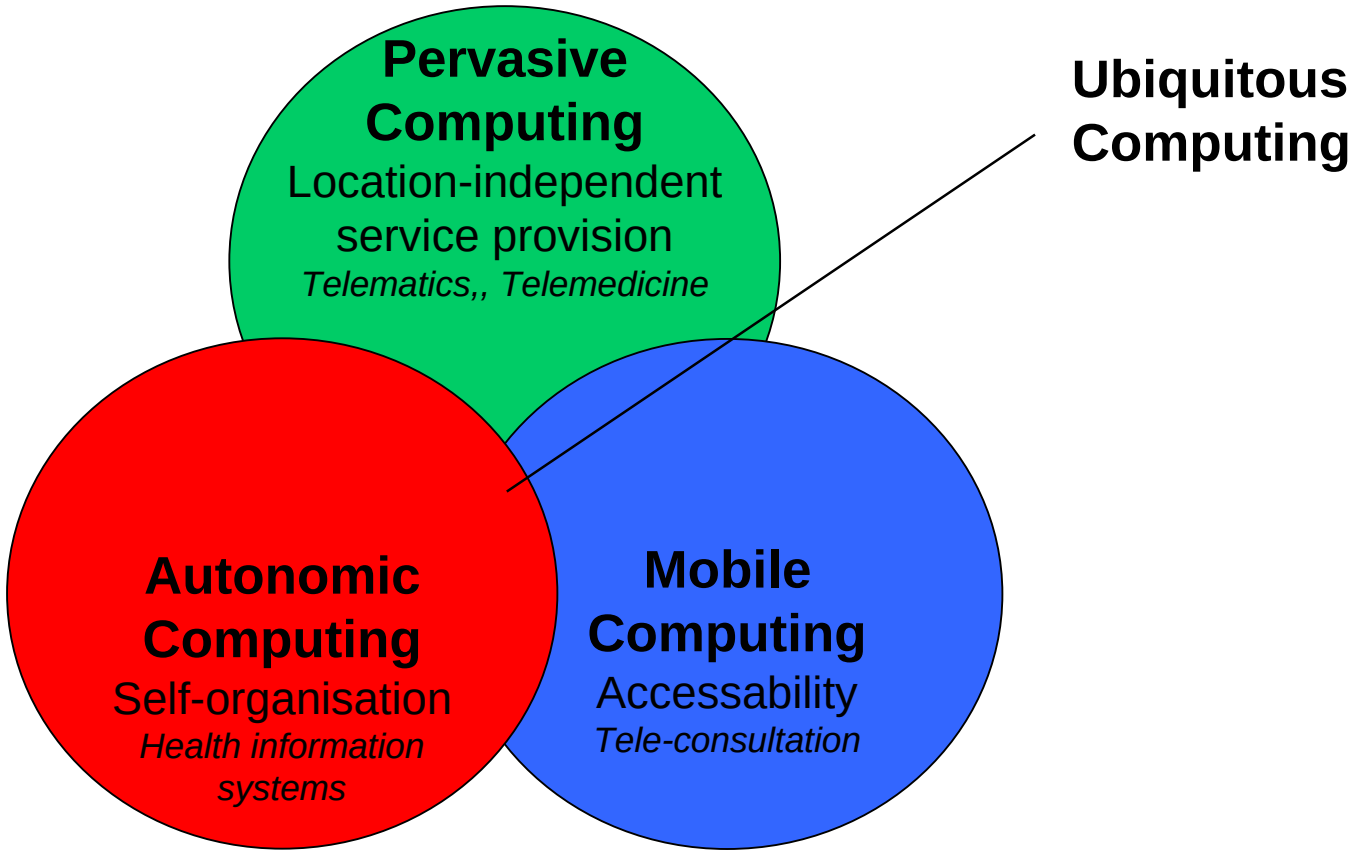
Bernd Blobel
eHealth Competence Center
Klinikum der Universität Regensburg

Background

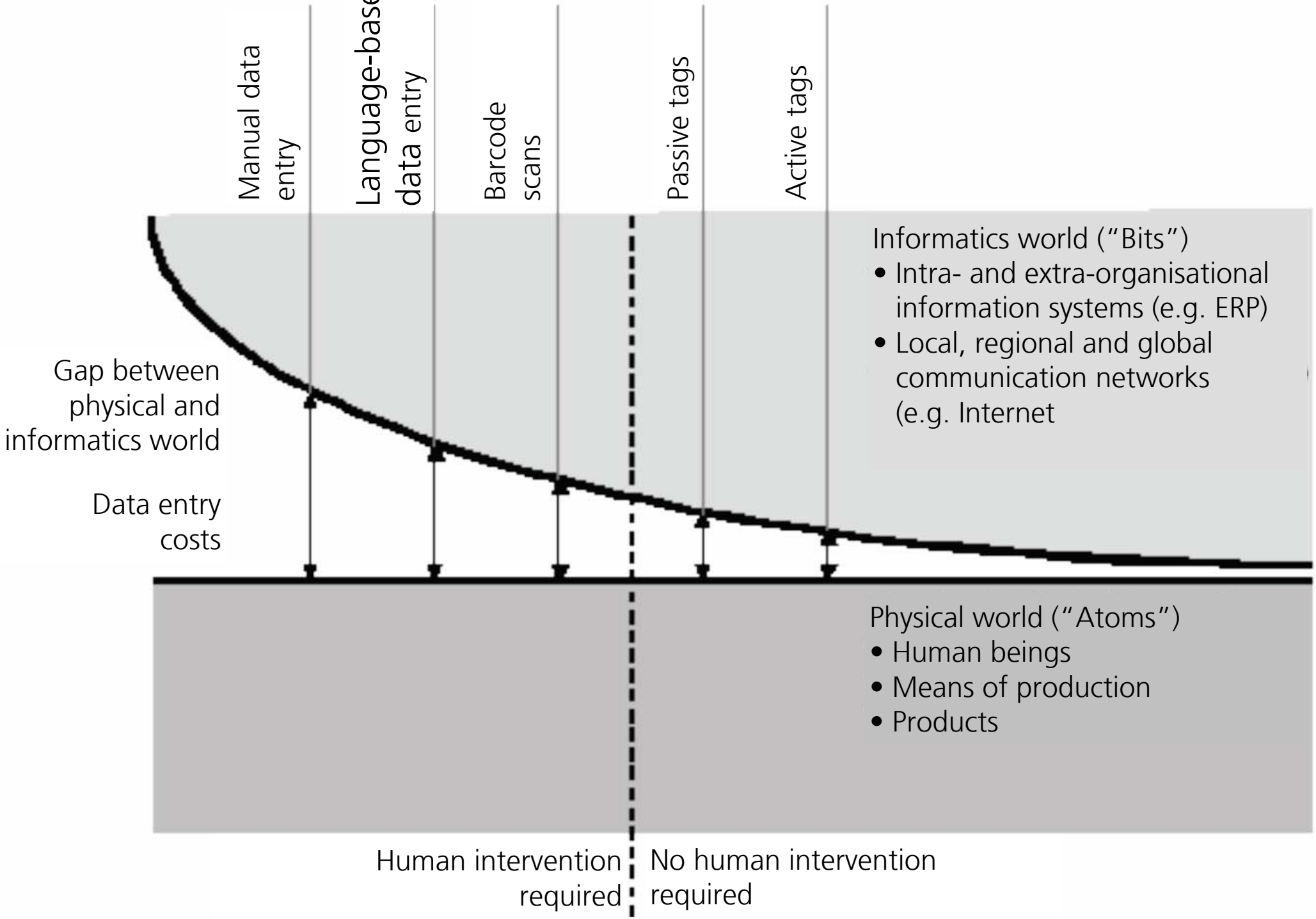
- 30 years CIO at Magdeburg University Hospital
- Director of the Institute for Biometry and Medical Informatics
- Past-Co-Chair, Security Working Group, German Medical Informatics Association
- Chair, WG “Security and Privacy in Health”, German Society for Privacy and Security
- Governmental Advisor, German National Health Telematics Platform Project
- Governmental Advisor, National eHealth Programmes in USA, Australia, Denmark, Finland, Malaysia, …
- Past-Chair CEN/ISSS eHealth Standardization Focus Group
- Chair, EFMI WG Security, Safety and Ethics
- Chair, EFMI WG Electronic Health Records
- Past-Chair, HL7 Germany
- Co-Chair, HL7 Security TC
- Member Security WG at ISO, CEN, CORBA, ASTM
- President, PROREC-DE

Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de


Specialised Systems Teleultrasound, Tele-dermatology, Telelear-ning, Teleradiology, Teleconsulting, etc)
Telehealth Application Frame-work (includes: user interfaces, patient record management and processing)
Communication Controller (compu-ter) and Network Operating Systems
Input Devices (includes: analogue and digital data)
Telehealth System
Output Devices (includes: analogue and digital data)
Reliability, Availability, Security, Maintenance and Diagnostics
Training, Policies, Operational Procedures
Environmental and Safety



Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de


Manual data entry
Language-based data entry
Barcode scans
Passive tags
Active tags
Gap between physical and informatics world
Data entry costs
Informatics world ("Bits")
• Intra- and extra-organisational information systems (e.g. ERP)
• Local, regional and global communication networks (e.g. Internet
Physical world ("Atoms")
• Human beings
• Means of production
• Products
Human intervention required
No human intervention required

Policy-Controlled Security and Privacy Requirements in the Context of Model-Driven Architectures

Architecture Definition

An architecture of a system describes its components, their functions and relationships.

Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de

System Requirements

- Openness
- Flexibility
- Scalability
- Portability
- User acceptance
- Service orientation
- Distribution at Internet level
- Based on standards
- Service-oriented interoperability
- Appropriate security and privacy services

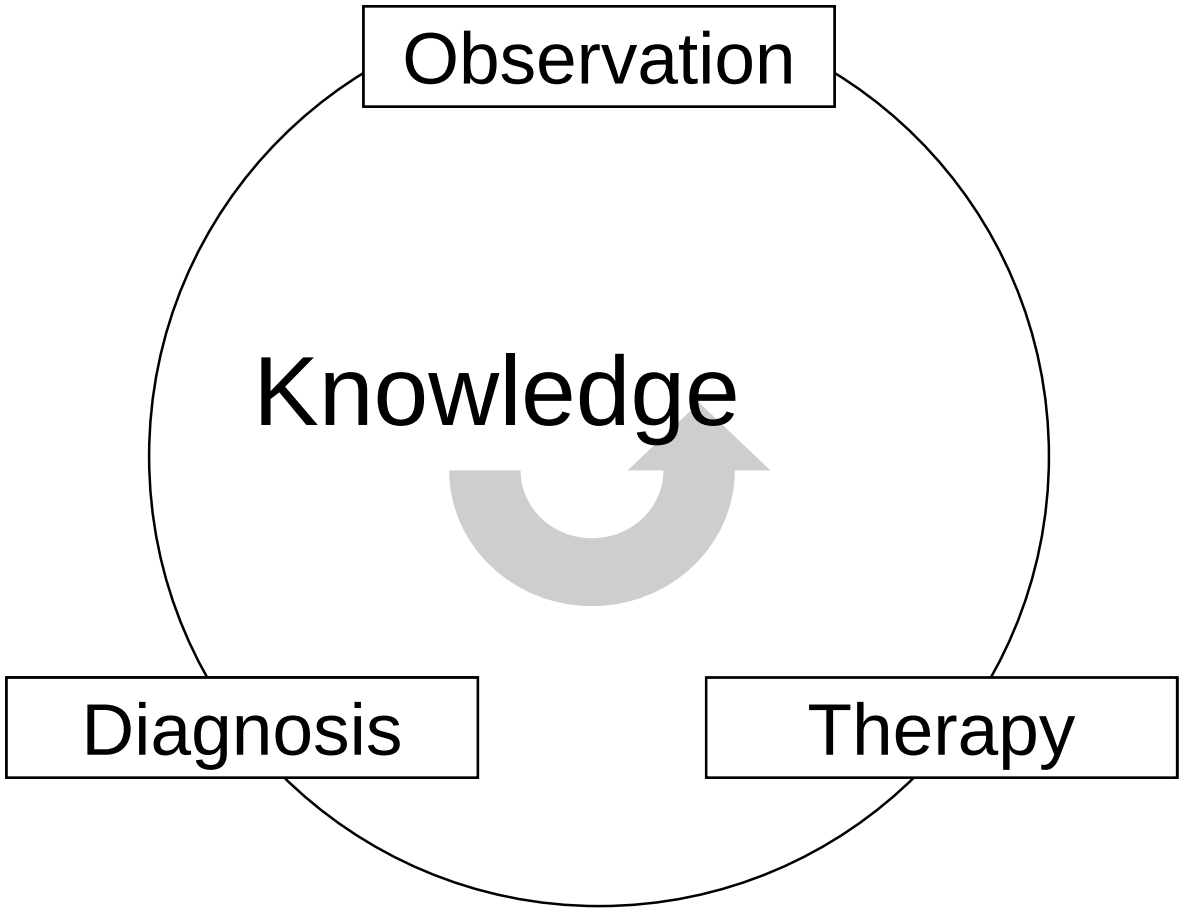
→ Model-driven approach

Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de

Model

A model is a partial representation of reality. It is restricted to attributes the modeller is interested in. Defining the pragmatic aspect of a model, the interest is depending on the addressed audience, the reason and the purpose of modelling the reality and using the resulting model for a certain purpose and for a certain time instead of the original. Therefore, the model as a result of an interpretation must be interpreted itself.

Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de



Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de

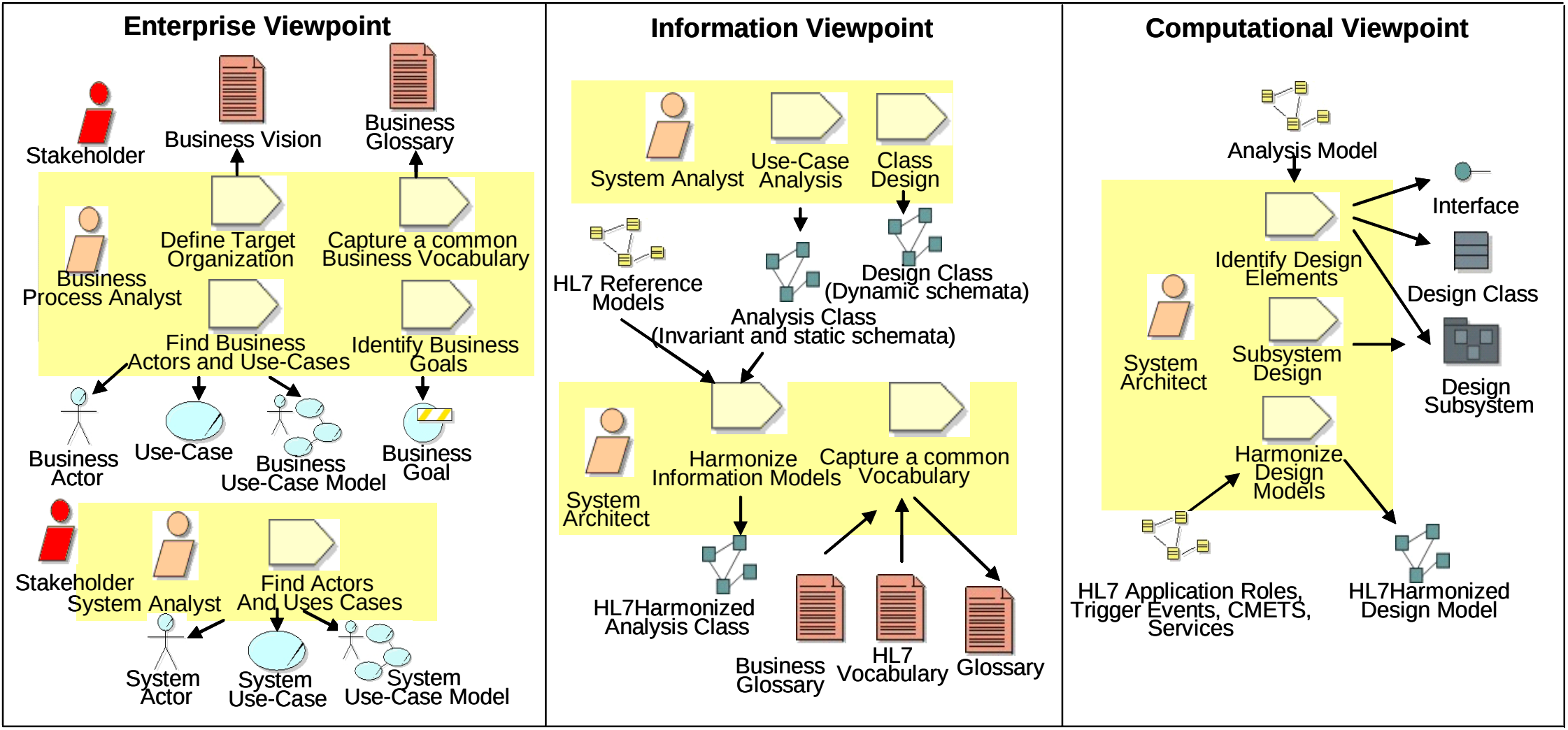
The Generic Component Model

Architectural Paradigms for Future-Proof Health Information Systems

- Distribution
- Component-orientation (flexibility, scalability)
- Separation of platform-independent and platform-specific modelling →
- Separation of logical and technological views (portability)
- Specification of reference and domain models at meta-level
- Interoperability at service level (concepts, contexts, knowledge)
- Enterprise view driven design (user acceptance)
- Multi-tier architecture (user acceptance, performance, etc.)
- Appropriate multi-media GUI (illiteracy)
- Common terminology and ontology (semantic interoperability)
- Unified process (semantic interoperability)
- Appropriate security and privacy services

Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de

Sicherheitskonzepte für zukünftige Systemarchitekturen in der medizinischen Forschung



Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de

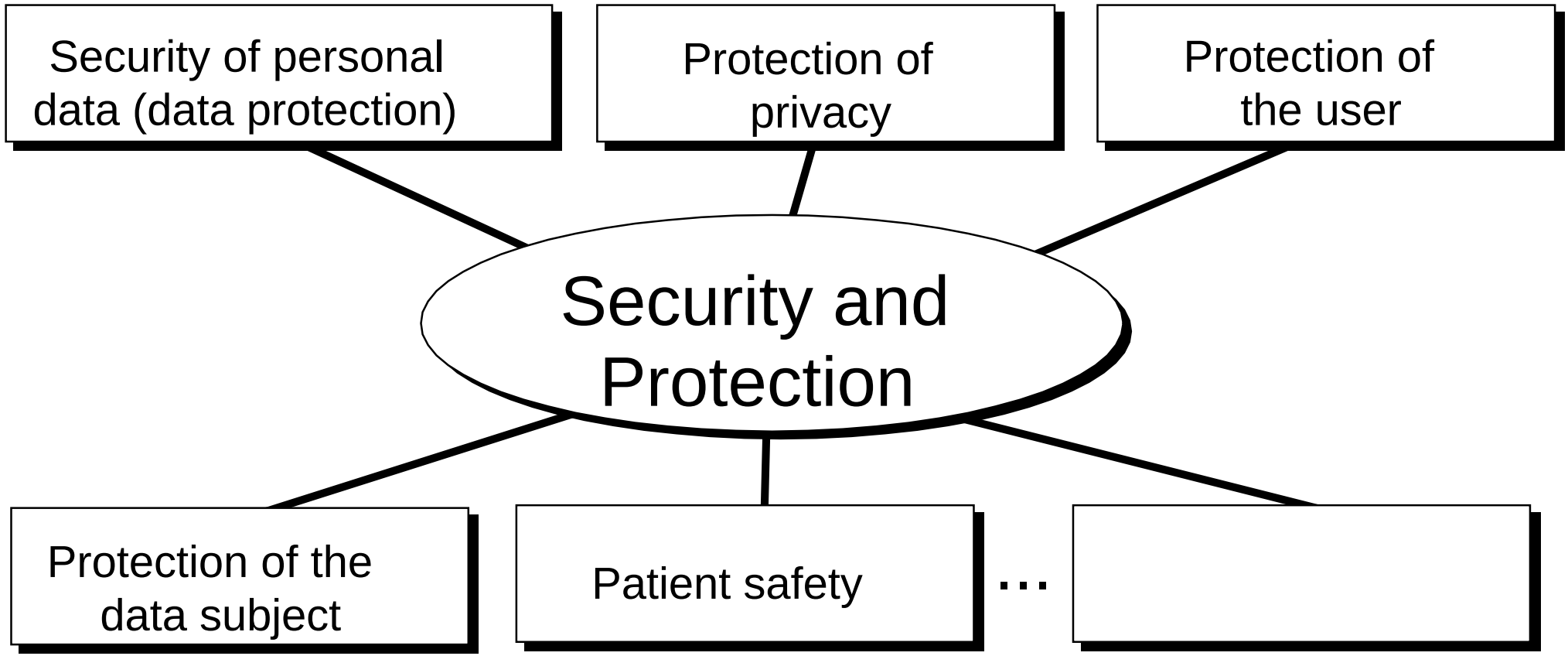
Telematikplattform für Medizinische Forschungsnetze e. V.

Key Principles for Improving and Developing a Culture of NIS

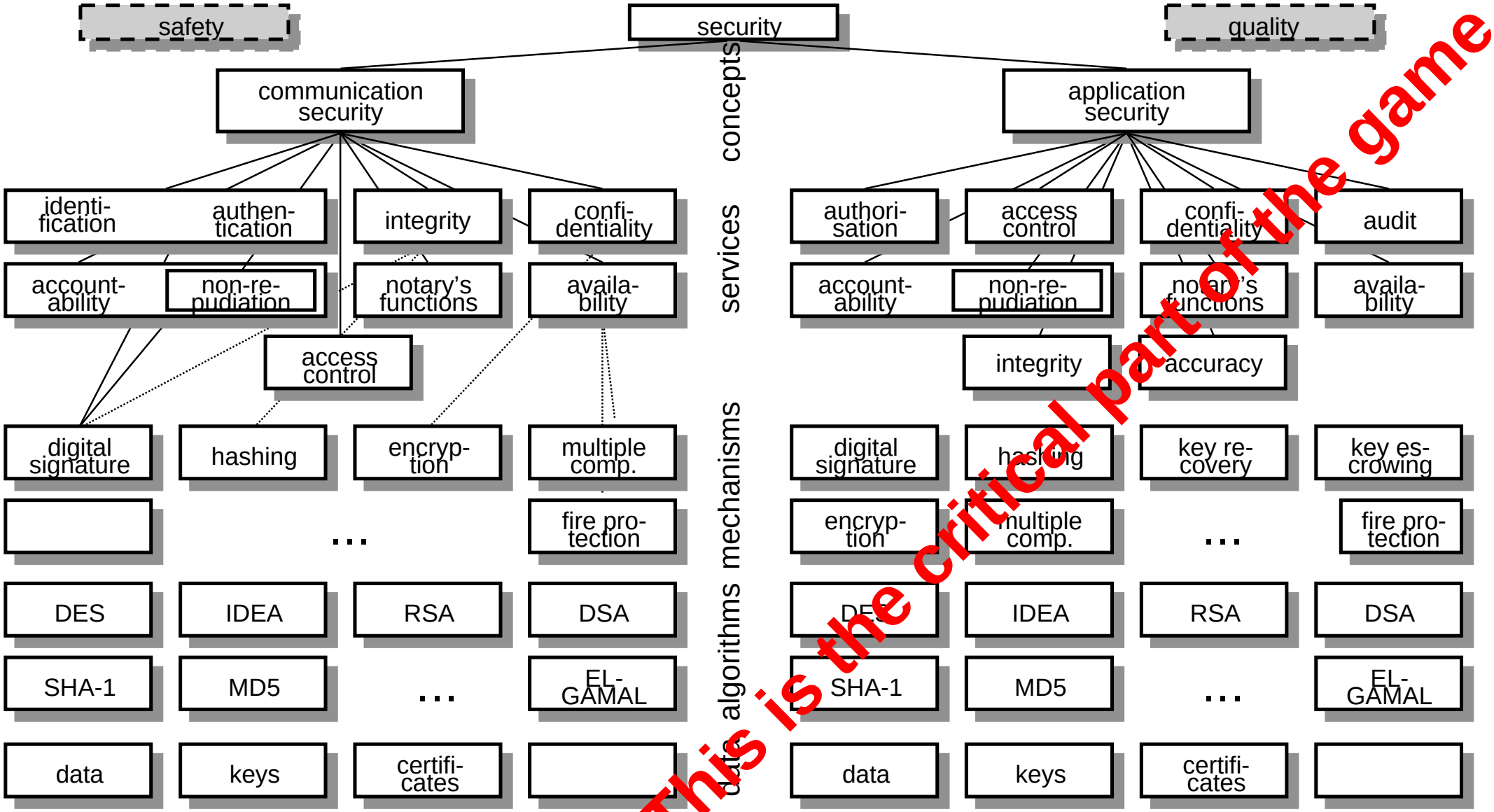
- Legal
  - Privacy and security are a prerequisite for guaranteeing fundamental rights on-line
- Economic
  - Present NIS as a virtue and an opportunity
- Social
  - Individual users need to understand that their home systems are critical for the overall security chain
- Technical
  - Promote diversity, openness and interoperability as integral components of security

Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de

Aspects of Protection and Security (after C. Laske)



Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de



Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de

Telematikplattform für Medizinische Forschungsnetze e.V.

Security Modelling for Analysis and Design

Models Used

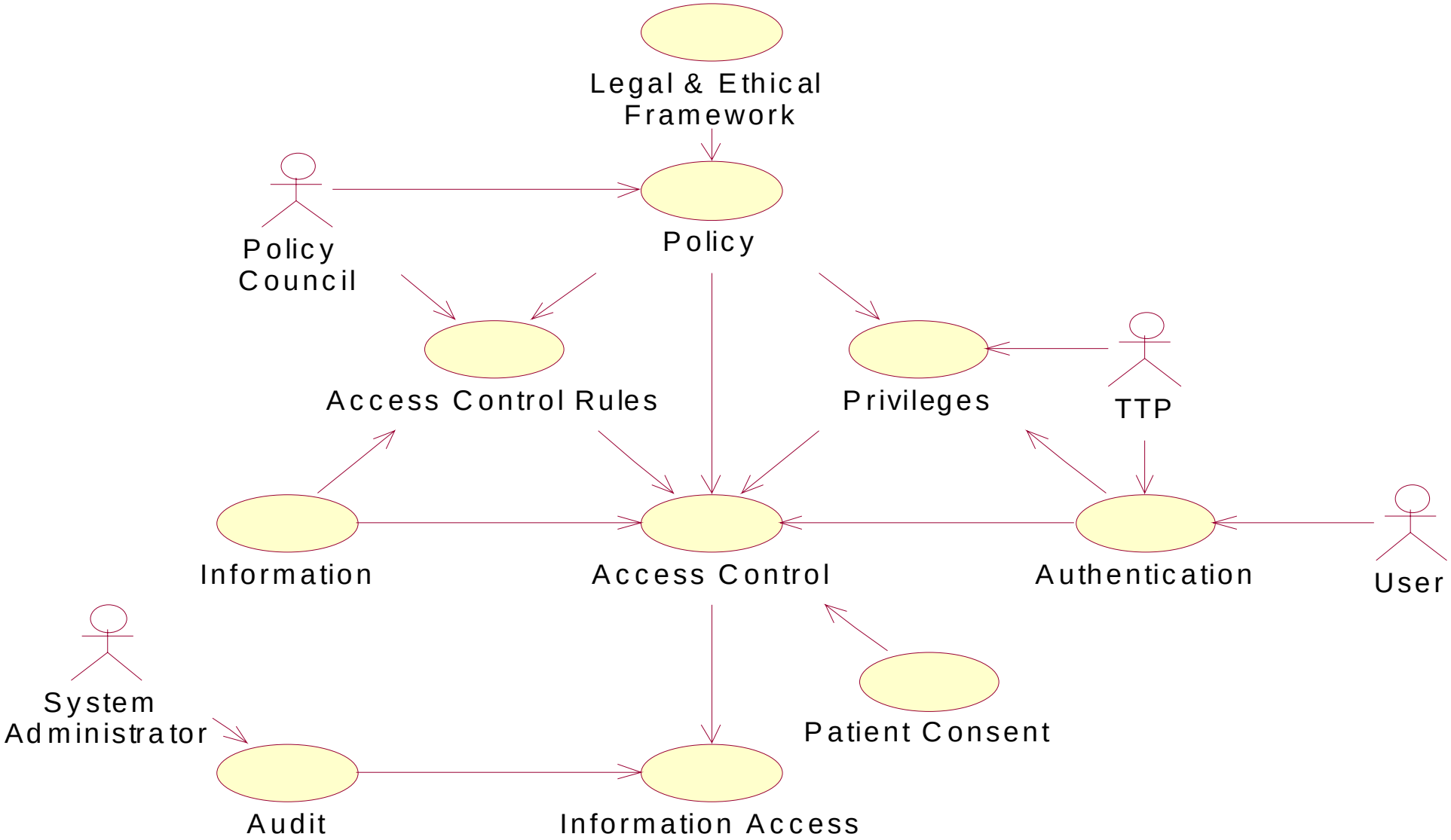
- Domain Model
- Document Model
- Information Distance Model
- Authentication Model
- Authorisation Model
- Communication Model
  - Secure Object
  - Secure Channel
- Policy Model
- Role Model
- Delegation Model
- Control Model
- Access Control Model
- Audit Model

Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de

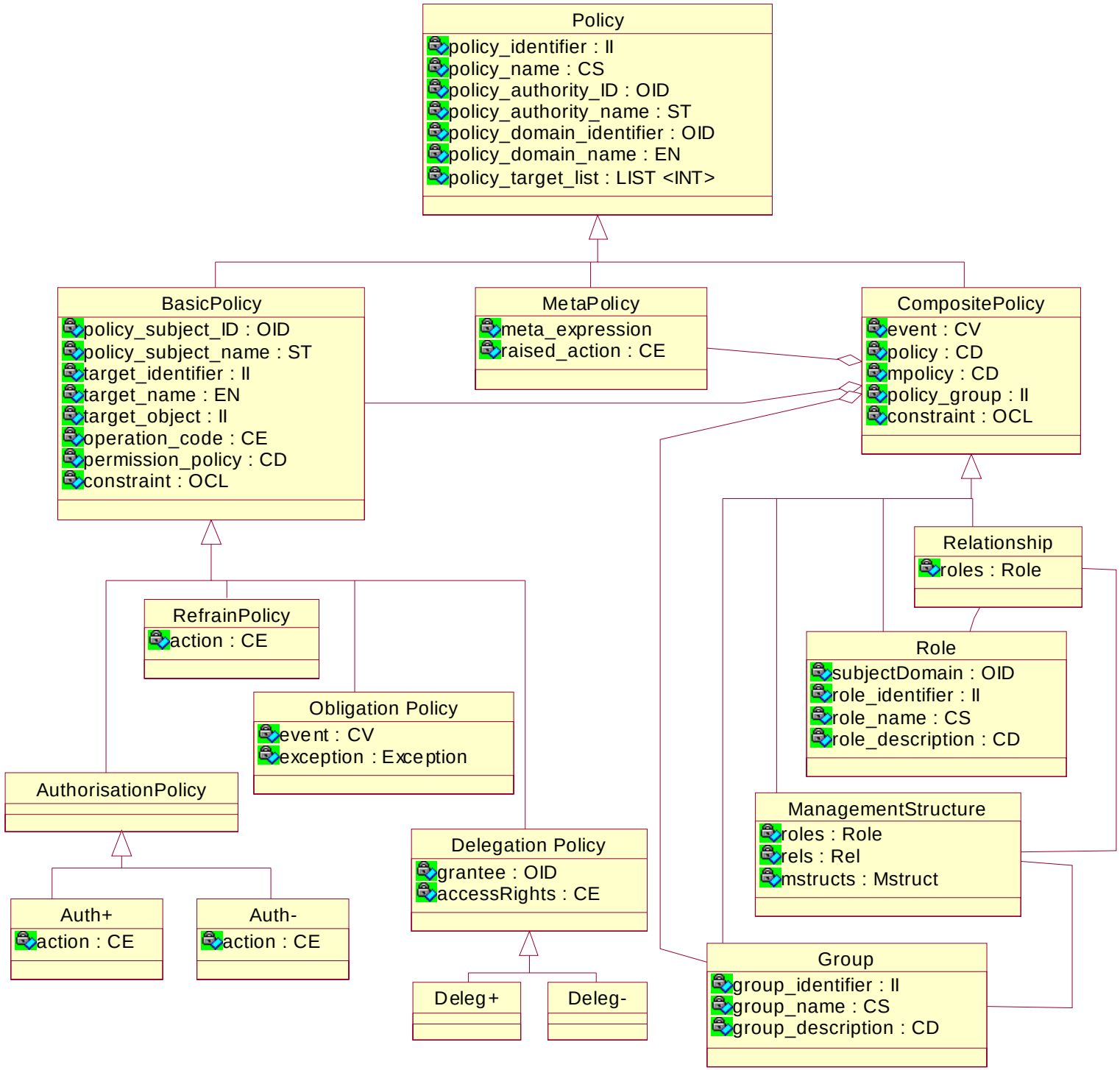
Domain Model

- The domain model describes the domain-specific constraints resulting from domain-specific requirements and representing the domain-specific knowledge for all the levels of abstraction mentioned. This concerns medical knowledge as well as legal basics, organisational relationships and the specific workflow.
- OMG has specified environmental domains, policy domains and technology domains.

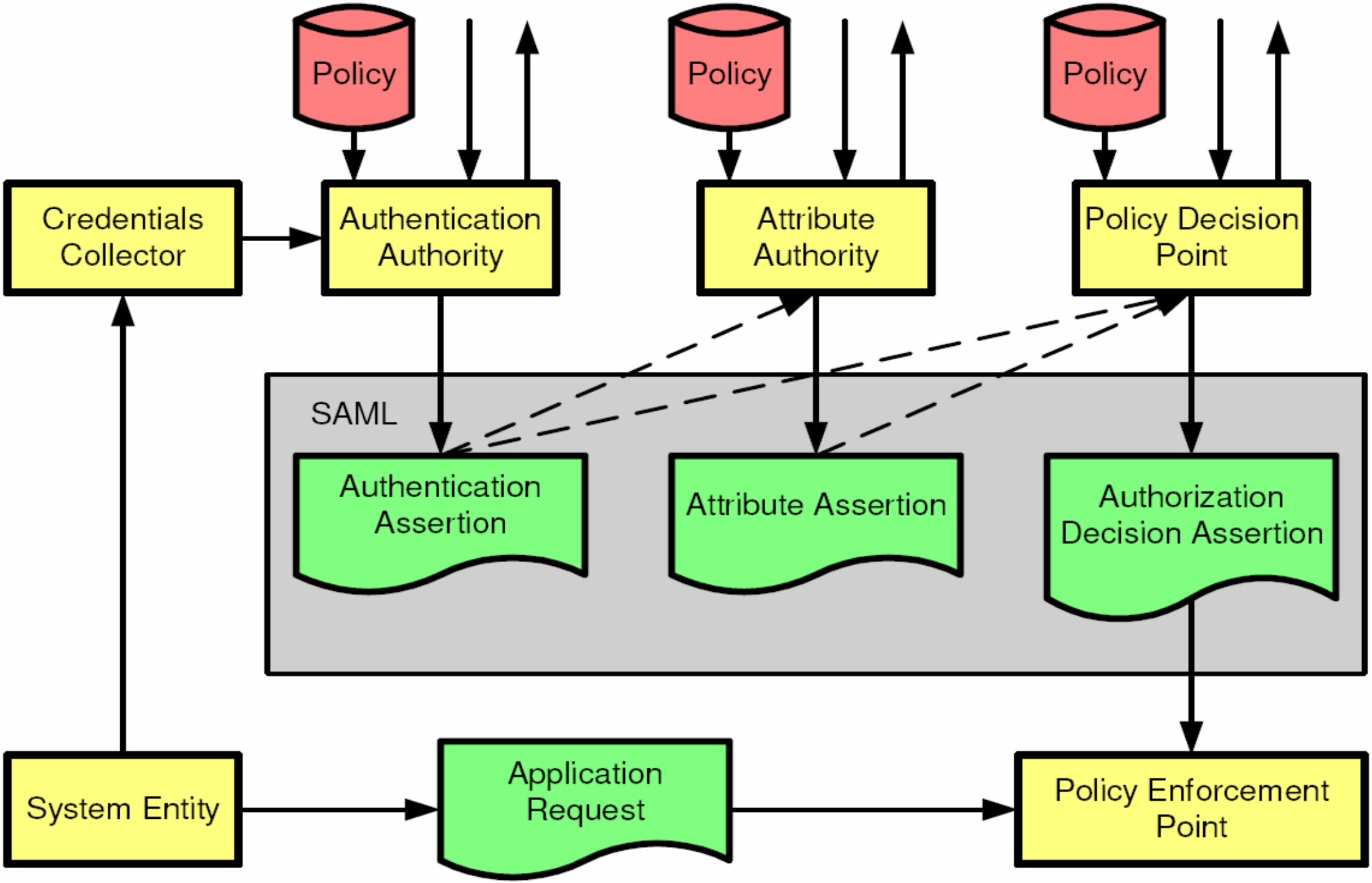
Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de



Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de

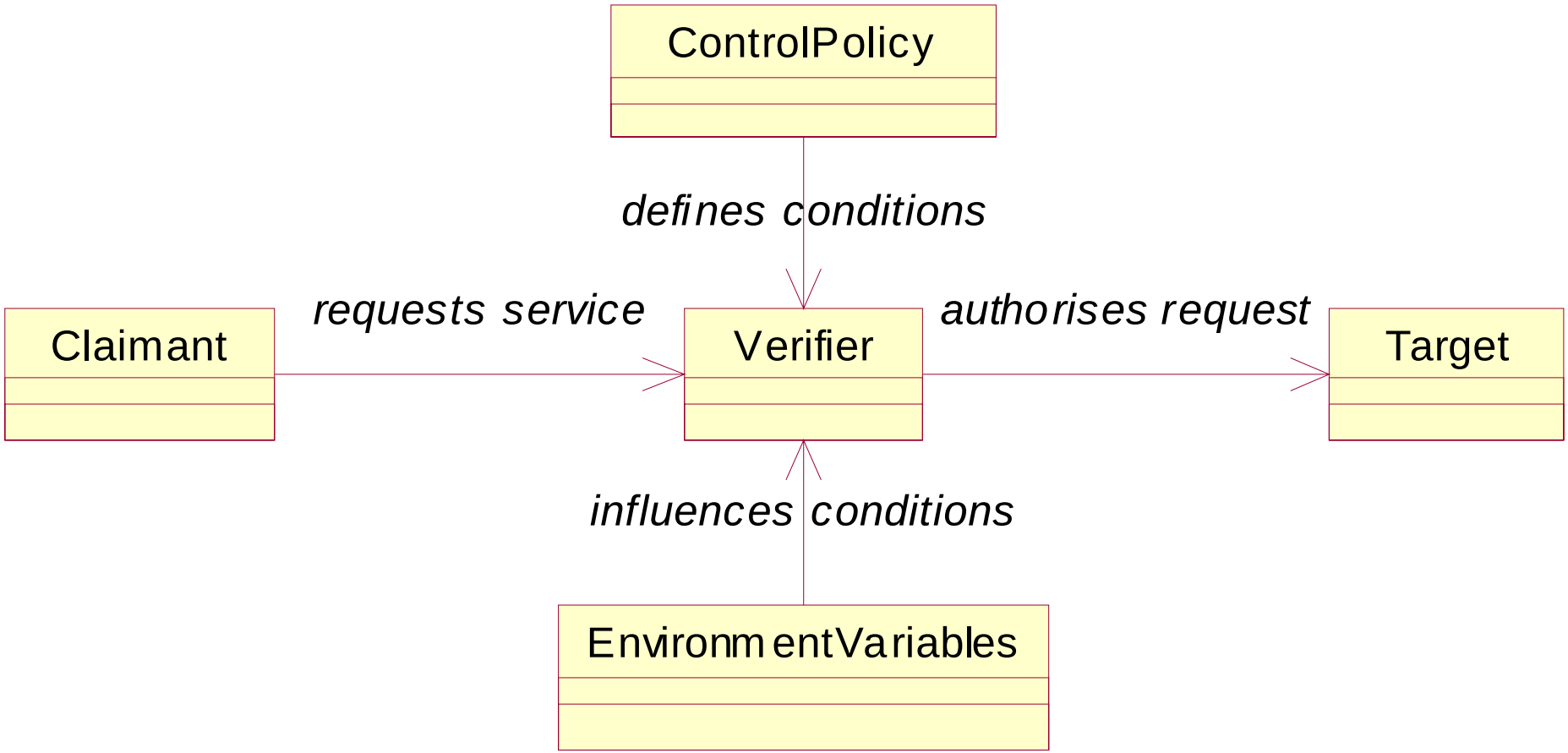

Policy
policy_identifier : II
policy_name : CS
policy_authority_ID : OID
policy_authority_name : ST
policy_domain_identifier : OID
policy_domain_name : EN
policy_target_list : LIST <INT>
BasicPolicy
policy_subject_ID : OID
policy_subject_name : ST
target_identifier : II
target_name : EN
target_object : II
operation_code : CE
permission_policy : CD
constraint : OCL
MetaPolicy
meta_expression
raised_action : CE
CompositePolicy
event : CV
policy : CD
mpolicy : CD
policy_group : II
constraint : OCL
RefrainPolicy
action : CE
Obligation Policy
event : CV
exception : Exception
AuthorisationPolicy
Auth+
action : CE
Auth-
action : CE
Delegation Policy
grantee : OID
accessRights : CE
Deleg+
Deleg-
Relationship
roles : Role
Role
subjectDomain : OID
role_identifier : II
role_name : CS
role_description : CD
ManagementStructure
roles : Role
rels : Rel
mstructs : Mstruct
Group
group_identifier : II
group_name : CS
group_description : CD

SAML Domain Model



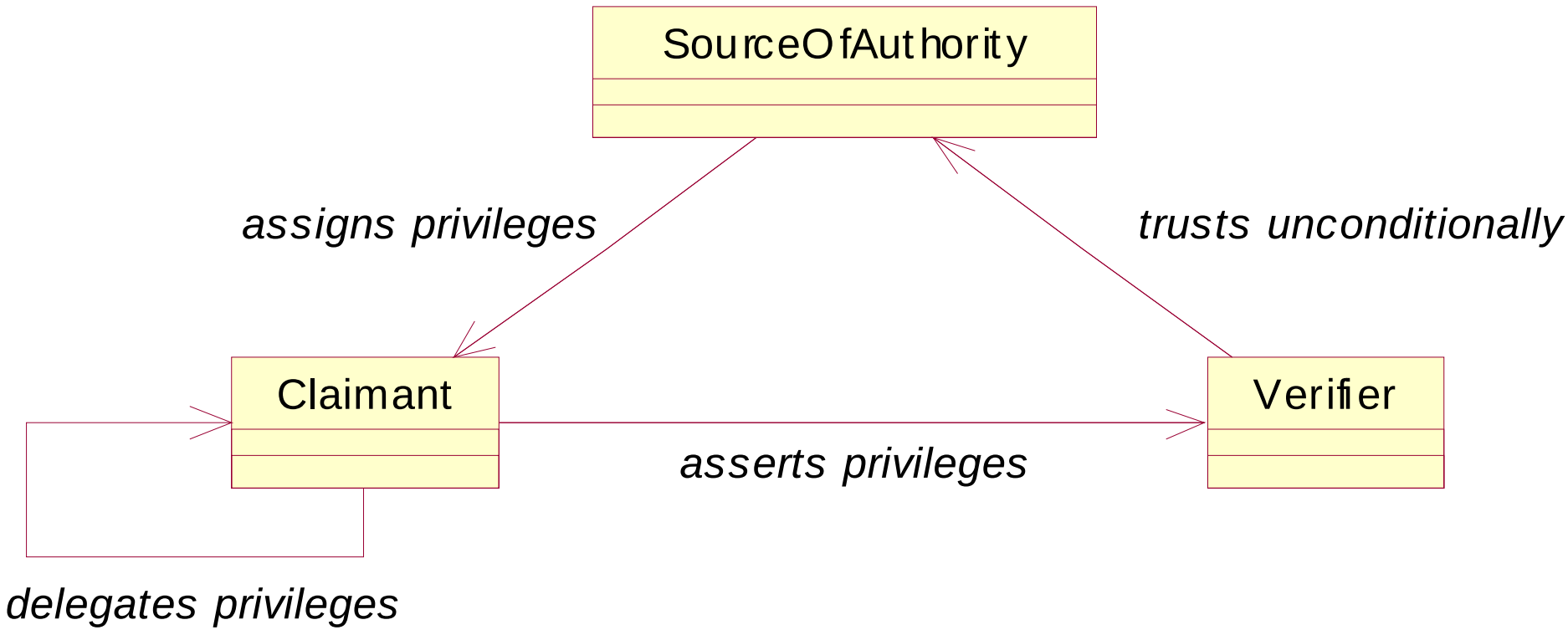
```
<S12:Envelope>
  <S12:Header>
    <wsse:Security>
      <saml:Assertion
        AssertionID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
        IssueInstant="2003-04-17T00:46:02Z"
        Issuer="www.opensaml.org"
        MajorVersion="1"
        MinorVersion="1"
          . . .
      </saml:Assertion>
      <wsse:SecurityTokenReference wsu:Id="STR1">
        <wsse:KeyIdentifier wsu:Id="…"
          ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-
token-profile-1.0#SAMLAssertionID">
          _a75adf55-01d7-40cc-929f-dbd8372ebdfc
        </wsse:KeyIdentifier>
      </wsse:SecurityTokenReference>
    </wsse:Security>
  </S12:Header>
  <S12:Body>
    . . .
  </S12:Body>
</S12:Envelope>
```

Control Model



Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de

Delegation Model



Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de

Roles

- For managing role-relationships between the entities, organisational and functional roles can be defined.
- Organisational roles specify relations between entities in the sense of competence (RIM roles) often reflecting organisational or structural relations (hierarchies).
- Functional roles are bound to an act. Functional roles can be assigned to be performed during an act. They correspond to the RIM participation.

Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de

Structural Role (ISO TS 17090)

- Regulated Health Professional
- Non Regulated Health Professional
- Sponsored Health Care Provider
- Supporting Organisation Employee
- Patient / Consumer

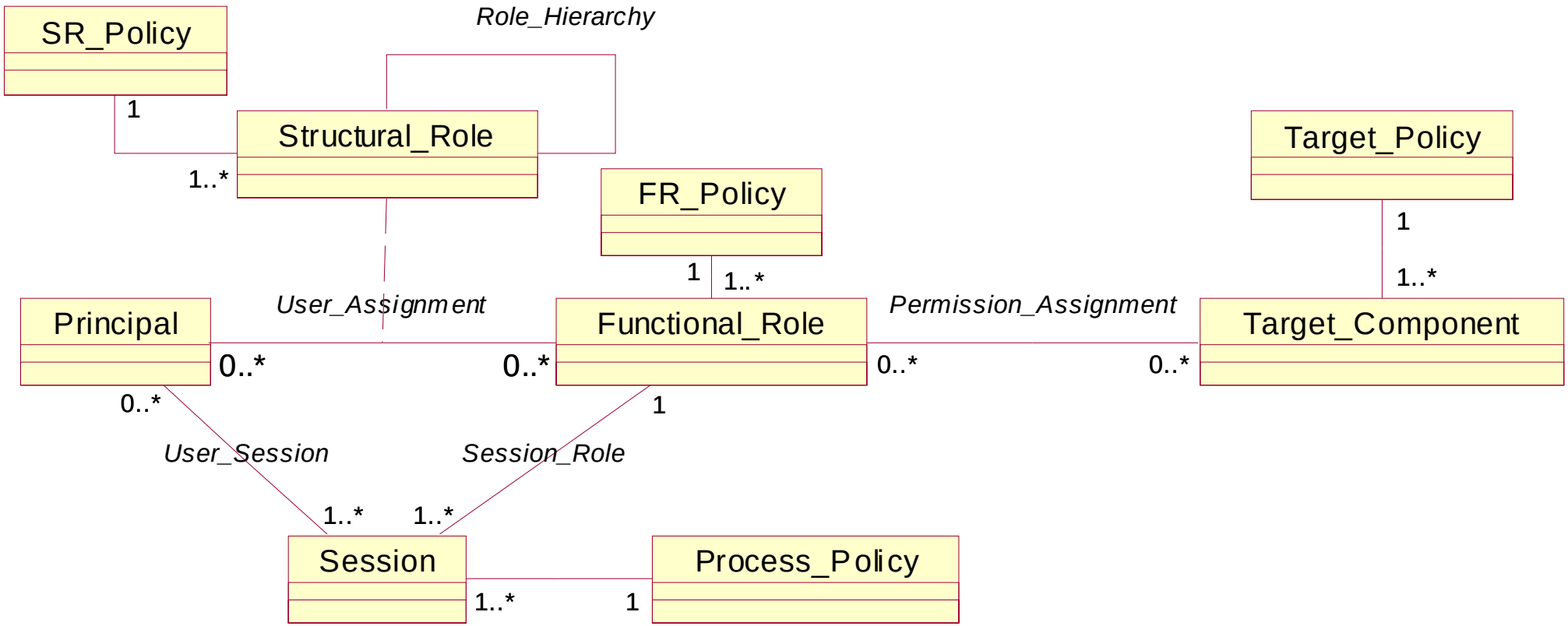
Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de

"Functional Roles" Established in the CEN ENV 13606 Revision

- Subject of care (normally the patient)
- Subject of care agent (parent, guardian, carer, or other legal representative)
- Responsible (personal) healthcare professional (the healthcare professional with the closest relationship to the patient, often his GP)
- Privileged healthcare professional
  - nominated by the subject of care
  - nominated by the healthcare facility of care (there is a nomination by regulation, practice, etc.)
- Healthcare professional (involved in providing direct care to the patient)
- Health-related professional (indirectly involved in patient care, teaching, research, etc.)
- Administrator (and any other parties supporting service provision to the patient)

Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de

Policy-Driven, Role-Based Access Control



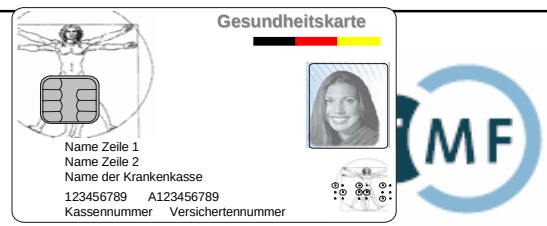
Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de

Telematikplattform für Medizinische Forschungsnetze e.V.

Important eHealth Components (logical view)

Knowledge Services	Application Services		Policy Services	ID CA Services
Client Services	EHR Systems	PKI	PMI	ACA Services
	Terminology Services		Audit Services	Directory Services

Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de



Conclusions

- Based on the Shared Care paradigm, health information systems require advanced security solutions
- Using cryptographic techniques, products are available for provision of both communication security and application security even on the open Internet
- Within projects funded by the European Commission and international standardisation bodies, the security infrastructure needed has been specified and implemented
- The security infrastructure of security tokens and TTP services is currently under standardisation
- Security complains legal, social, organisational, technical and psychological aspects
- Awareness, education and training of the health professionals are important security issues and challenges

Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de

BioHealth

Security and Identity Management Standards including Biometrics - Specific Requirements in eHealth having an Impact on the European Society and on Standardisation

BioHealth

- http://mirc.gsf.de/biohealth/
- bernd.blobel@klinik.uni-regensburg.de

- Innova
  - Web: http://www.europe-innova.org
  - Contact: Entr_europe-innova@cec.int

Bernd Blobel, Ph.D., Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Email: bernd.blobel@ehealth-cc.de

Telematikplattform für Medizinische Forschungsnetze e.V.

MEDTEL 2006 International Conference - eHealth Promotion, December 7 - 8, 2006

Announcement

eHealth: Combining Health Telematics, Telemedicine, Biomedical Engineering and Bioinformatics to the Edg

INTERNATIONAL CONFERENCE 2007
December 2-5, 2007
REGENSBURG / GERMANY

eHealth Competence Center
eHCC
REGENSBURG

For more information visit the Conference Website, please.

www.cehr.de

Conference Chair:
Bernd Blobel, PhD, Associate Professor
eHealth Competence Center
University of Regensburg Medical Center
Franz-Josef-Strauß-Allee 11
D-93042 Regensburg
Germany
Email: bernd.blobel@ehealth-cc.de
Email: bernd.blobel@klinik.uni-regensburg.de
Phone: +49-941-944 6769
Fax: +49-941-944 6766
http://www.ehealth-cc.de