International Congress “Information Technologies in Medicine”
13-14 October 2016 in Moscow, Russian Federation

Изменения парадигмы здравоохранения требуют новых подходов к безопасности и конфиденциальности – Часть 2

Prof. Dr. habil. Bernd Blobel, FACMI, FACHI, FHL7, FEFMI

Medical Faculty, University of Regensburg, Germany

Пожалуйста, смотрите 1 часть презентации в материалах пленарного заседания ИТМ2016 13.10.2016!

Bernd Blobel
University of Regensburg
Medical Faculty

Основные принципы построения культуры сетевой и информационной безопасности (СИБ) в информационном обществе (after Andrea Servida)

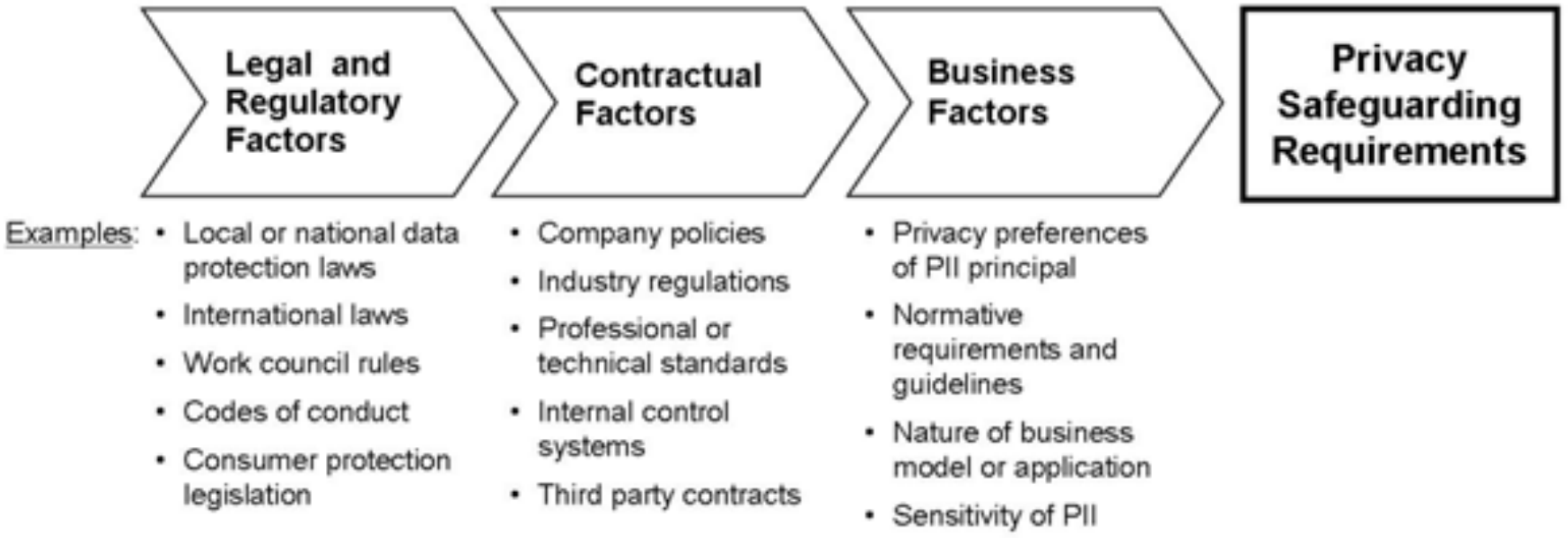
- Правовой
  - Конфиденциальность и безопасность являются предпосылками обеспечения базовых прав on-line
- Экономический
  - СИБ представляется как преимущество и набор возможностей
- Социальный
  - Конечный пользователь должен понять, что его домашние системы являются критическим звеном в цепи обеспечения безопасности
- Технический
  - Разнообразие технологий, открытость и интероперабельность должны рассматриваться как неотъемлемые компоненты безопасности

Злонамеренные действия: сфера конфиденциальность after ISO 29100

- Рекламные и шпион-программы
- Присвоение ресурсов
- Шантаж
- Раскрытие информации
- Мошенничество
- Нарушение целостности данных
- Дискриминация
- Вымогательство
- Передача данных 3м компаниям
- Подделка
- Хищение идентификационных данных
- Проникновение
- Потеря контроля
- Утеря данных
- Злонамеренное использование данных
- Фишинг
- Домогательства
- Спам
- Несанкционированный телемаркетинг
- Несанкционированная передача третьим лицам

Bernd Blobel
University of Regensburg
Medical Faculty

Факторы, влияющие на требования по обеспечению конфиденциальности after ISO 29100



Bernd Blobel
University of Regensburg
Medical Faculty

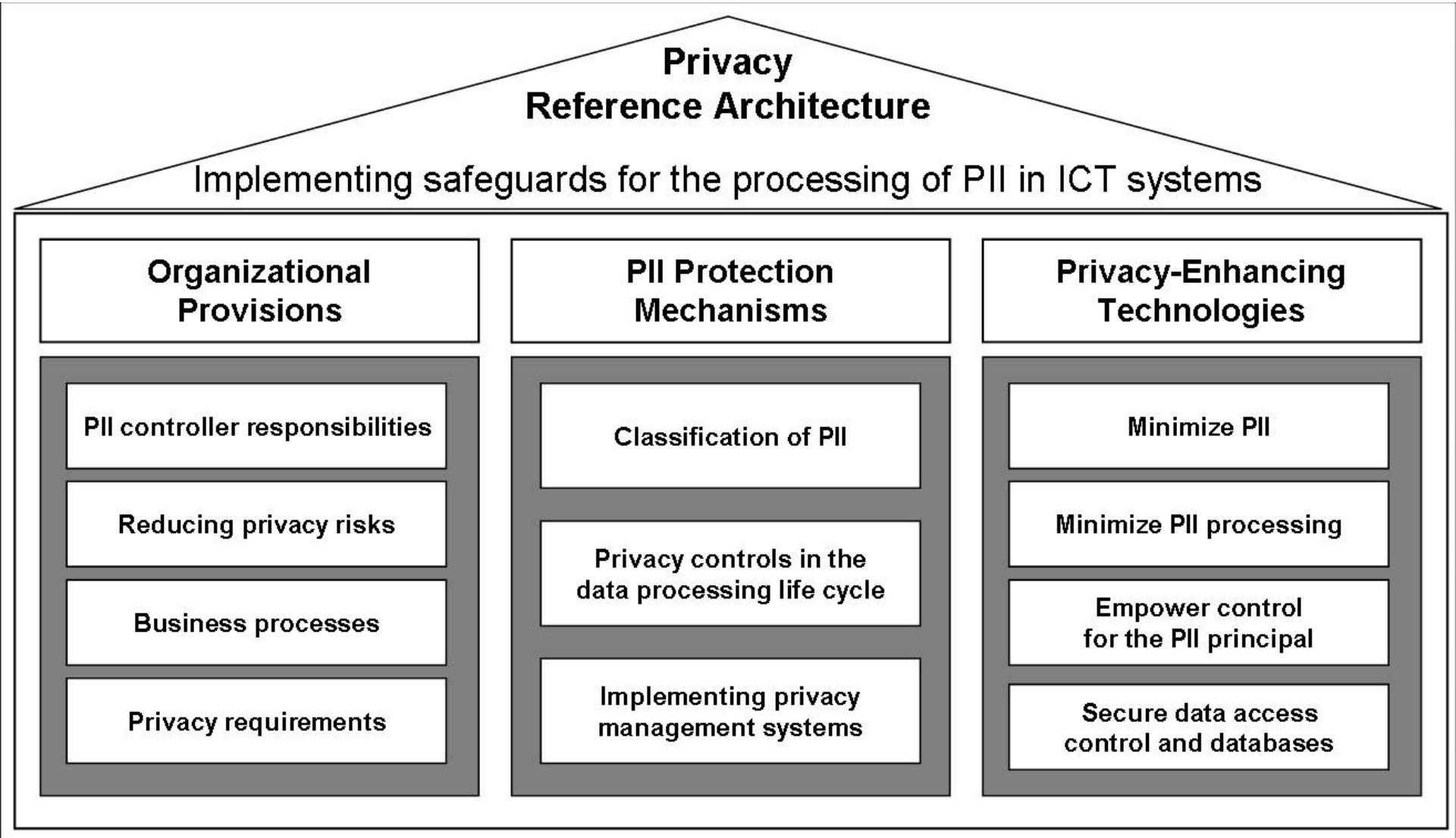
Принципы сохранения конфиденциальности

after ISO 29100

1. Информированное согласие и выбор
2. Правомерность и целенаправленность использования данных, технические требования
3. Ограниченный сбор информации
4. Ограничения относительно использования, хранения и раскрытия информации
5. Минимизация данных
6. Точность и качество данных
7. Открытость и прозрачность политики распоряжения данными и средства информирования/оповещения
8. Личная вовлеченность и доступ к информационным ресурсам
9. Отслеживаемость данных
10. Инструменты обеспечения безопасности
11. Нормативно-правовое соответствие

Bernd Blobel
University of Regensburg
Medical Faculty

Основные элементы эталонной архитектуры (по ISO 29101 Information Technology – Security techniques – Privacy reference architecture)



Security and Privacy Services Required for Универсального pHealth (after Ruotsalainen and Blobel)

- Управление доверием:
  - Службы информирования
  - Оценка уровня доверия
  - Измерение доверия на основе индикаторов
- Управление политикой:
  - Описание политики
  - Согласование, гармонизация (разрешение конфликтных ситуаций)
- Контроль доступа
- Инфраструктурные службы
  - Управление идентификаторами
  - Де-идентификация, псевдонимизация
  - Другие службы в среде
  - Управление объектами данных (в том числе потеря данных и шифрование)
- Другие возможные службы: оценка риска в реальном времени (каждая транзакция)

Bernd Blobel
University of Regensburg
Medical Faculty

Примеры персональной идентифицирующей информации (ISO/IEC 29100 Privacy Framework)

Национальный идентификатор (# паспорта)

Номер клиента

Биомедицинские идентификаторы

Номер счета в банке или # кредитной карты

Имя

Пол

Дата рождения

Домашний адрес

Персональный телефонный номер

Персональный адрес эл. почты

IP адрес

Фото или видео, позволяющие идентифицировать человека

Членство в профсоюзе

Сексуальная ориентация

Судимость и совершенные преступления

Финансовая информация о человеке

PIN и пароли к финансовым счетам пациентов

Любая информация, которая собрается во время оказания услуги

Потеря работоспособности

Раса и национальность

Религиозные воззрения

Особые потребности граждан в группах риска

Персональный и психологический профиль

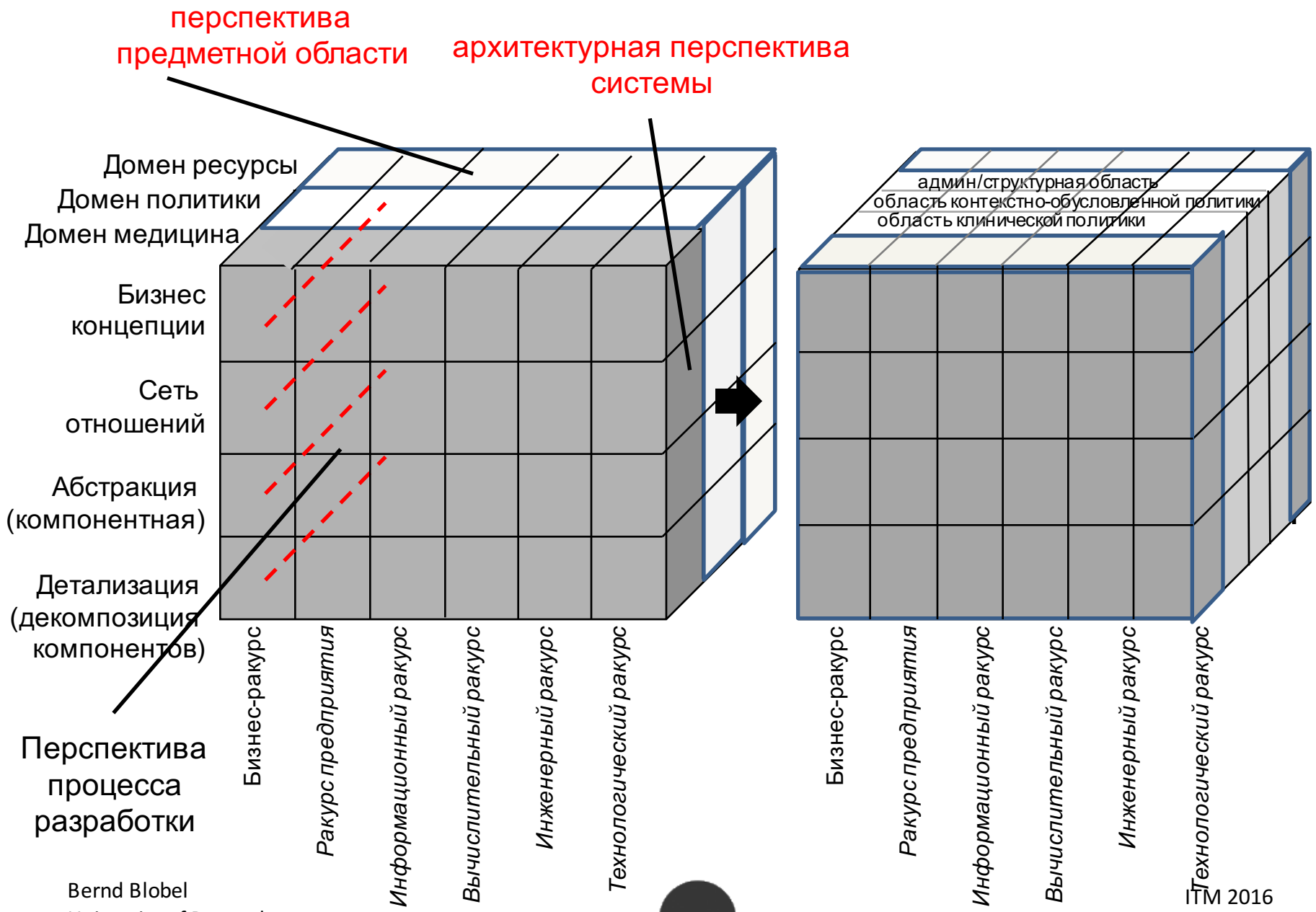
Данные местонахождения человека, полученные из телекоммуникационных систем

Предпочтения относительно продуктов и услуг, полученные из CRM систем

Персональный психологический профиль с учетом поведения человека в сети

Комбинированные данные

Paradigm changes in health system require new approaches to security and privacy

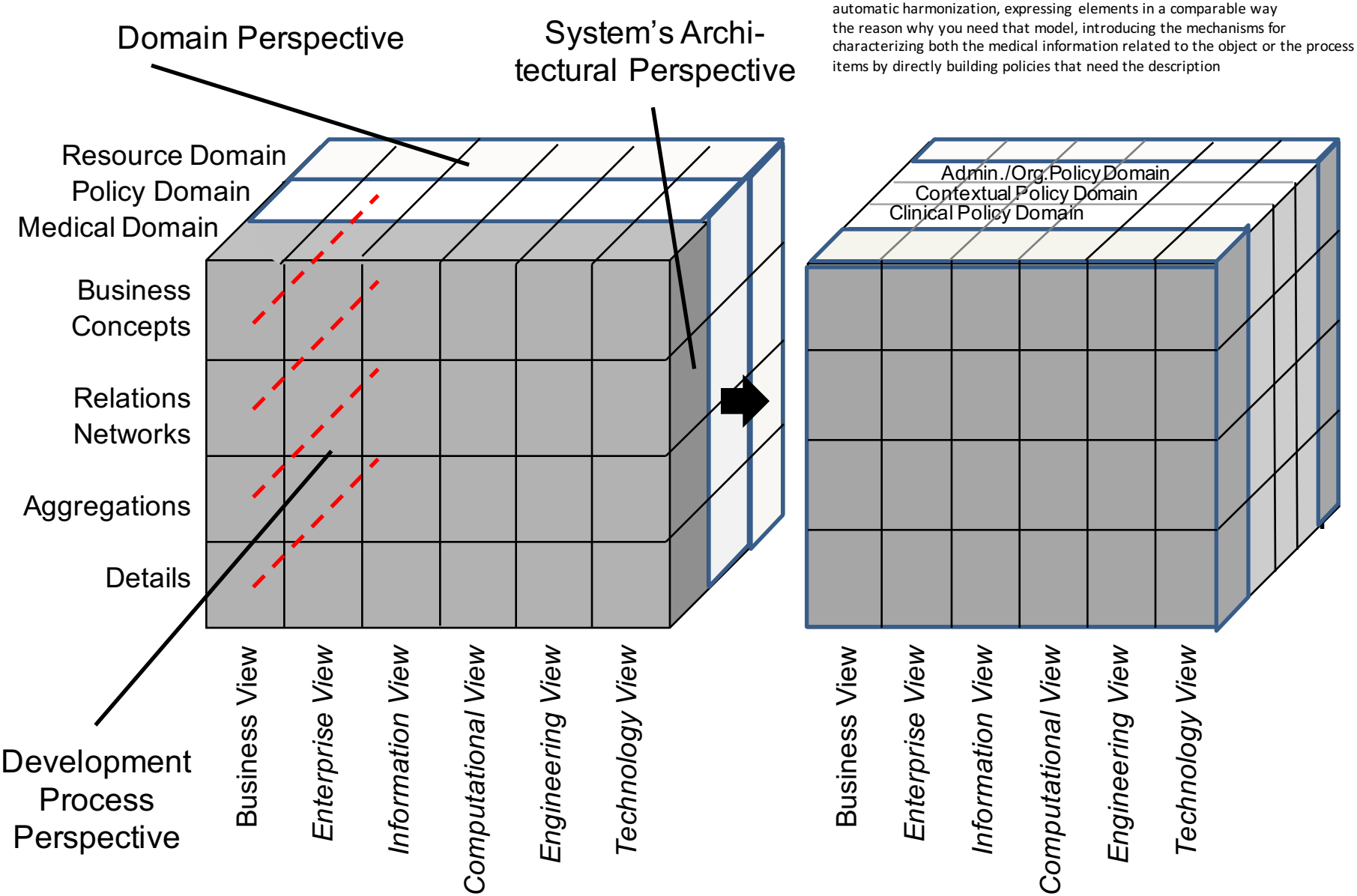


Bernd Blobel
University of Regensburg
Medical Faculty

ITM 2016
13-14 October 2016
Moscow, Russian Federation

Paradigm changes in health system require new approaches to security and privacy

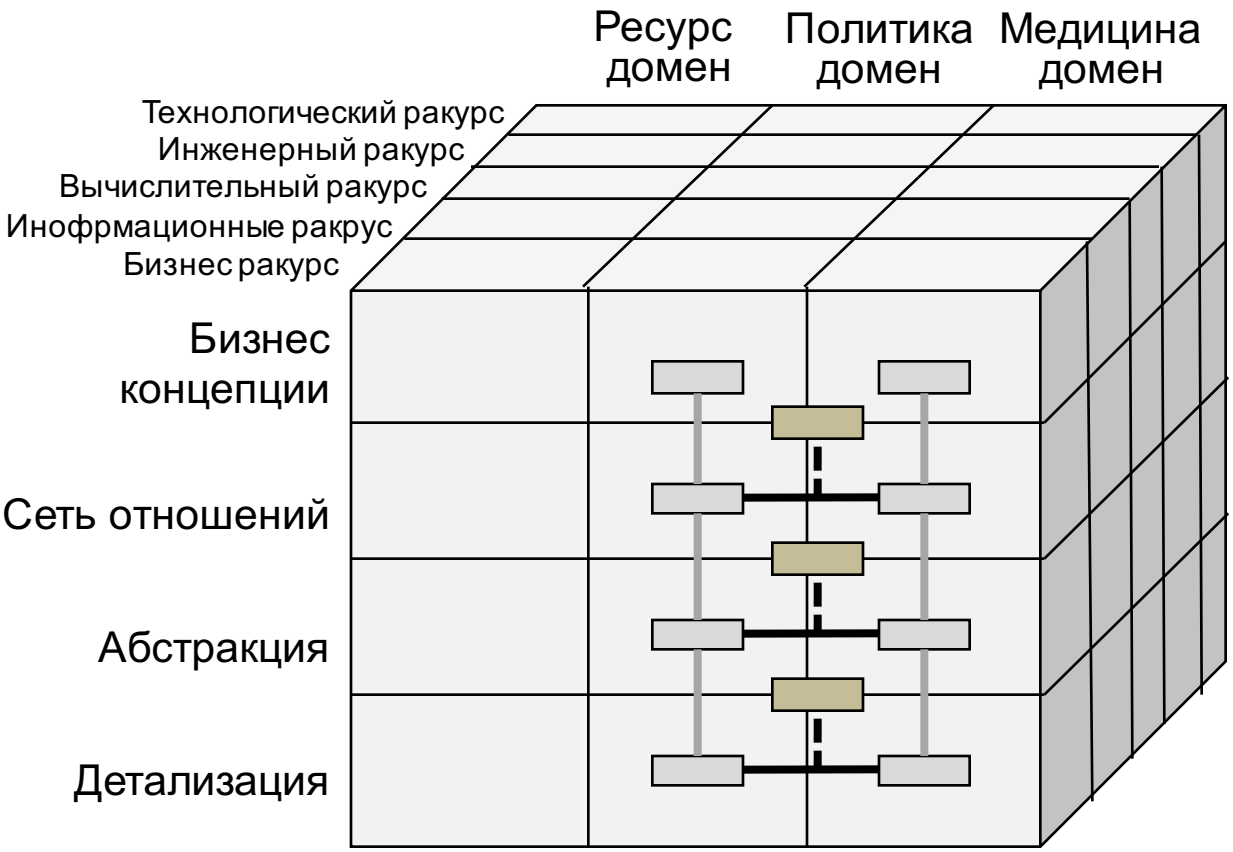
formalization of the system, its elements,
automatic harmonization, expressing elements in a comparable way
the reason why you need that model, introducing the mechanisms for
characterizing both the medical information related to the object or the process
items by directly building policies that need the description



a b

Bernd Blobel
University of Regensburg
Medical Faculty

Paradigm changes in health system require new approaches to security and privacy



Bernd Blobel
University of Regensburg
Medical Faculty

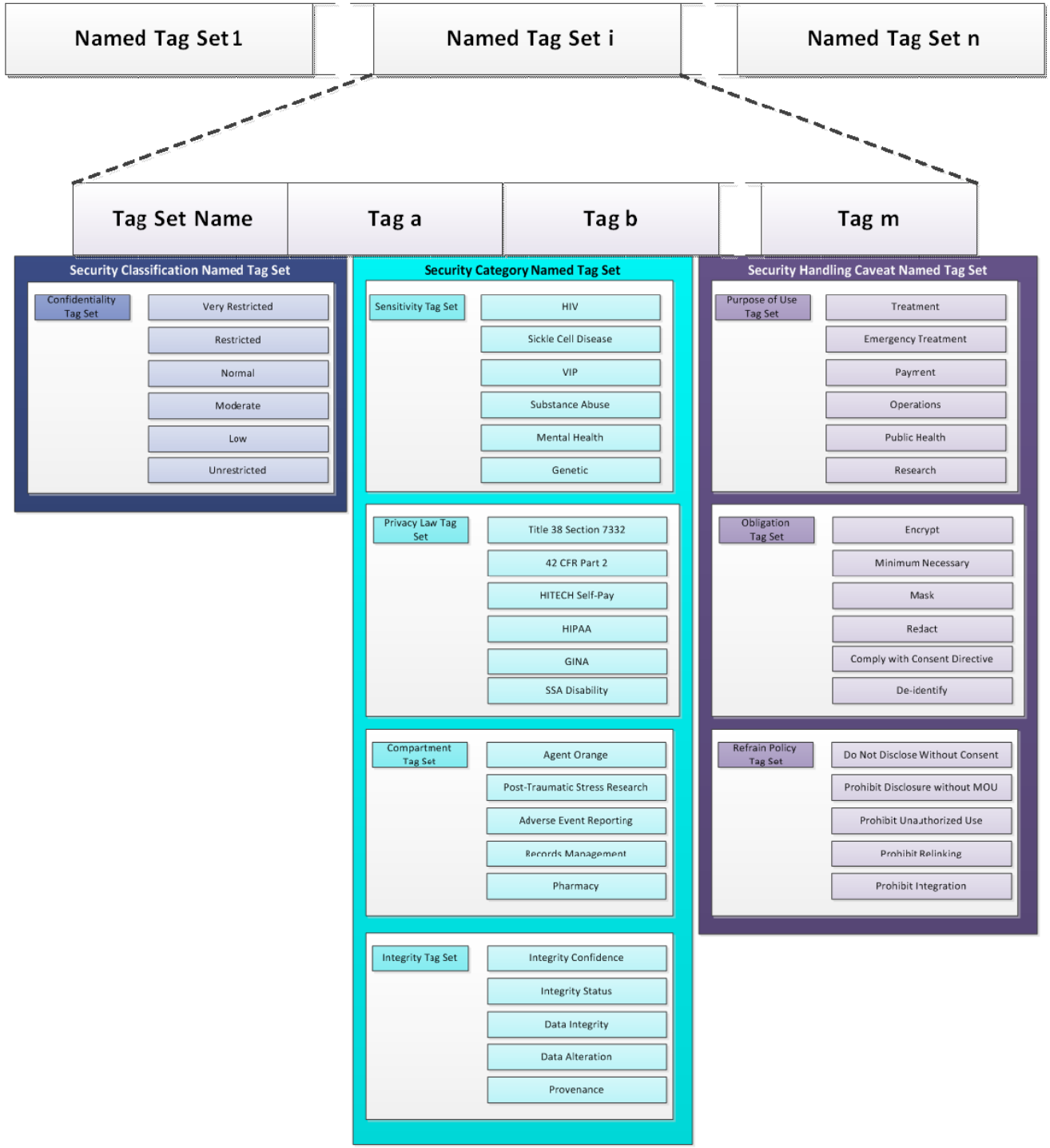
ITM 2016
13-14 October 2016
Moscow, Russian Federation

Маркировка защищаемой информации

- Маркеры безопасности являются метаданными персональной медицинской информации (PHI). Маркеры описывают ограничения относительно доступа и использования персональной информации для контекстов и принципала (действующее лицо, которое не всегда являетя человеком): КТО, КАК, КОГДА, ГДЕ, ЗАЧЕМ и ПОЧЕМУ

- Маркеры безопасности являются тэгами, связывающими информационные обьект с набором атрибутов безопасности и конфиденциальности. Маркируются не только данные – в HL7 также маркируются люди и ресурсы. В новой Медицинской системе классификации безопасности и конфиденциальности (HL7 HCS) определяются следующие маркеры: конфиденциальность, важность, целостность, категория и операционные ограничения.

HL7 Healthcare Privacy and Security Classification & NIST FIPS 188 Security Label



handling caveats рисками to deal with constraining processes, the other columns deal with restricting the information items

Bernd Blobel
University of Regens
Medical Faculty

2016
2016
ation

Логическая архитектура контроля доступа

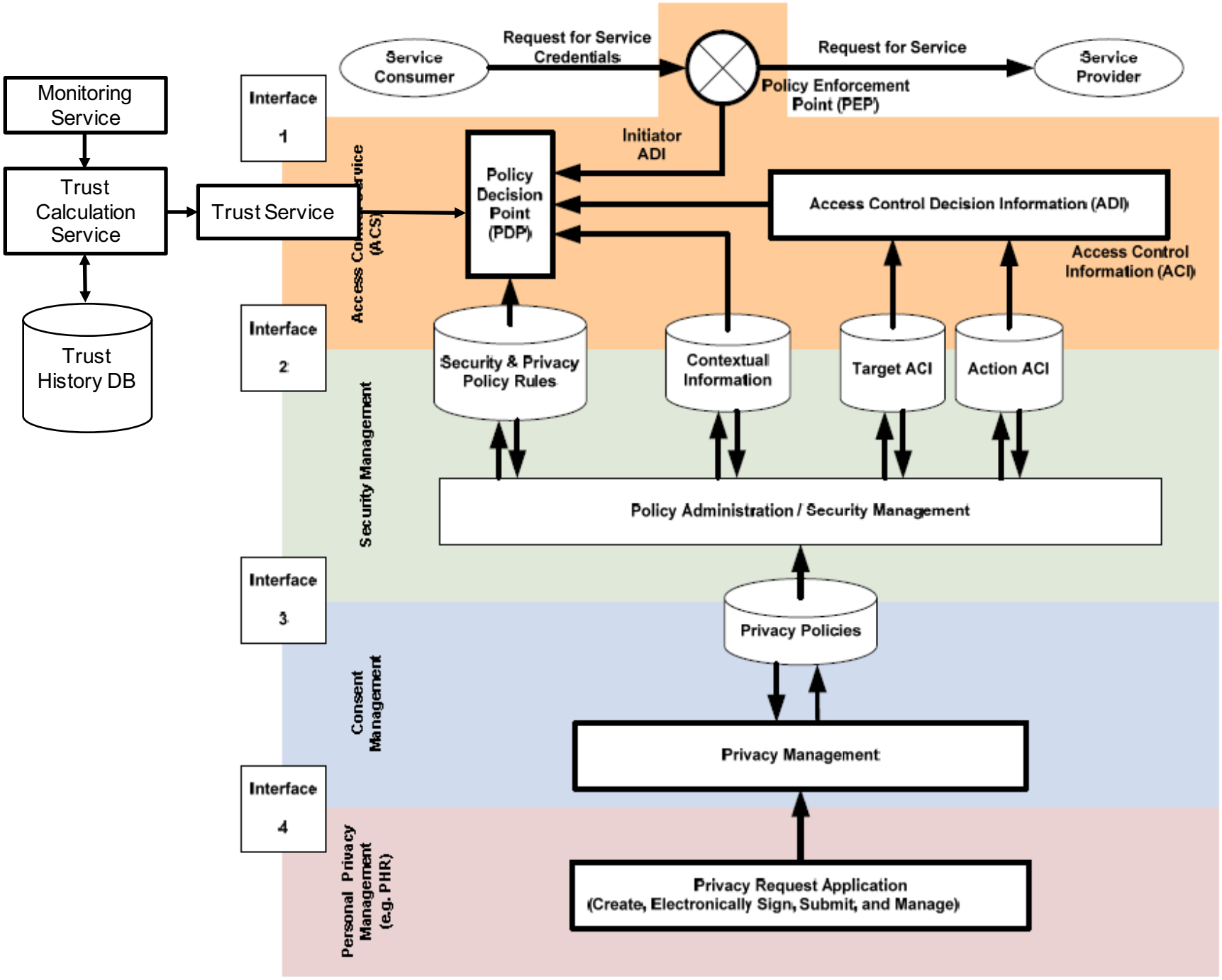


Illustration 2 Authorization Reference Model

Изменение роли руководителя по информационной безопасности – от безопасности к управлению рисками

- Роль Chief Information Security Officer (CISO) претерпевает изменения: от эксперта в сфере безопасности к специалисту по развитию бизнеса; специалист, который участвует в гармонизации бизнес стратегии и безопасности, а также в интеграции инструментов обеспечения защиты данных, безопасности и конфиденциальности.
- Он/она оценивает человеческий фактор в сфере обеспечения безопасности и конфиденциальности, а также помогает добиваться максимально возможной защиты минимумом средств. Комплексный подход к вопросам обеспечения безопасности и конфиденциальности на базе управления рисками в реальном времени.
- Он/она будет возглавлять новые процессы.
- Знания, способности и навыки CISOs будут влиять на политику безопасности изначально.

Privacy by Design (after Brendan Seaton)

- "Privacy by Design" refers to the philosophy and approach of embedding privacy into the design specifications of various technologies. "Privacy by Design" defines the fundamental principles needed to ensure that your project complies with privacy legislation and best practices for information privacy management.
- Foundational Principles of "Privacy by Design"
  1) Proactive not Reactive; Preventative not Remedial
  2) Privacy as the Default Setting
  3) Privacy Embedded into Design
  4) Full Functionality - Positive-Sum to Zero-Sum
  5) End-to-end Security - Full Lifecycle Protection
  6) Visibility and Transparency - Keep it Open
  7) Respect for User Privacy - Keep it User-Centric

What do privacy professionals need to know about security? (after Brendan Seaton, changed)

- Principles of information security
  - **Information security** - protecting data & IT assets, information security management, threat and risk assessment
  - Ensuring confidentiality, availability & integrity
  - **Security and data-protection program** considerations - people, process and technology
  - **Information security critical assets** - data, services, hardware/software, personnel, intangible (e.g. reputation, goodwill)
  - Case Study
  - Measuring **Sensitivity**, Asset Register & Statement of Sensitivity
  - Threat Agents
  - **Information Security Program elements** - written security policy, security organization, security risk assessment and plan to manage security risk
  - Need for permanent risk assessment

Bernd Blobel
University of Regensburg
Medical Faculty

Cyber-Security Research and Development Requirements (after Fraunhofer)

- Cloud security
- Cyber-physical systems
- Data protection and privacy management
- Power generation and energy supply
- Early warning systems
- Industrial production and automation
- IT forensik
- IT security for mobility
- Media security
- Network security
- Piracy protection
- Physically embedded cyber security
- Secure engineering
- Secure mobile systems
- Security against lateral channel and error attacks
- Security management
- Trustworthy systems
- Relation between safety and security

Bernd Blobel
University of Regensburg
Medical Faculty

EU Cyber-Security Roadmap

Policy Objectives:

- Overcome current ICT security products and solutions supply market fragmentation to create a European single market for innovative ICT security products and solutions helping European supply industry achieve economies of scale and compete on a European and global level
- Secure European digital technologies - ensure that European citizens, enterprises (including SMEs), public administrations have access to the latest digital security technology developments, which are interoperable, competitive, trustworthy and based on European rules and values
- Limit the risk and the impact of cybersecurity incidents, while increasing consumers' and citizen's trust and fostering the EU digital economy

Cyber Security Coordination Groups Across Europe

- The Cyber Security Coordination Group (CSCG) of CEN, CENELEC and ETSI is the only joint group of the three officially recognized European Standardization Organizations with a mandate to coordinate Cyber Security standards within their organizations. The CSCG was created in late 2011 to provide strategic advice on standardization in the field of IT security, Network and Information Security and Cyber Security. ENISA (European Union Agency for Network and Information Security) participates in CSCG.
- All Member States and their Member Bodies are requested to implement an analog structure.

Legal Developments

- In the communication between EU and USA, the Safe Harbor Principles have been replaced by the Privacy Shield Agreement.
- The EU Data Protection Directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) and the Council Framework Decision 2008/977/JHA have been replaced by the EU Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and the Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

Выводы 1

- Изменения парадигмы в системах оказания медицинской и социальной помощи ведут к сильно распределенным, открытым средам с интеграцией множества областей права и политик предметных областей, технологий, знаний и стилей представления концепций, языков, методологий, интересов и восприятий, культурных сред, ожиданий, образования и навыков и т.д., **обозначая потребность в сложных продуктах по обеспечению интероперабельности**. Проблематика интероперабельности не ограничивается ИКТ, включает в себя весь спектр действующих лиц.
- Грамотно подобранные решения в сфере обеспечения безопасности и конфиденциальности повышают степень доверия, таким образом улучшают восприятие проектов в сфере здравоохранения и служб IT-поддержки.
- Учитывая это, страны-лидеры в сфере применения ИКТ и телемедицины выделяют 50% бюджета на средства обеспечения безопасности и, в особенности, на решения в сфере обеспечения конфиденциальности информации.
- Технологии обеспечения безопасности и конфиденциальности не являются тормозом развития, это новые, прорывные технологии с поддерживающим эффектом.

Summary and Conclusions 2

The State Privacy Ombudsman of Berlin, Dr. Alexander Dix, has summarized the responses to Big Data challenges as follows:

- There is no absolute security and anonymity, but there are privacy-friendly and privacy-unfriendly solutions. Despite all de-identification possibilities, anonymization is better than personal data openly available on the Internet. This also includes pseudomized data which are still personal data. Nevertheless, pseudonymization is an appropriate measure for reducing personalization of data.
- Not justified and court-enabled searches and comprehensive analyses performed by secret services do not comply with democratic principles.
- There is a need for an international Code of Practice for monitoring the Internet traffic and the citizens‘ behavior
- International privacy guarantees should be part of the UN Human Rights Declaration

Summary and Conclusions 3

- We need publicly funded research and development of technical privacy solutions for Internet users including a less-vulnerable European Cloud Model.
- There are no accepted innovations without sensible privacy-by-design.
- Collecting personal data is attractive for legitimated and non-legitimated users. Therefore, Big Data must be protected against attacks, and the collection of personal data must be limited.
- Big Data do not necessarily need to be Big Personal Data.
- Data minimization and transparency are inevitable basic principles.
- The EU strategy for a right to be forgotten should be boosted through a new Internet protocol which enables deleting personal data.

Bernd Blobel
University of Regensburg
Medical Faculty

Большое спасибо за ваше внимание!

Contact:

Prof. Dr. habil. Bernd Blobel, FACMI, FACHI, FHL7, FEFMI
Past-Co-Chair, HL7 Security WG
Past-Chair, EFMI WGs „Security, Safety and Ethics“ and „EHR“
Past-Chair, GDD WG „Privacy and Security in Health and Social Care“
University of Regensburg, Medical Faculty
c/o HL7 Germany
An der Schanz 1
50735 Köln
Germany
Email: bernd.blobel@klinik.uni-regensburg.de

Related Important Event

We invite you to actively attend the
pHealth 2017 Conference
12-14 May 2017
Eindhoven, The Netherlands
More information: www.phealth2017.eu

Bernd Blobel
University of Regensburg
Medical Faculty