

Health Information Privacy Day - Toronto 24/09/2007

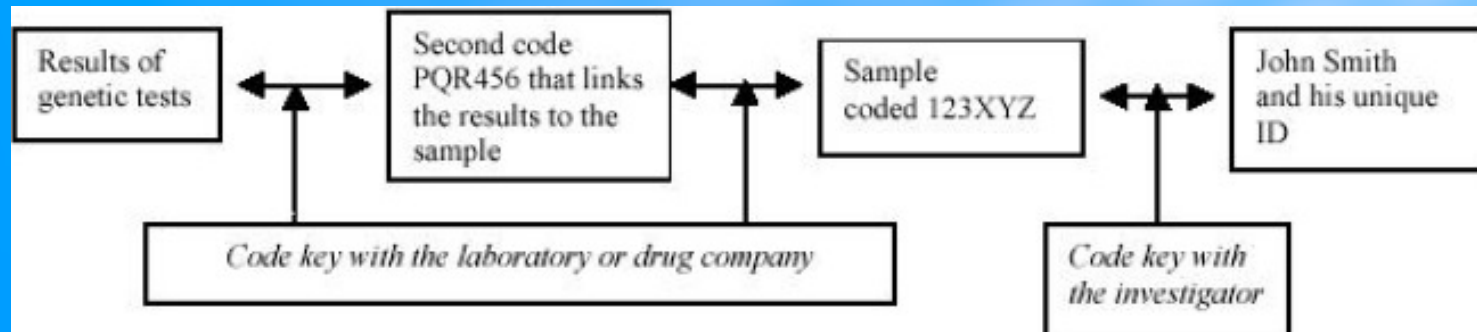
***Genetics and Privacy
Biobanking – Trustees -
Audits***

Lukas Gundermann

*Independent Centre for Privacy Protection
Schleswig-Holstein
Holstensr. 98, D-24103 Kiel, Germany
+49 431 988 1205
gundermann@datenschutzzentrum.de*

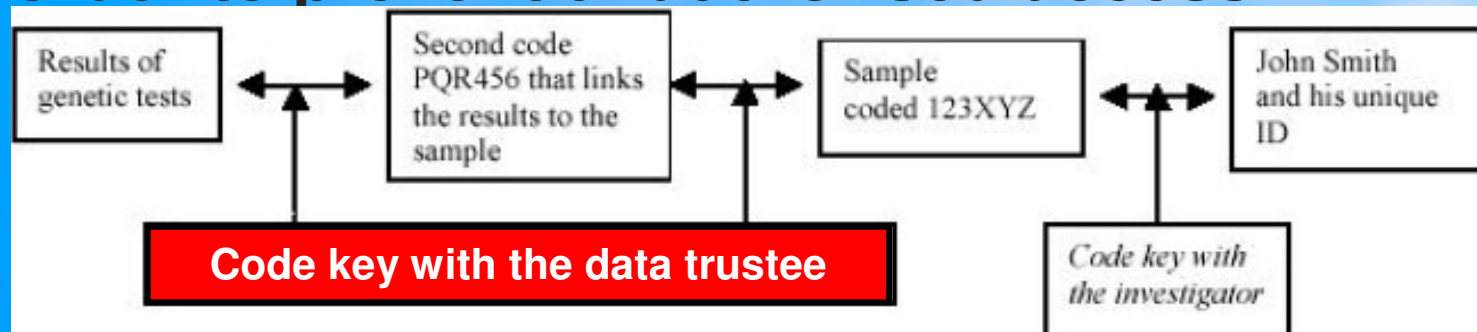
Prerequisites 1

- **Project bdc\Audit** (Biobank Data Custodianship\Audit Methodology and Criteria) → riddled with prerequisites
- **Biobanks**
 - Collection of tissue samples + socio-demographic data + medical data
 - Highly sensible data → special protection, both legally and technically
 - Application of PET, as suggested by EMEA



Prerequisites 2

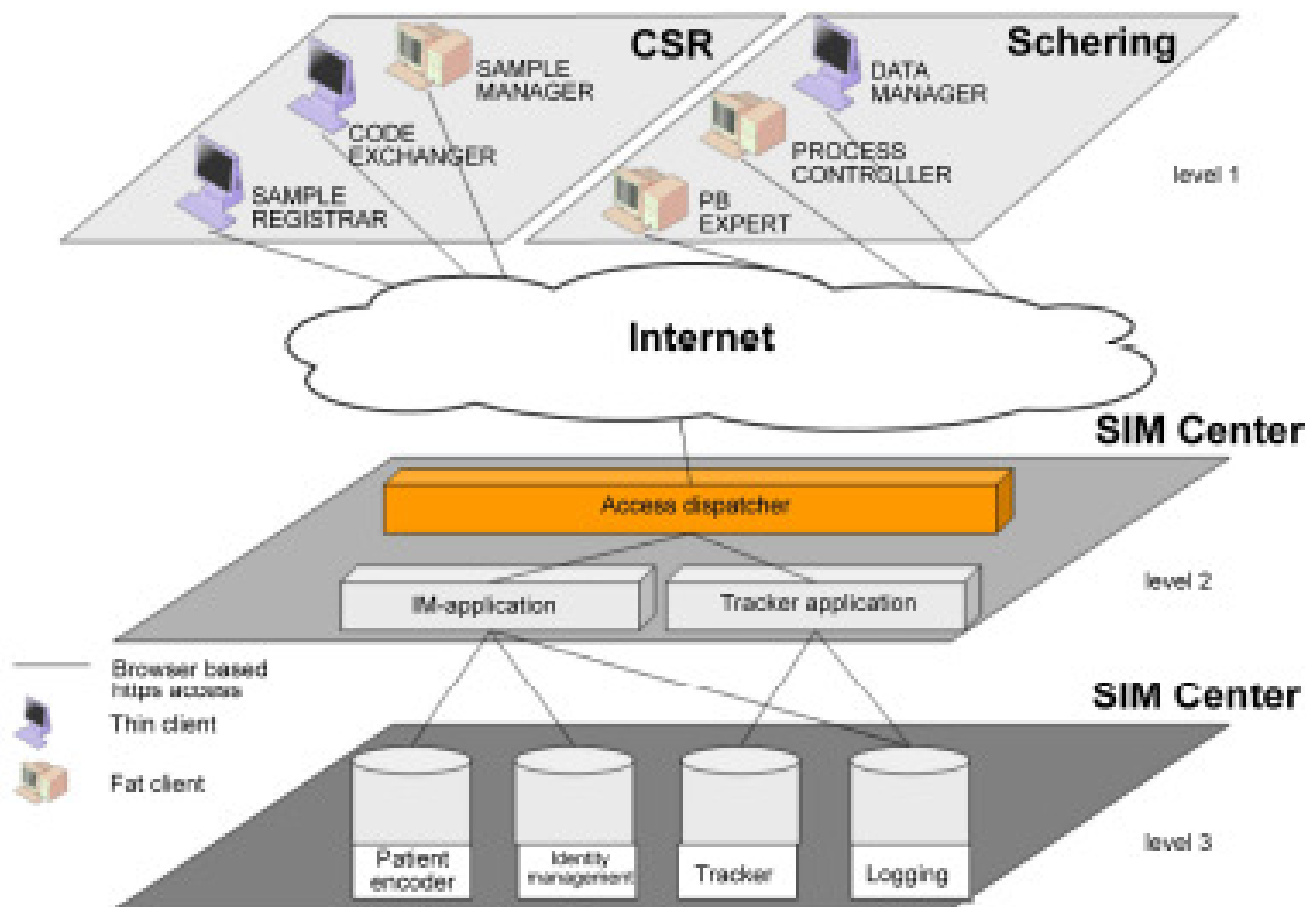
- **Data custodianship (or data trustee)**
 - Ideally: third party, independent from the owner of the biobank
 - Administering keys and / or data
 - Aim: distribution (or scattering) of knowledge in order to prevent unauthorised access



- Possibly: checking the adherence to the guidelines
- Who could take over such role?
 - Notary public, DPAs, DP officers?

Data trustee - technical implementation

GENOmatch Architecture



Prerequisites 3

- **Audit**

- Voluntary data protection audit
- See also audit DP audit manual of UK Info Commissioner 2001
- Assessment of data protection management system within organisational structure of data controller
- Concept (or adequacy) audit and implementation (or compliance) audit
- Longstanding experience of ULD
- Start of EU project EuroPriSe
→ embedding DP audits into European framework
- Talk at Montreal conference



Project approach 1

- **Empiric research**

- Survey to identify actual work procedures and precautions taken with regard to data protection in 9 biobanks
- 2 rounds of experts interviews

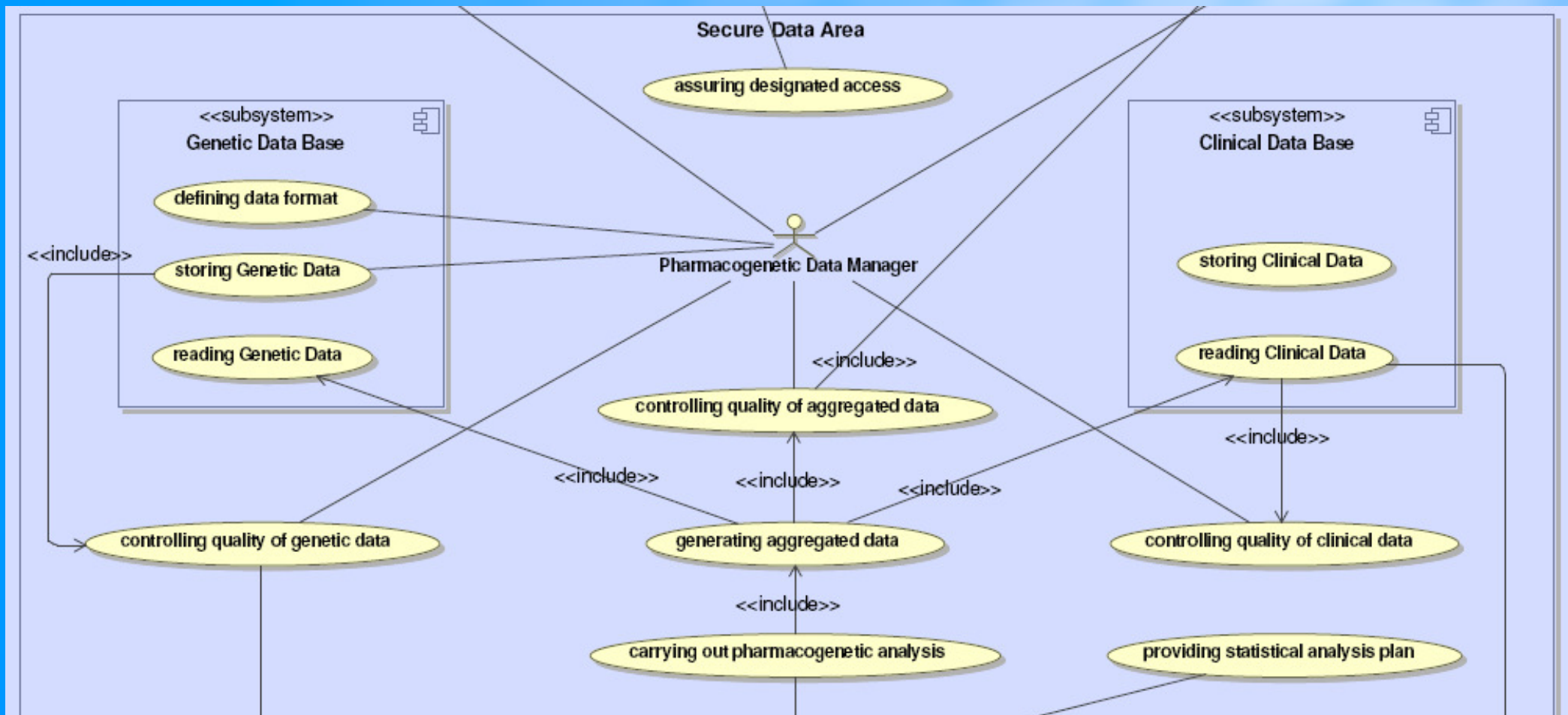
- **Identification of appropriate modelling language**

- UML (Unified Modeling Language)
- UMLsec
- SeeMe (link on request)
- Common Criteria – creation of a protection profile?

Project approach 2

- **Creating descriptive elements**
 - Most likely in UML or UMLsec
 - To describe typical biobank procedures
- **Producing an Audit Manual, containing**
 - **Criteria** (legal, organisational, technical)
 - **Methodology** (approach to audit, modelling language)
- **Development of graphical user interface**
 - as half-automated guidance for the auditor

UML modelling - example



Implications, questions, limits 1

- **Criteria – where to derive them from?**
 - DP Acts, other laws, guidelines, recommendations
 - Few exist (eg. CoE Recommendation Rec(2006)4)
 - Many issues are contentious, e.g.:
 - Anonymisation vs. pseudonymisation
(→ can genetic data ever be anonymised?)
 - Feedback mechanisms needed?
 - Broadness of consent?
 - Concept of trustees rarely reflected in regulatory texts
 - Some criteria are self-generated, open to discussion

Implications, questions, limits 2

- **Modelling**

- **Modelling language only provides descriptive elements**
- **Must be assembled by the auditor on a case by case basis**
- **No off-the-shelf descriptions of complete biobanks or processes will be available**

Conclusions

- **An comprehensive, adjustable tool kit for auditing in the field of biobanking will be developed**
- **Providing a possibility for benchmarks against the state of the art in biobanking**
- **Criteria will be transparent and flexible, so they can be adapted to different regulatory environments**



ULD-i

Datenschutz *innovativ*

<http://www.uld-i.de/>