PRIWAY
Security in Context

Making the Net forget

- a Security by Design pathway project in Healthcare
Addressing "S & Marper vs. United Kingdom"

RFIDsec

Stephan J. Engberg
Priway
Sje webmail at Priway com

SIME HEALTH

Privacy is NOT about right

Goal	Source of problems	Problems
Security (avoiding bad)	• Anti-crime • Gatekeepers • Legacy ”security”	Accumulating Risks Creating the problems
Innovation (needs-driven change)	• **Command & Control Economics** • Lock-in • Kartel standards • Profilling outside context	Preventing change Power moving from demand to supplier

Definition: Privcacy is security (& control)
from the point of view of one stakeholder

A choice - two worlds

”Trust me with your secrets”

A world where the **databases control people**

Identified connections – **data is created for secondary abuse**

Control is server-side and **power concentrates**

Rules, polices & obscure technologies to ”produce” trust (fail)

When database security fails – **bad happens**

or

”Avoid creating secrets !”

A world where **people control the databases**

Context-specific connections - **data is created for secondary use**

Key Control is edge/client side and **power is distributed**

Creating trust by **avoiding risks independant of jurisdiction**

When database security fails – **use the backup and go on**

3 models co-existing → improving

Anarchic
Cannot prevent

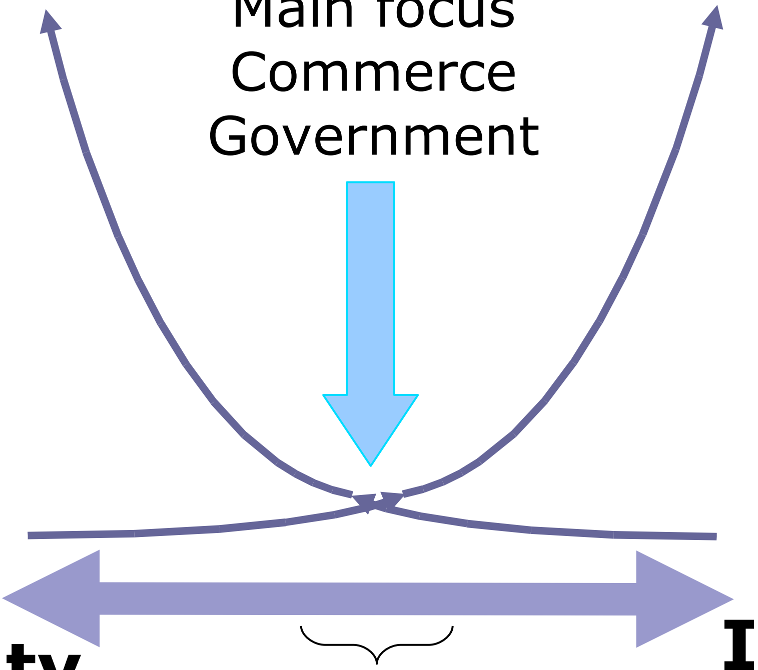
Contextual Id

Surveillance
Cannot secure

Risks grow
Crime/fraud
Lack of traces

Main focus
Commerce
Government

Risks grow
Crime/fraud
Id Theft etc.
Interdependance
Power concentrate



Anonymity

Identification

Structured Pseudonyms

Case: ”S & Marper vs UK”

PRIWAY
Security in Context

- Dec 4, 2008 – DNA/biometrics/tissue most sensitive
  - Verdict: privacy violation if related to non-sentenced citizens

- Feb 20, 2009 – Ministry note to Danish parlament

  ”The court finds, that storage of tissue, dna-profiles and fingerprints is a violation of privacy according to EMRK’s article 8.”

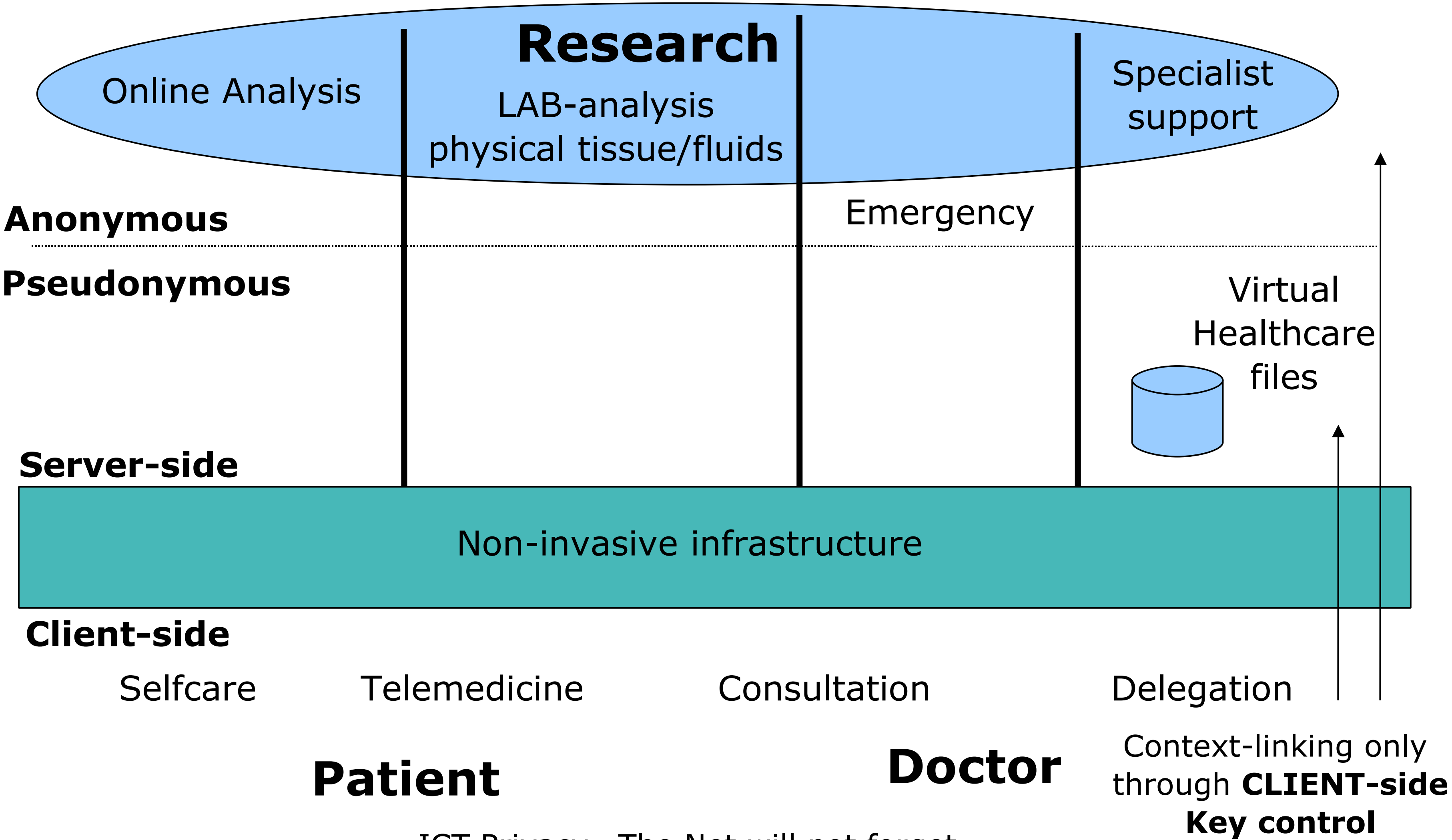
  ”The Court also finds that storage of fingerprints concerning an identified or identifable individual is a violation of privacy."

  http://www.ft.dk/samling/20081/almdel/REU/spm/254/svar/endeligt/20090220/646924.HTM

- Feb 24, 2009 – Annonce National DNA DB with Id
- May 2009 – Legal article on ”S & Marper” - 10 years is fair
- June 2009 – Hearing on collecting guests fingerprints on discos

”Proportionate”

Healthcare security overview



Research

Online Analysis

LAB-analysis
physical tissue/fluids

Specialist
support

Emergency

Anonymous

Pseudonymous

Virtual
Healthcare
files

Server-side

Non-invasive infrastructure

Client-side

Selfcare

Telemedicine

Consultation

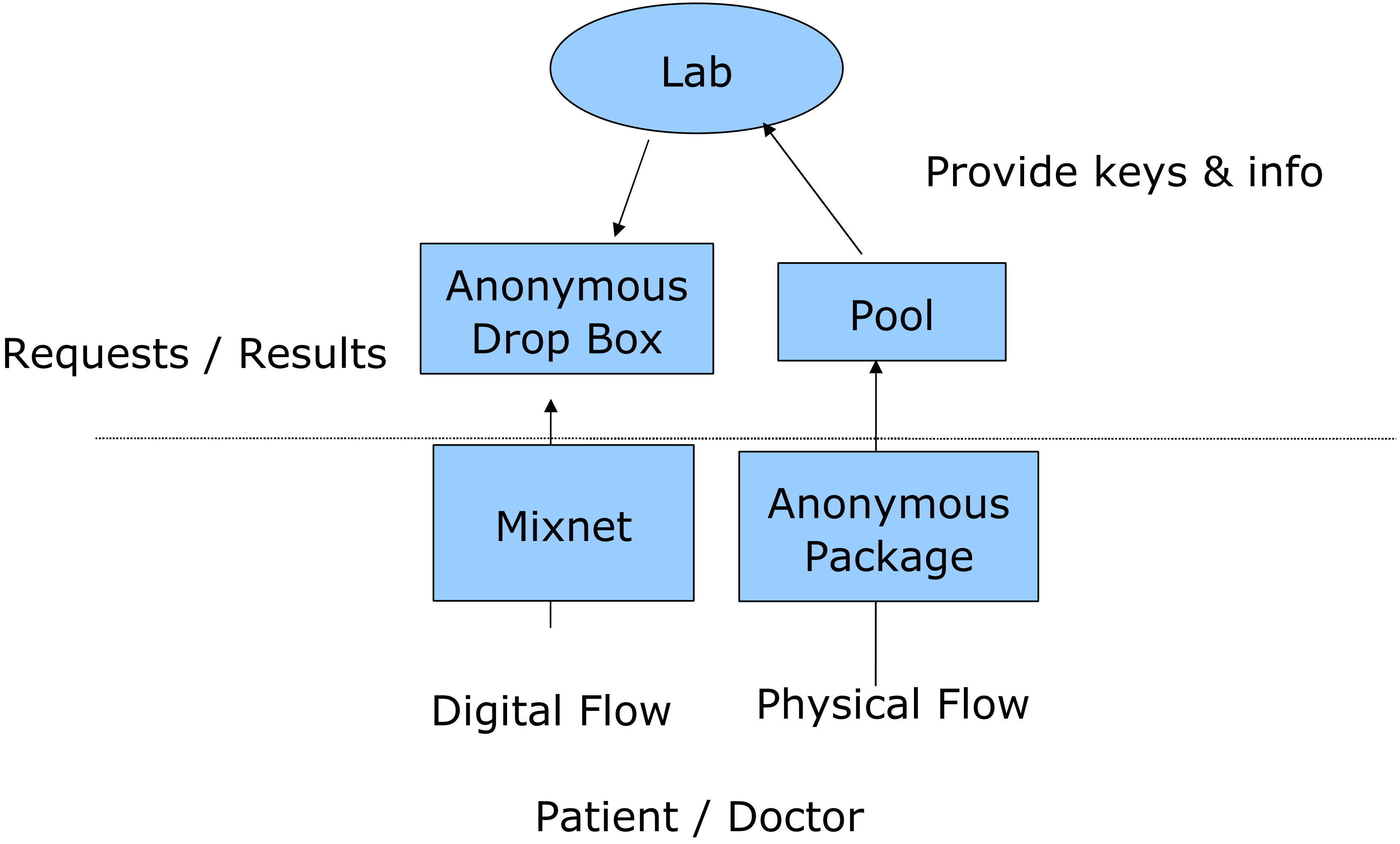
Delegation

Patient

Doctor

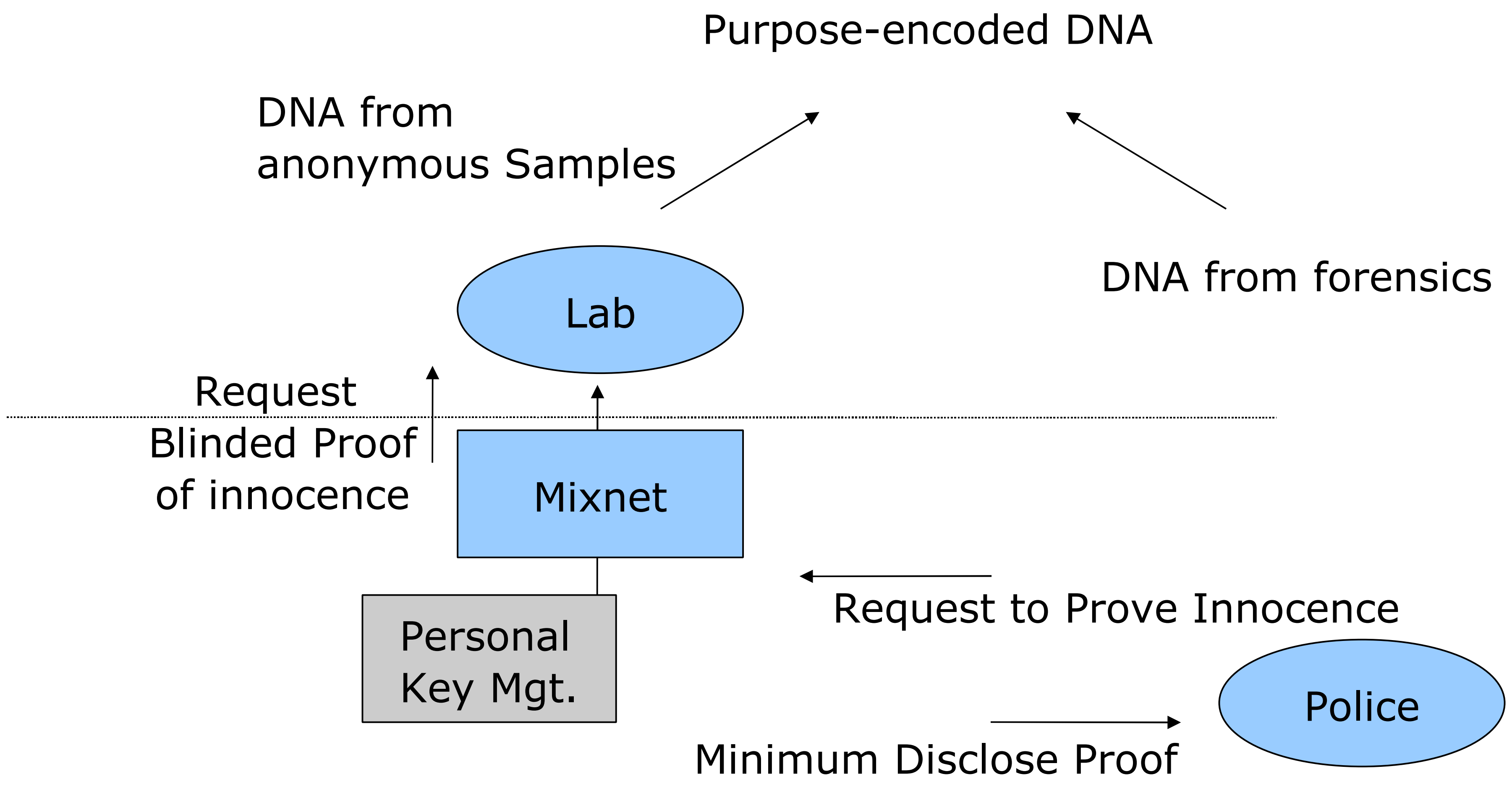
Context-linking only
through **CLIENT-side**
Key control

The simple version



Police don't need DNA with id

PRIWAY
Security in Context



Purpose-encoded DNA

DNA from
anonymous Samples

DNA from forensics

Lab

Request
Blinded Proof
of innocence

Mixnet

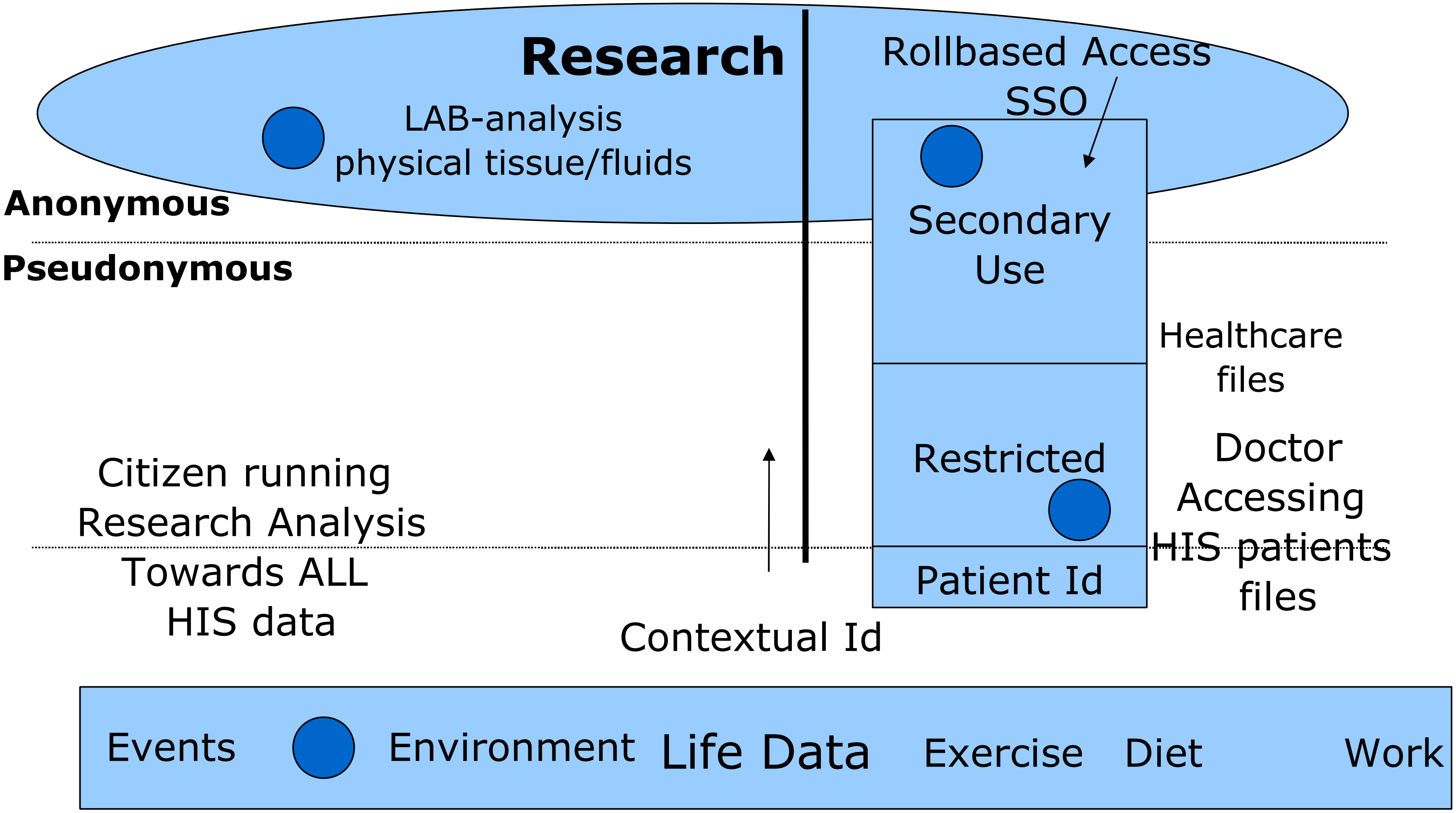
Personal
Key Mgt.

Request to Prove Innocence

Police

Minimum Disclose Proof

Research perspecitives



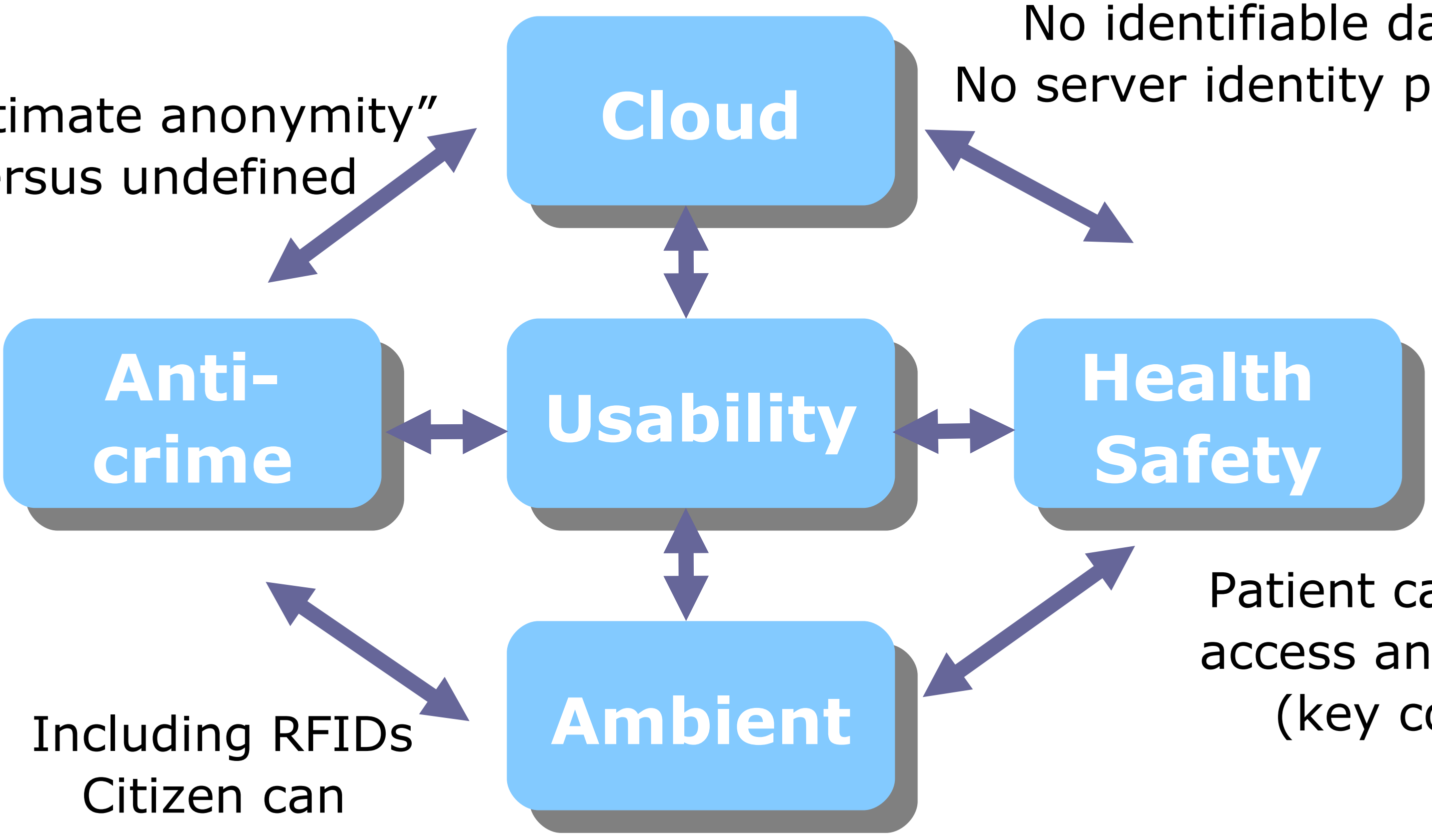
Compare Invasive model with Security by Design

Question	”Trust me”	Security by Design
Basic	Tissue identified Patient / Doctor known	Tissue anonymous Patient/doctor unknown
Shipment	From: Sender disclosed To: ”HIV-test Lab”	Sender anonymous Receiver gradually known
Requests	Identified Request Barcode verifiable	Anonymous Request End-to-end RFID authentication
Results	Returned & stored Identifiable. Lab can contact patient	Deposited in online Drop Box Lab cannot contact doctor/patient
Research	Restrictions trying to preserve privacy	Researchers are ”free” Further data require consent
Police checks Specific	Against identified DNA	Against unidentified DNA Innocent DNA remain anonymous Fast check against convicted
Police generel	Fast search	Checks involve citizens Frequency, location, geography

Complex Challenges

”Legitimate anonymity”
versus undefined

No identifiable data
No server identity people



Cloud

Anti-crime

Usability

Health Safety

Ambient

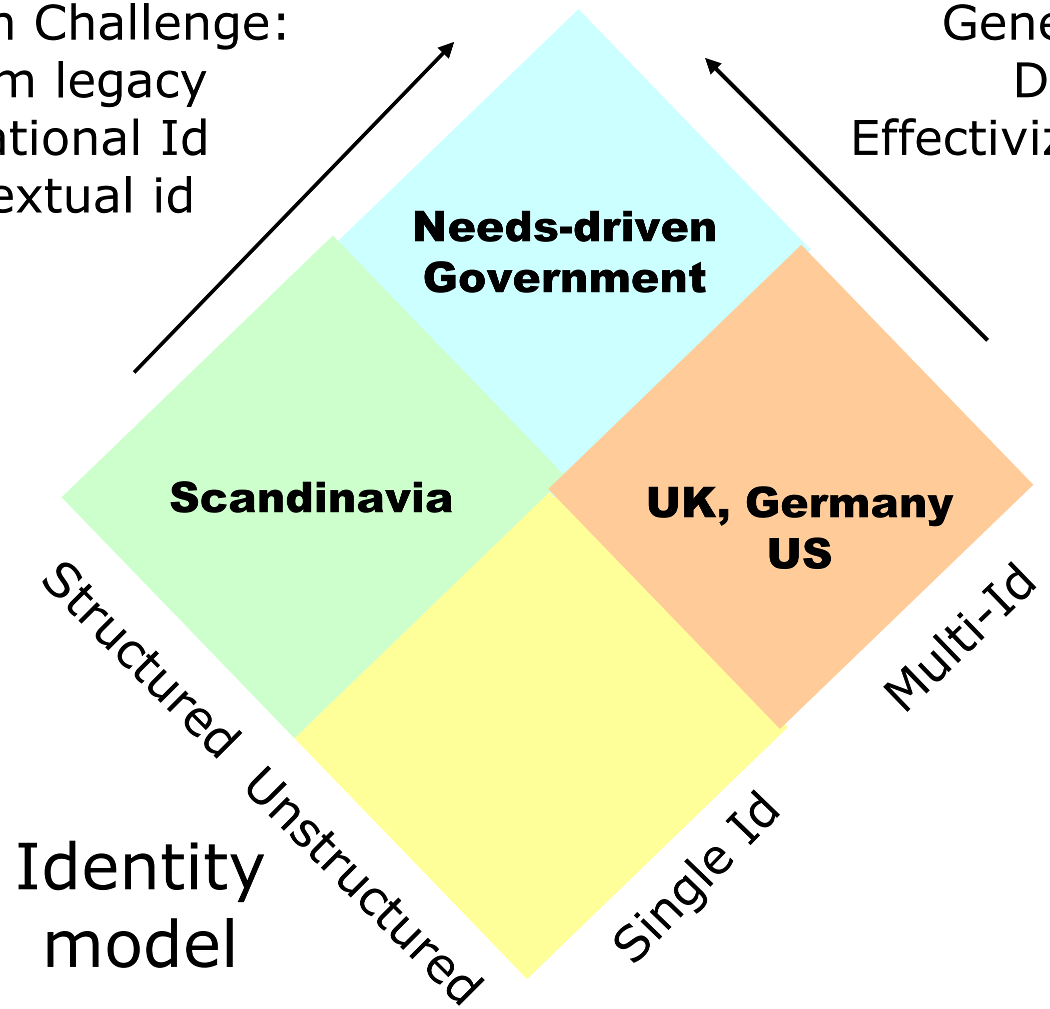
Patient can control,
access and delegate
(key controls)

Including RFIDs
Citizen can
Control end-to-end
without leaking
Identifiers

Towards National Id 2.0

Scandinavian Challenge:
Move from legacy
Single National Id
to Contextual id

General Challenge:
Demand Pull
Effectivization / innovation
AND
security



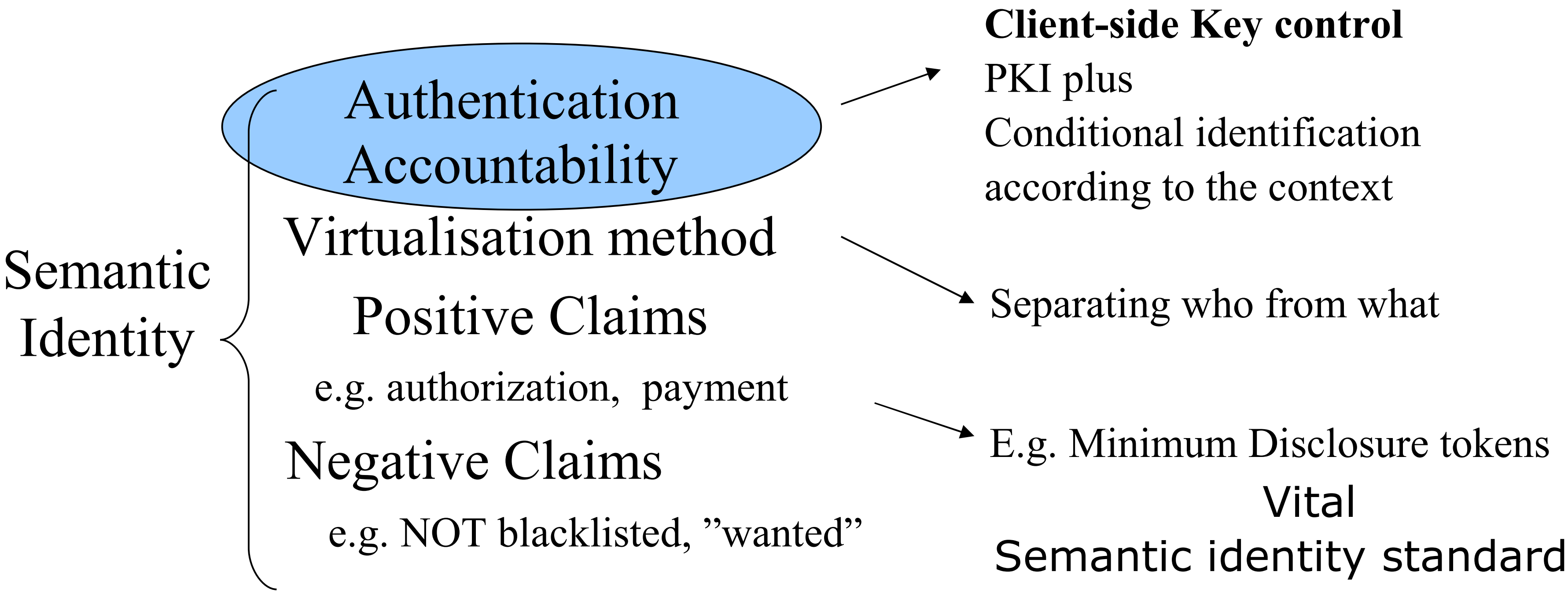
UK challenge:
Skip the traps of
Single National Id
moving straight to
Contextual id.

Identity model

ICT Privacy –The Net will not forget
Stephan Engberg – Making the Net forget

Semantic Identity

Contextual Id negotiated and customised to context
Consist of a random identifier and a set of attributes



Semantic Identity

Authentication
Accountability

Virtualisation method

Positive Claims

e.g. authorization, payment

Negative Claims

e.g. NOT blacklisted, ”wanted”

Client-side Key control
PKI plus
Conditional identification
according to the context

Separating who from what

E.g. Minimum Disclosure tokens

Vital
Semantic identity standard to
enable interoperability betweer
identity models & technologies

Summary – Security by Design

- There is (better) life after ”S & Marper vs. United Kingdom”
- Trust less. Perimeter security fail and so does trust.
  - Focus on “legitimate” value-creating applications
- Empowering Citizens & Design for ”secure” secondary use
  - Provide a sustainable security paradigme
  - Resolve trade-offs & barriers
  - Fokus on demand to drive change & innovation
- Win-win Cases
  - Securing, improving & legalising Biometrics
  - Setting new standards for Government services