PRIWAY
Security in Context

Pseudonymisering er nøglen til sikkerhed og privacy By Design

Stephan J. Engberg

PRIWAY
Security in Context
.. because the alternative is not an option

www.priway.com

Hvem er Priway?

PRIWAY
Security in Context

- En voksende gruppe af virksomheder
  - Priway ApS (opr. 1999)
  - RFIDsec Aps (2005)
  - Sime Health (under stiftelse)
- Med stærke samarbejdspartnere
  - Delta, BusinessTree, m.fl.
  - Private investorer (ingen venture)
- ca. 20 ansatte
  - 4 ph.d., IT, ingeniører, læge m.fl.
  - Gennemsnitsalder ca. 50 år
- Internationalt fokus, specielt EU
- De gennemgående faktorer
  - Mennesket i kontrol – alle aspekter
  - Security by Design & Brugervenlighed
  - Bæredygtige forretningsmodeller
  - Høj værdiskabelse uden at gå på kompromis
  - Kobler forskningsbaseret udvikling til slutkundebehov

Hjemmehørende på IT-Universitet, 5te

Agenda

PRIWAY
Security in Context

The digital learning – Servers are either secured by design or an accumulating bomb waiting to explode

Hvorfor skal borgeren have kontrol ?

Hvor ligger de store problemer i dag ?

Hvordan løser vi tunge sikkerhedsproblemer ?
RFID, Biometri & Digital Forvaltning

CASES: Biobanken specifikt og Sundhed generelt

I takt med at teknologien bliver stadigt mere intim og alting integreres digitalt
skal teknologi, infrastruktur og processer designes så kontrollen skubbes til borgeren.

Privacy

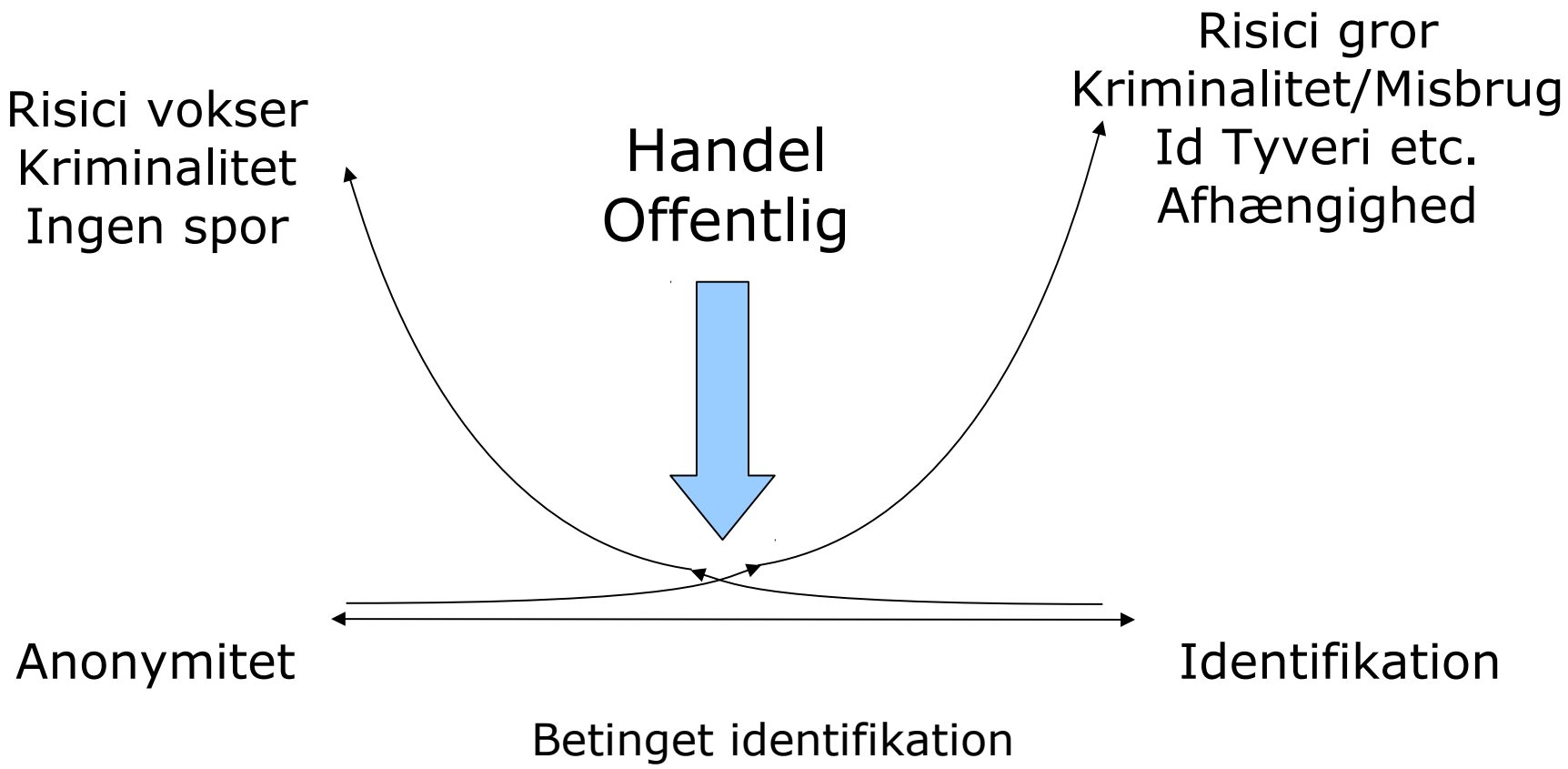
PRIWAY
Security in Context

- Privacy drejer sig IKKE om ”Informeret samtykke”
  - På det tidspunkt er det for sent (pest eller kolera)
- Privacy er ”SIKKERHED set fra en interessent”
  - Fokus er risiko-MINIMERING af trusler mod borgeren som samfundets vigtigste aktiv (subjekt)
  - Juraen er (var) konsistent – man SKAL !
- FORMÅLET er SIKKER VÆRDISKABELSE
  - At designe teknologi og samfundsprocesser så vi skaber services UDEN at skabe unødvendige risici.
  - At forebygge og sikre kritiske infrastruktur – Digital Identitet er nøglen til alt andet.
  - Det er nemt at sikre MOD borgeren – meget svært at sikre borgeren og systemerne.

Empowerment & Fallback security
Nøglen til Digital Id troværdighed

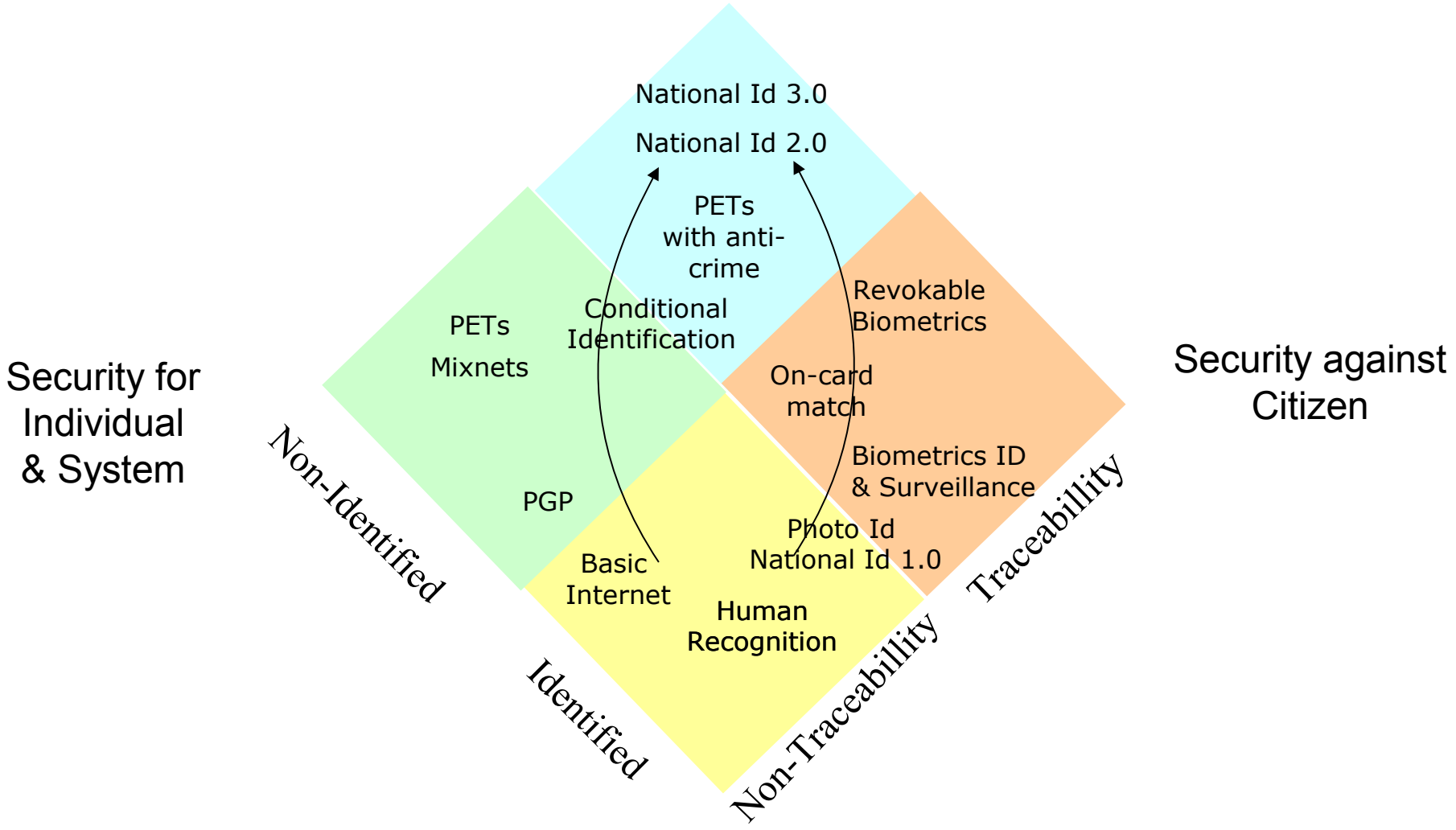
PRIWAY
Security in Context

National ID 2.0



Priway Identity Model
Roadmap to PETs & Biometrics

PRIWAY
Security in Context



Myter om Overvågning

PRIWAY
Security in Context

- Overvågning skaber ansvarlighed !?
  - Ansvarlighed dækkes af Betinget Identifikation
  - Overvågning skaber kun trusler som ikke kan sikres
- Overvågning sikrer mod de uønskede !?
  - Credentials kan valideres uden identifikation
  - Identifikation skaber risiko for identitetstyveri
- Overvågning skaber tryghed !?
  - Personlig safety kan sikres uden overvågning
  - Overvågning tilfører tryghedsdestruerende aspekter

Pseudonymisering som løsningsmodel

PRIWAY
Security in Context

- Sikkerhed & Privacy by Design
  - Forebyggelse & risikominimering – troværdige systemer
- Innovation & Velstand
  - Kunden selekterer blandt overudbud af muligheder.
- Effektivisering af den offentlige sektor
  - Kontrollen følger behovet – behovsdrevet tilpasning
  - One-size-fits-all skaber planøkonomisk ineffektivisering
- Compliance – opfyldelse af lovens krav
  - Implicit Opt-In – Eksplicit Opt-Out
- Sociologisk – Behovet for kontrol, Frihed under ansvar
- Politisk stabilitet – modvirke magtkoncentration & risici

Kilde: Debatbog ”De Overvågede”, TÆNK 2009, sidste kapitel

Security Tools available

PRIWAY
Security in Context

Available or soon available

- Anonymous Credentials
  - Certified profile & attribute data
  - E.g. Credentica
- Identity metasystem
  - Heterogeneous id environment
  - E.g. Microsoft
- Private Biometrics & Biometric encryption
  - Client-side Biometrics
  - E.g. readers on card
- Anonymisers
  - Mixnets / onion routing
  - E.g. TOR, ANON
- Hardware-traceability
  - Verifiable accountability
  - E.g. TCG

”Privacy Highway” inventions

- Secure RFID with PET
  - RFID with privacy control
  - Anti-counterfeiting & Anti-theft
- Non-linkable Digital Payment
  - Anti-counterfeit, Anti-theft,
  - Anti-laundering, Credit, additional
- Conditional Identification
- Citizen Id Cards - Anti-Identity Theft
  - Create & manage new ids to context
  - Traceable & accountable to Root Id
  - Privacy Authentication
  - Instant revocation
  - Id Accountability negotiation
- Other
  - Receiver-controlled Communication
  - Indirect means to e.g. control Cameras
  - GRID Context Security

Det tekniske RFID privacy-problem er løst win-win

PRIWAY
Security in Context

- Kontrollen over RFID skal overgå til forbrugeren
  - Juridisk ejerskab ensrettes med teknisk ejerskab
  - Ejer (bruger) har eksklusiv kontrol
- Vores bud (RFIDsec)
  - Multiple nøgler hvor brugeren har hovednøglen
  - Zero-knowledge nøgle-verifikation
    - Langtidsholdbar - den svage part bestemmer
    - LÆKKER IKKE INFORMATION TIL LOGS
    - INGEN ”tillid” til 3. parter eller readers.
  - Hver enkelt nøgle kan checkes uafhængigt anonymt
  - Chippens sikkerhedsmodel kan dynamisk tilpasses
  - Forbrugeren styrer SELV om hun digitalt vil kobles tilbage til butik/leverandør. Butik/leverandør services stiller sikkerhedskrav til credentials

Strategic Advisory Board
FP7 Security Research Roadmapping

PRIWAY
Security in Context

Biometrics has played, and will increasingly play an important role in crime forensics and in non-repudiation but also for self-protection and proving innocence **What is critically important is to recognise that the goal should not be identification and surveillance, but the balance of security needs**. For instance biometrics is problematic for use for authentication as the **"secret key" is not secret, revocable or unique** – biometrics can be spoofed and victims of identity theft cannot get a new set of biometrics, and using several spoofable biometrics can merely create more "fake security".

Empowerment considerations involve ensuring that the use of biometrics is Identity and key management is based on easily and **securely revocable keys** such as **privacy biometrics** (integration of biometrics characteristics in mobile tamper-resistant reader-devices) or **bio-cryptography** (integration of biometrics characteristics in revocable cryptography keys) while enabling the use of a plurality of identity schemes. Indeed, **Empowerment and dependability are not achievable if control is always with someone else and attacks commit identity theft based on faking biometric credentials.**

ICAO Passports & danish passports
in clear VIOLATION with security needs

Source: www.securitytaskforce.eu - Recommendations, p. 14

Dom for biometrisk overgreb

PRIWAY
Security in Context

”Dom, som er nævnt i spørgsmålet, er afsagt af Den Europæiske Menneskerettighedsdomstol den 4. december 2008 i sagen S. og Marper mod Storbritannien (storkammerafgørelse). .. Menneskerettighedsdomstolen fastslår i dommen, at Storbritannien har krænket artikel 8 .. i Den Europæiske Menneskerettighedskonvention (EMRK).

Stk. 1. Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance.
Stk. 2. **Ingen offentlig myndighed må gøre indgreb i udøvelsen af denne ret**, medmindre det sker i overensstemmelse med loven og er **nødvendigt i et demokratisk samfund** af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres rettigheder og friheder.

Domstolen finder, at opbevaring af celleprøver, dna-profiler og fingeraftryk udgør et indgreb i retten til respekt for privatlivet i EMRK’s artikel 8’s forstand.

I den forbindelse fremhæver Domstolen bl.a., at celleprøver indeholder følsomme oplysninger om den pågældende persons helbred, og at celleprøver indeholder en unik genetisk kode, der er af stor betydning for såvel det pågældende individ som hans eller hendes pårørende (præmis 72).

Domstolen finder, at også opbevaring af fingeraftryk vedrørende et identificeret eller identificerbart individ udgør et indgreb i retten til respekt for privatlivet (præmis 85-86). "
http://www.ft.dk/samling/20081/almdel/REU/spm/254/svar/endeligt/20090220/646924.HTM

4 dage senere ..
En national "Biobank" !?

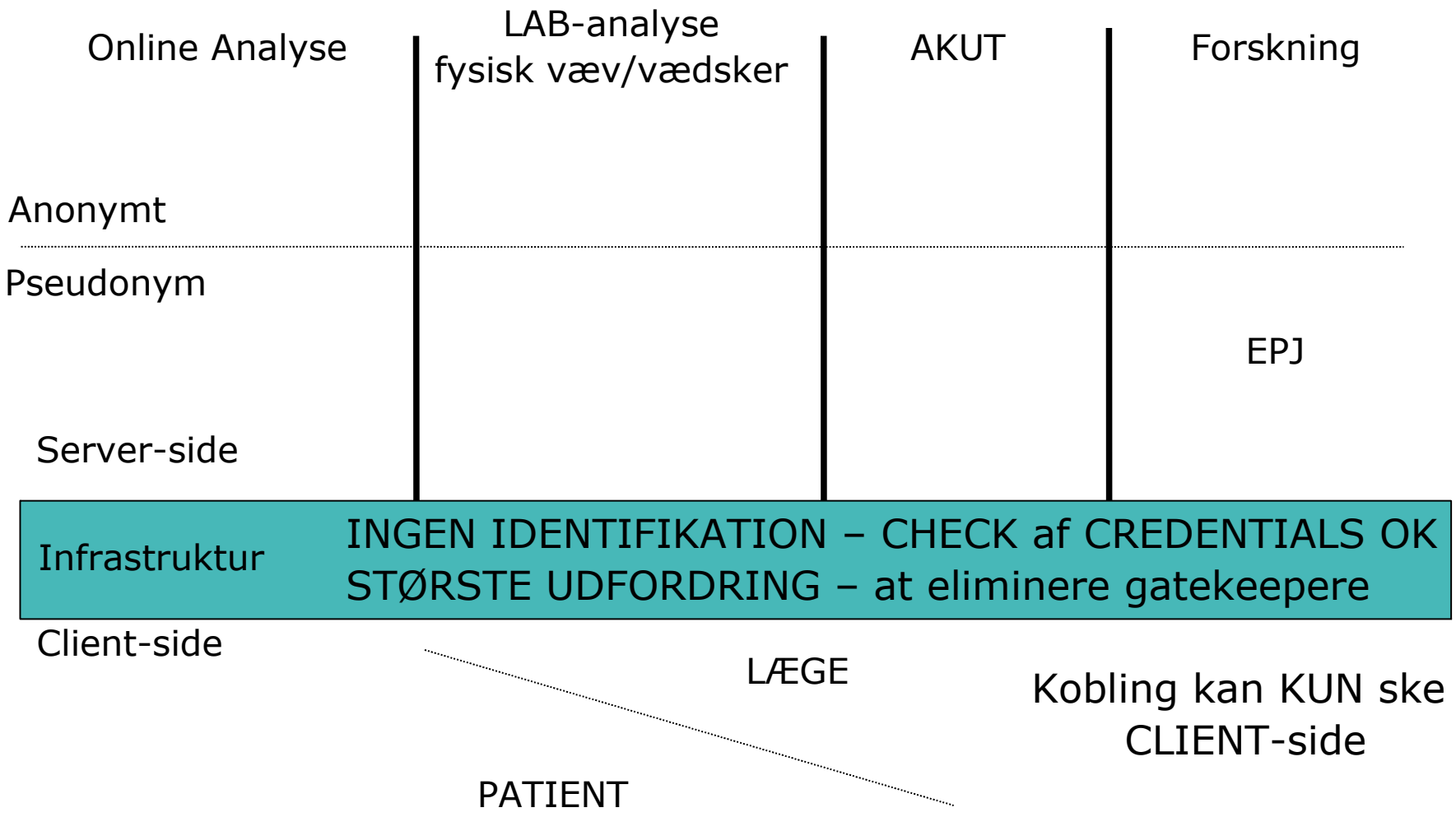
PRIWAY
Security in Context

Pressemeddelelse fra VTU, 24. februar 2009
Danmark er allerede internationalt førende, når det gælder registerforskning, fordi vi er så gennemregistreret en befolkning. Nu får befolkningen og forskerne oveni en national biobank i verdensklasse. Biobanken vil være et sted, hvor det overskydende materiale fra for eksempel blod og vævsprøver udtaget fra patienter i sundhedsvæsenet opbevares.
http://vtu.dk/nyheder/pressemeddelelser/2009/danmark-faar-national-biobank-i-verdensklasse/danmark-faar-national-biobank-i-verdensklasse

3 mulige standpunkter:
1) Forskerne (og ministeriets embedsfolk) skal registrere og have adgang til alt - ingen lov, ret eller principper må stå i vejen
2) Det er klart ulovligt – stop projektet
3) Lad os (fremtids)sikre projektet og gøre det lovligt og forsvarligt

Privacy som Løsning

Healthcare - sikkerhed



Sikre biobanker ?

PRIWAY
Security in Context

Eliminer personhenførbarheden totalt !

Laboratoriet har INTET behov for at vide HVEM de analyserer på

ADSKIL prøven og identiteten ved kilden
Laboratoriet kan bruge konklusioner til forskning (gør de alligevel)
Kun patienten/egen læge kan bruge den i relation til patienten

Vores løsningsmodel med eksisterende teknologi

1. Prøven sendes anonymt. Prøven tilknyttes en RFID. 2 nøgler – Lab / Patient.

2. Laboratorium modtager pointer til Online anonym "box" via lab-nøglen.

3. Patient/læge deponerer AnalyseRequest og modtager svar i den anonyme box.

Til Request knyttes en krypteret check af prøvens RFID mod forveksling. RFID-svar vedlægges.

Konklusion – win-win uden man skaber persondata

Sikring af "Biobank" forskning

PRIWAY
Security in Context

- Princip:

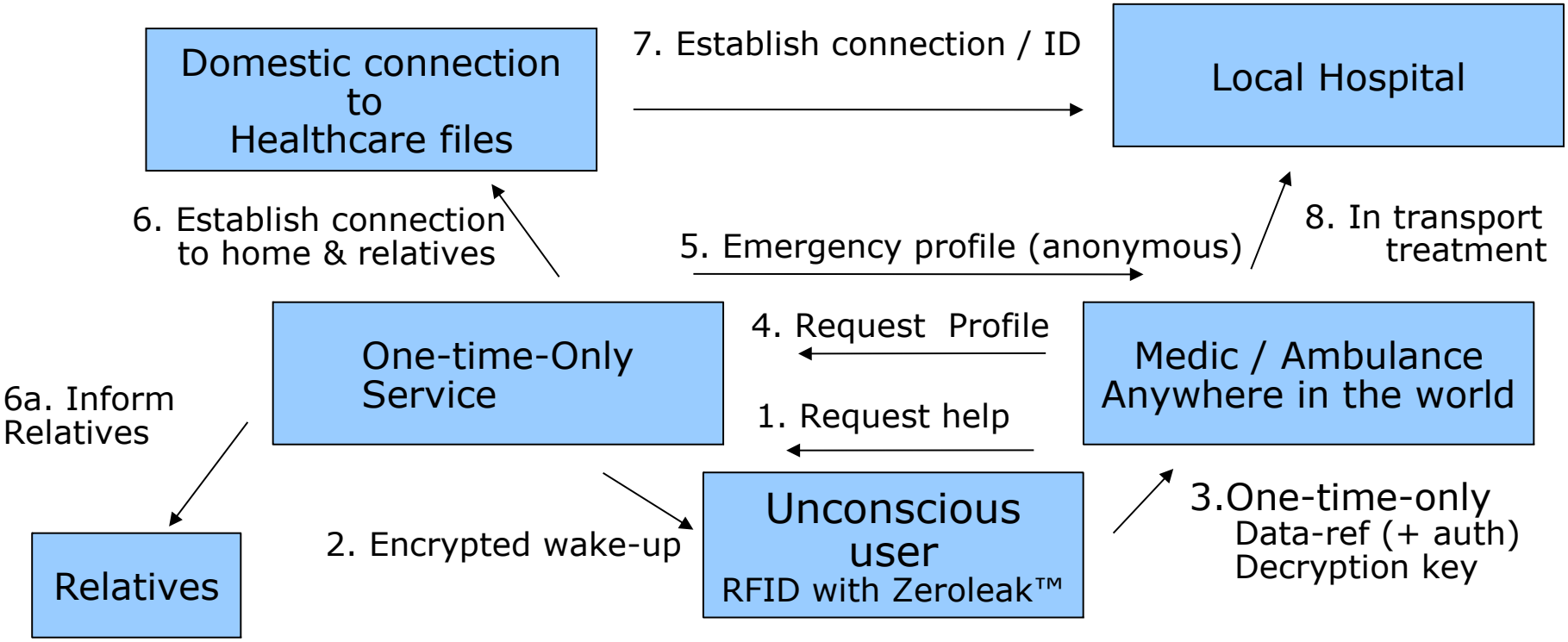
For at forebygge og sikre stadig mere intim teknologi skal kontrollen "skubbes" til borgeren.

- Vævs- og prøve bank skal være 100% anonym
  - Patientbehandling "requester" analyser anonymt
  - Specifik læring omsættes til input til forskning
- Fremtidens "registerforskning" distribueres
  - Forskning indenfor kontekst, dvs. sikret i bunden
  - Lægen kan gøre del analyse på de data, de kan se.
  - En Borger kører analyser på ALLE DERES data
  - Specifikke alarm-signaler deponeres i "boxen"
  - Forskerne sender "Request for cases" og "Alerts"

Healthcare Emergency / akut

PRIWAY
Security in Context

Stepwise RFID-based one-time-only Identification



Presented at SHI2007 - ”One-time-only access to Patient Healthcare files with graceful degradation – Unconsciousness Patient Emergency Safety enabled with PETs

Nye modeller med RFID smartcard

PRIWAY
Security in Context

Én Identitet er blot en nøgle som tilknyttes credentials af forskellige art

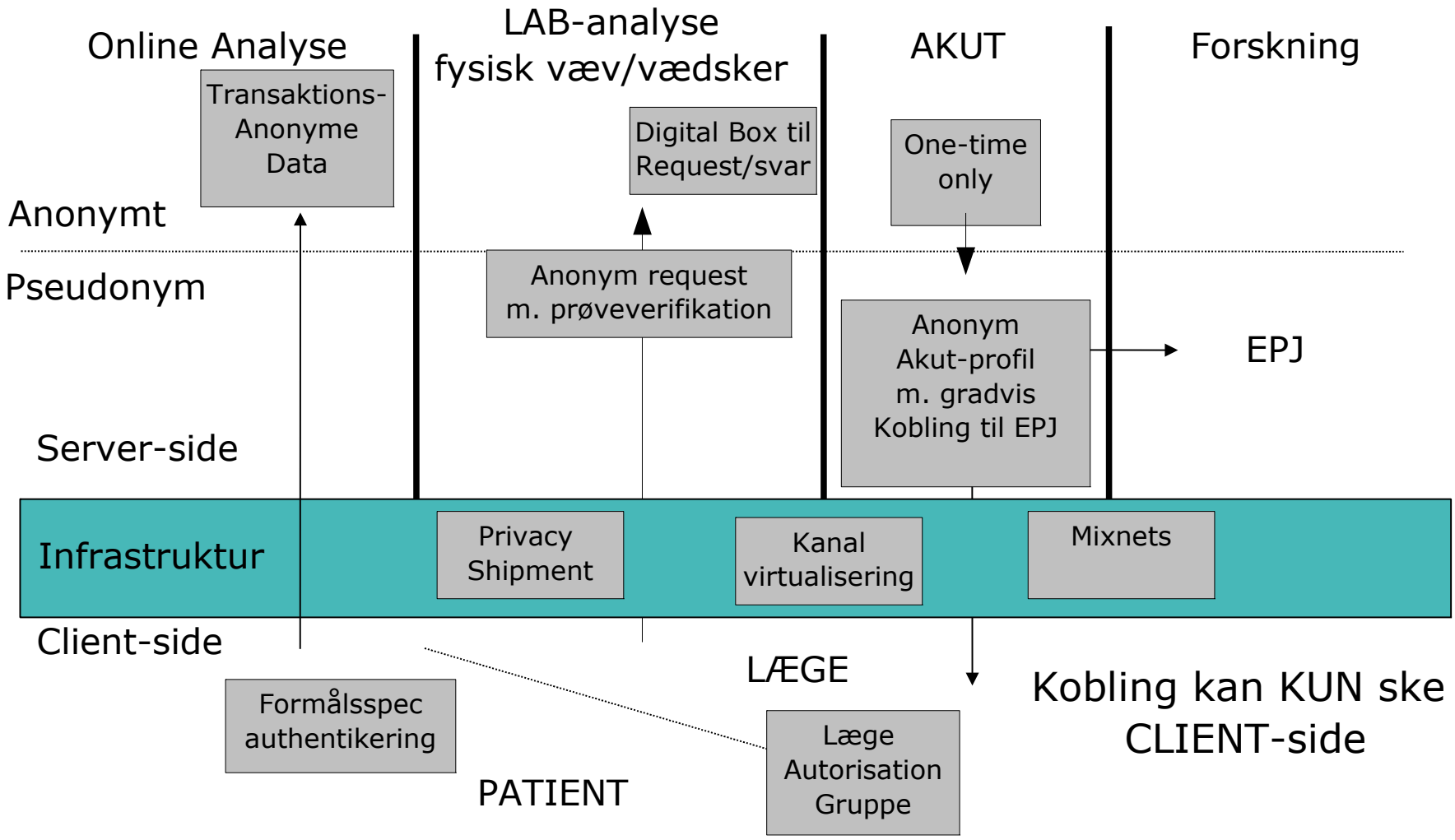
KRITISK: Hver type problem skal løses med FORSKELLIGE mekanismer
INGEN af nedenstående løses hensigtsmæssigt med Identifikation

Identitet
- Virtualisation
- Authorisation
- Authentication
- Negative Credentials
- Revokation
- Accountability

- Virtualisering/mixnets
- Gruppe tilhørsforhold
- Verifikation af ny nøgle UDEN ID
- Bevis for at man IKKE er på liste
  Nemmest at vende modellen
- Mange løsningsmodeller
- Betinget Identifikation
  Afledt deponering/selvinkriminering

Healthcare – sikkerhed
Hvad kan vi i dag

PRIWAY
Security in Context



DanId er ikke en Digital Signatur

PRIWAY
Security in Context

Lov om Digital Signatur

§ 10.

Stk. 3. Nøglecentre må ikke opbevare eller kopiere de personers signaturgenereringsdata, som nøglecentret gennem udstedelsen af certifikater måtte have fået kendskab til.

1) Videnskabsministeriet havde IKKE mandat til at sanktionere DanId med centralt kontrollerede nøgler som en Digital Signatur.

2) Sikkerhedsmæssigt kan vi ikke bruge en man-in-the-middle model som Digital Signatur. Den etablerer central overvågning og aflytning låst til en kommerciel kartelinteresse og legacy-model - ingen af parterne kan vide sig sikre.

3) Problemet kan IKKE løses ved at forbedre sikkerheden mellem borger og DanId. Digital Signatur udgør borgernes personlige suverænitet – den er ukrænkelig i henhold til Grundloven. Og bør klart være det.

4) VTU misbruger Digital Signatur. Man (gen)bruger IKKE en Digital Signatur til at åbne døre.

Opsamling

PRIWAY
Security in Context

- **Privacy er sikkerhed med fokus på borgerens sikkerhed**
  - Alle principielle faktorer taler for – både handel og offentlig
  - Går den forkerte vej – særinteresserne vinder over demokratiet
  - Store problemer i Danmark – DanId, Pas, Digital Forvaltning
- **Vi KAN få både sikkerhed og services – selv de værste**
  - Anonymisering til sikring af biobanker og laboratorieprøver !
  - One-time-only med pseudonymisering til nødsituationer
  - Formålsspecifik anonymisering til online services
  - Online Pseudonymisering af Elektroniske Patientjournaler

Enorme gevinster at hente i Digital Forvaltning med borgeren i centrum – hvorfor henter vi dem ikke?

Questions?

PRIWAY
Security in Context

From Central Command & Control to Citizen Empowerment & Dependability

Use non-invasive mechanisms maintaining post-transaction balances.
Only activate Surveillance when a specific threat is detected

Stephan J. Engberg
Priway
Security in context
.. because the alternative is not an option

Without changing our pattern of thought, we will not be able to solve the problems we created with our current patterns of thought.
Albert Einstein

