Making
Privacy
Default

Sikkerhed uden privathed skaber .. usikkerhed.

Indlæg ved: Stephan J. Engberg
Open Business Innovation

Web: www.obivision.com
Email: Stephan.Engberg@obivision.com

April 2004

Det politiske klima

” Da terroristerne ramte USA, angreb de selve de værdier, som vi bygger vores samfund på – demokrati, frihed, retsstaten, menneske- og minoritetsrettigheder. I dag er vi selv nødt til i en periode at gå på kompromis med disse værdier for at kunne forsvare dem. I givne situationer må vi bryde nogle af de regler, vi ellers værner om,«
Uffe Elleman-Jensen, Information, 28. feb 2004

Pas, Data Retention, Digital Signatur, etc. etc.

MEN også aktuelt

EU Parlamentet truer med at indbringe Kommissionen for Domstolen for at give efter overfor US i spørgsmålet om Passagerdata.
Fast deadline i denne uge.

Privacy paradigmer - fiaskoer

- Code of Conduct – Mistillid/massivt misbrug
  - Case: US FTC Telemarketing do-not-call
    - 55 million personer registreret i løbet af 2003 (57%)
- Informeret samtykke – Avanceret afpresning
  - Ingen privathed eller ingen Service ⇒ fatalisme og mistillid
  - UK analyse: 70% – ”cannot avoid registering” *)
  - EU Data Beskyttese – bureaukratisk men sikrer IKKE privathed
- Anonymitet – Sælger ikke og frygt for kriminalitet
  - Case: Zero-Knowledge, DigiCash

*) http://www.strategy.gov.uk/2002/privacy/report/pdf.htm

Gartner Group
Om privatlivets fremtid

”Om 10 år vil anonymitet og beskyttelse af Privatsfæren være begrebet næsten uden betydning.”

“De tre teknologier (SJE: RFID og langdistance trådløs radiokommunikation) vil skabe et samfund, hvor alle er online konstant, og en lang række informationer lagres om den enkelte.”

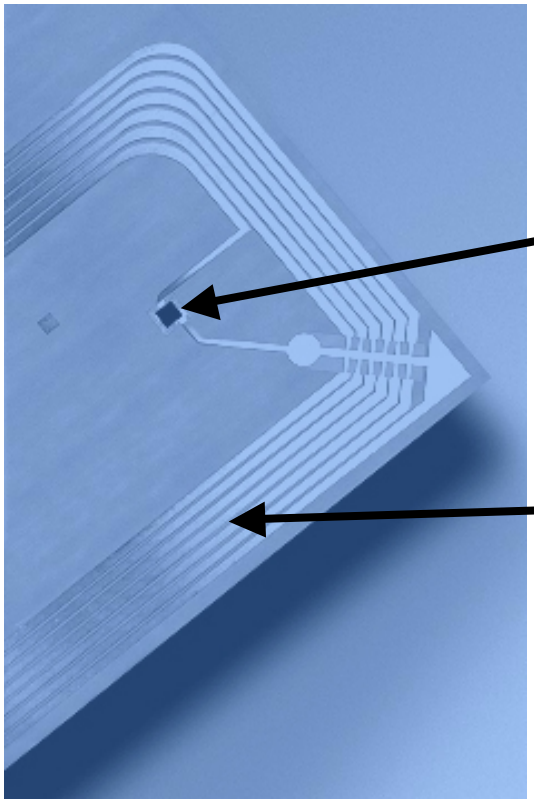
“Information om hvem vi er, hvor vi er og hvor vi har været, vil ikke længere være en privat sag, men derimod informationer, som til enhver tid kan genskabes”

”De forskellige privatsfærer smelter sammen”

Gartner Group, April 2004, http://www.jp.dk/itogc/artikel:aid=2374038/

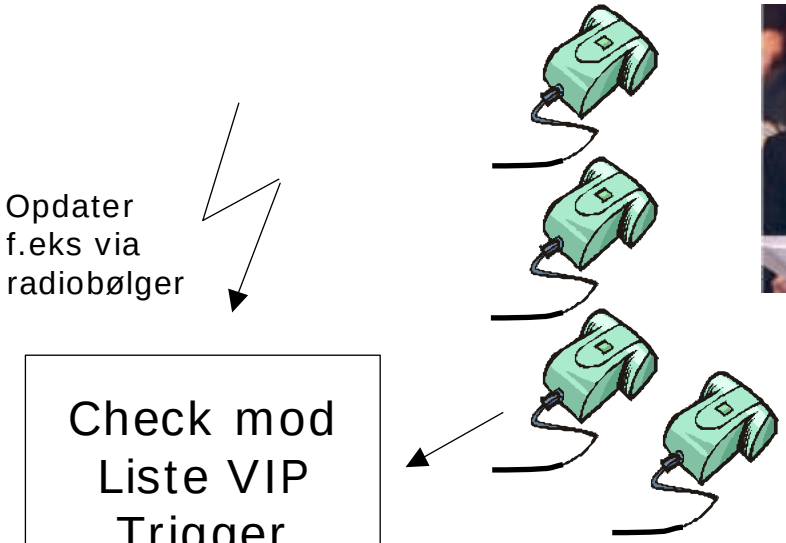
Hvad er **R**adio-**F**requency **Id**entification (RFID) tag?

- Smart, småt og pervasive



Er konstant identifikation sikkert?

Case: Paparazzi-centralen



Hvis mennesker er målet
Leverer devices sigtet

RFID Attackers

- Terrorister –
- Tyve -
- VIP –
- Workplace –
- Social –
- Retail –
- Erhverv –
- Hackers –
- Government –
- Government –

RFID har mange positive applikationer
Men uden redesign også
Sikkerhed risici
Data Lækager
Tracking/Sporing
Etc.

Translates into ***Trust destruction***
CLOSE – in the face of the individual

A dramatic escallation of
the Surveillance Society

Biometri - Problemer

- **Biometri er IKKE perfekt !**
  - Sænker årvågenheden / selvbetjening / fast track
  - Udbydere sælger SNAKE-OIL

- **Biometri kan spoofes/identitet kan stjæles**
  - Falsk biometri (f.eks. kunstige fingeraftryk)
  - Identitetstyveri via dårlig id kontrol
  - I sidste ende er der ALTID korruption

- **Konsekvensen ved Identitetstyveri store**
  - Kan blive udelukket fra dit liv / Black-listet
  - Dit ”gode navn” kan blive ødelagt / f.eks. ingen kredit

- **Best case er worst case**
  - Udbredning og central opsamling nærmest garanteret
  - E.g. restauranter/barer i US bruger til at ”genkende”
  - Balanceret sikkerhed gøres umulig
  - E.g. Vidnesbeskyttelse umulig

”*Biometrics Revealed*” - http://heise.de/ct/english/02/11/114/
”Ban Biometrics ” - http://www.anu.edu.au/people/Roger.Clarke/DV/Biom030908.ppt

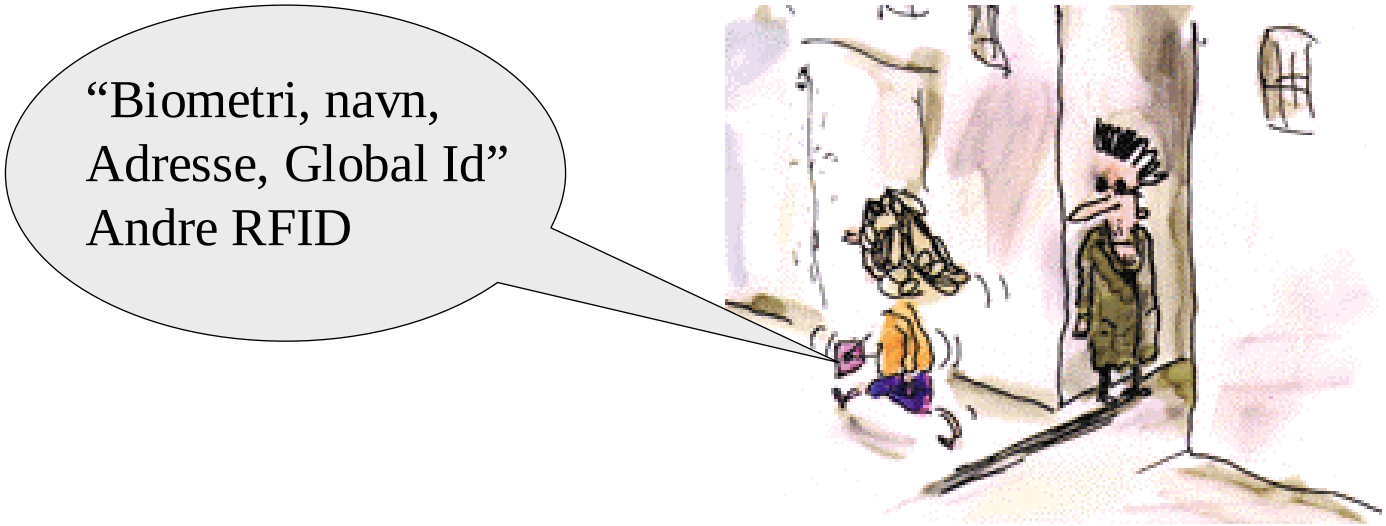
Den ultimative applikation

- ICAO specificerer brugen af Biometri OG RFID i pas fra 2004 (udsat)

- Bruges til ?
  - Absolut Identikation
  - Hurtig Håndtering.

Andre muligheder

- Generel tracking og RFID linking



- Nemt for *enhver* at spore personer og transaktioner
- Politiets efterretnings værktøjer gjort tilgængelige for enhver

Politikerne taler om ”Borgeren i Centrum”

”Personlig Frihed før Systemkontrol”
Regeringsgrundlaget, efterår 2001

Godt – men hvad betyder ”Borgeren i Centrum”?

Personlig Frihed?

Systemkontrol?

Skal man overføre kommerciel CRM til det offentlige system?

"Eliminate the need for multiple systems and limit the manual processes. **Manage data by utilizing fully integrated solutions. Data is stored in a single system** allowing access to time data, payroll data, employee data, and safety and health data."

Kathleen Hirning

IBM, Business Consulting Services Executive

Den Digitale Taskforce

Government Conference 2004

April 14, Copenhagen

REGISTERSAMKØRING?

EN INDGANG TIL DET OFFENTLIGE?

Forbrugeren oplever

Stigende systemkontrol – faldende frihed

Infrastruktur
Telekom, Banker, ISP, Netværk

Profilering
Markedsføring, kundeservice, kreditcheck, helbredscheck, ansættelse, dating etc.

Det offentlige
Økonomi, helbred, social, Arbejde, overvågning etc.

Fysisk overvågning
Kameraer, mobil-sporing, Biometri, Adgangskontrol etc.

"Nye tal fra Forskningsministeriet ..
"7 ud af 10 bryder sig ikke om at indtaste personlige oplysninger på en hjemmeside.
Her har virksomhederne en opgave, de er nødt til at løse, hvis de vil have kunder på nettet."
Erhvervsminister Ole Stavad 1. Marts 2001

Open Business Innovation

Vision

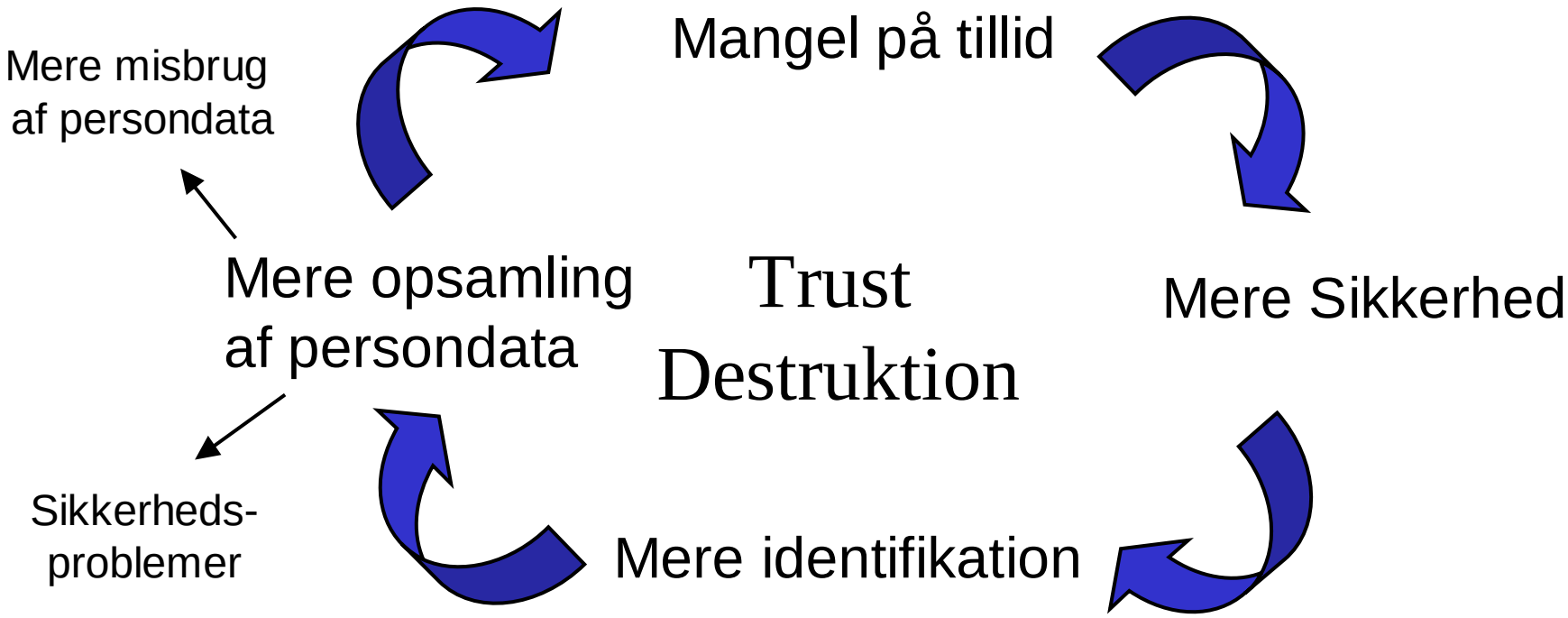
Making Privacy default

Mission

Provide knowledge, services and solutions
based on Individual Privacy Control,
Accountability and Convenience
in order to
empty the databases of the world
for identified personal information
and fill them with the pseudonymous information
needed for close long-term relationships

With security and privacy e-consumer's top priority, identity services have a long way to go before they meet consumers basic needs and win their support.
[Gartner Group, Dec 2001]

Negativ Trust Cirkel



IDENTIFIKATION SKABER RISIKO
OG DESTRUERER TILLID

EU on Trust & Confidence

Technological products should be in all cases developed in compliance with the applicable data protection rules. But being in compliance is only the first step. **The aim should be to have products that are not only privacy-compliant and privacy-friendly but if possible also privacy-enhancing.**
Source: PET Workshop

Protection of personal data, authentication, and **identity management** are primary issues where no public service should ever fail. Public institutions should always ensure that digital transactions and communications are secure and that personal data will remain protected. Citizens should always be able to control access to their personal data, and how these data have been stored, used, and accessed. Failure to ensure this may, in addition to breaching the law, entail significant social and economic costs. **Only data that are necessary for the fulfilment of the respective purpose may be collected. To this end, the use of privacy enhancing technologies should be favoured.**

Significant developments in electronic identity and authentication systems have taken place over the past few years. Access to citizen data must be in full compliance with the European and national data protection legislation, where **the choice of technology should empower citizens as much as possible to retain control of their personal data.**
Source: EU Commission Statement 2/10 - COM(2003) 567 final

IT & Privacy Barrieren

IT rummer meget store potentielle
og ikke udnyttede fordele.

Men Informationssamfundet skal bruge stadig flere
persondata for at levere værdi som lovet

Problemet er Privacy - forbrugerne vægrer sig

”2/3 af erfarne brugere forlader normalt et website,
når de bliver bedt om personlige data” [*]

Forbrugerne beskytter sig
ved at undgå registrering !!

*) Kilde US Statistical Research, Spring 2001

Privacy – Definition

Privacy can best be understood as a protection against certain kinds of risks – risks of injustice through such things as unfair inference, risks of loss of control over personal information, and risks of indignity through exposure or embarrassment.

Source: DEMOS – The Future of Privacy
http://www.demos.co.uk/catalogue/thefutureofprivacyvolume1_page30.aspx

Privacy / Privatlivets Fred

Privacy is generally defined as

> the claim of individuals to determine for themselves, when, how and to what extent information about them is communicated to others.

Erfaring & Tryghed

”Man skulle tro at uerfarne internetbrugere ville have en større mistro til virksomhedernes forvaltning af e-privacy, end folk der generelt er fortrolige med mediet.

Men det forholder sig lige omvendt.”

”Jo mere erfaren forbrugeren er med internettet, des mere usikker er han på, hvorvidt hans personlige informationer er beskyttet.

”Den garvede internetbruger har simpelthen et større overblik over, hvad der kan gå galt”

E-business Manager René Claus Larsen,PriceWaterhouseCoopers, Januar 2001
http://www.bitconomy.dk/magasin.asp?article=1511&showmenu=4

Privathed – Ikke så simpelt

”Although privacy is broadly recogniced as a dominant concern for the development of novel interactive technologies, our ability to reason analytically about privacy in real settings is limited.”

Palen & Dourish, Unpacking ”Privacy” for a Networked World
http://portal.acm.org/citation.cfm?doid=642611.642635

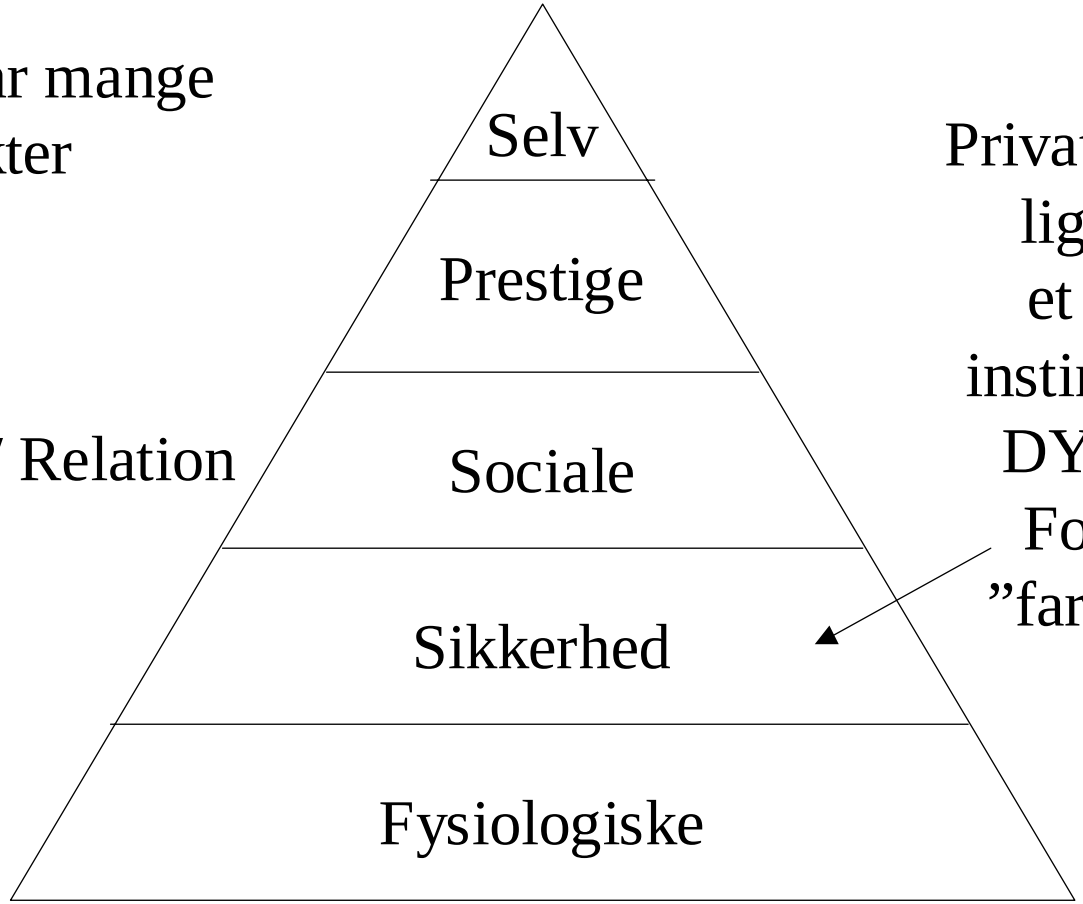
Maslows behovspyramide

Privathed har mange Aspekter

Image

Intimitet / Relation

Tryghed

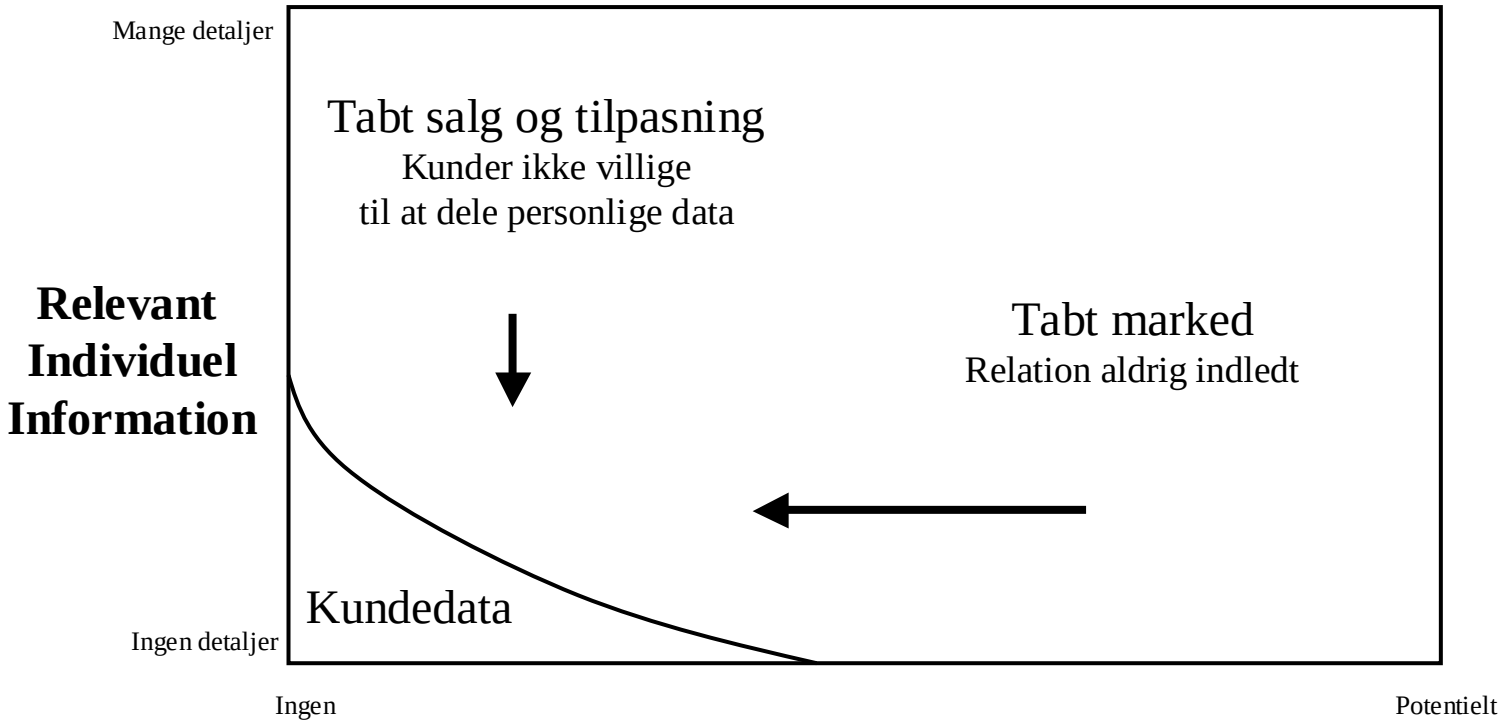


Privathed som behov ligger generelt et sted mellem instinkt og følelser. DYBT forankret Forbindes med ”fare” og ”risiko”

Vores definition på Privathed
= Individets Behov for kontrol

”The Strongest Force on Earth is
the Individual Need for Control
of his own Universe.”
Tom Peters

Privatheds Omkostninger



Om RFID Privathed

»I USA har der været protestbevægelser i gang, som tåler sammenligning med de store anti-atomkraftbevægelser.

Derfor er det meget vigtigt, at der bliver taget hånd om privatheds-problematikken,« siger Preben Mejer.

Ingeniøren, fredag 16. April 2004

Sikkerhedens myter

Trust – Identifikation

0%

Identifikation giver tryghed

Den stigende Identifikation er
Informationssamfundets
Største Tillids- og Sikkerhedsproblem

Valget i den digitale verden

Teknologien kontrollerer Mennesket !

eller

Mennesket kontrollerer Teknologien !

Systemkontrol:

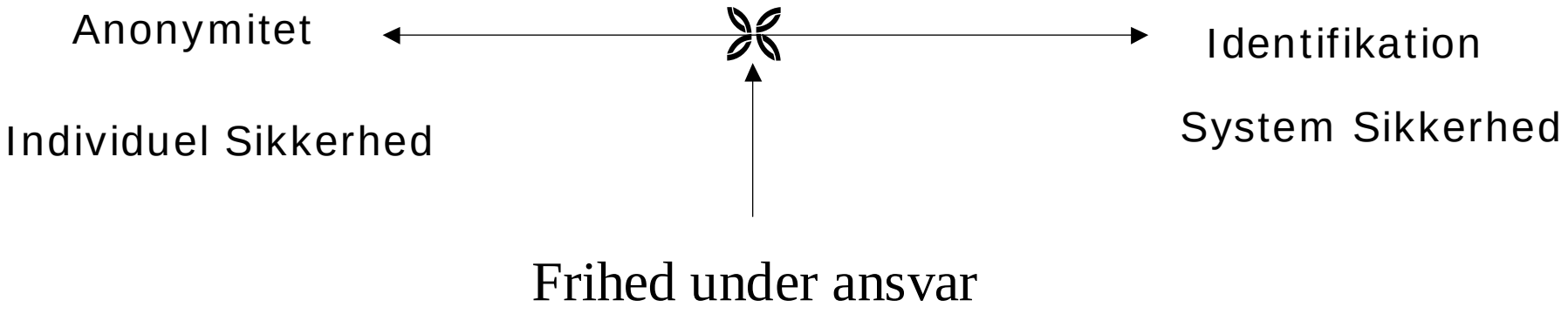
Vi er ALTID er identificeret, overvåget og registreret i databaser udenfor vores kontrol.

Personlig frihed:

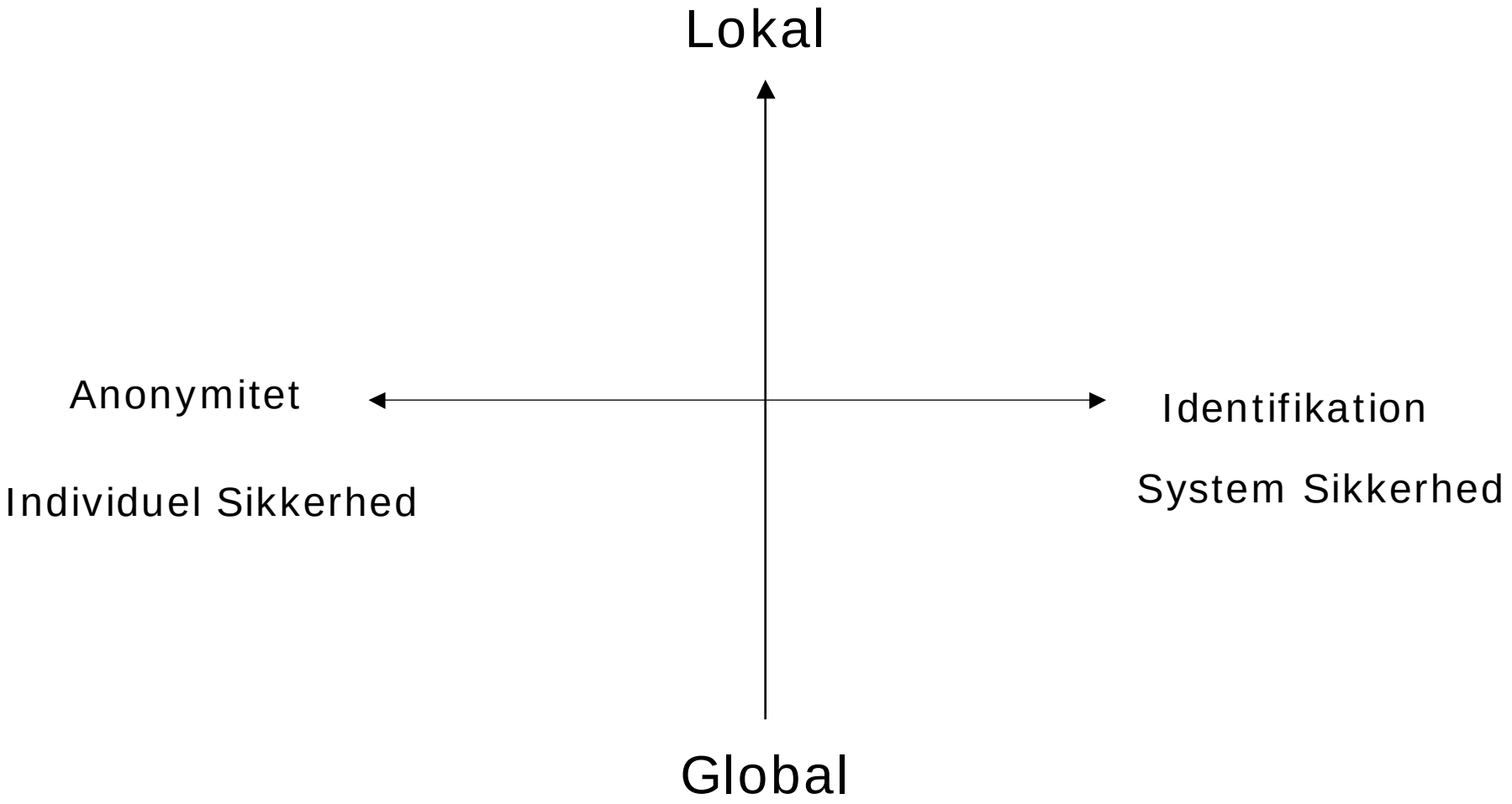
Vi bruger teknologien til at give individet kontrollen med persondata i databaserne.

Kan den digitale verden overhovedet fungere, hvis mennesket føler sig eller er sat uden for kontrol?

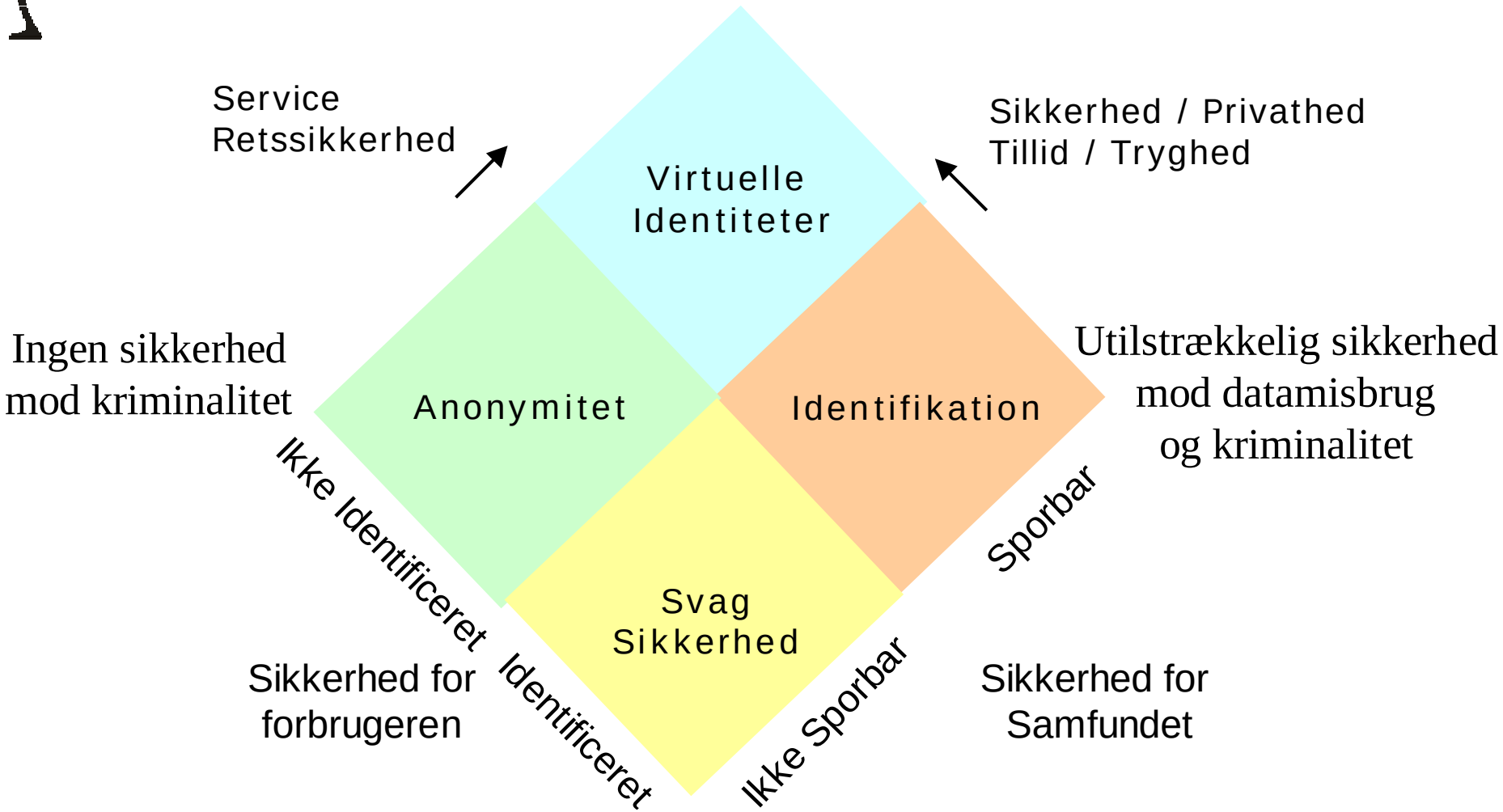
Det klassiske Problem



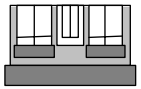
Tænk flere dimensioner



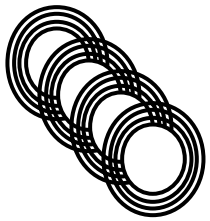
Open Business Innovation
Identitets Model



Infrastructure
Security and Privacy Platform



Lokale Identiteter
(Trusted Pseudonyms)
Multi-channel, Persistent



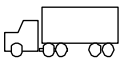
Multistep Identity
Disclosure Process

No single point of
Trust failure

Signatures
Authentication
Id support

ISP
eMail/SMS
Telecom
WLAN

Payment



Shipping

Privacy Enhancing Technologies
Deployed across Infrastructure

Home

At work

In store

Travel / Mobile

- Patent pending

Privacy in Pervasive Computing

Device to Authenticate

No persistent Identifier

Smartcard

1. Request Session

2. Request Authentication

Subscription Telecom

Authenticating Unit

5. Non-linkable session

4. Session Authentication

Privacy

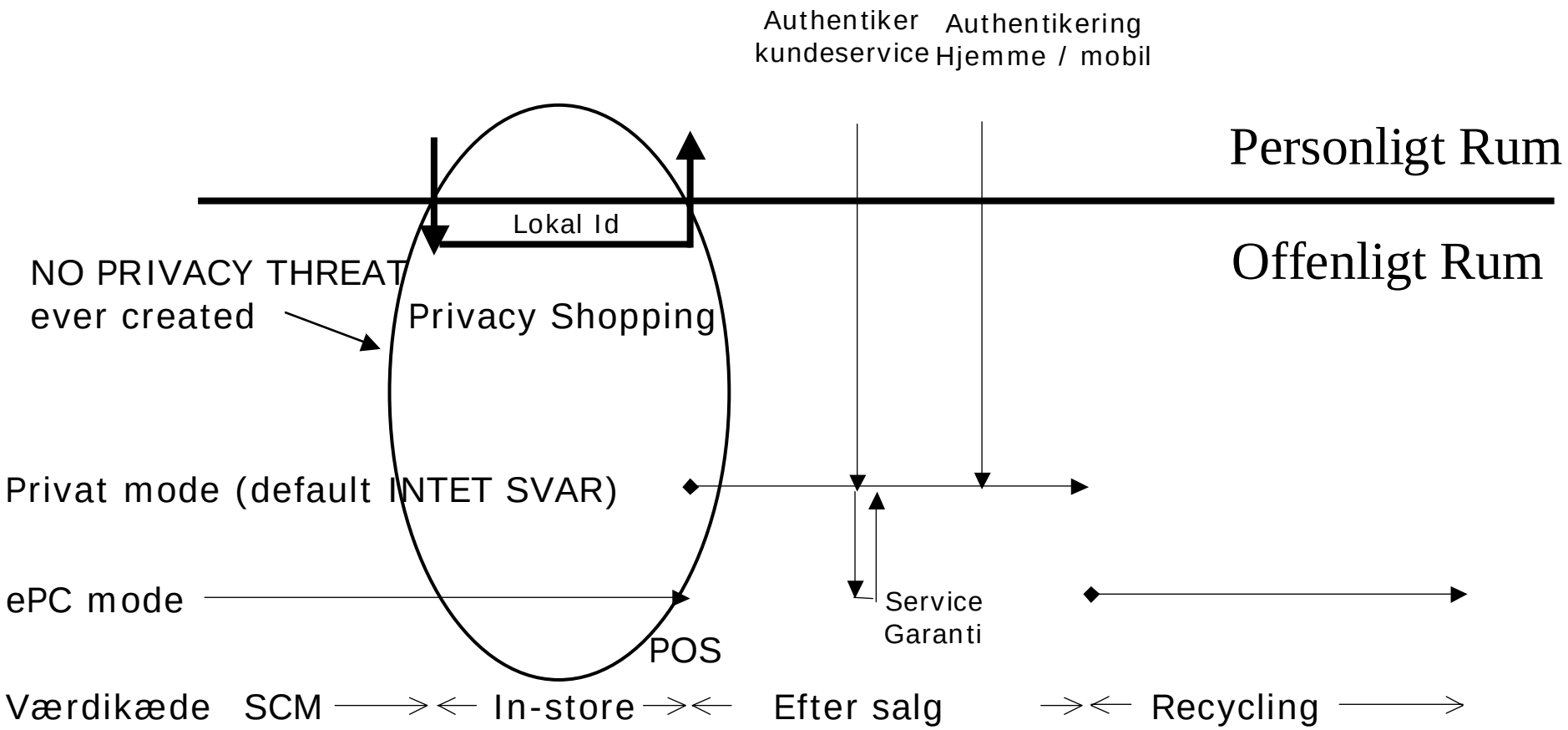
Accountability

3. Zero Knowledge Authentication

Local:

- Bluetooth
- Infrared

RFID Privathed overblik

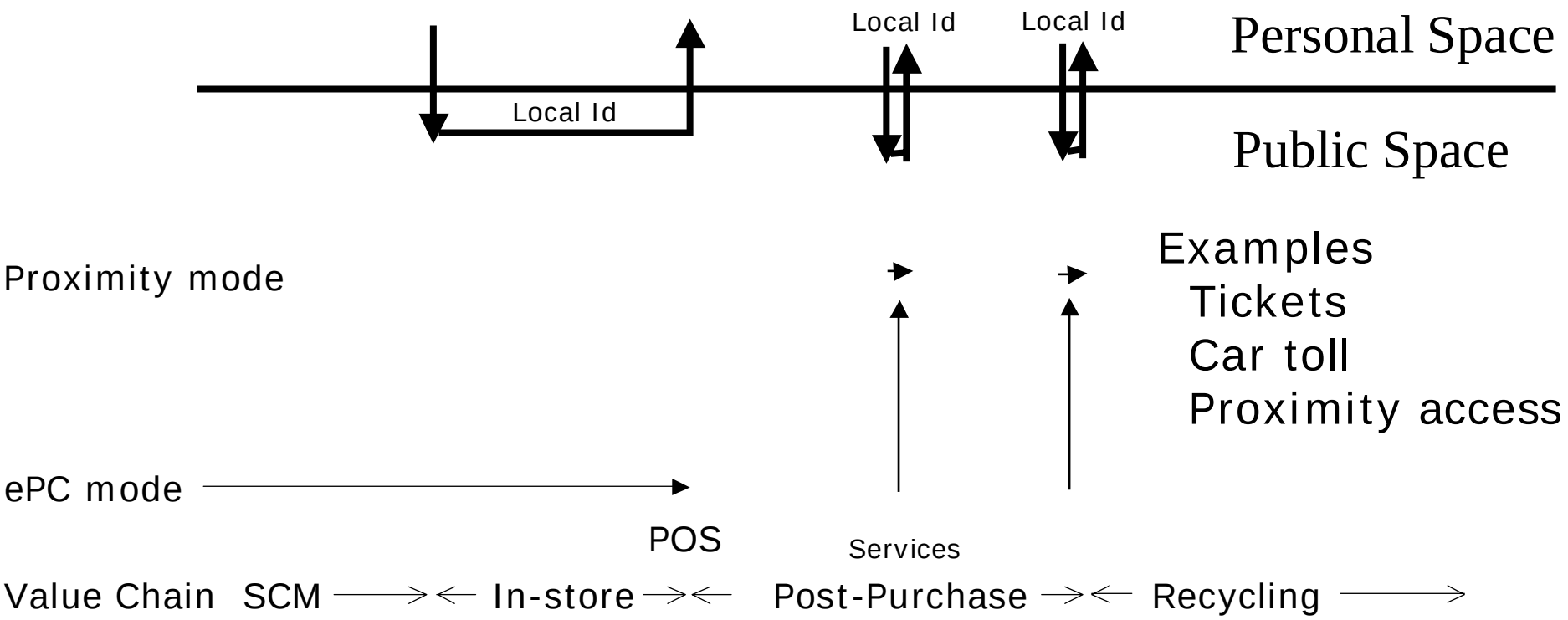


RFID Privacy Mode

- Ved salg overføres KONTROLLEN til forbrugeren !!
  - RFID ”Privat mode” aktiveres og RFID bliver tavs
  - RFID forbliver *killed* medmindre forbrugeren aktiverer
- Zero-knowledge Device Authentication
  - Low computational PET skalerbar til asymmetriske nøgler
  - Lækker ikke information / transaktionsanonym
- HVIS RFID er aktiv på vej UD af butikken, så
  - Produktet bliver stjålet – aktiver overvågning etc.
  - Butikken/leverandør spyware – dokumenter og tilkald Politi
- Privathed bliver til en win-win løsning
  - RFID aktiv for integration, kundeservice og genbrug etc
  - Kan SENERE opgraderes til intelligente services
  - Selvbetjeningsvenlig – SPECIELT med Privacy Shopping
  - Åben kundetilpasning langs værdikæden (ordreproduktion)
  - Kun lille trade-of mellem privathed og CRM programmer
  - Kan endda gøres FULDT anonymt med kreditbetalinger !!!

RFID Privacy overview II

Passports, Payment Cards, National Privacy Id Cards,
Healthcare, authenticity, library not described here.



Biometri – JA, men

- **Biometri fordele**
  - Ikke NEMME at kopiere
  - Komplekse
  - Altid med - kræver ikke at man husker dem
  - Kan gemmes som templates, dvs. irreversibelt kodet

- **Kan derfor bruges til at give DIG adgang til DINE NØGLER**
  - Multiple CLIENT-side identiteter !!!
  - ALDRIG UDEN FOR INDIVIDETS ABSOLUTTE KONTROL

- **MEN IKKE ALENE, kræver (Er, Har, Ved)**
  - Passwords mod spoofing
  - Revokability for at kunne blokere mod misbrug
  - En form for kryptering for at beskytte tamper-resistens
    - SPECIELT hvis der er tale om certificeret biometri

Anbefaling: LOKAL Biometri KAN give INDIVIDET bedre kontrol

Data Retention ???

Oplæg til principper

1. Ansvarlighed -> Frihed under ansvar.
   - Kriminel handling sporbar til dig (et offer giver en indgang)
   - Men ikke sporing af din færden

2. Sporing af enkeltborger -> Under kontrol
   - Vil vi kunne koble alle handlinger om en person?
   - I så tilfælde – hvordan undgår vi at det omfatter ALLE?

3. Krav om aflytning?
   - Adgang til aflytning kræver
     1. Ødelæggelse af sikkerheden ved Digital Signatur / PGP
     2. Kontrolaflytning af alt / sikre protokoller over åben linje
     3. Fjernkontrol med DEVICES (Trusted Computing)
   - Men Teoretisk umuligt at garantere
     - Peer-to-Peer over WLAN, Langdistance kortbølge etc.
     - Steganografi (signal skjult i støjen)

Terrorpakken ???

BAD GUYS KAN ALTID BESKYTTE SIG

HVORFOR ØDELÆGGER VI SÅ SIKKERHEDEN?

Er vi i færd med at kriminalisere tankeforbrydelser?

Bemærk
Teleselskaberne har intet problem med at
sætte sig på borgernes privatliv - tværtimod
(Gatekeepere/Google GMAIL om igen)

Opsummering

- **”Privatliv og anonymitet forsvinder”**
  - Nej – det destrueres af de forkerte årsager
  - Privatliv er en skaber af SIKKERHED OG VÆKST
- **Vi kan beholde (megen) Privatliv**
  - Faktisk uholdbart og økonomisk destruktivt uden
  - MEN Biometri og dårlige standarder er alvorlige trusler
- **Internettet er et fysisk net**
  - Men MANGE LOGISKE PEER-to-PEER forbindelser
  - Decentralisering i stedet for centralisering
- **Nationalt ID kort kan blive en LØSNING**
  - Bedre sikkerhedsinfrastruktur til alle
  - MOD til gengæld -> kontrol til BORGEREN
- **Danmark kan differentiere sig via RFID**
- **Grundstrategi**
  - Giv den enkelte ret og mulighed til at beskytte sig selv.
  - Men det betyder IKKE at man skal være naiv

Identifikation ødelægger Sikkerhed og destruerer tillid