PRIWAY
Security in Context

Empower the Citizens

to pull the Digital Information Value Chains

Stephan J. Engberg
Priway
Stephan.engberg @ priway.com

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

Agenda

PRIWAY
Security in Context

- What is trust?
- The burning platform
  - The failure of ”Walled Fortress”
  - Security self-destruction
  - The security ”market”
- How to build Trust
  - The ”Open Metropolis”
  - Empowerment through infrastructure
  - Emerging Technologies – building blocks
- Government Identity – different roads
- Summation - Empowerment

What is Trust?

Trust :: the amount of Risk willingly accepted in a given context

**Risk can be managed and designed
So can Trust & Security**

Nobody is ”trustworthy”

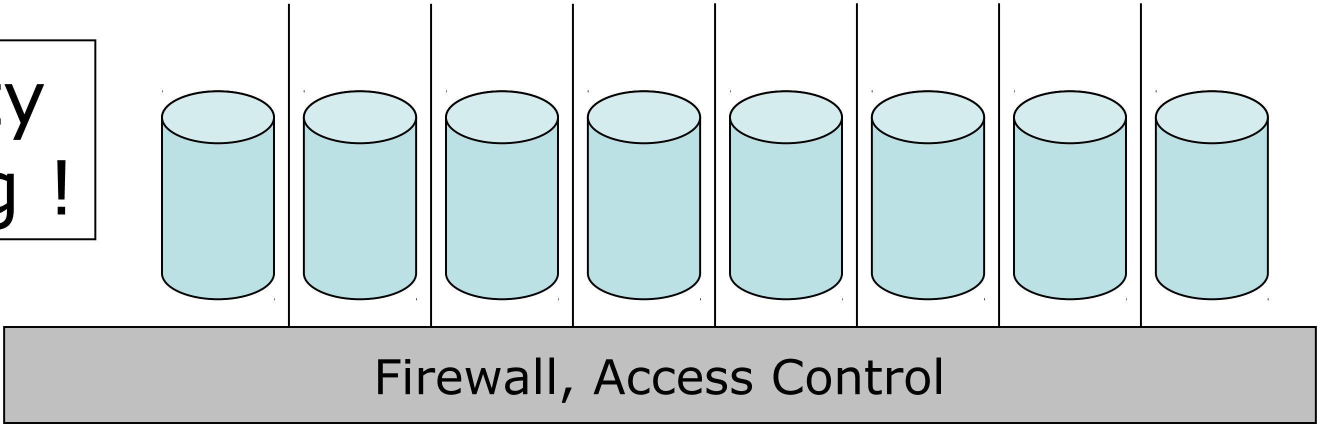
Except in rare cases, risks are avoided and minimised,
i.e. risk involve trade-offs and compensations.
(convenience, price,dis-loyalty etc.)

Lack of Control create resistance

Walled Fortress – no future

Physical Silos and ”perimeter security”

Security Eroding !

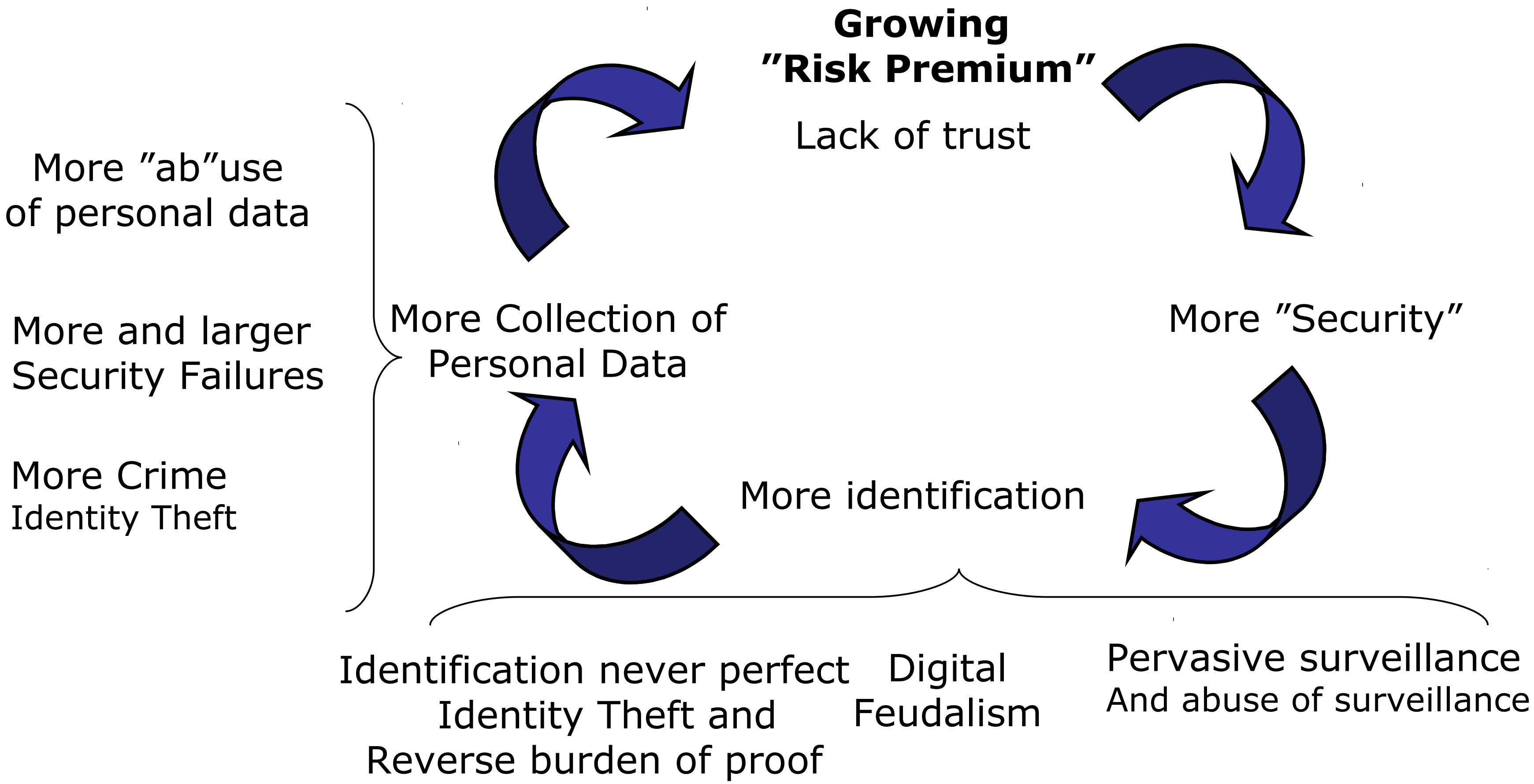


Infrastructure Convergence

Public/private partnerships
Virtual DB Integration
Direct to data source / semantic
New channels & devices
GRID

AMBIENT

The security distrust circle



Growing
”Risk Premium”

Lack of trust

More ”Security”

More identification

More Collection of
Personal Data

More ”ab”use
of personal data

More and larger
Security Failures

More Crime
Identity Theft

Identification never perfect
Identity Theft and
Reverse burden of proof

Digital
Feudalism

Pervasive surveillance
And abuse of surveillance

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

Biometrics - rethink

- Biometrics is keys that are
  - Non-revocable
  - Non-changeable
  - Non-hideable
  - Spoofable
  - (ab)Usable out of context
  - Assumed perfect

Reverse Burden of proof creating

Identity Theft weapons !!

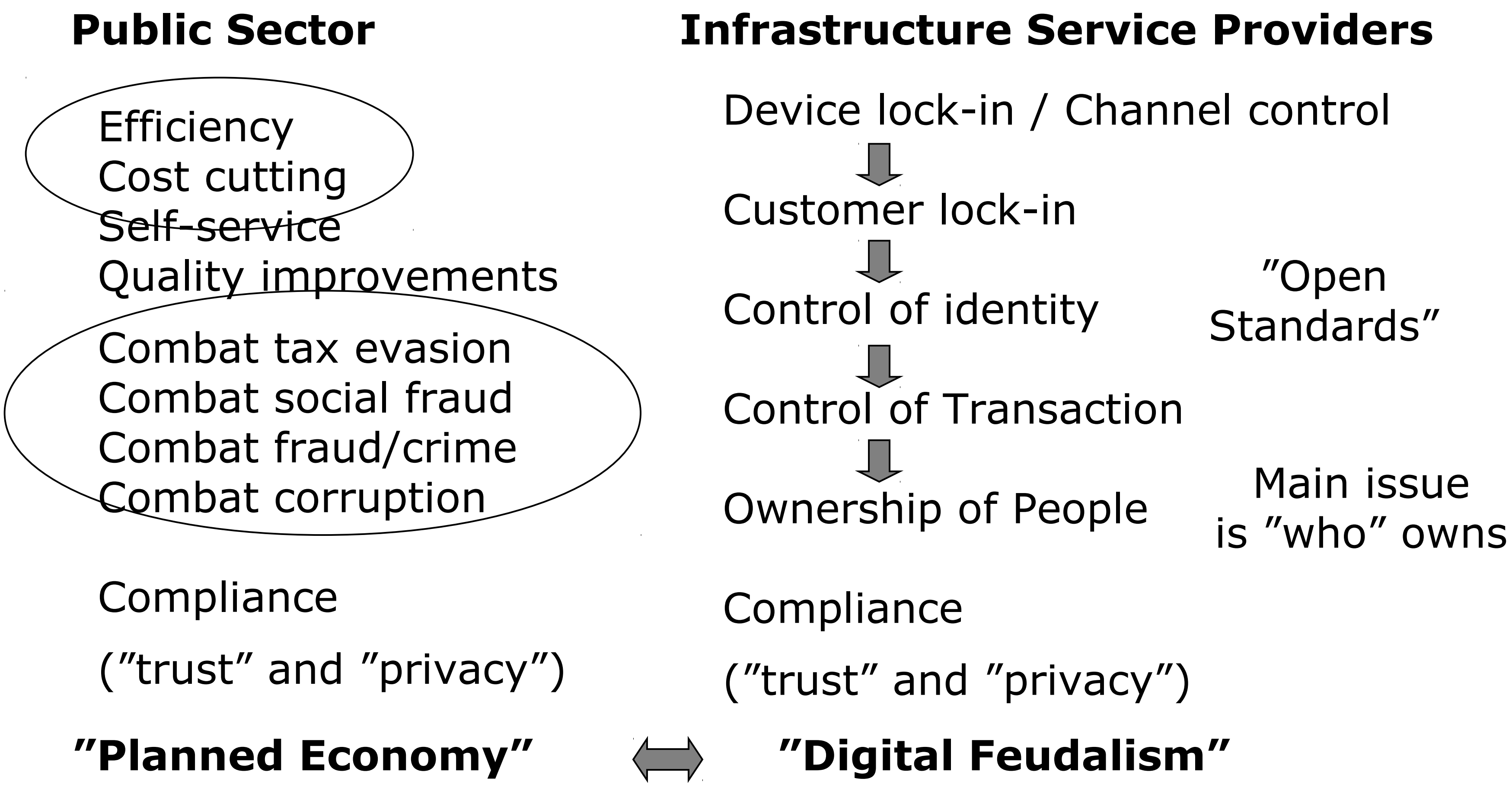
What happens to wictims
of Identity Theft
with blacklisted biometrics !?

Rule:: Never use Biometrics for Authentication

But - Biometrics is usefull as Private biometrics.

PRIWAY
Security in Context

Security market distortions



Public Sector

Efficiency
Cost cutting
Self-service
Quality improvements

Combat tax evasion
Combat social fraud
Combat fraud/crime
Combat corruption

Compliance

(”trust” and ”privacy”)

”Planned Economy”

Infrastructure Service Providers

Device lock-in / Channel control

Customer lock-in

Control of identity

Control of Transaction

Ownership of People

”Open Standards”

Main issue is ”who” owns

Compliance

(”trust” and ”privacy”)

”Digital Feudalism”

Who is ensuring Security & Trust?

Scandinavian ”Trust”-model

PRIWAY
Security in Context

The history lesson:
The hardest act for any system is to reinvent itself to solve inherent weaknesses before they cause crisis.

The Security & Trust-model of Scandinavian Single National Id systems increasingly looks like **”The Emperors New Clothes”.**

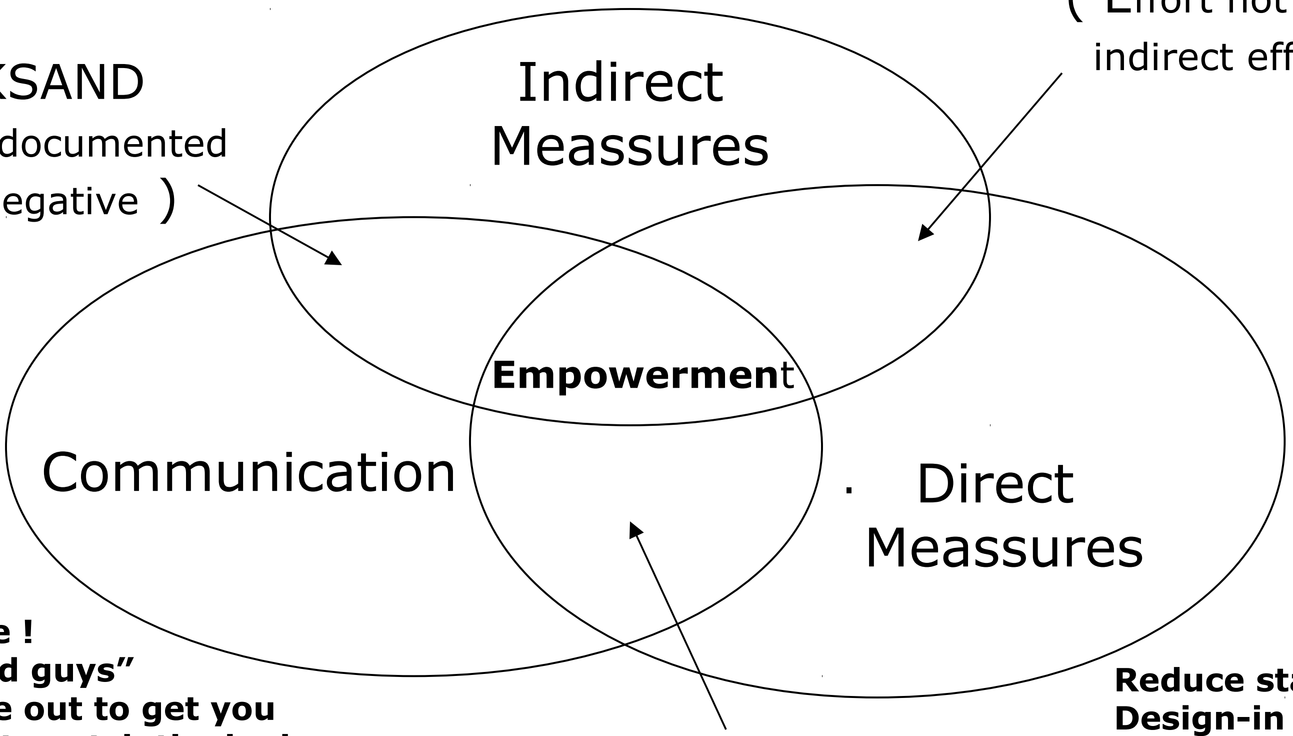
DK Cases (naive trust)
- 62% depend on statefunding
- Higher PC Virus penetration
- Id Theft Healthcare case

The strength of the Scandinavian Countries is the **cultural willingness to debate openly and change when needed without leaving anyone behind.**

Now it is needed again !!

How to build Trust

Policies
Regulation
Fraud prosecution & punishment
Codes of conduct/guidelines
”Do-not-call” type initiatives



QUICKSAND
(Effect not documented
Perhaps negative)

BACKGROUND
(Effort not visible
indirect effect)

Indirect
Meassures

Empowerment

Communication

Direct
Meassures

ISOLATED
(Only partly effect)

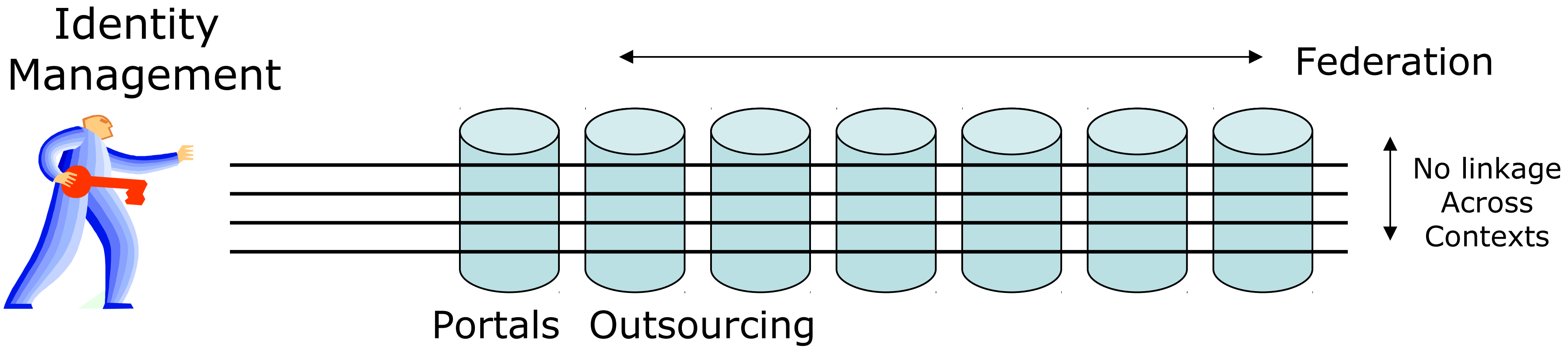
You can trust me !
”We are the good guys”
The bad guys are out to get you
We need means to catch the bad guys
Nothing to hide nothing to fear
Underplay breaches to protect legitimacy

Reduce stakeholder Risk
Design-in security
Isolate context
Distribute control
Context-specific Id

Open Metropolis - context

PRIWAY
Security in Context

Logical Security – Lock data to context
Multi-level Security fallbacks

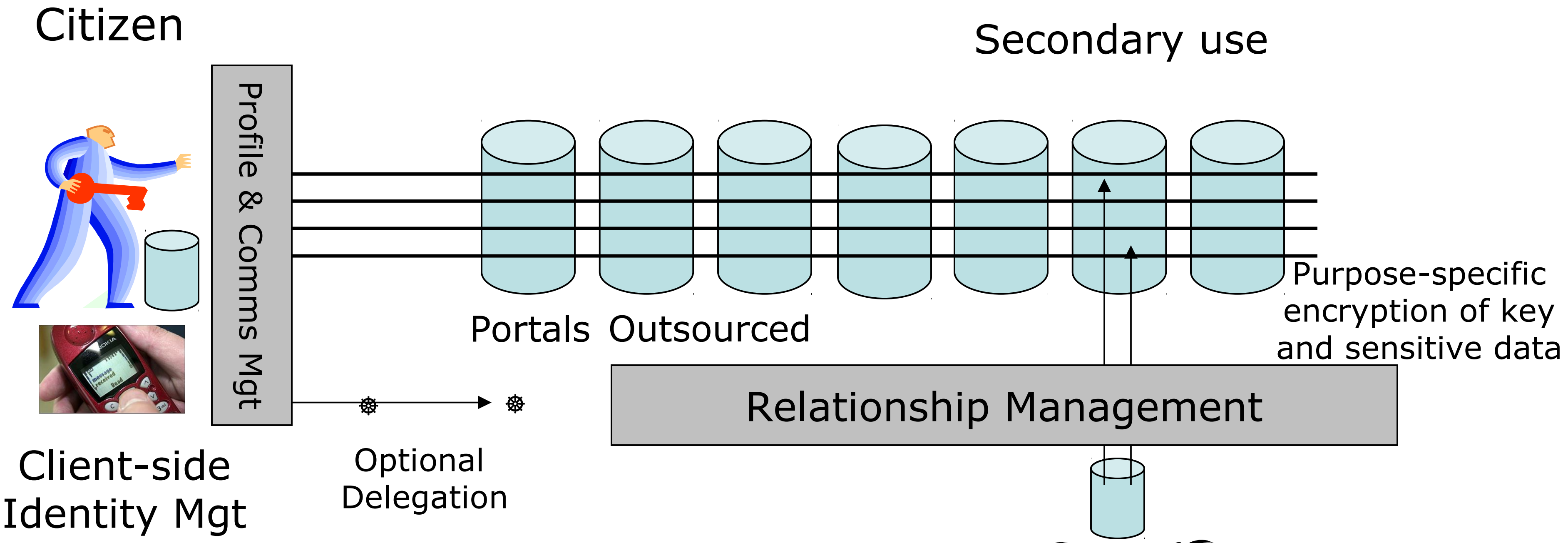


Data locked to a logical context:
- Secure by design -> trust
- Default ”free flow” data -> integration
- End-user empowerment -> innovation

Establishing and maintaining context:
- Clear adaptable accountability model
- Person, device & channel virtualisation

Open Metropolis – free flow

Server Security will fail – simply distribute the data keys Client-side



Citizen

Secondary use

Profile & Comms Mgt

Portals Outsourced

Purpose-specific
encryption of key
and sensitive data

Relationship Management

Client-side
Identity Mgt

Optional
Delegation

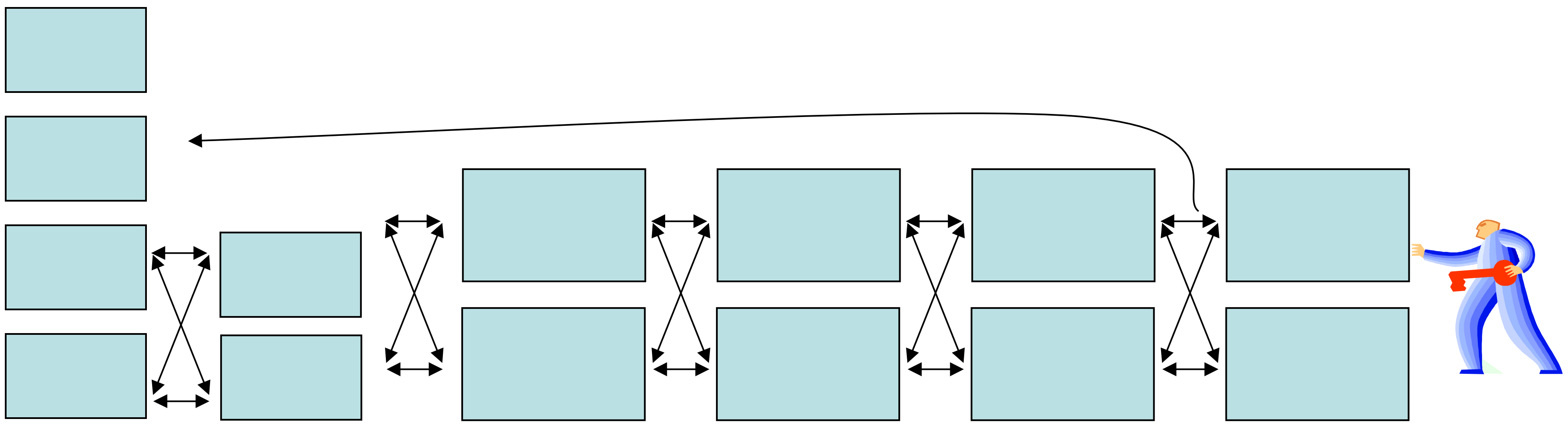
The design task is how to structure data, keys and processes.

Context security can co-exist and be gradually implemented

Empower in Infrastructure

PRIWAY
Security in Context

Ensure citizens can drive innovation



Public Service

Outsourced

Portal Services

Infrastructure Identity support

Channel providers

Client-side Identity mgt.

Open interfaces

Focus on Authentication in context – NOT Identification

Security Toolbox

PRIWAY
Security in Context

Available or soon available

- Credentials
  - Certified profile & attribute data
  - E.g. Credentica
- Identity metasystem
  - Heterogeneous id environment
  - E.g. Microsoft
- Private Biometrics
  - 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

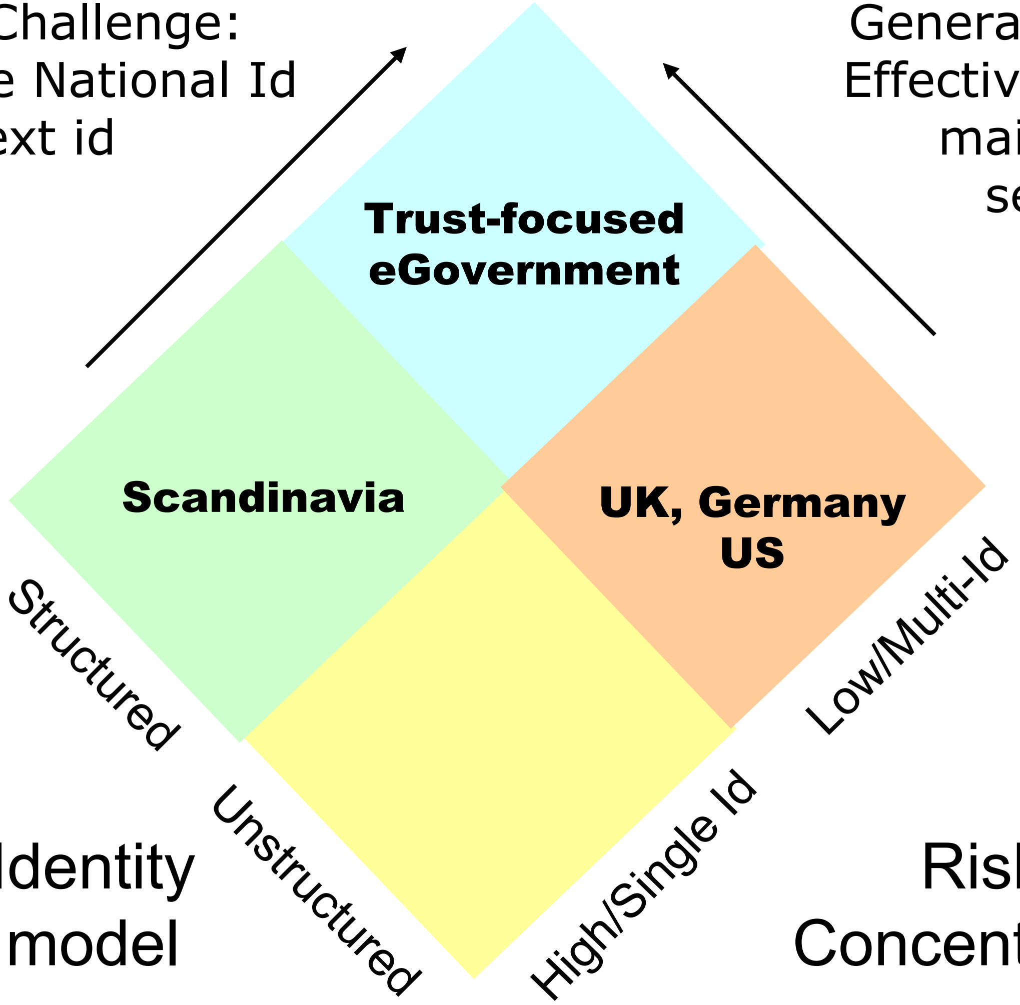
- Secure RFID
  - RFID with privacy control
  - Anti-counterfeiting & Anti-theft
- Non-linkable Digital Payment
  - Anti-counterfeit, Anti-theft,
  - Anti-laundering, Credit, additional
- Citizen Id Cards - Anti-Identity Theft
  - Create & manage new ids to context
  - Traceable & accountable to Nat. Id
  - Privacy Authentication
- Id Accountability negotiation
  - Dynamically adapt accountability
  - I.e.. threat level, transaction req.
- Other
  - Receiver-controlled Communication
  - Indirect means to e.g. control Cameras
  - GRID Context Security

eGovernment id model

PRIWAY
Security in Context

Scandinavian Challenge:
Move from Single National Id
To Context id

General Challenge:
Effectiveness while
maintaining
security



Identity
model

Risk
Concentration

Summation – Citizen Pull

- Move from ”perimeter” security to ”context” security
  - Need to replace failling physcial security with logical borders
  - Lock data to context -> Security by Design
- We need BOTH stronger traceability AND empowerment
  - Identification is creating security problems & Id theft
  - ”Ban” biometrics for authentication
  - Data Retention in context – no problem !
- To make effective, secure & trustworthy eGovernment
  - Design as if there is no trust -> Trustworthy
  - National Id is only a platform for Context Id -> Free Flow Data
  - Open Interfaces towards Citizens -> Innovation
  - Empower Citizens to pull Digital Value Chains -> Drive value

Trust & Security is DESIGNED