DO's and DONT's in Biometrics

Stephan J. Engberg
Priway

Danish Product Award 2007
Ingeniøren
TRADE AWARD
IT

HYDRA
www.hydra.eu.com

PRIWAY
Security in Context
www.priway.com

RFIDsec
www.rfidsec.com

Danish Biometrics
Research Project Consortium

Danish Biometrics

Strategic Advisory Board
EU ICT Security &
Dependability Taskforce
www.securitytaskforce.eu

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 Passport & EU VISA
in clear VIOLATION

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

7 Rules of Biometrics Security

PRIWAY
Security in Context

1. Ensure upgrade ability - Change is the only certain Aspect
2. Ensure Fallback – Never collect non-revocable biometrics
3. Purpose Specification – Mix with purpose specific secrets
4. Proportionality – Exhaust non-invasive security tools first
5. Minimize Interdependence - User Control and revocable id
6. Semantic Interoperability – Don’t standardise at technology
7. Design assuming failure – Critical infrastructure fault tolerance

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

What is Privacy?

PRIWAY
Security in Context

Privacy is security

from the point of view of a single stakeholder

Multi-stakeholder
Balance is needed
in transactions.

Risk Minimisation
Purpose specification
and revokability.

Application Specific
Context determine
Security requirements.

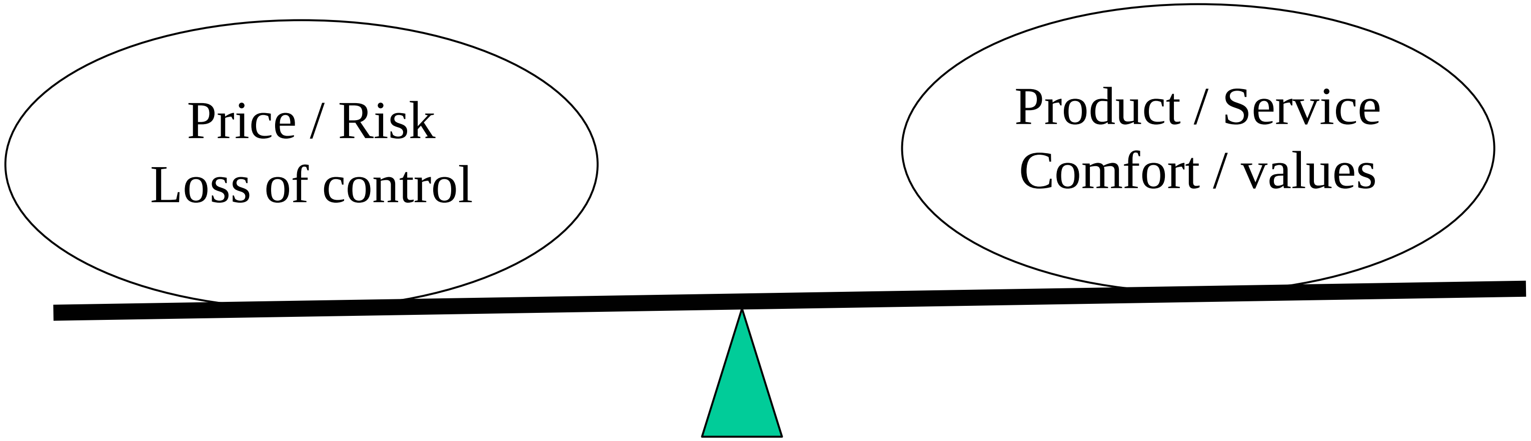
No Security without Privacy

If breach of your security breach security of others

What is Trust?

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

Citizens make subjective rational choices



Price / Risk
Loss of control

Product / Service
Comfort / values

Nobody ”wants surveillance” - they want bad guys caught, but nobody likes to be controlled

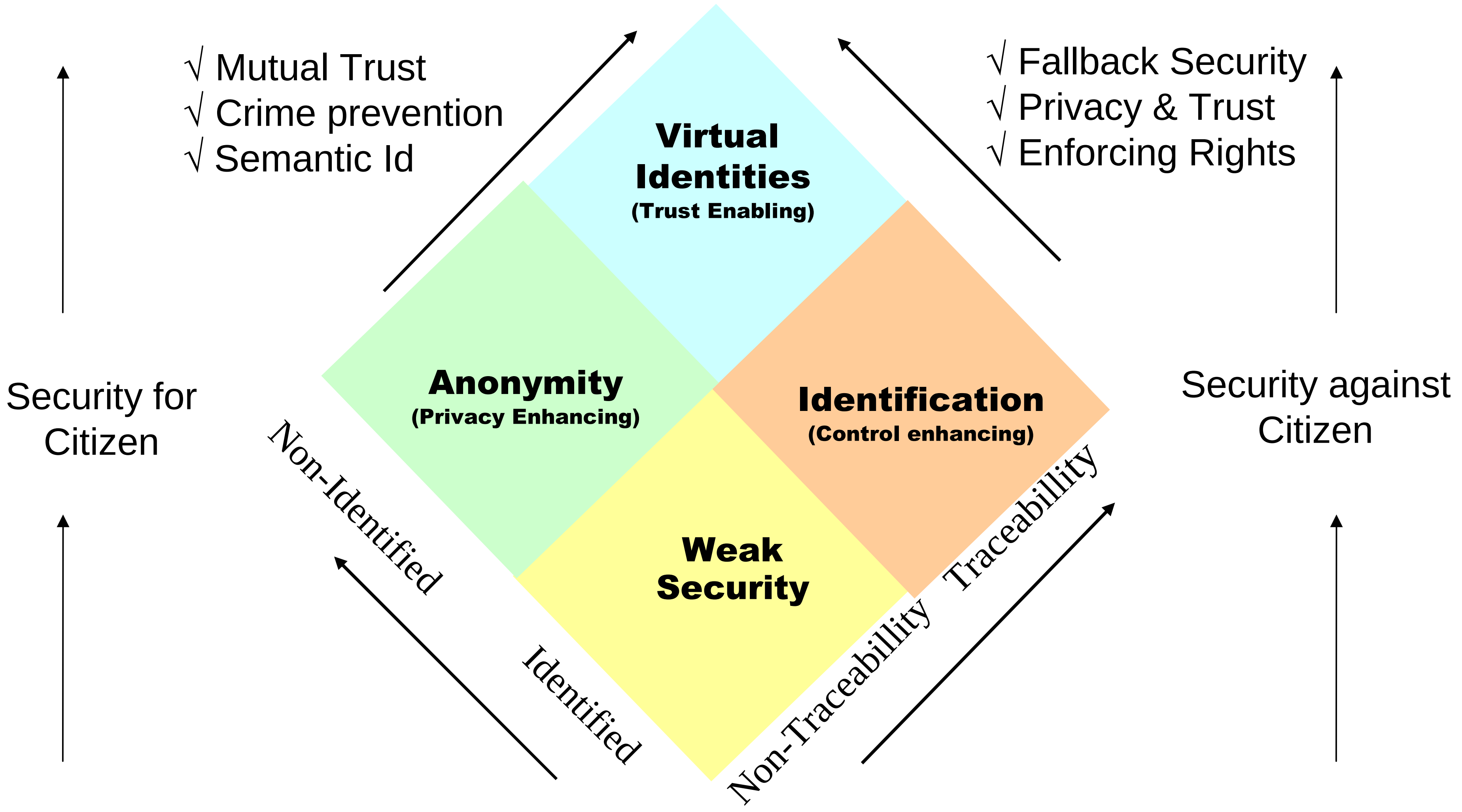
What is a PET?

A Privacy Enhancing technology or PET
is a technology or system
enabling citizen security and control
that **breaks the assumption
of zero-sum trade-offs**
Freedom vs. Security, Sharing vs. Privacy

A PET will make Pareto improvements
E.g. facilitate data sharing.
value creation or mitigate risks
without creating interdependance
and accumulating threats
to citizens and systems

Security/Privacy NOT Zero-sum
Priway Identity Model

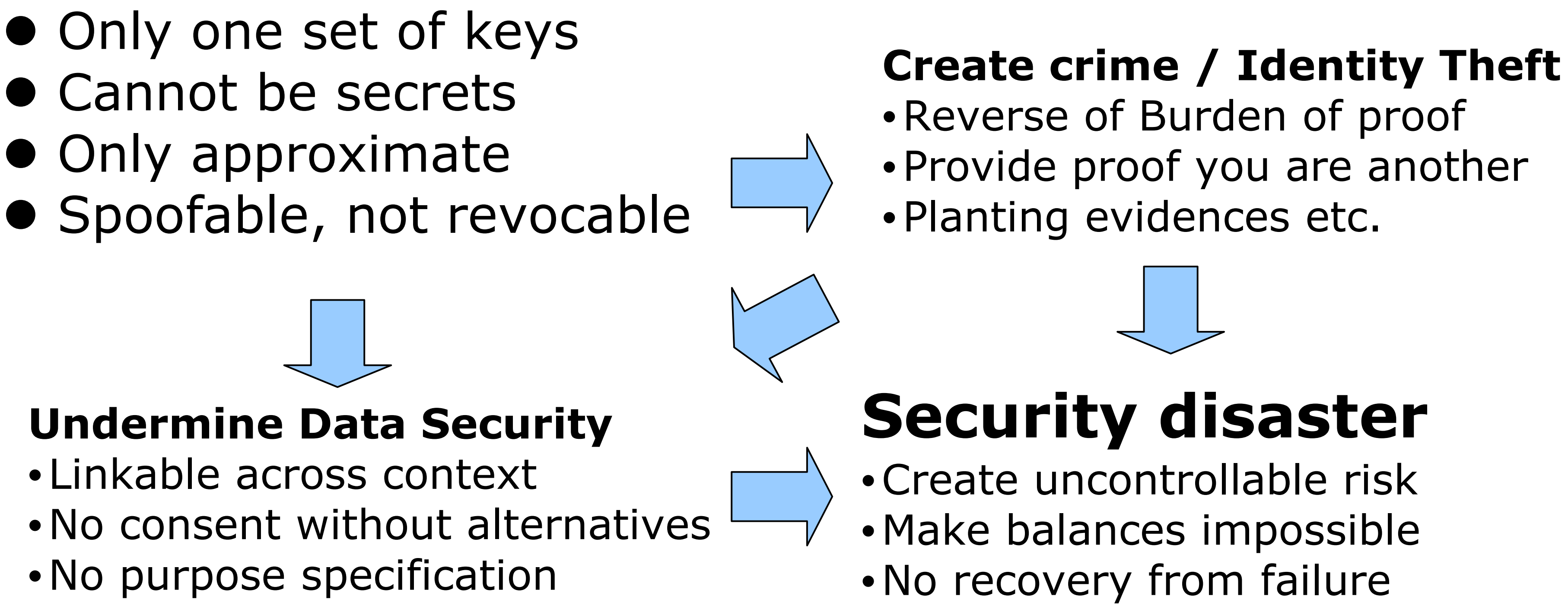
PRIWAY
Security in Context



Danish Biometrics

Biometrics – basic problems

Biometrics used for Identification without user control



- Only one set of keys
- Cannot be secrets
- Only approximate
- Spoofable, not revocable

Create crime / Identity Theft

- Reverse of Burden of proof
- Provide proof you are another
- Planting evidences etc.

Undermine Data Security

- Linkable across context
- No consent without alternatives
- No purpose specification

Security disaster

- Create uncontrollable risk
- Make balances impossible
- No recovery from failure

Rethink – critical need for security and two-way revocability!

Different challenges: Root ID, Id Device mgt, threat escalation, post-crime forensics

Security Tools available

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
- 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

Priway Identity Model

Roadmap to PETs & Biometrics

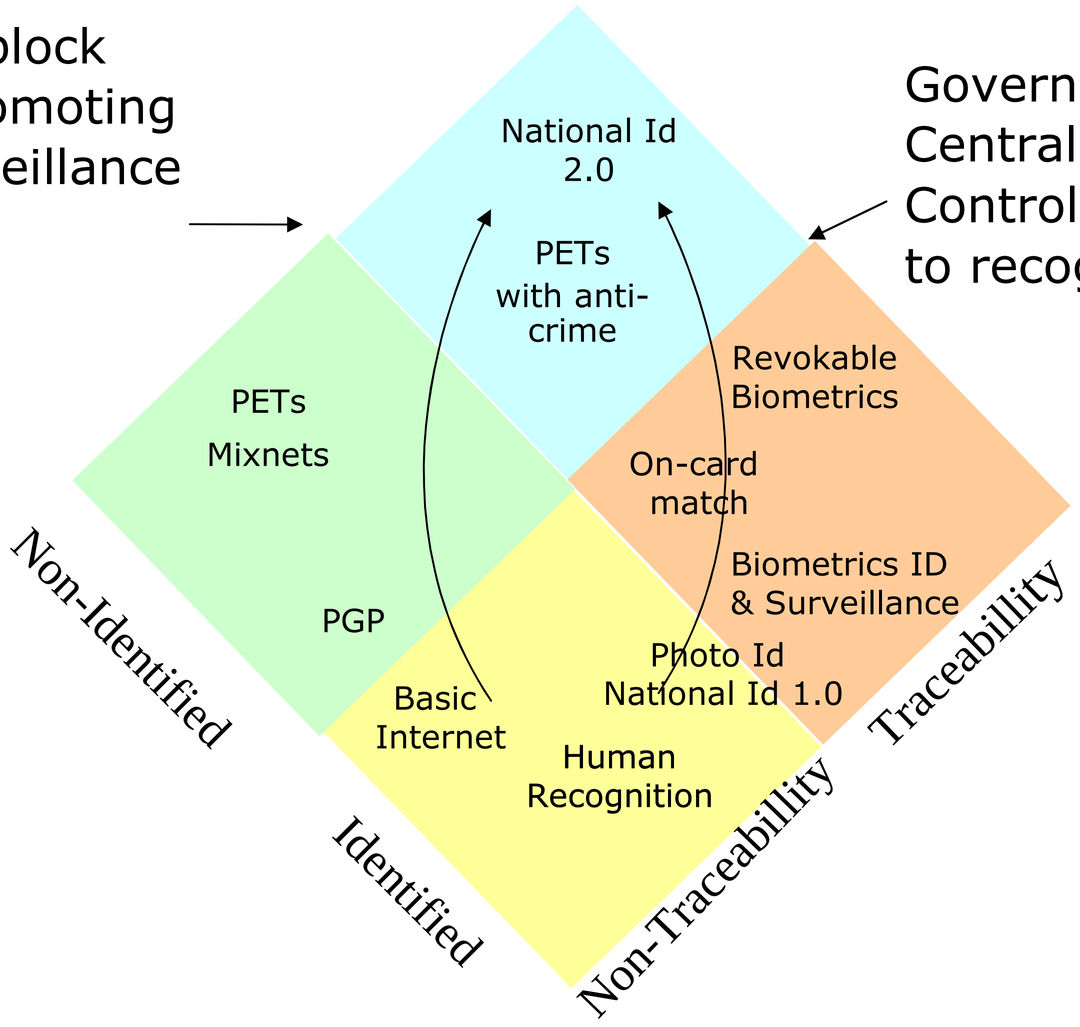
PRIWAY
Security in Context

Government block market by promoting & buying surveillance

Government block here Central Command & Control Paradigm fail to recognice needs

Security for Individual

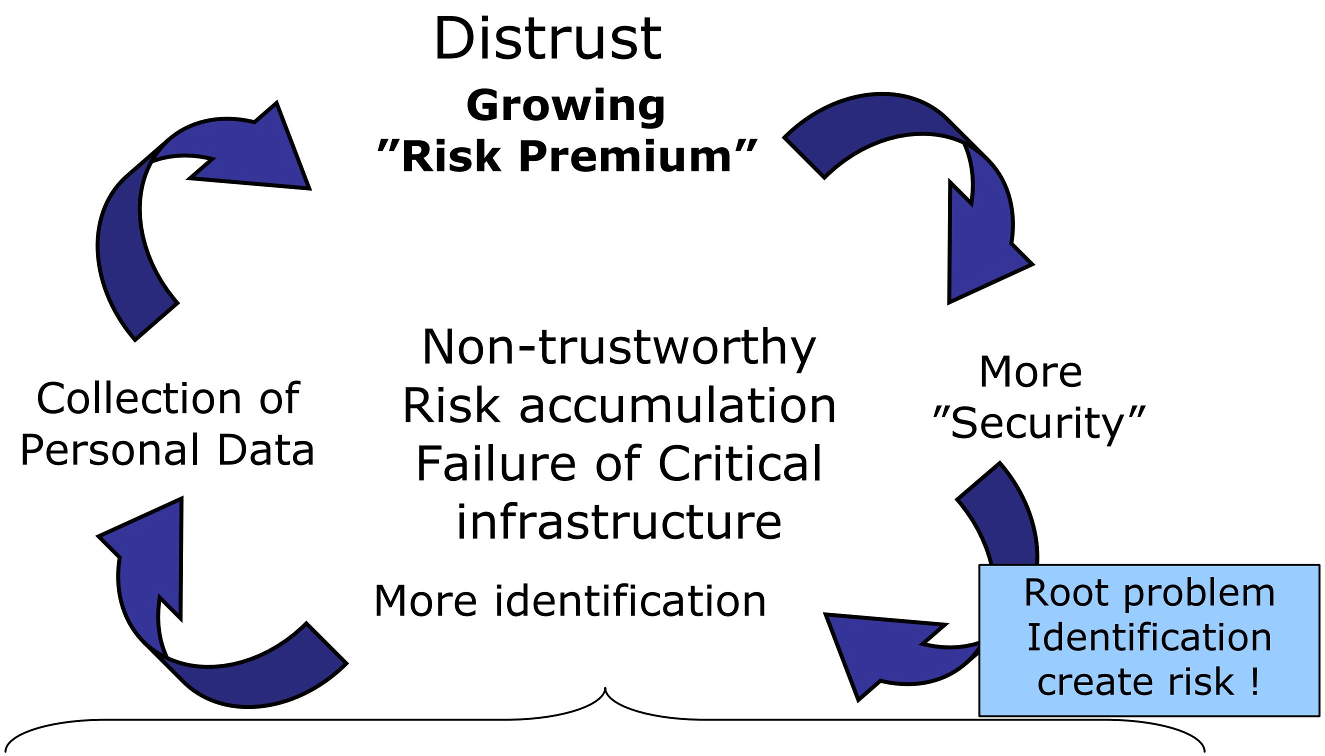
Security against Citizen



Danish Biometrics

© Priway, Nov, 2007

Problem # 1 - Security erode



Distrust

Growing ”Risk Premium”

More ”Security”

Non-trustworthy
Risk accumulation
Failure of Critical infrastructure

Collection of Personal Data

More identification

Root problem
Identification create risk !

More ”ab”use of personal data

More and larger Security Failures

More Crime
Identity Theft

Identification Credentials
E.g. biometrics spoofing.
More Identity Theft and
Reverse burden of proof

Business
Silos
Id as
Property

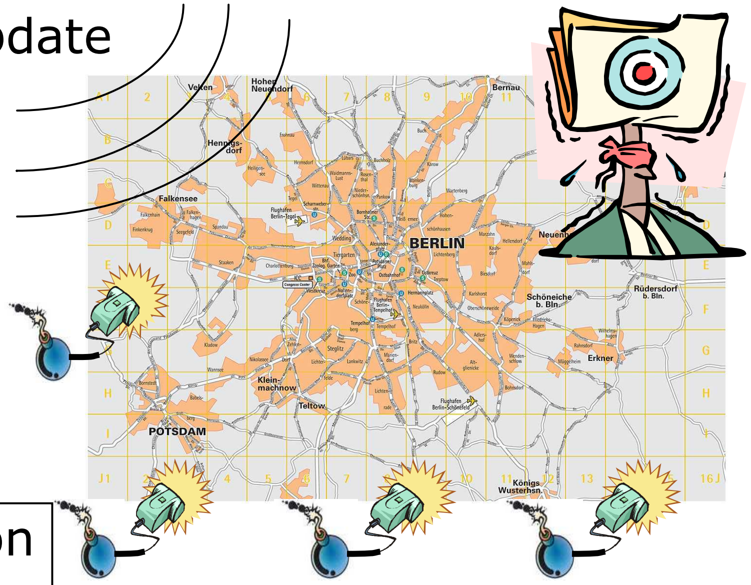
Pervasive surveillance
And abuse of surveillance
“Criminals can do everything government can do”

Problem #1.2 - Living at Gunpoint
CASE: Surveillance Smart Bombs

PRIWAY
Security in Context

Assume deployment of

- A series of small RFID-bombs
- Attached to passive RF-reader
- Located at fashionable locations
- Close to normal RFID-reader
- Triggers updated via FM-radio
- **Proximity-triggered by target**



Radio-update

NEW – Bioemtrics or Face Recognition version tapping into any camera & advertising sign.

Busines case – Bombs for hire

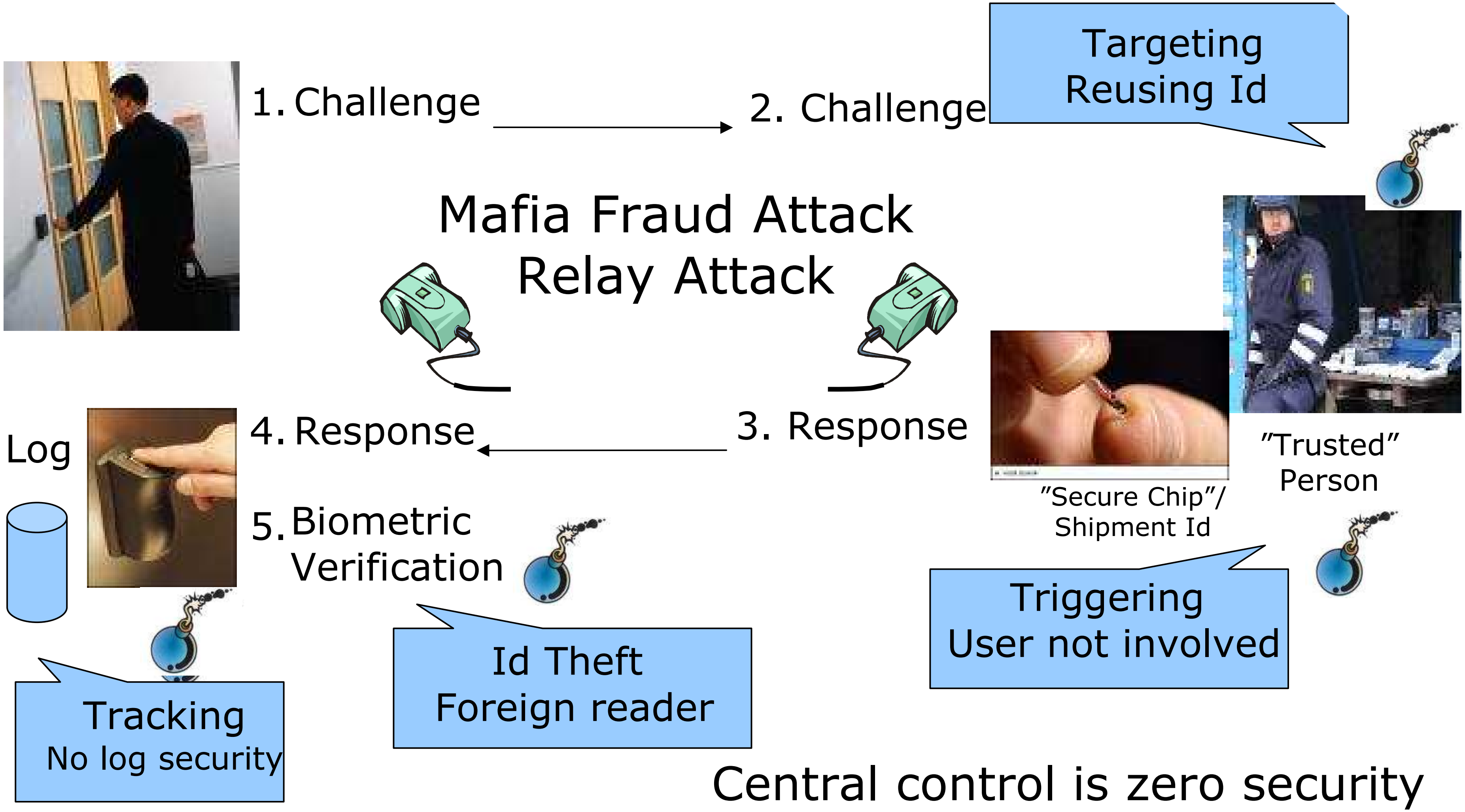
Highly scalable business model, bombs dispersed in major Cities near parliaments. We will get your man in 10 days.

Loading the Gun #2
Attacks emerging, more later

- US force Iraqis to enroll in a biometric Id system without Citizen Control. Risk is ethnic cleansing.
  - Is US guilty of aiding Genocide if this happens?
  - What is the security difference to EU plans?
- ICAO Passports have bad security, collection of biometrics and no fallback. Risk are attacks, identity spoofing, data security failures etc.
  - What do we do when the ICAO setup fails?
- Italien and Greek wiretapping scandals using inside abuse of surveillance weapons
- MS voice recognition spoofed by system speaker

No automated Identification !

PRIWAY
Security in Context



1. Challenge

2. Challenge

Targeting
Reusing Id

Mafia Fraud Attack
Relay Attack

Log

4. Response

3. Response

5. Biometric
Verification

"Secure Chip"/
Shipment Id

"Trusted"
Person

Triggering
User not involved

Id Theft
Foreign reader

Tracking
No log security

Central control is zero security

Biometric Surveillance
Assaults on society in progress

PRIWAY
Security in Context

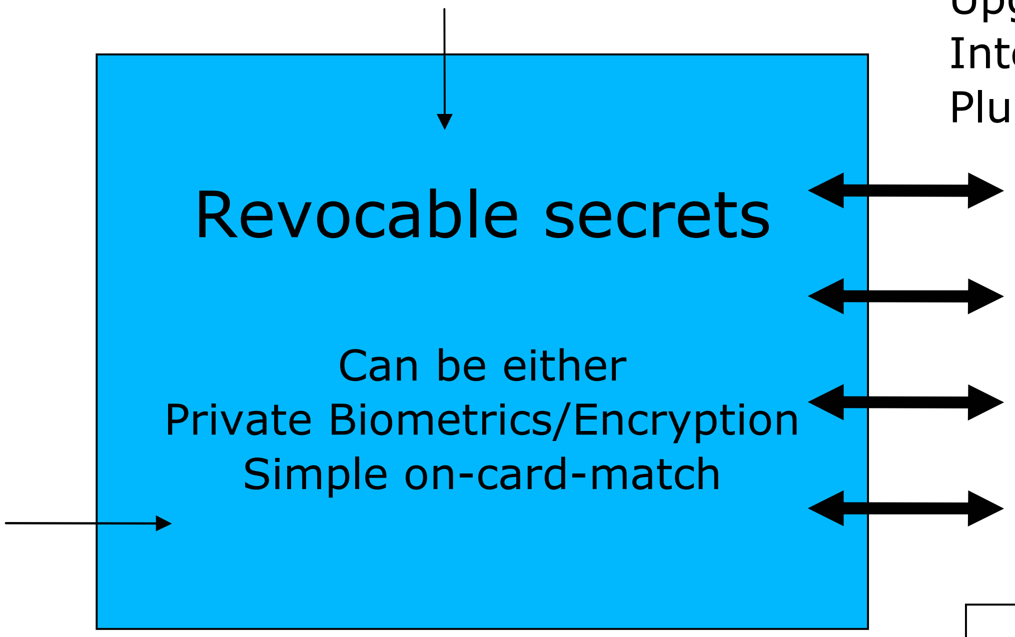
- The Security perspective – Overkill and legacy
  - Biometrics surveillance - overkill without balances or fallback
  - Question is NOT Security or anti-Crime – but how to get both.
- The Digital Economy Perspective – Digital Polution
  - Can be compared with the environment question – EITHER production OR Environment – lead to disaster
  - Today we know we need enzymes, catalysts and sustainability
- The rights perspective - a Camera is a gun
  - At gun-point, you have a right to disarm removing threats
  - If you see others in emergency, you are obligated to aid
- The Innovation Perspective – Who's preferences?
  - In the old days, suppliers listened to customers servicing customer needs
  - Unless careful, in the future suppliers will identify customers pushing supplier wants

Biometrics and interoperability

PRIWAY
Security in Context

SAME as old biometrics:
- Convenient
- Customisable/Inclusive
- Traceable
- Visible inspection

But ALSO:
- Security / Privacy
- Purpose Specific
- Upgradeable
- Interoperable
- Plurality



User Interface
incl. Pin/passwords

Revocable secrets

Can be either
Private Biometrics/Encryption
Simple on-card-match

Client-side
Biometrics
Collection
ONLY

Any
Protocol
Cryptographic
Identity Model

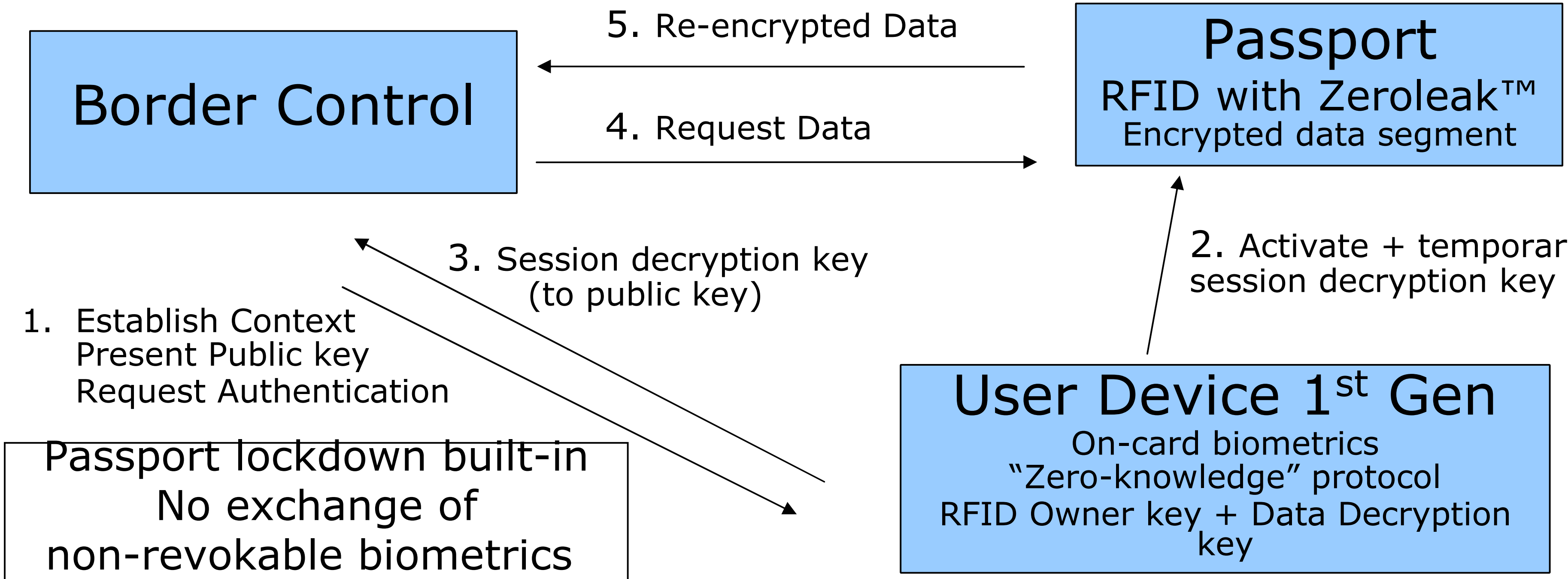
Tamper resistent User Device
Entire Card must be revocable

VISA 1:N Check
DO NOT REQUIRE
IDENTIFICATION

RFID only support person Id Control MUST be in USER device

PRIWAY
Security in Context

(User control of activation & passport revocation)



Border Control

Passport
RFID with Zeroleak™
Encrypted data segment

User Device 1st Gen
On-card biometrics
"Zero-knowledge" protocol
RFID Owner key + Data Decryption key

1. Establish Context
Present Public key
Request Authentication

2. Activate + temporary session decryption key

3. Session decryption key (to public key)

4. Request Data

5. Re-encrypted Data

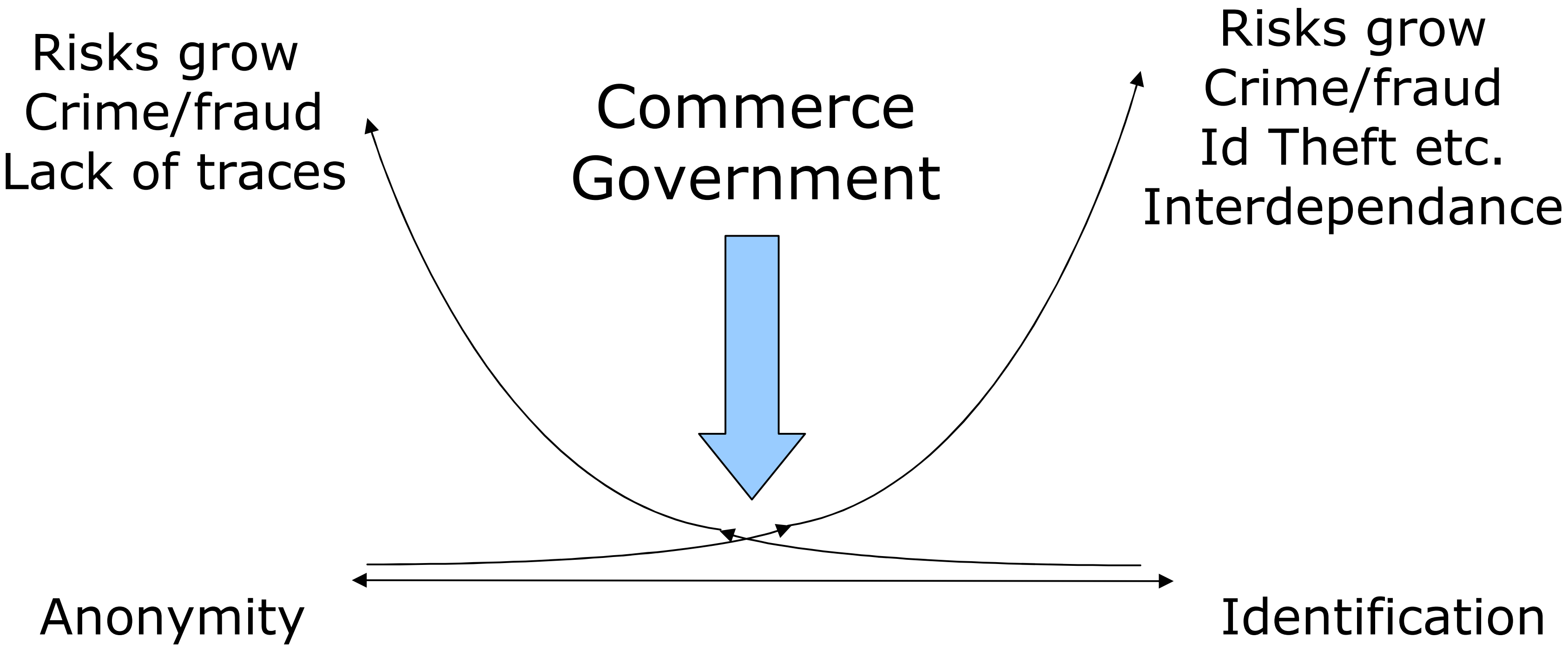
Passport lockdown built-in
No exchange of
non-revokable biometrics
needed – VISA can be
added as blinded certificate
No 1:N needed

Danish Biometrics

Empowerment & Fallback security
Key to National Id trustworthiness

PRIWAY
Security in Context

National ID 2.0



Risks grow
Crime/fraud
Lack of traces

Commerce
Government

Risks grow
Crime/fraud
Id Theft etc.
Interdependance

Anonymity

Identification

Problem # 2
PETs critical for innovation

PRIWAY
Security in Context

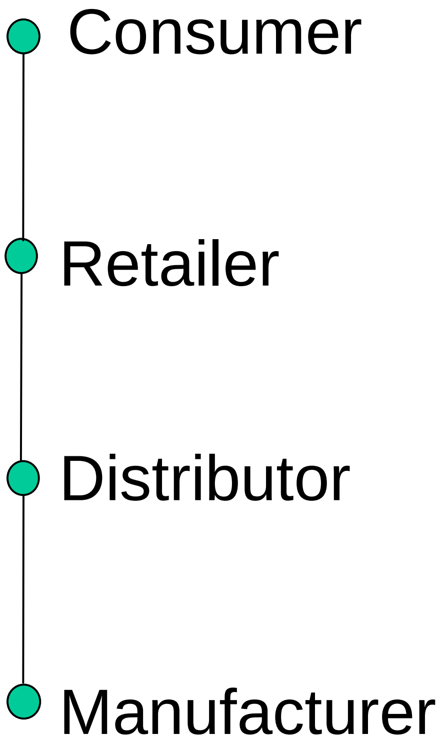
Surveillance societý versus **PET world**

Who ”own” customer?

Profile marketing
Cross-context data
Collection and use

Supply Push

9-9.9 out of 10
new products fail



Demand-driven innovation

Demand Pull

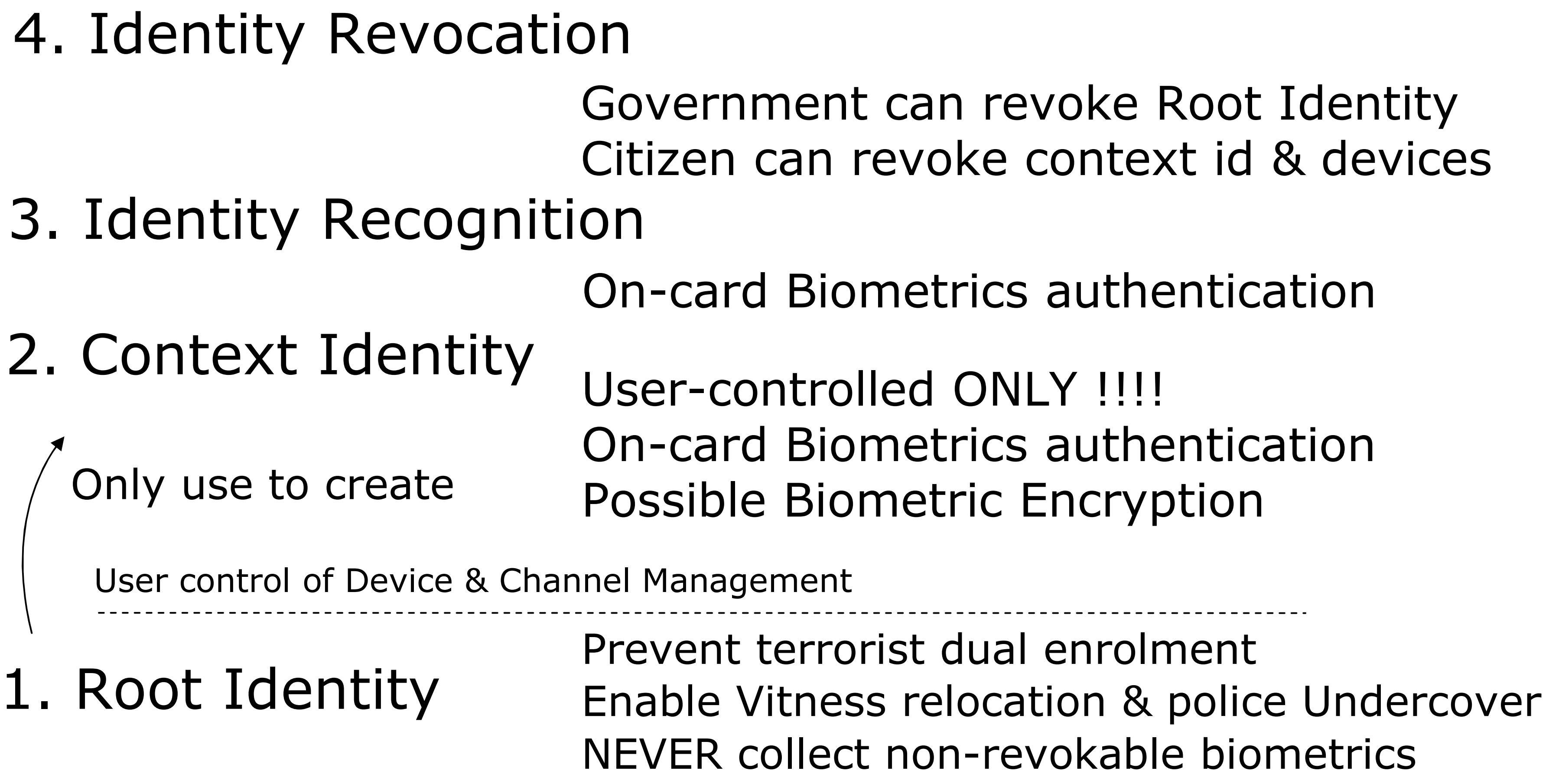
Servicing Needs

Purpose-specific sharing
Value network sourcing

Mass customisation

Customer force focus
on actual needs
& gradual improvements

User-controlled Biometrics



4. Identity Revocation

Government can revoke Root Identity
Citizen can revoke context id & devices

3. Identity Recognition

On-card Biometrics authentication

2. Context Identity

User-controlled ONLY !!!!
On-card Biometrics authentication
Possible Biometric Encryption

Only use to create

User control of Device & Channel Management

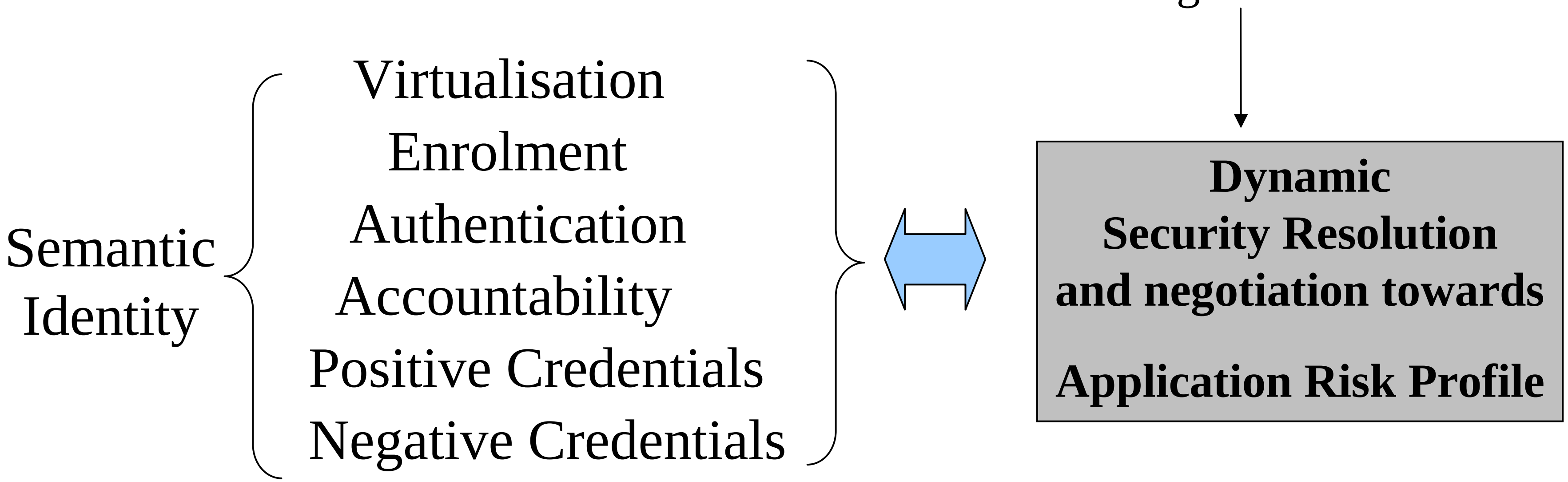
1. Root Identity

Prevent terrorist dual enrolment
Enable Vitness relocation & police Undercover
NEVER collect non-revokable biometrics

Semantic Resolution of Security Semantic Interoperability !!

Id negotiated and customised to context
Can be recognised / reused

Incl dynamic reponses to
external alerts
E.g terrorthreat



Semantic Identity

Virtualisation
Enrolment
Authentication
Accountability
Positive Credentials
Negative Credentials

**Dynamic
Security Resolution
and negotiation towards**

Application Risk Profile

No need for surveillance until specific
threat do not respond to requests using
Non-invasive means

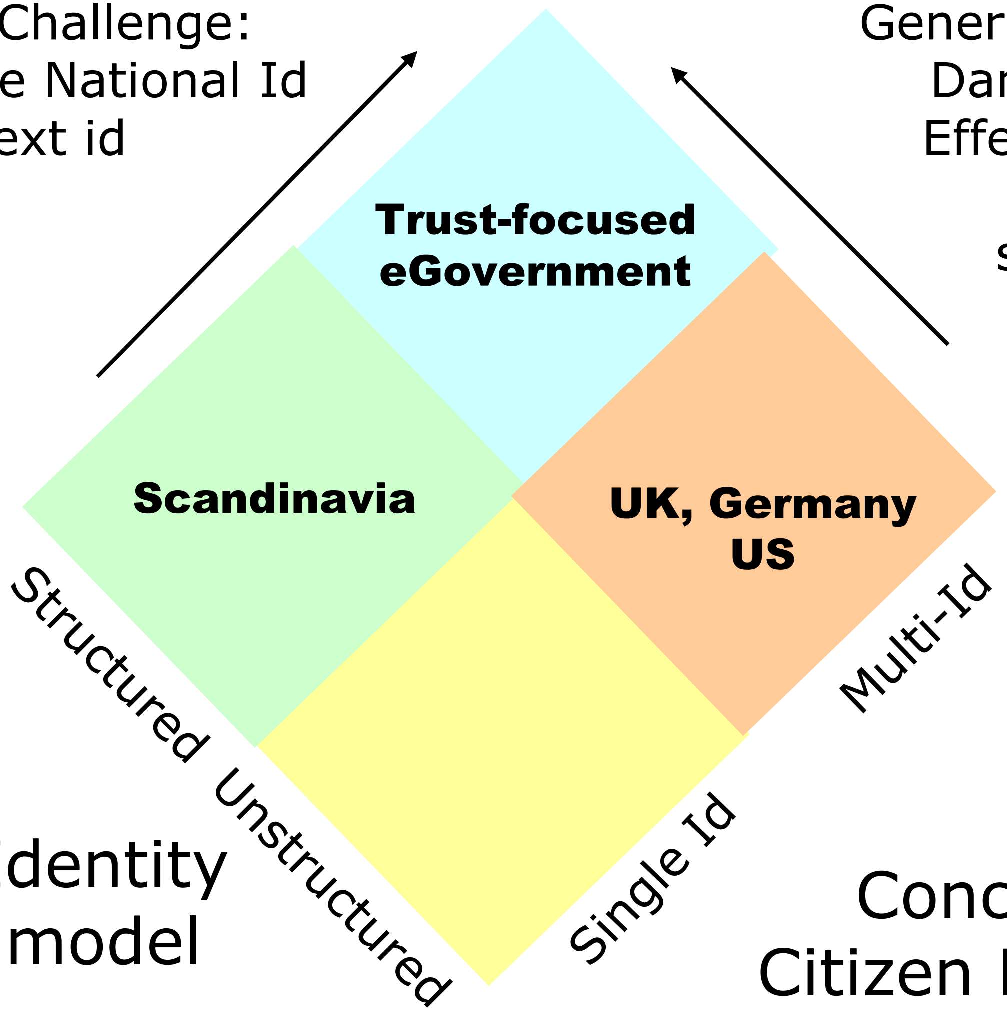
HYDRA

www.hydra.eu.com

eGovernment id model

Scandinavian Challenge:
Move from Single National Id
To Context id

General Challenge:
Damand Pull
Effectivisation
AND
security



Trust-focused eGovernment

Scandinavia

UK, Germany
US

Structured

Unstructured

Single Id

Multi-Id

Identity
model

Risk
Concentration
Citizen Demand Pull

Danish Biometrics

7 Rules of Biometrics Security

1. Ensure upgrade ability - Change is the only certain Aspect
2. Ensure Fallback – Never collect non-revocable biometrics
3. Purpose Specification – Mix with purpose specific secrets
4. Proportionality – Exhaust non-invasive security tools first
5. Minimize Interdependence - User Control and revocable id
6. Semantic Interoperability – Don’t standardise at technology
7. Design assuming failure – Critical infrastructure fault tolerance

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

Summation

PRIWAY
Security in Context

- **Biometrics can be a disaster OR better security for all**
  - The strength of biometrics is also its source of certain failure
  - Ensure revocability at all levels - critical for biometrics to work
  - Purpose-specific Id, Open Semantic resolution & interoperability
- **We need BOTH stronger traceability AND empowerment**
  - PETs MUST be supported already in ID Cards – Citizen Id
  - User devices facilitating Trust in Id & key management
  - Can be made to support multiple models in parallel
- **Strong and urgent need for re-adjusting policies**
  - Justice: Stop distorting security markets and blocking innovation
  - Technology: Include interoperability, empowerment and fallback
  - Tear DOWN those Digital Walls – ICAO Passports & VISA fail

Mr. Frattini – Europe cannot afford these mistakes !!

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