

From Central Command & Control to Citizen Empowerment & Dependability

Stephan J. Engberg
Priway

PRiWAY
Security in Context
www.priway.com



<http://www.hydra.eu.com>

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

Agenda

1. Burning Platform - security paradigm sustainability
 - Crime & abuse is escalating - BECAUSE of the security paradigm
2. Disarming the conflict - how deep is the rabbit hole?
 - Sustainable principles for Identity & Security - top-down principles
3. Designing for Trustworthiness & Innovation
 - Distributed Empowerment - Passports and Emergency cases

Root Issue

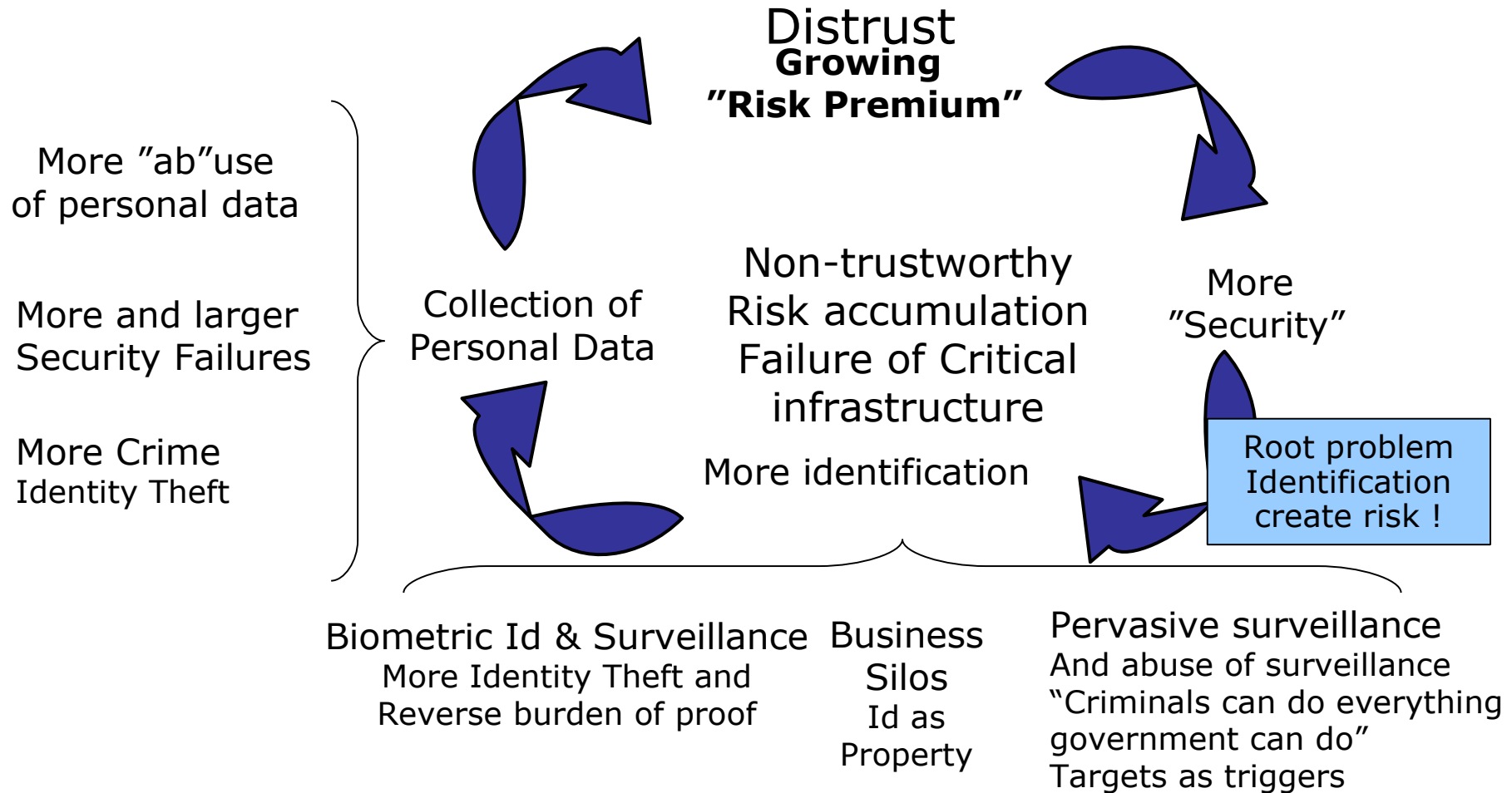
- The root conflict
 - Protecting the citizen from others
 - Protecting others from the citizen

- When does this balance tip ?
 - When it tips – can we be certain to get access?
 - If so, how can we be certain it not abused?

- New protections emerging
 - All-edge wireless routing, strong encryption on top of weak encryption, steganography hidden channels, identity lending/renting

- Fact about back doors – we cannot secure NOR assure them

The Security Death Spiral

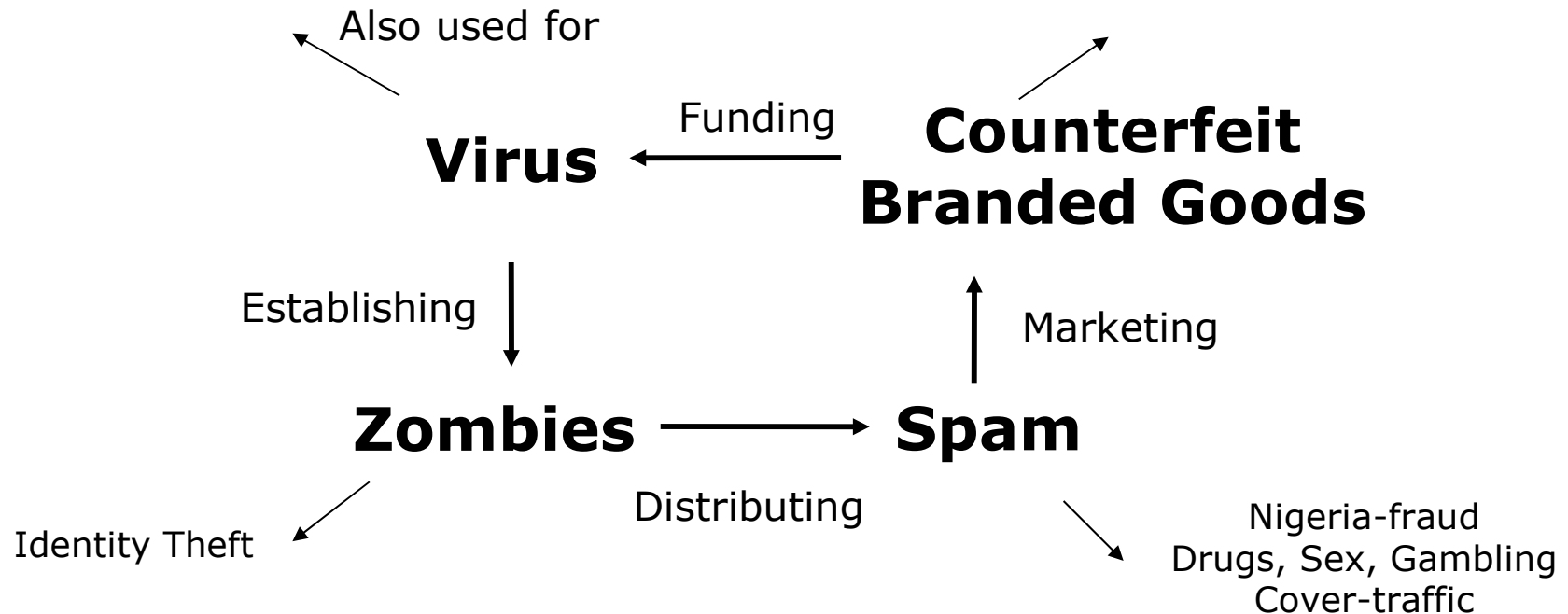


Criminals as professionals

One causal view !

Hacking, Blackmail
Denial-of-Service
Industrial Espionage

7-10% of World Trade
Eroding brands
Funding what ?

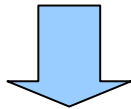
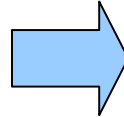


BOTNETs – Separation of Motives and Capabilities !

Biometrics – wake up

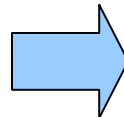
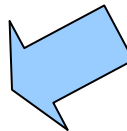
Biometrics used for Identification without user control

- Only approximate
- Publishing “passwords”
- By definition spoofable
- Cannot be revoked



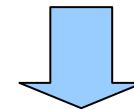
Destroy Data Security

- Linkable across context
- Does NOT ensure consent
- Can only have one id/key



Create crime / Identity Theft

- Reverse of Burden of proof
- More only worsen the problem
- Lack plausible deniability



Deterministic failure

- Create uncontrollable risk
- Make Empowerment impossible
- Make Dependability impossible
- Likely fail 100% -> Feudalism

The ONLY secure Biometrics – is user-controlled!

Reserve for Root ID, Id Device mgt, threat escalation, post-crime forensics

No automated Identification !



1. Challenge → 2. Challenge

Targeting
Reusing Id

Mafia Fraud Attack
Relay Attack



Log

4. Response ← 3. Response

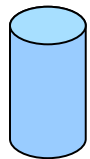


"Trusted"

"Secure Chip"/
Shipment Id

Pe

5. Biometric Verification



Tracking
No log security

Id Theft
Foreign reader

Triggering
User not involved

Central control is zero security

Surveillance kills !

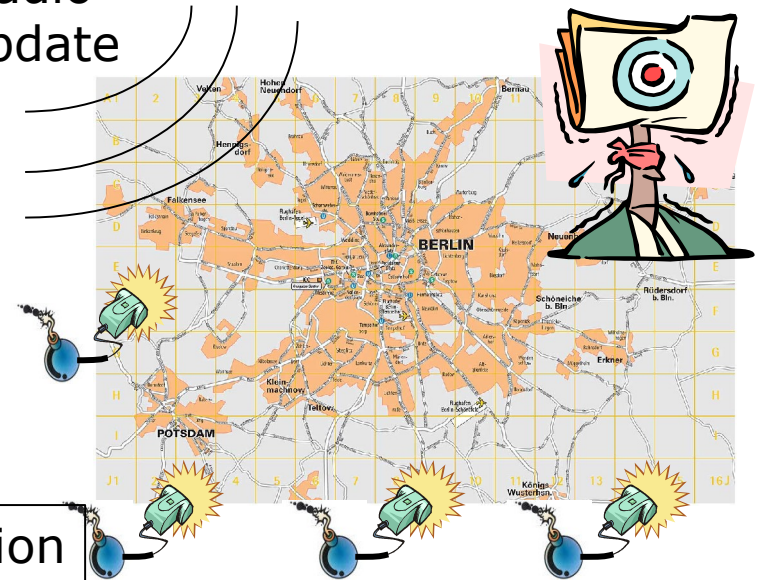
CASE – Ambient Smart Bombs

Assume deployment of

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

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

Radio-update

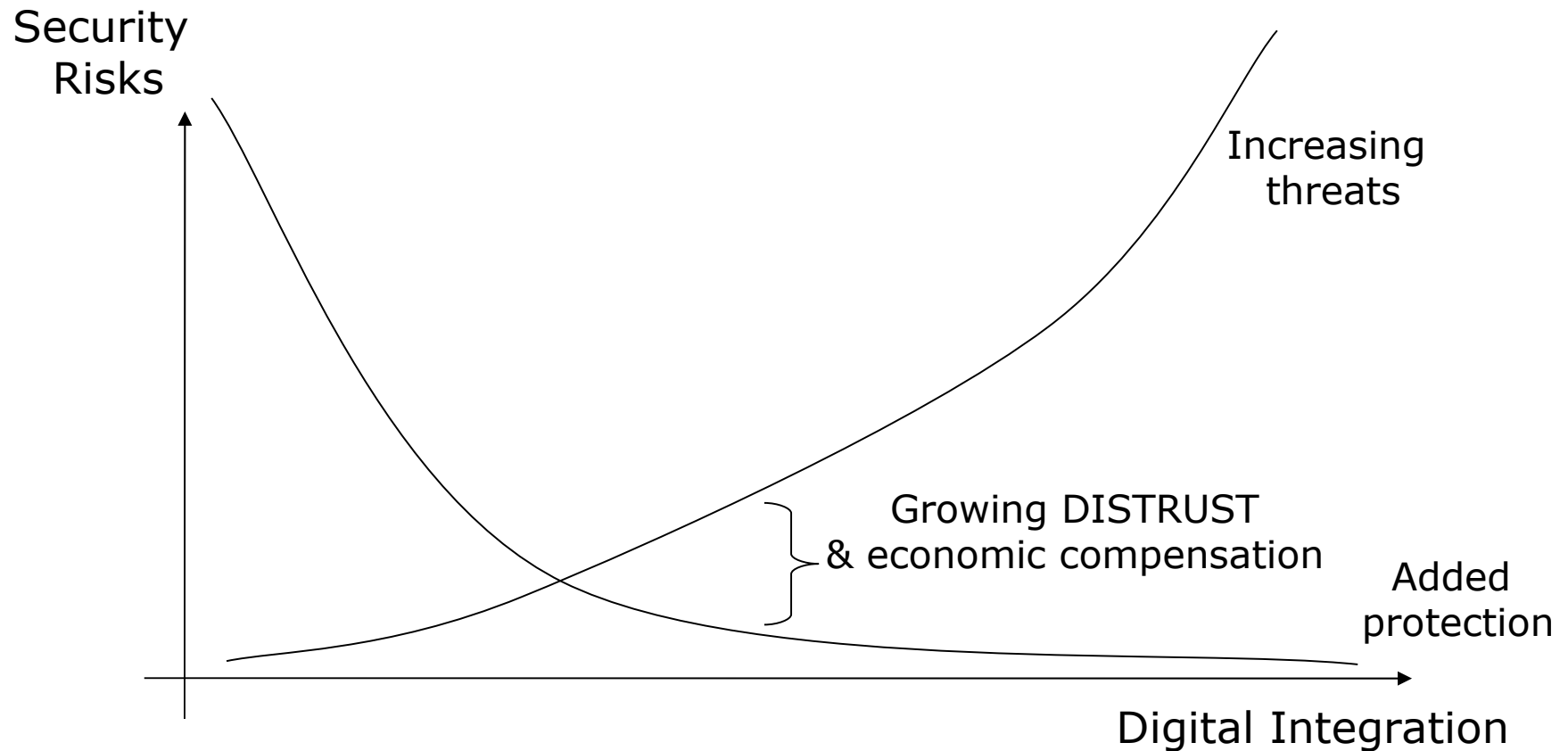


Business case – Bombs for hire

Highly scalable business model, bombs dispersed in major Cities near near parlements. Will get your man in 10 days.

OBS: Frenchaise available – free guidelines – winner will get 50% !!!

The Security Gap of Central Command & Control



Empowerment & Fallback security Key to National Id trustworthiness

National ID 2.0 Building identities on Identification Contextual Id's

Crime/fraud
Lack of trace

Crime/fraud
Id Theft etc.

Commerce
Government

Focus on Value-creating
Services & activities.
Enforce customer control
for demand-driven markets

Semantic Security
Channel Control

Mutual revokability

Anonymity

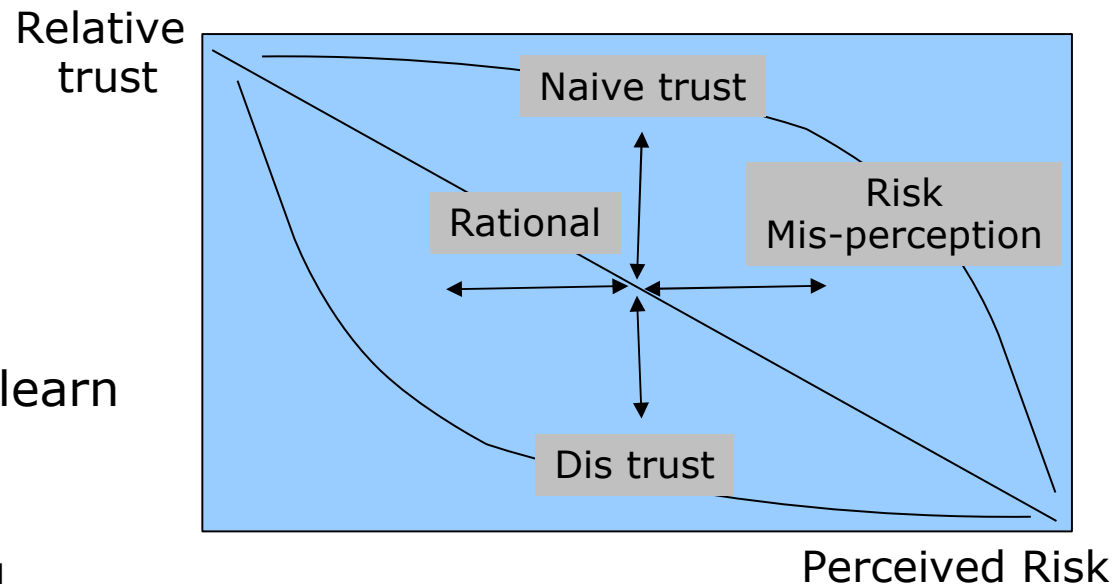
Identification

Trust Socio/Economics

Trust = Amount of (perceived) Risk willingly accepted in a context

Direct linkage between risk model and behaviour

- Citizens want:
 - Convenience / usability
 - Value for money
 - Control (no risk)
- Citizens evaluate, trade & learn
 - Reality catches up
 - More risk = less business
 - Context Id = Demand-pull



Empowerment -> Security, Growth & Demand-driven innovation

Conclusion: DESIGN for Empowerment !

From Identification to Context Specific Adaptable Identity

Use of biometrics

Forensics

Citizen pre-stored

No - Specific Keys

Biometrics "negotiation"

User-controlled

On-card Biometrics

Semantic Security

4. Identity Revocation

3. Identity Recognition

Device & Channel Management

2. Context Identity

Method of Virtualisation
Method of Identification
Method of Authentication
Method of Accountability
Positive Credentials
Negative Credentials

Transaction Id

Dynamic Security Resolution and negotiation towards Application Risk Profile

User control of Device & Channel Management

Non-linkability

NO "TRUSTED" Part

Accountability

Biometric Enrollment

NO storage of certified biometrics outside user control

1. Root Identity

National Id
TransNational Id

Dynamic Security Escalation

Least invasive means by default

Biometric Id & Surveillance

(last resort)

National Id

(Singular Id)

Trusted Id

(Trusted party)

Trustworthy Id

(Transaction Accountable)

Credential Id

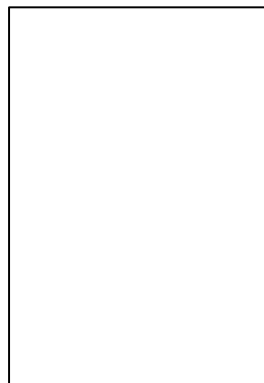
(specific credential proofs)

Local Id

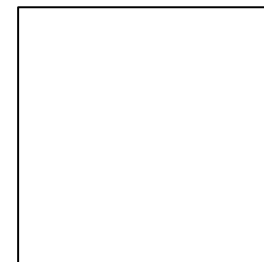
(anonymous handle)



Normal



Heightened

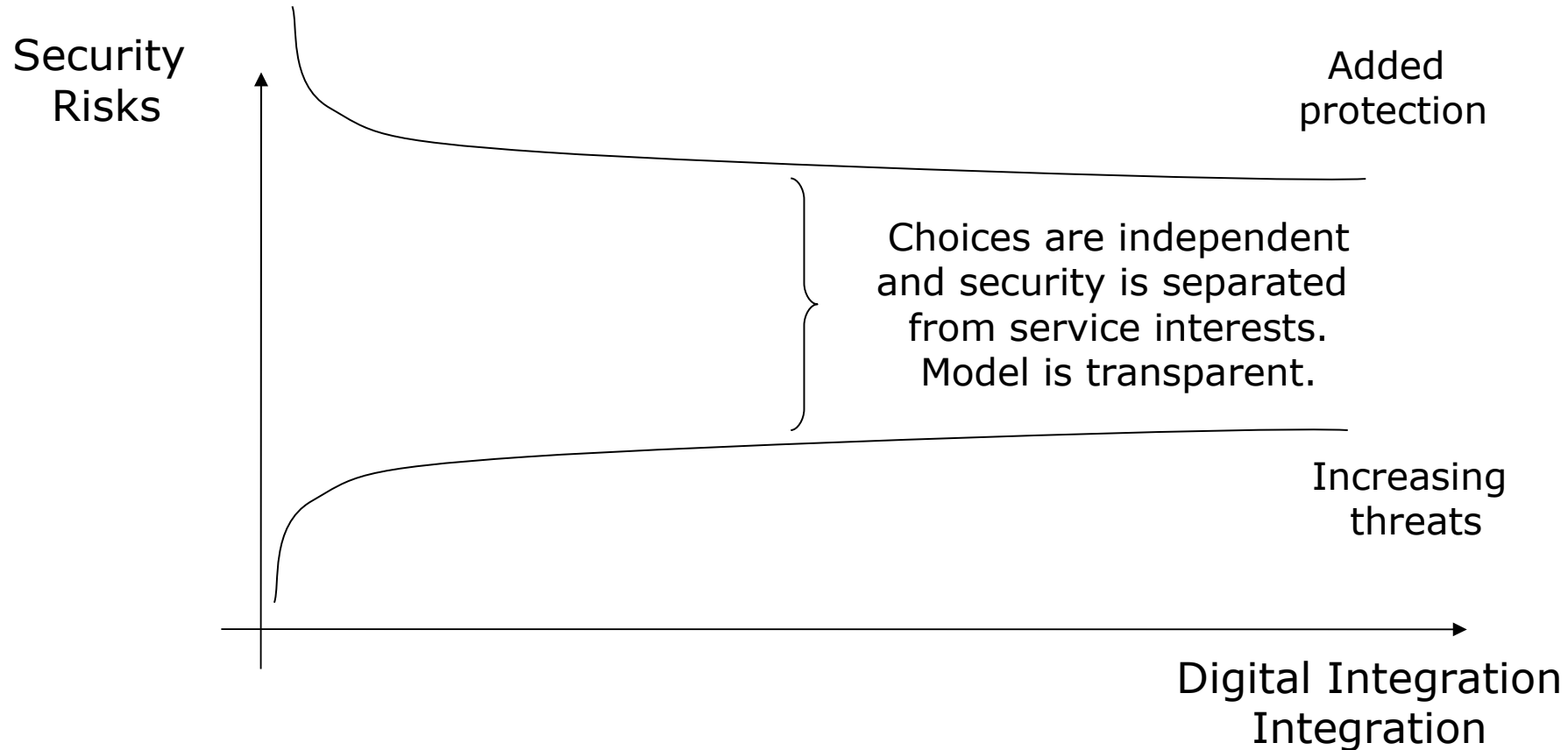


Critical

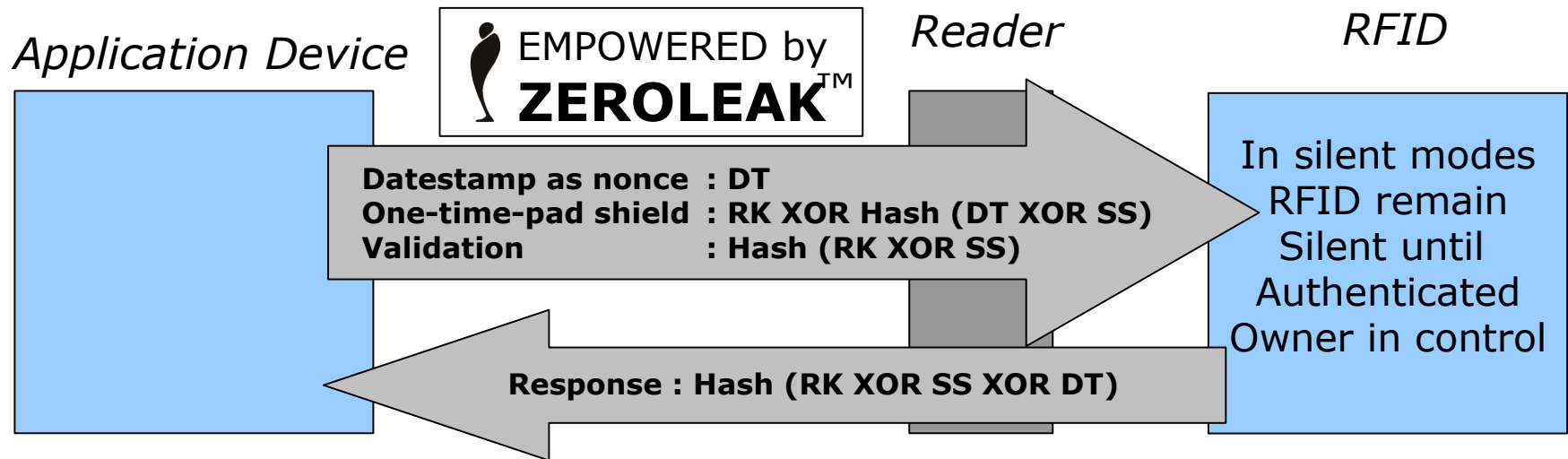
Negative credentials
(each present NOT on a fugitive-list)

Threat Status

The Security Gap eliminated with Citizen Empowerment



Design for CITIZEN EMPOWERMENT EU COM 2007(96) on RFID



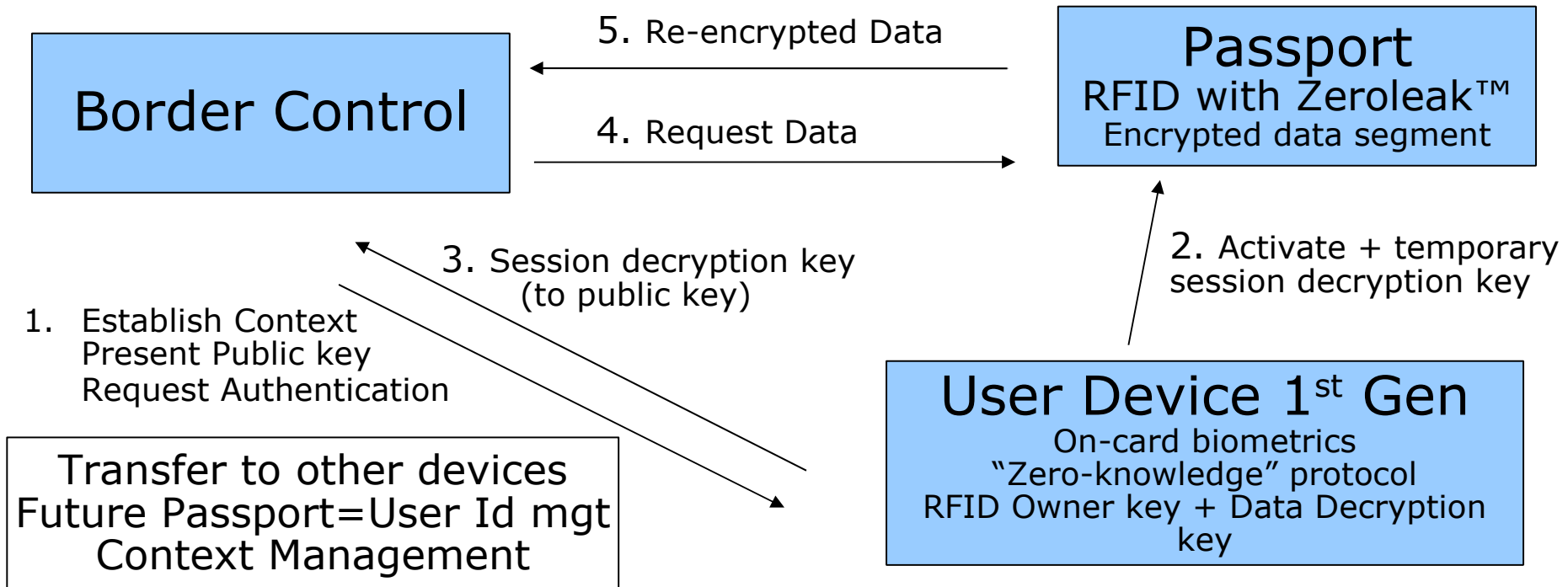
- Ability to create a new key and **TRANSFER CONTROL to Owner**
- Change to stealth Mode where **RFID remain silent until authenticated**
- **Owner communicate with RFID without leaking identifiers**
- Integrity & confidentiality – dangerous goods, data on chip (transport)
- RFID still hold keys to validate product authenticity & safety
- In supply chain – smart barcode. In use – part of critical infrastructure

In mass production




Securing RFID in Passports

(User control of activation & passport revocation)



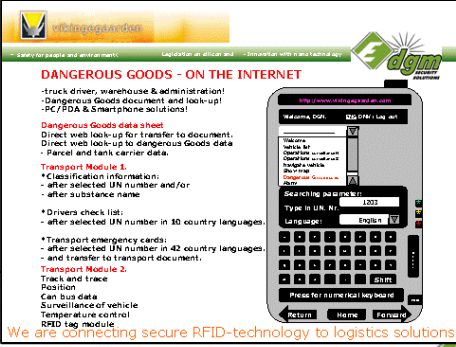
Dangerous Goods

• Case: DGM-SS for Dangerous Goods Management



SECURE RFID-tag TECHNOLOGY

We are connecting secure RFID-technology to logistics solutions



DANGEROUS GOODS - ON THE INTERNET

- Truck driver, warehouse & administration!
- Dangerous Goods document and look-up!
- PC, PDA & Smartphone solutions!

Dangerous Goods data sheet
Direct web look-up for transfer to document.
- Parcel and tank carrier data.

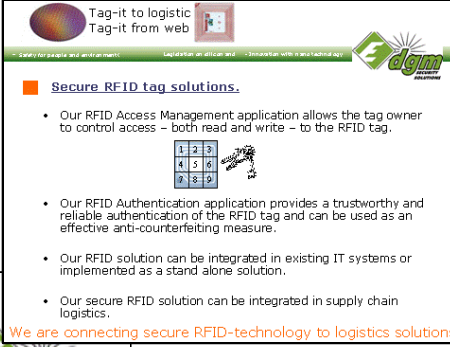
Transport Module 1.
* Classification information.
- after selected UN number and/or
- after substance name

* Drivers check list:
- after selected UN number in 30 country languages.

* Transport emergency cards:
- after selected UN number in 42 country languages
- and transfer to transport document.

Transport Module 2.
Track and trace
Position
Can bus data
Surveillance of vehicle
Temperature control
RFID tag module

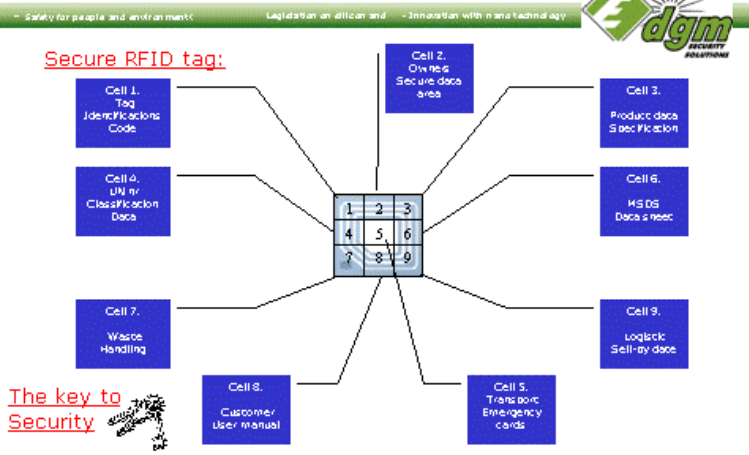
We are connecting secure RFID-technology to logistics solutions



Secure RFID tag solutions.

- Our RFID Access Management application allows the tag owner to control access – both read and write – to the RFID tag.
- Our RFID Authentication application provides a trustworthy and reliable authentication of the RFID tag and can be used as an effective anti-counterfeiting measure.
- Our RFID solution can be integrated in existing IT systems or implemented as a stand alone solution.
- Our secure RFID solution can be integrated in supply chain logistics.

We are connecting secure RFID-technology to logistics solutions

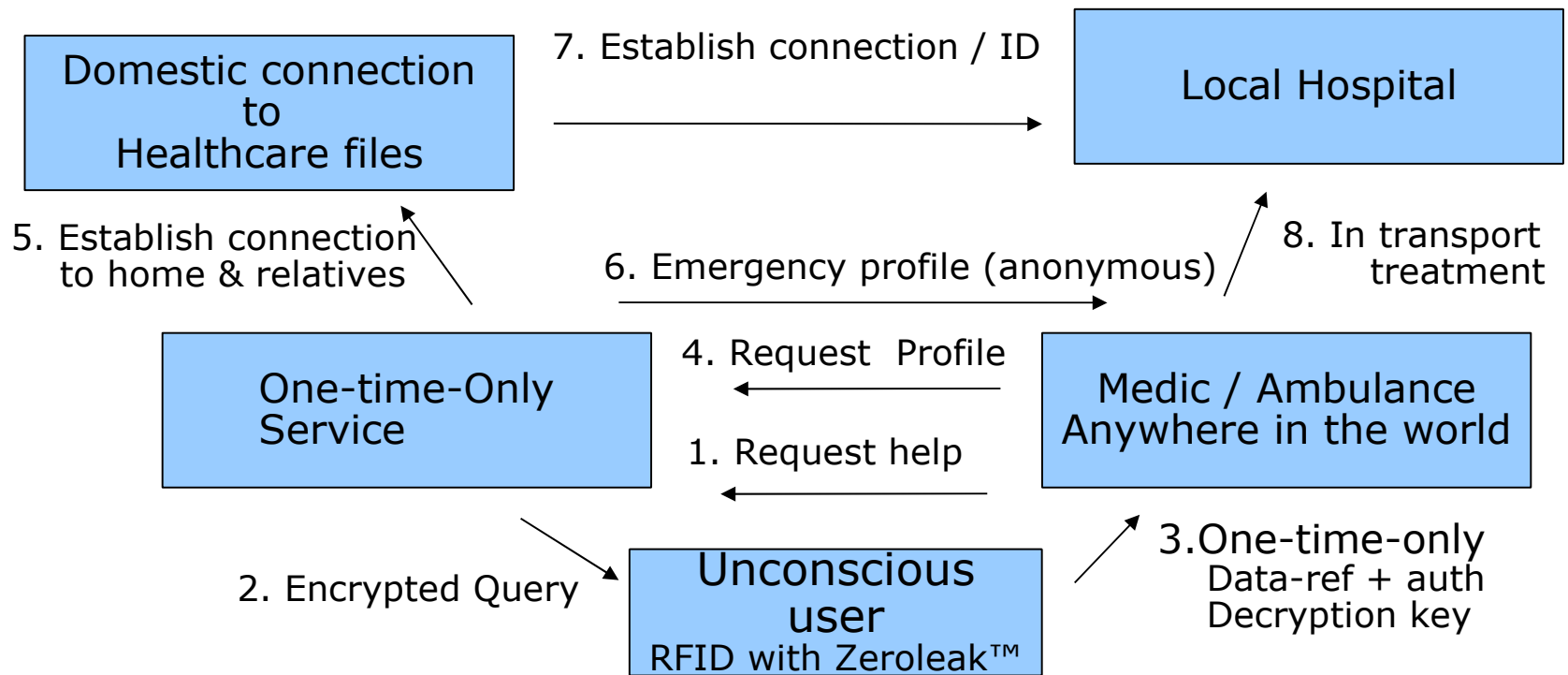


The key to Security

We are connecting secure RFID-technology to logistics solutions

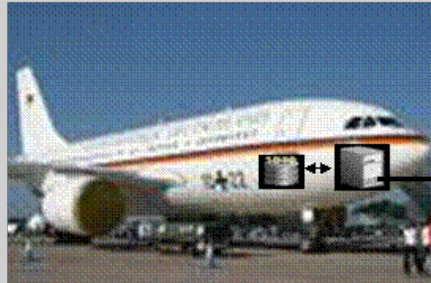
Healthcare Emergency / disaster

Stepwise RFID-based one-time-only Identification



Balance by Design

- Different data areas on the RFID can have its own Access Key(s) with associated Read and/or Write Access rights



Access Key	Data
w3e4r5t	EPC
xyz9876	Current Record
6y7u8i9	Birth Record
1 234567	Scratch Pad
	Service Record 1
	Service Record 2

	Service Record n

- Secure read/write data provided
- No unauthorised access to RFIDs
- Part originality can be checked

- The Service Mechanic can;
 - Read and Write the Scratch Pad and the Service Records
 - Read the Current Record and the Birth Record
 - If specifically authorised to this, then update the Current Record

Dynamic Security Context/ Semantic Security Resolution

User Identity Devices – Control Context

Ability to establish new, manage and negotiate trustworthy Identity
Ability to manage channels (receiver-controlled, id & purpose specific)
Shut-down capabilities critical to security

Slave Devices – Adapt to user control

Protocols that do not leak identifiers – identity is deliberate
Under user control – complex rules/negotiation/usability problem

Balance Requirements through multi-key

- End-user control
- Provider liability / SLA
- Fraud prevention
- Value creation

Security Context Resolution

Negotiate Id root, authentication level, credentials, accountability
Threat alerts dynamically raise requirements AND invasiveness

Security resolution based on
WHAT you are rather than
WHO you are

Application Security Management

Define security requirements and thresholds
Resolve interoperability rather than identify users and devices

From Protection to Security by Design

- Central control as Security Paradigm is unsustainable
 - We create the vulnerabilities that lead to abuse
- The Critical Trust Ecosystem is getting polluted
 - Focus on value-creating activities – Government & Trade
- The devil is in the design of technologies
 - Starting with the way we design National Id !
 - New technologies – blinded certificates, On-card, semantics
 - FOCUS: End-user Control of Devices, Channels & Context Id
- Move to Empowerment & Distributed Dependability
 - Security by mutual Revocability. Innovation by Demand-pull
 - Security & Freedom - two sides of the same coin