

Balancing Security and Privacy
Sustainable Security in a Digital World
From Identification to Identities

Stephan J. Engberg
Priway

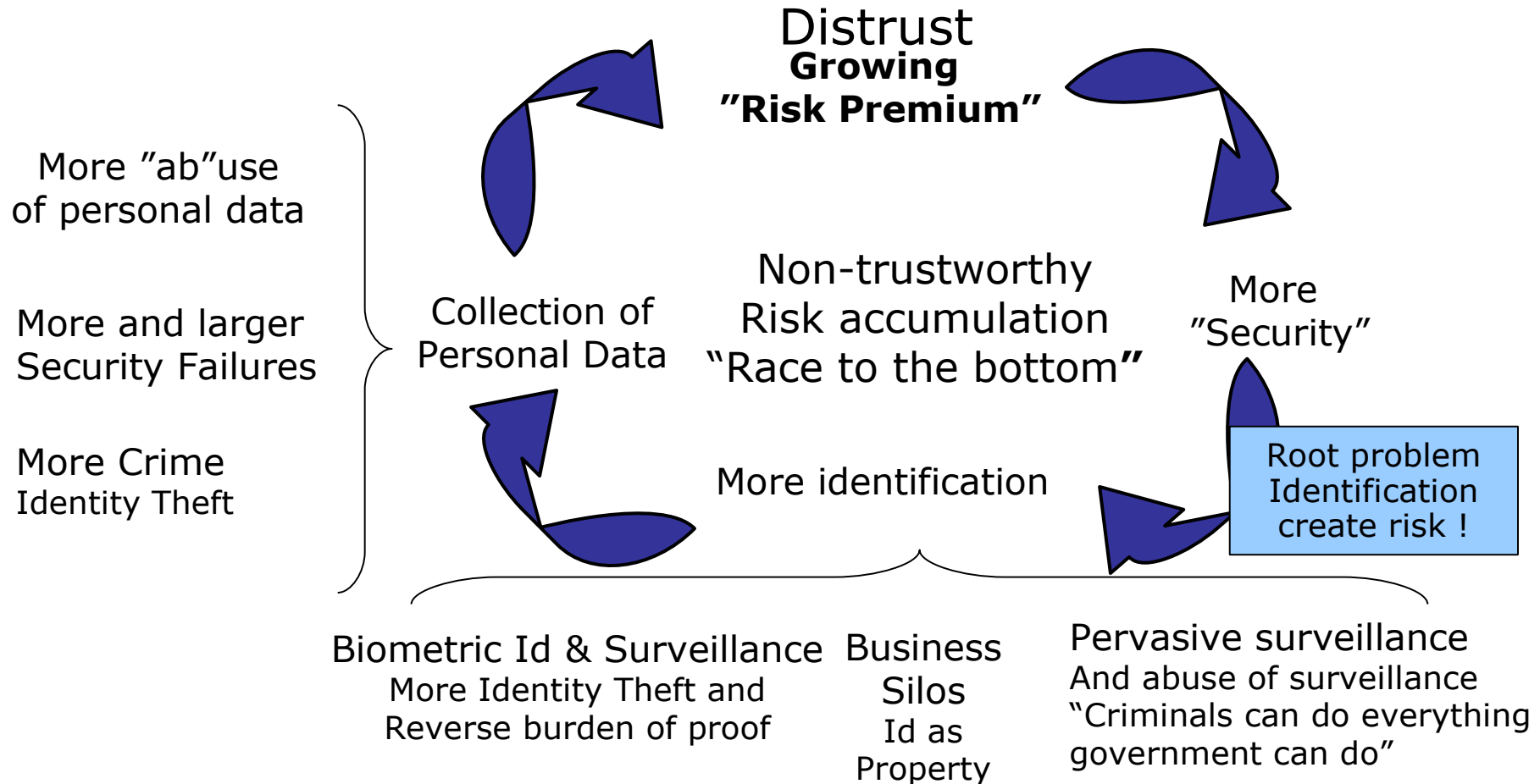
PRiWAY
Security in Context
<http://www.priway.com>

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

Agenda

1. Questioning security paradigm sustainability
 - Designing for problems – ICAO & Digital Identification
2. Disarming the conflict – how deep is the rabbit hole?
 - Sustainable principles for Identity & Security – a top-down approach
3. Designing for Trustworthiness & Dependability
 - Hardcore RFID problems – Passports and Emergency & Disaster

The Security Death Spiral



No automated Identification !



1. Challenge → 2. Challenge

Targeting Reusing Id

Mafia Fraud Attack
Relay Attack



PKI



Log

4. Response ← 3. Response



"Secure Chip"/
Shipment Id

"Trusted"
Person

5. Biometric Verification



Id Theft
Foreign reader

Triggering
User not involved

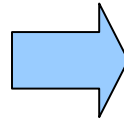
Tracking
No log security

Central control is zero security

Biometrics – wake up

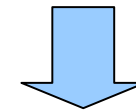
Biometrics used for Identification without user control

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



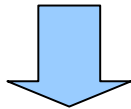
Create crime / Identity Theft

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



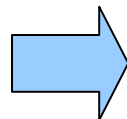
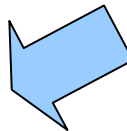
Deterministic failure

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



Destroy Data Security

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



The ONLY secure Biometrics – is user-controlled!

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

Need to revisit thinking

- ICAO / Electronic Travel Documents
 - Based on and pushing an **unsustainable identity model**
 - Using **biometrics** in a security destructive way
 - Using **RFID-technology** with insufficient security
- The wider problem – **distrust & crime is growing**
 - Integration and ambient escalate security problems
 - Biometric surveillance is a fundamental threat out of control
 - Corporate, political, commercial, social
 - Power concentration & Single Point of Trust Failure
 - Existing eGovernment have no sustainable trust model

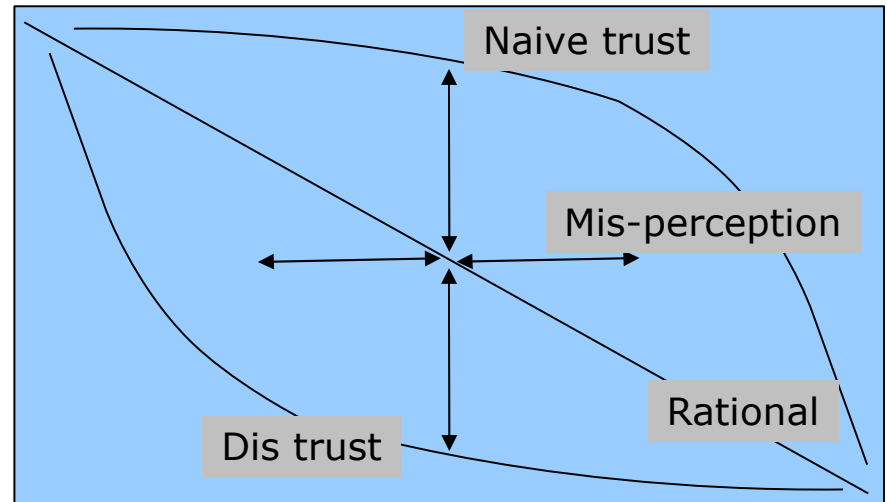
**Digital Identification is the problem
Not the solution !**

Trust Socio/Economics

Trust = Amount of Risk willingly accepted in a context

- Technical - accepted dependence
- Users want:
 - Convenience
 - Value for money
 - Control (no risk)
- Underlying risk is growing
 - Ubiquitous & On-line integration
 - Targeted attack is profitable
 - Stakeholder learning

Relative trust



Perceived Risk

Direct linkage between risk model and behaviour

From Identification to Context Specific Adaptable Identity

Use of biometrics

Forensics
Citizen pre-stored

No - Specific Keys

Biometrics "negotiation"

User-controlled
On-card Biometrics

4. Identity Revocation

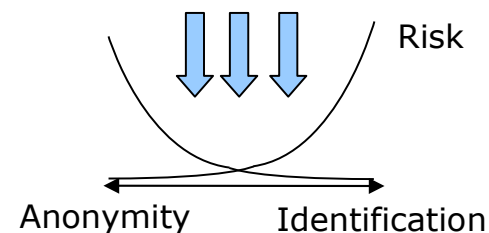
3. Identity Recognition Device & Channel Management

2. Context Identity

Semantic Security

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

Device & Channel Management



Transaction Id

Dynamic Security Resolution and negotiation towards Application Risk Profile

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 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

Security Context Resolution

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

Application Security Management

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

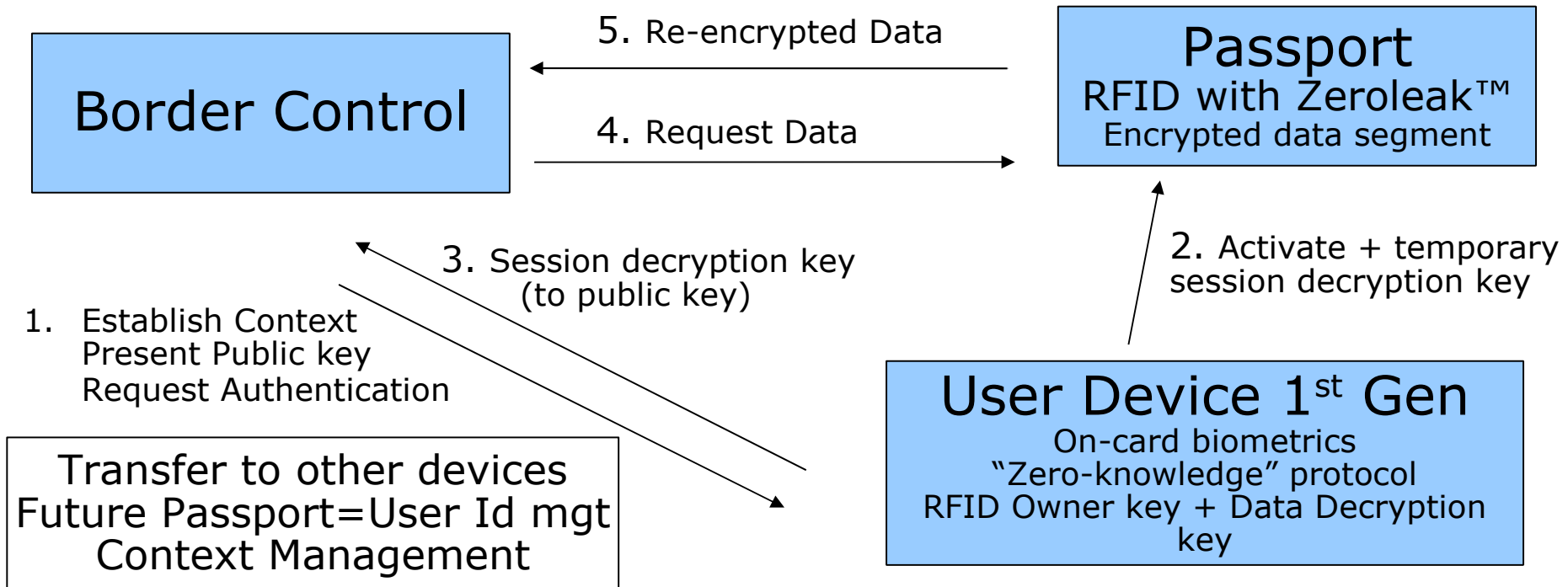
Balance Requirements through multi-key

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

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

Securing RFID in Passports

(User control of activation & passport revocation)



From Protection to Security by Design

- Identification as Security Paradigm is unsustainable
- The Trust Ecosystem is getting polluted
 - Focus on value-creating activities – Government & Trade
- Move to Distributed Dependability & Empowerment
 - Ensure End-user Control of Adapting Devices & Biometrics
 - Make Security Resolution Dynamic, Negotiable & Explicit
 - Balances is in Effective Revokability & Accountability
- Specifically for passports – ICAO heading for trouble
 - Short-term OPTION
 - Ensure Passport Owner can control the Passport RFID
 - Move Biometrics to On-Card & Optionally negotiate release
 - Need to move to Dynamic Identity – even for passports