

TACD – RFID & Pervasive Computing

From (un)Security by Central Command & Control
to
Security by Citizen Empowerment & Dependability
& Privacy Enhancing Technologies in RFID

Stephan J. Engberg
Priway

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

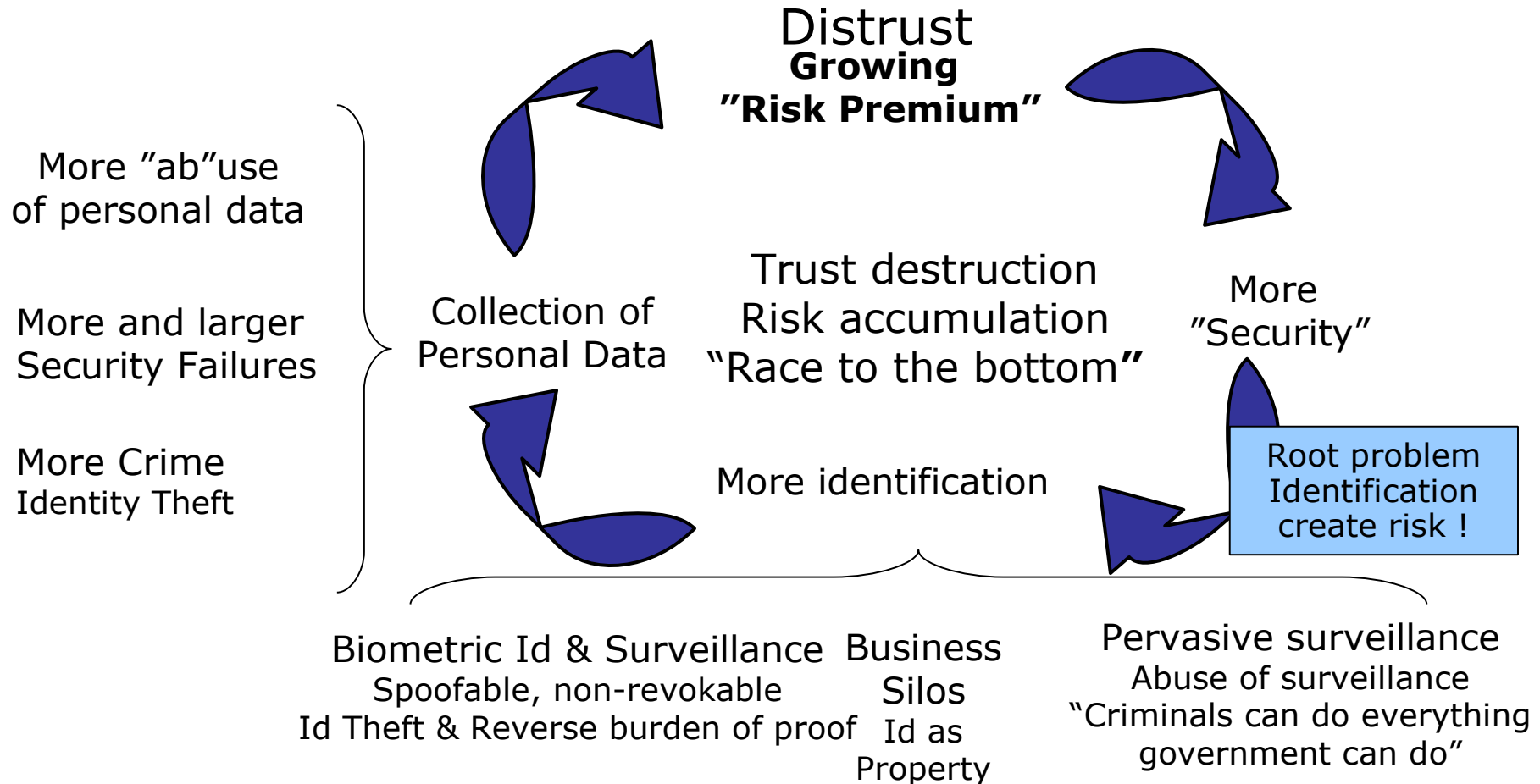
HYDRA 
<http://www.hydra.eu.com>

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

Summary From loose-loose to win-win

- **Consent: An act of trust, not given by blackmail**
 - From Security OR Service - the illusion of Autonomy
 - To Security AND Service - default control & autonomy
- **Security: Stakeholder Empowerment & dependability**
 - From upfront Identification – risk, fraud & distrust escalation
 - To virtualisation, Empowerment and National Id 2.0 - Security, Innovation & Democracy
- **RFID: User control by default-NOT for Auto Person Id**
 - Transfer of Control by default (no back doors/trusted parties)
 - Transaction non-linkability “should” be default Post-Sales
 - AUTONOMY to consent by action & act “irrational”

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"

Pe

5. Biometric Verification



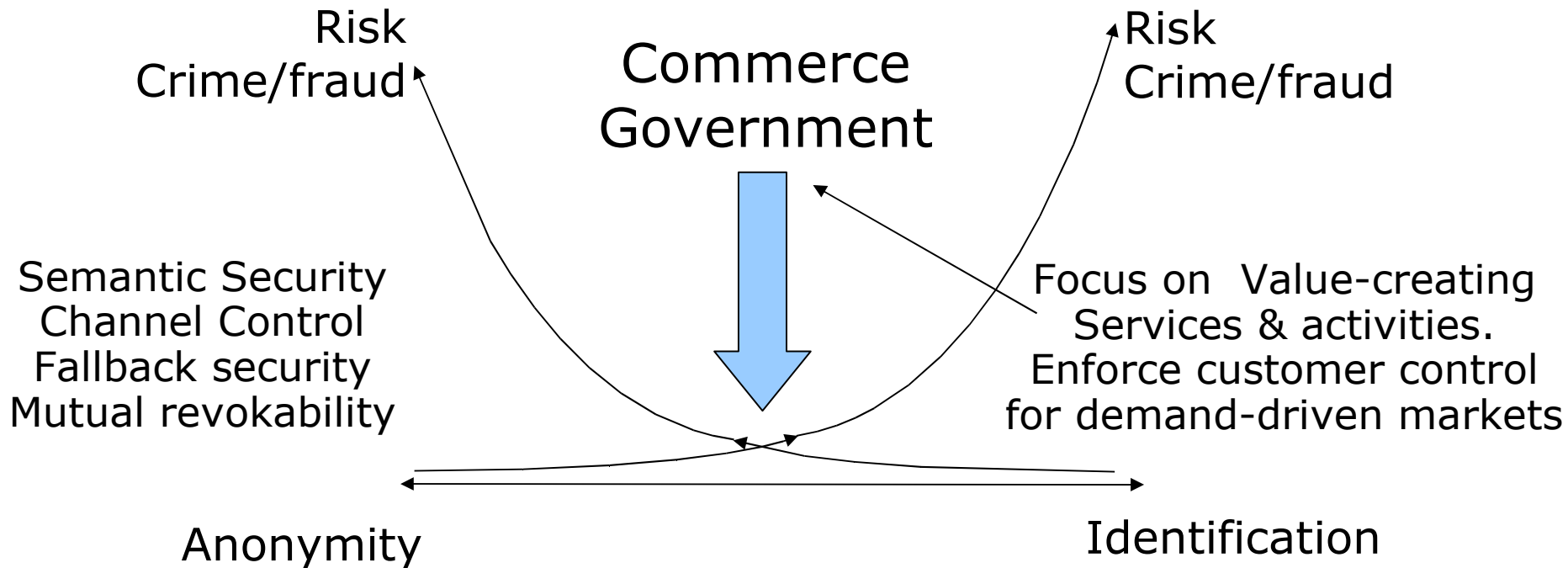
Id Theft
Foreign reader

Triggering
User not involved

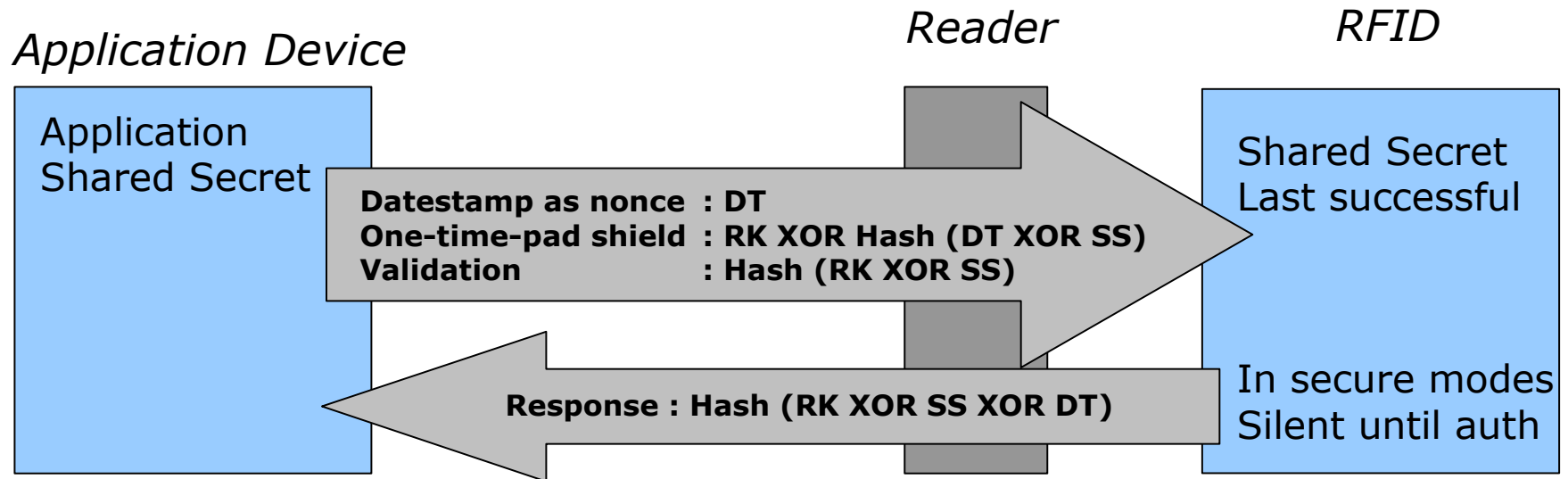
Tracking
No log security

Virtualisation – key to innovation & making National Id trustworthy

National Id 2.0 Building identities on Identification Contextual Id

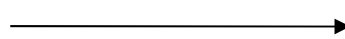


Context security in RFID



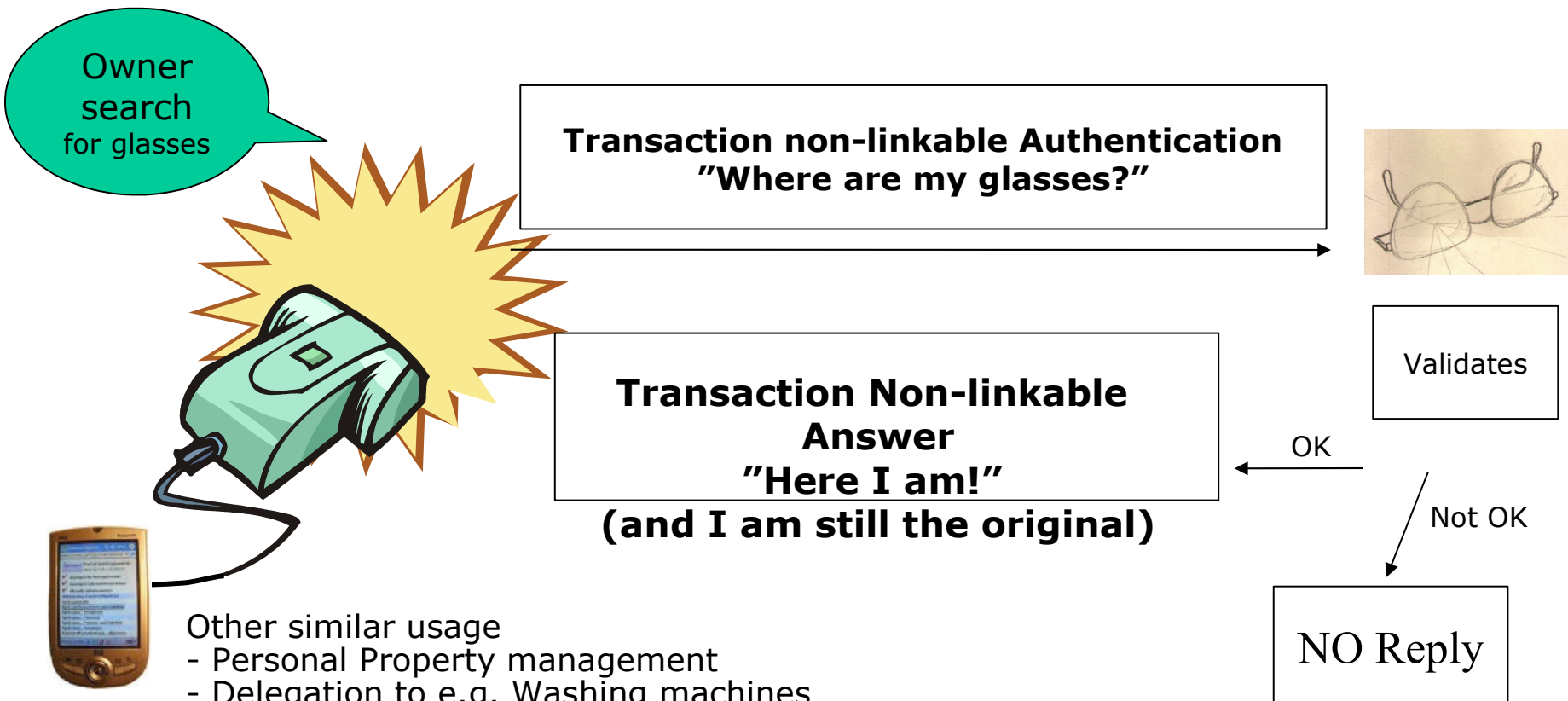
- ◆ Each RFID can hold **multiple keys for dynamic access control**
- ◆ Can dynamically change keys, identifiers, mode and **TRANSFER CONTROL**
- ◆ **Latest at Point of Sales, the RFID has to go into PRIVACY MODE**
- ◆ In Silent Modes **RFID remain silent until authenticated by the owner**
- ◆ Application dev. and RFID can **communicate without leaking identifier**
- ◆ RFID still holds a key to **validate product authenticity** with user accept
- ◆ User can make keys & data for special purposes – recycling, one-time etc

In mass production



TACD – RFID Security & Privacy

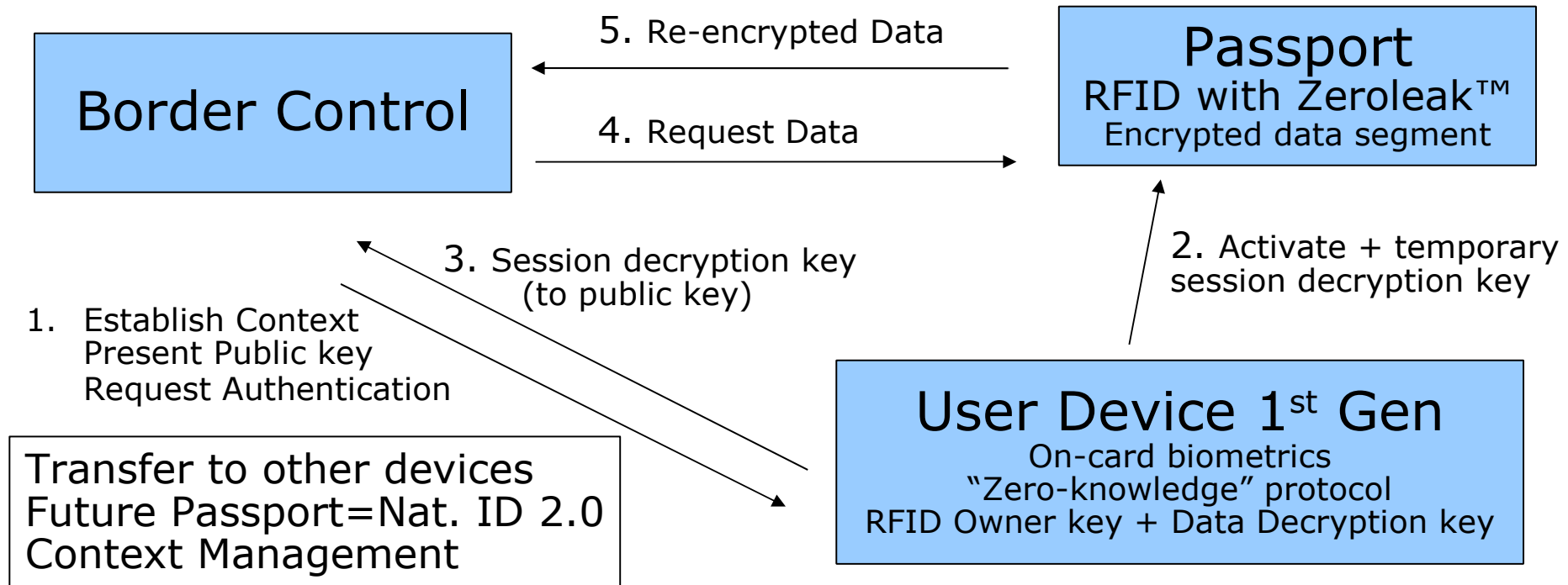
Simple consumer scenario



- Other similar usage
- Personal Property management
 - Delegation to e.g. Washing machines
 - Anti-theft,
 - Libraries, Dangerous goods shipment
- Etc.

Securing RFID in Passports

(User control of activation & passport revocation)

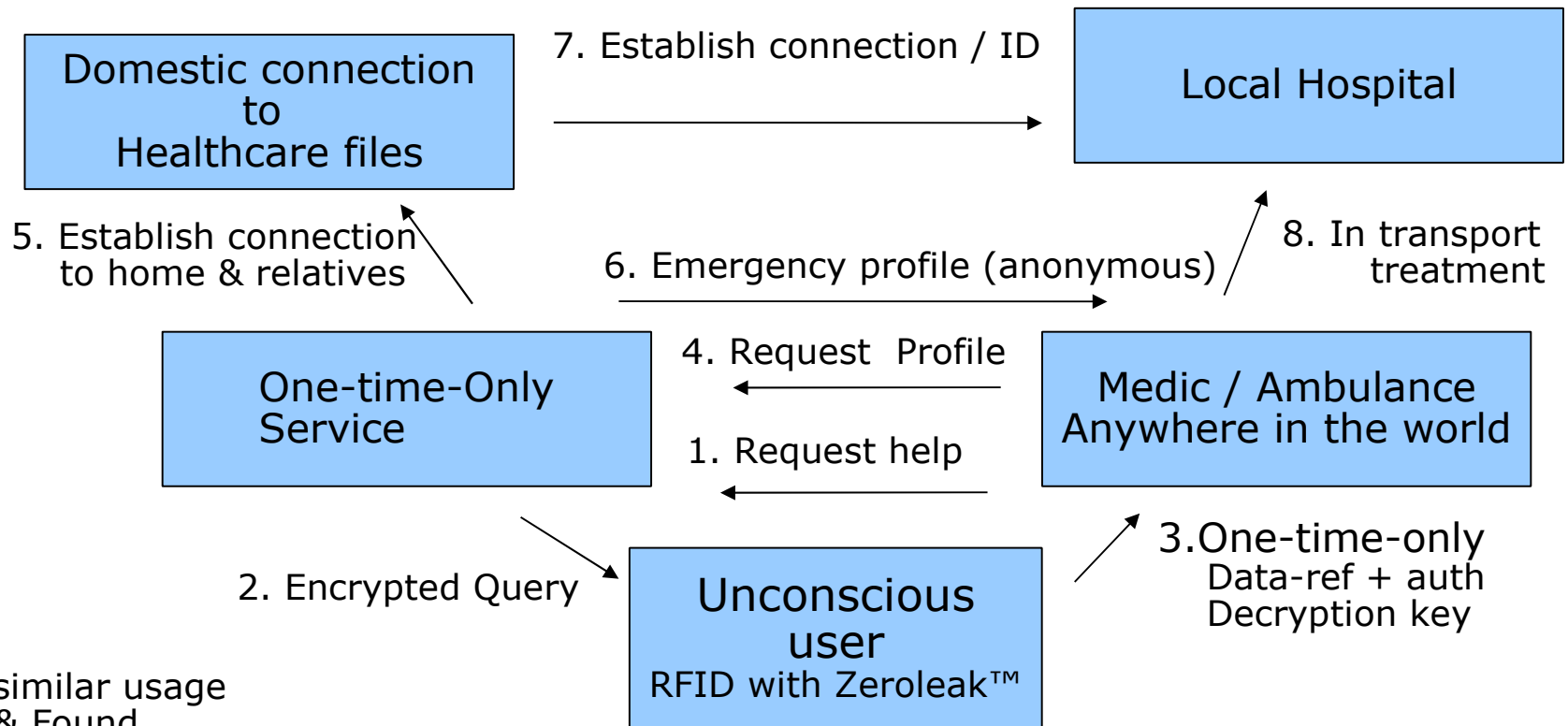


Other similar usage
- Anonymous home medication
- Context specific id
Etc.

Model is resistant to physical inspection
- key NOT in the RFID tag
RFID revocable when stolen or lost

Healthcare Emergency / disaster

Stepwise RFID-based one-time-only Identification



Other similar usage
- Lost & Found
- Recycling
- Tickets
Etc.

Balance by Design

Summary - Control by default

- **Consent:** An act of trust, not given by blackmail
 - From Security OR Service - the illusion of Autonomy
 - To Security AND Service - default control & autonomy
- **Security: Stakeholder Empowerment**
 - From upfront Identification – risk, fraud & distrust escalation
 - To virtualisation, Empowerment and National Id 2.0 - Security, Innovation & Democracy
- **RFID: User control by default-NOT for Auto Person Id**
 - Transfer of Control by default (no back doors/trusted parties)
 - Transaction non-linkability “should” be default Post-Sales
 - AUTONOMY to consent by action & act “irrational”
- Don't regulate or standardise without room for innovation