European Commission
Information Society and Media

PRIWAY
Security in Context

# Towards Trustworthy RFID Security and Privacy by design


***Stephan J. Engberg***

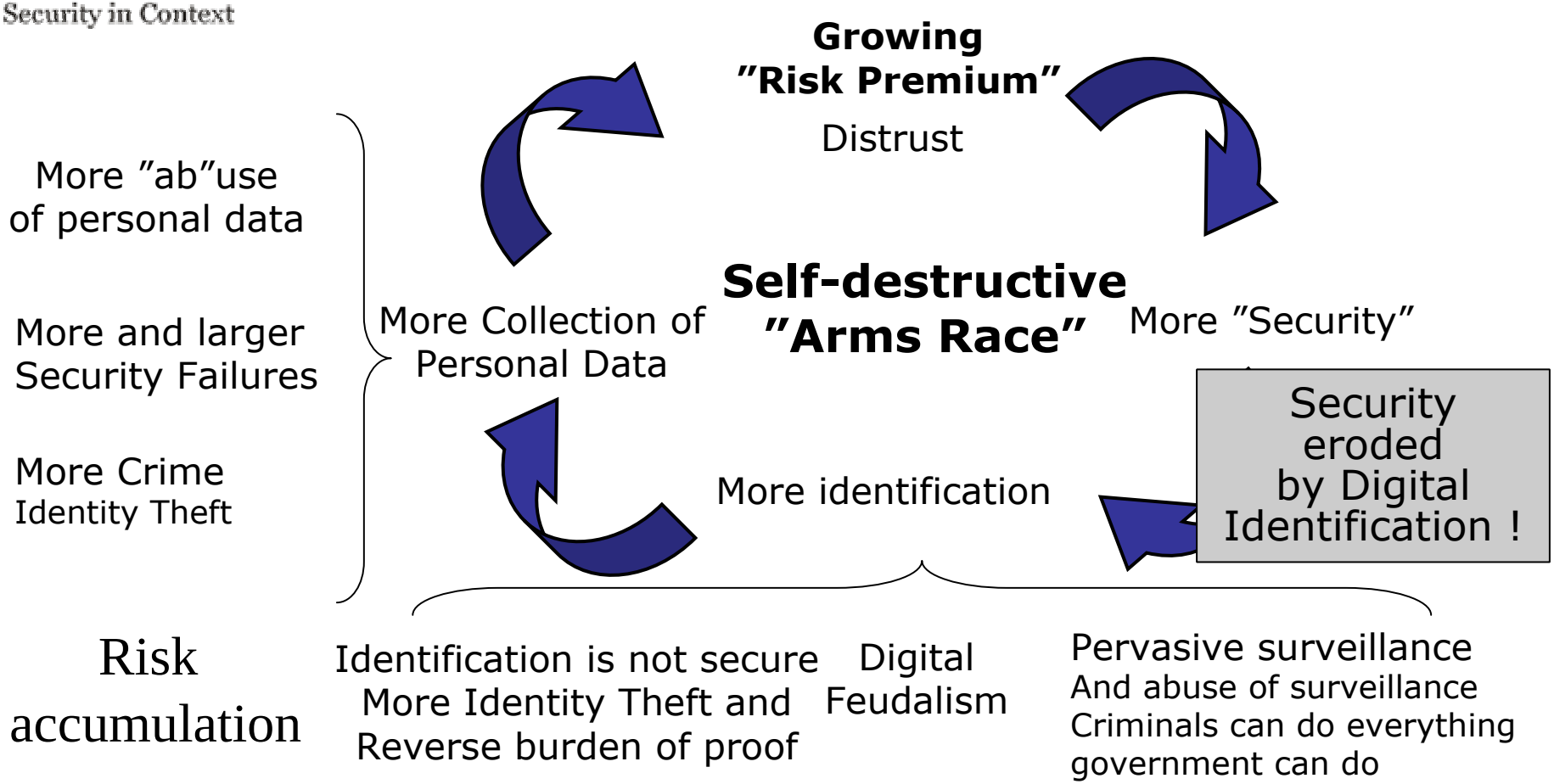
PRIWAY
Security in Context

***Denmark***

European Commission
Information Society and Media

PRIWAY
Security in Context

# The present Security Paradigm



European Commission
Information Society and Media

PRIWAY
Security in Context

# No lack of RFID threats

- Spam Triggering – "Bluetooth" problem
- Insufficient RFID security – Fraud & counterfeit
- Tagging, cloning, cracking, targeting etc.
- Lack of central data security model – data abuse
- Attempts to monopolised name space
- Identity Theft – Mafia Fraud Attacks

RFID is much more than a barcode
and the security model need to reflect this.

European Commission
Information Society and Media

PRIWAY
Security in Context

# A Context Security Framework

- Zeroleak™ (Making Devices adapt to ambient context security needs)
  - E.g. Citizen (multi-)Id Devices for anti-id theft
    RFID with PET access controls

RFIDsec

- PrivacyId™ (Making Trusted parties Trustworthy)
  - E.g. Privacy-enabled PKI & Mobile devices
    Anonymous Payments w/ anti- laundering

- PrivacyTrust™ (Resolving security assertions in Transaction Context)
  - E.g. Multi-hub Online Healthcare
    Crossborder eCommerce

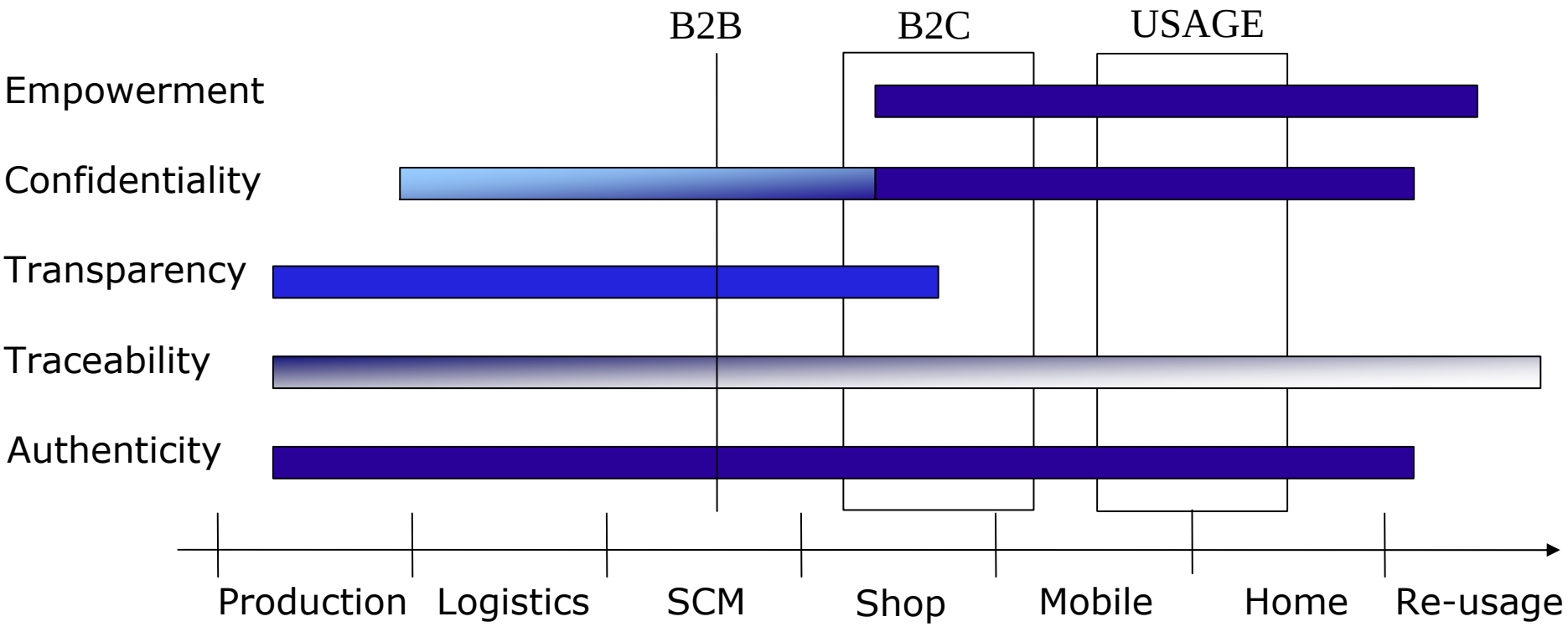
 

European Commission
Information Society and Media

PRIWAY
Security in Context

# RFID Value Chain

## As we move closer to the end-user. Security requirements Change !!



European Commission
Information Society and Media

PRIWAY
Security in Context

RFIDsec

# "Zero-knowledge" Device Authentication

- **Low-computational PET even for passive RFID**
  - **One-step Proof of knowledge of shared secret**
  - **Many solutions & non-algorithmic key change against brute-force**
  - **User device and RFID communicate without leaking identifier**
- **RFID key structure change through value chain**
  - **RFID support multiple dynamic keys and "relationships"**
    - **ProducerKey, OwnerKey, application keys**
  - **RFID support different modes**
    - **Highspeed – transparent mode / optimistic authentication**
    - **Privacy – RFID silent unless first authorised by OWNER**
- **RFID Control is transferred to the Consumer !**
  - **OwnerKey control access to other keys !!**
  - **No digital "pollution" - RFID adapt to contexts**

http://www.obivision.com/Papers/PST2004_RFID_ed.pdf

European Commission
Information Society and Media

PRIWAY
Security in Context

# RFID post-purchase privacy

- RFID start in transparent mode containing a ProviderKey
- When a product is transferred to consumer shopping basket,
  - RFID get a new Owner key and change to a silent "Privacy Mode". Product code is deleted from RFID for trust and security.
  - Consumer get the OwnerKey, that control access
- Afterwards (out of range) consumer changes the RFID Ownerkey to ensure exclusive knowledge of the key and RFID control.
- **The RFID remain silent unless Consumer authenticate**
- **Consumer can get services and communicate with RFID**
- **End result: Security, Privacy AND Service**

European Commission
Information Society and Media

PRIWAY
Security in Context

# Making sense of Consent

## Today – Informed Consent leads to blackmail
## Consent means Service OR Security

- With ZEROLEAK™ RFID, consumers can choose
  - To "KILL" the RFID at POS (concern about technology)
  - To receive the RFID Owner key (don't care or maybe useful)
  - To transfer valuable to "collections" (e.g. Books, clothes etc.)
  - To prepare one-time-only category information for disposal
  - To validate an RFID over the Internet, e.g. Home Medication.

## Tomorrow – Default is Service AND Security
## Consent means free choice, trust and acceptance of risk

European Commission
Information Society and Media

PRIWAY
Security in Context

# Zeroleak™ for RFID

EMPOWERED by ZEROLEAK™

- **Trust programme based on agreements**
  - Agreements/license to build trust in RFID
    - Each party in the value chain agree to principles,
    - agree to enforce on next step or "kill" the RFID,
    - and ensure RFID "transfer of control" to Owner
  - **Technical requirements to isolate RFID "contexts"**
    - RFID not allowed for authentication of people (Anti-Identity Theft require USER EMPOWERMENT)
    - No out of context data leakage when communicating
    - Fallback security for dependability
  - **Create a simple principle of control**
    - **If RFID communicate unauthorised -> trouble!**

European Commission
Information Society and Media

PRIWAY
Security in Context

# Open Naming Standards

- Ongoing attempts to control namespace(s)
  - ***E.g.: Manufacturer.Product.Serialnumber@monopolly.com***
  - monopolly.com translate to <manufacturer>.com for a fee and data
- Priway suggest URLs/DNS as default
  - ***[http://][product Ref].<provider.eu>***
  - ***Example http://<Serial#>.<Product>.<Manufacturer>.eu***
- Rationale – Flexibility, security and innovation
  - Providers are already registered through in DNS – another ICANN?
  - XML product descriptions incl. Certificates
  - Structured names spaces (e.g. EPC) as attribute certificates
  - Flexible and open to innovation – [ref].<serviceprovider.com>

European Commission
Information Society and Media

PRIWAY
Security in Context

# Summary

RFIDsec

- With Zeroleak™ consumers get control
  - **Minimum requirement is Transfer of Control**
  - But take care of stakeholder risks such as anti-counterfeit
- Usability is vital but an application issue
  - MANY user application solutions in parallel
- RFID Security is critical infrastructure for Europe
  - Make it trustworthy or kill it - **Prevent Digital "Pollution"**
- People are not things turned into targets !!
  - Design for trustworthiness - Emergency is one-time-only!
- European Values built into technology
  - Vital support for SME Innovation & trust