The emerging Security Paradigm

Empowerment & Context Security
The Route to Growth & Security

Stephan J. Engberg
Priway

PRIWAY
Security in Context

.. because the alternative is not an option

http://www.priway.com

©Priway, Mar 21, 2006

Agenda

PRIWAY
Security in Context

1. Risk – linking security, privacy, economy and trust
2. The present self-destructive security paradigm
3. Empowerment & Context Security – future security
4. Problem solving using Security by Design
    1. Citizen ID – a context security adding value to National Id
    2. RFID – adapting security to the value chain requirements
5. Summary

©Priway, Mar 21, 2006

What is Trust?

PRIWAY
Security in Context

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

Technical Term
Accepted
Dependability

The Perception of Risk can in context both be overestimated (fear) and underestimated (naïve) but

Over time learning will align risk perception to reality

Except in rare cases, risks are avoided and minimised, i.e. risk involve trade-off's and compensations.

Lack of Control create resistance

SWAMI

©Priway, Mar 21, 2006

Biometrics – attackers dream

PRIWAY
Security in Context

Biometrics with foreign verification of bodily constants

- Only approximate
- Publishing passwords
- Can always be spoofed
- Cannot be revoked

Create crime / Identity Theft
- Reverse of Burden of proof
- More only worsen the problem
- Lack plausible deniability

Destroy Data Security
- Linkable across context
- Does NOT ensure consent
- Block User-centric Id mgt.

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

The ONLY secure Biometrics – is NOT to use Biometrics!

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

SWAMI

©Priway, Mar 21, 2006

Biometrics is not a solution
It is a primary threat !

PRIWAY
Security in Context

Politicians should not be asking how to promote biometrics.

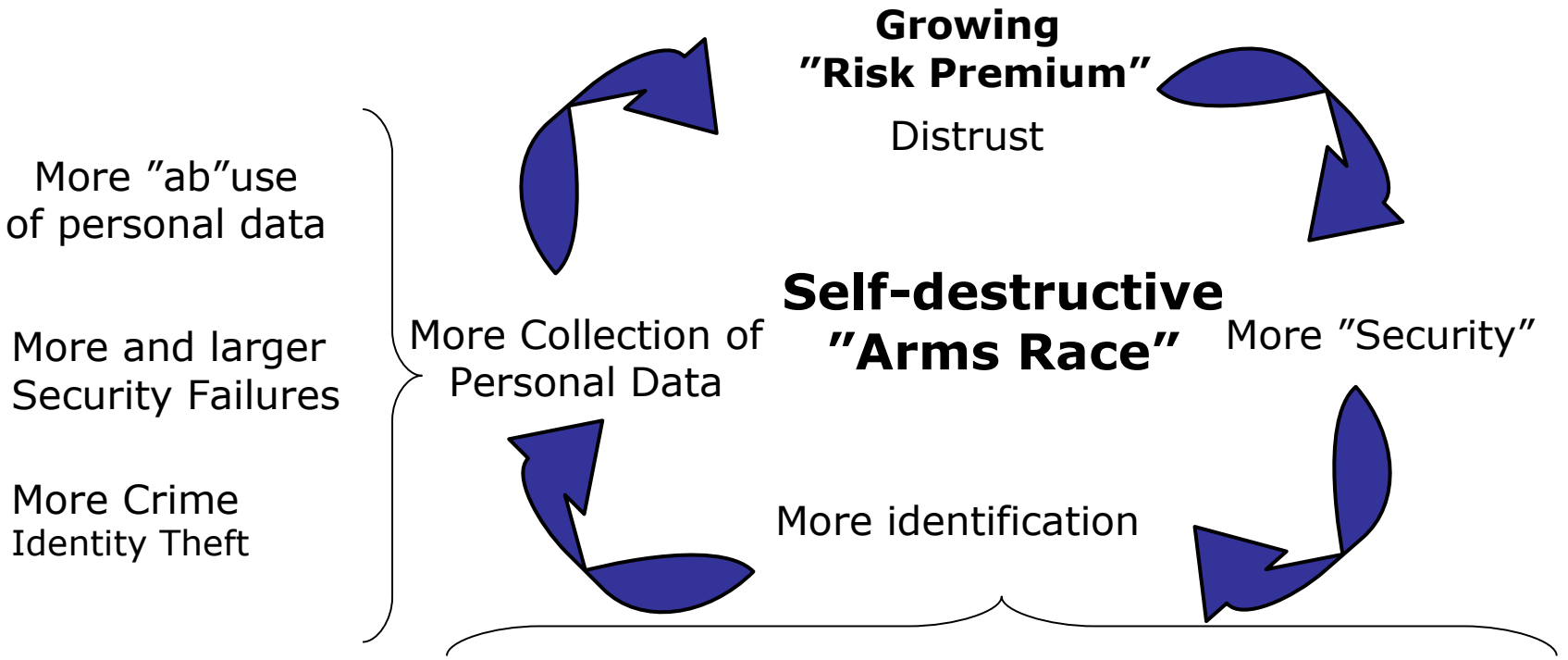
Politicians have a serious problem on how to **prevent crimnal abuse of biometrics** and pervasive surveillance !

Publishing Biometrics for Plausible deniability?

SWAMI

The dying Security Paradigm

PRIWAY
Security in Context



Risk accumulation

Identification never perfect
More Identity Theft and
Reverse burden of proof

Digital Feudalism

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

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

SWAMI

©Priway, Mar 21, 2006

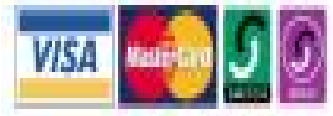
No Security without privacy

PRIWAY
Security in Context

1. Challenge → 2. Challenge

Targeting
Reusing Id

Mafia Fraud Attack



PKI

"Secure Chip"/
Shipment Id

"Trusted"
Person

Log

4. Response ← 3. Response

5. Biometric
Verification

Tracking
No log security

Id Theft
Foreign reader

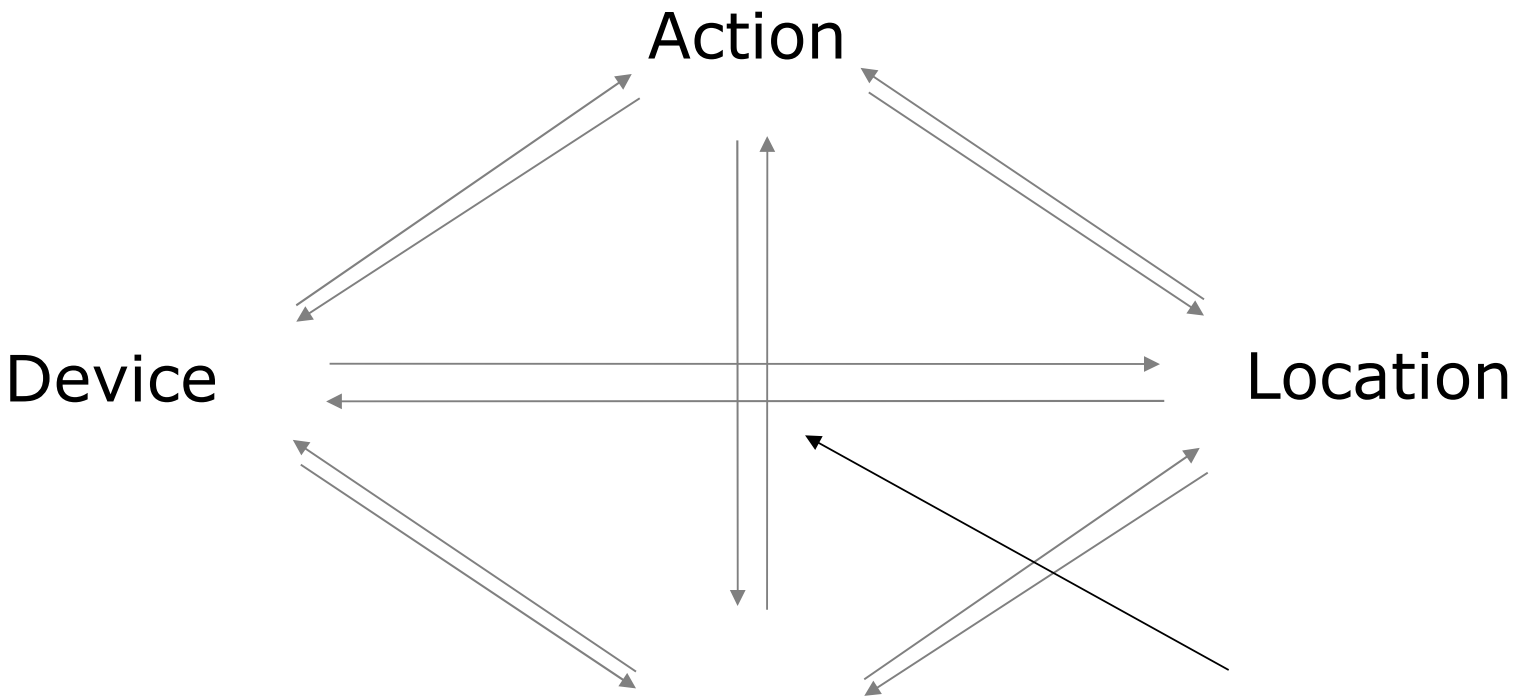
Triggering
User not involved

Central control is zero security

SWAMI

Fribourg Privacy Diamond

PRIWAY
Security in Context

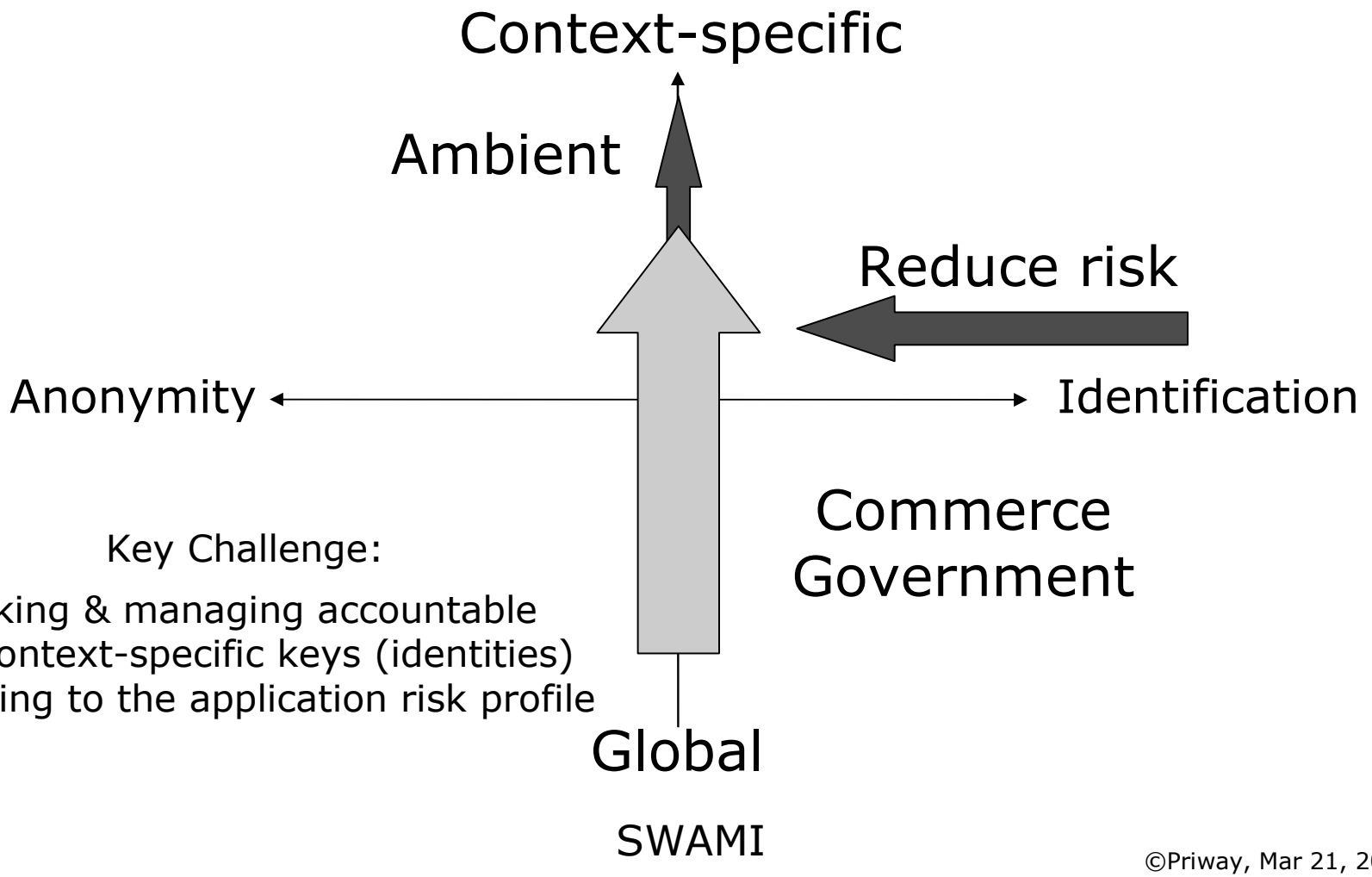


SWAMI

Think new dimensions

PRIWAY
Security in Context

Priway Identity Model



©Priway, Mar 21, 2006

Priway emerging solutions

PRIWAY
Security in Context

- Zeroleak™ (Making Devices adapt to context)
  - Slave & P2P Devices & Sensors
  - Master communication Devices
  - Identity Devices

Citizen Id

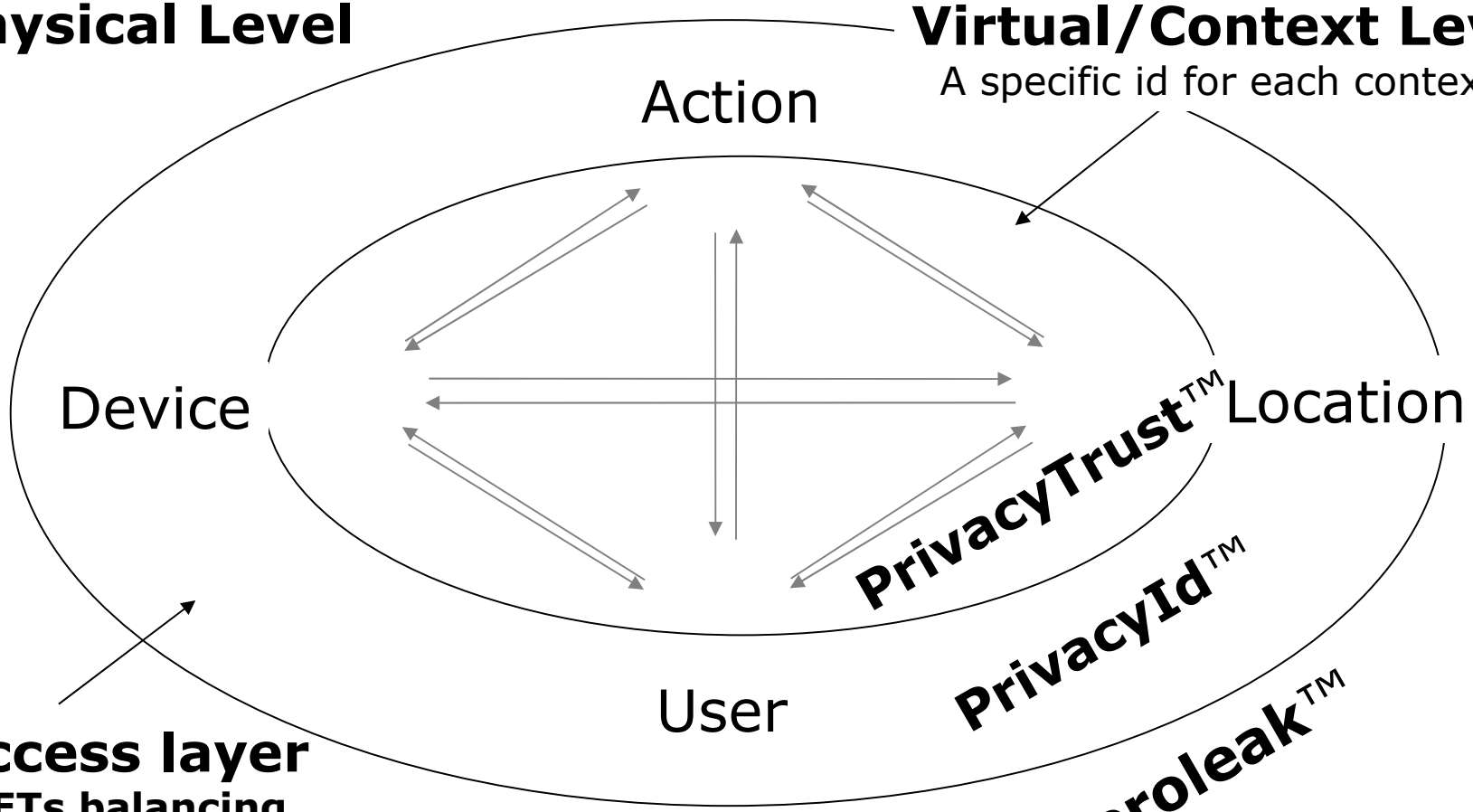
- PrivacyId™ (Making Trusted parties trustworthy)
  - Privacy-enabled PKI
  - Cross-channel User-centric ID management.
- PrivacyTrust™ (Transaction in context)
  - Managed Service resolving security assertions in context

What matters is not how it works, but how it fails.
Bruce Schneier

©Priway, Mar 21, 2006

Priway Security Diamond

PRIWAY
Security in Context



SWAMI

©Priway, Mar 21, 2006

Citizen Id is context-specific

PRIWAY
Security in Context

- Priway User-centric & anti-identity theft Devices
- Java-card or similar that
  - Detect context BEFORE it assume or create an identity
  - Making National Id a solution (instead of a problem)
  - Integrate with Channel management
  - Adapt to security requirements in context
  - Is instantly revocable by Owner
  - ONLY on-card Biometrics readers for self-protection
- Controlling a secure Master Communication device
  - E.g. mobile phone extended with Privacy Authentication
- Many additional aspects

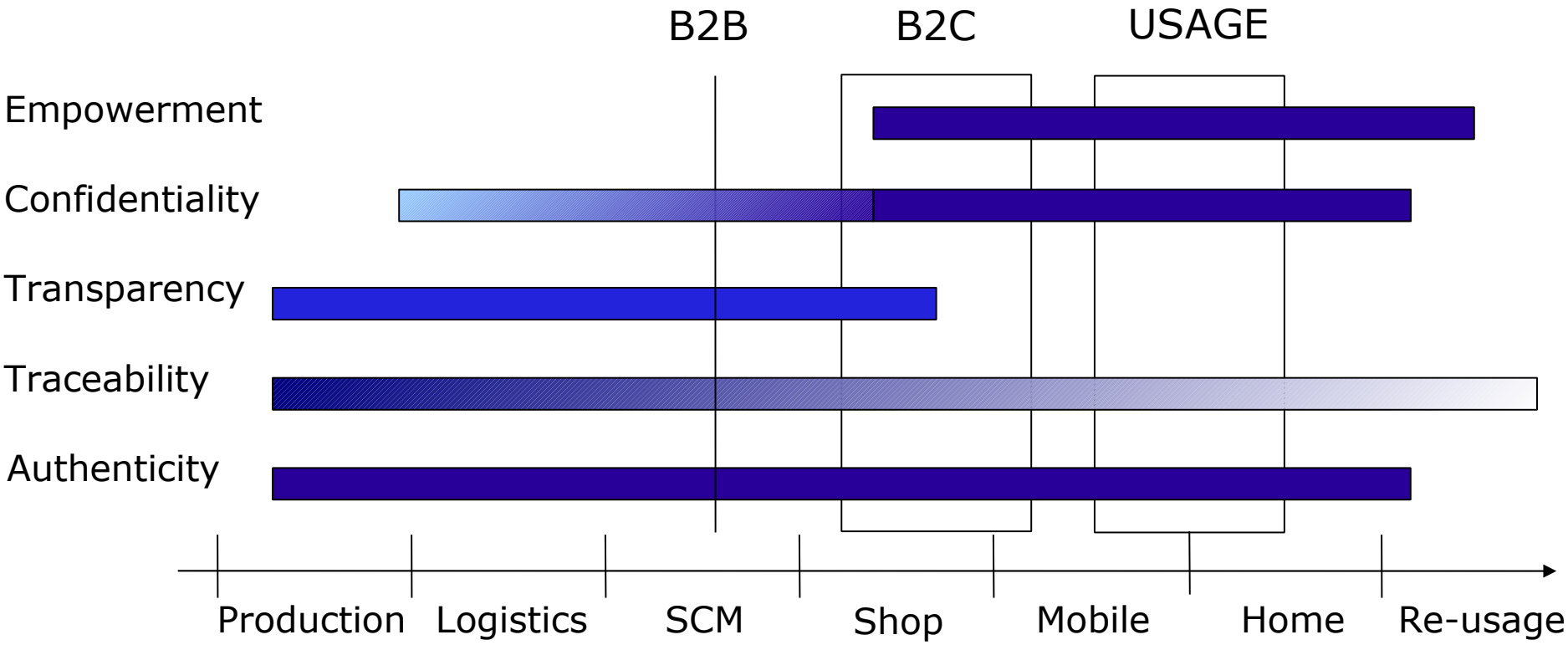
http://www.securitytaskforce.org/dmdocs/workshop2/stephan_engberg.pdf

©Priway, Mar 21, 2006

RFID Value Chain

PRIWAY
Security in Context

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



But so does the value

SWAMI

©Priway, Mar 21, 2006

RFID security has to adapt

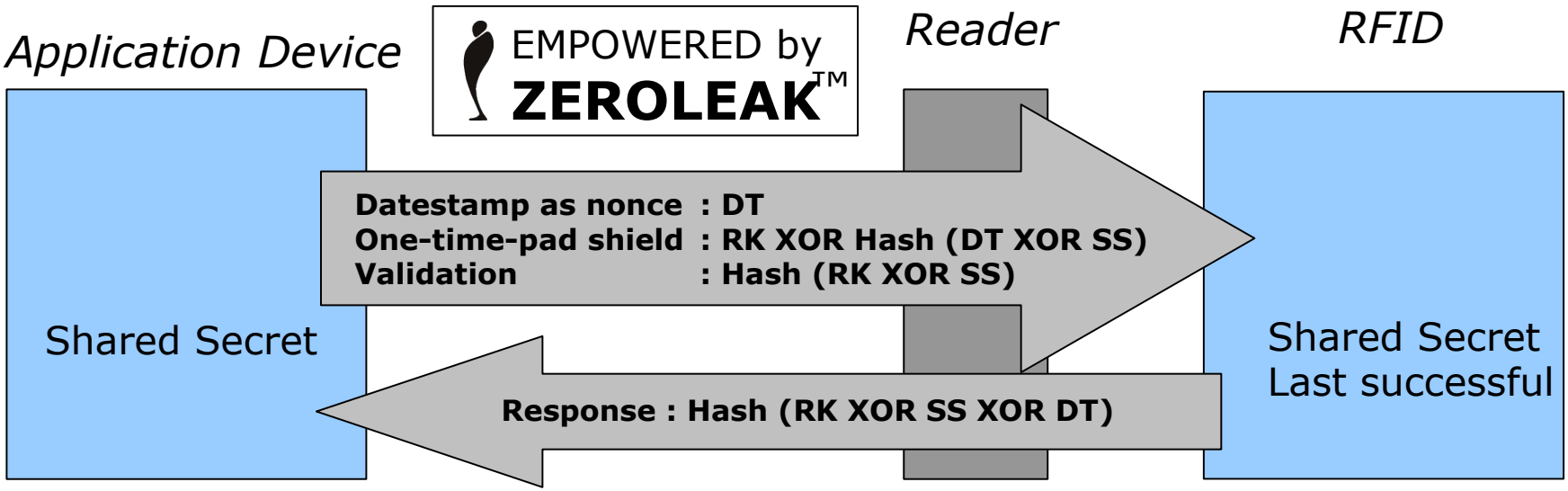
PRIWAY
Security in Context

- Security requirements change in the value chain
  - So device security model has to adapt accordingly
- Multiple and changing modes
  - Transparent, Encrypted, Stealth
- Multiple and Changing context
  - Dynamic Key structure, multiple keys
- Central EPC databases are zero security
  - We can not trust their confidentiality

©Priway, Mar 21, 2006

Context security in RFID

PRIWAY
Security in Context



- Each RFID holds **multiple keys (typically 3-5)**
- Each key can be **verified transparently without leaking identifiers**
- RFID have **multiple modes** determining response type to a request
- **Random Session Key** used for session communication & command
- **Low-computational "overkill"** – padding random with pseudo-random
- **Many solutions** – cannot brute-force attack off-line & key changes

Moving into production → RFIDsec

SWAMI

©Priway, Mar 21, 2006

What RFID privacy problem?

PRIWAY
Security in Context

”KILL” RFID or Transfer Control

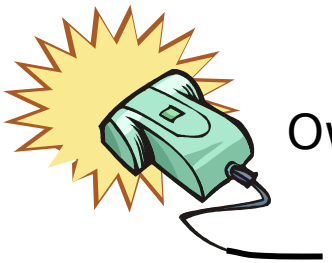
EMPOWERED by ZEROLEAK™

3. Point of Sales
New Owner Key
Swith to ”Privacy Mode”

4. Privacy AND services
Owner control RFID
Authenticity key protected

2. Logistics
EPC number transperent
Online anti-counterfeit

Consumer device



Owner Key
EPC

Owner Key
Authenticity Key

RFID Tag

1. Manufacturer
Authenticity key

RFIDsec

SWAMI

Security without Privacy? – An illusion

PRIWAY
Security in Context

Reasons for Privacy – Stakeholder security

- SECURITY — Prevent targeting, fraud prevention
- DEPENDABILITY — Security by Design, Risk reduction
- DAMAGE CONTROL — Fall-back, Context separation
- ECONOMY — Demand-Pull, Take-up
- CONVENIENCE — Adaption to context
- USABILTY — Context-awareness
- QUALITY — Customer-orientation
- EFFICIENCY — Aligning Digital Value Chains
- BASIC NEEDs — Self-determination, control, etc.
- COMPLIENCE — To law and ”principles”

©Priway, Mar 21, 2006
17

Summary

PRIWAY
Security in Context

- Trust is about real risk and perception of control
- Central Control & Surveillence destroy security
  - We cannot protect data or make secure surveillance
  - Biometrics is a serious threat to security & trust
  - Identification of people or devices create risk & distrust
  - Identity Theft force allignment of security & privacy
- Empower Citizens through context security
  - From context awareness to context management
  - Device & person id adapt to context to balance security
- Build trust by isolating risk for demand-pull growth
  - Privacy is security, security is privacy – prevent targetting
  - Using privacy as a European competitive advantage

©Priway, Mar 21, 2006