PRIWAY
Security in Context

The changing Security Paradigm

From Central Command & Control to Distributed Dependability & Empowerment

Stephan J. Engberg
Priway

PRIWAY
Security in Context

.. because the alternative is not an option

http://www.priway.com

Priway emerging solutions

PRIWAY
Security in Context

- Zeroleak™ (Device in context)
  - Slave & P2P Devices & Sensors
  - Master communication Devices
  - Identity Devices
- PrivacyId™ (Identity & channels in context)
  - Privacy-enabled PKI
  - User-centric ID & Channel management.
- PrivacyTrust™ (Transaction in context)
  - Service resolving security assertions in context

RFIDSec
When Security Means Business

Citizen Id

You can trust it, when you dont have to trust it

Plenty security challenges

PRIWAY
Security in Context

- Criminals can do anything a trusted party can do
  - Ask the Greek Prime Minister on wiretapping !
- Server perimeter security is an illusion
  - How many examples do you want ?
- Digital Crime is turning into an industry
  - Professionalised and very innovative
- Much ”security” will do more damage than good
  - What happens when someone fake your biometrics?
- Why is technology mostly deployed with bad security?
  - WLAN, Credit Cards, SMTP, PKI, mobile .. and now RFID ?

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

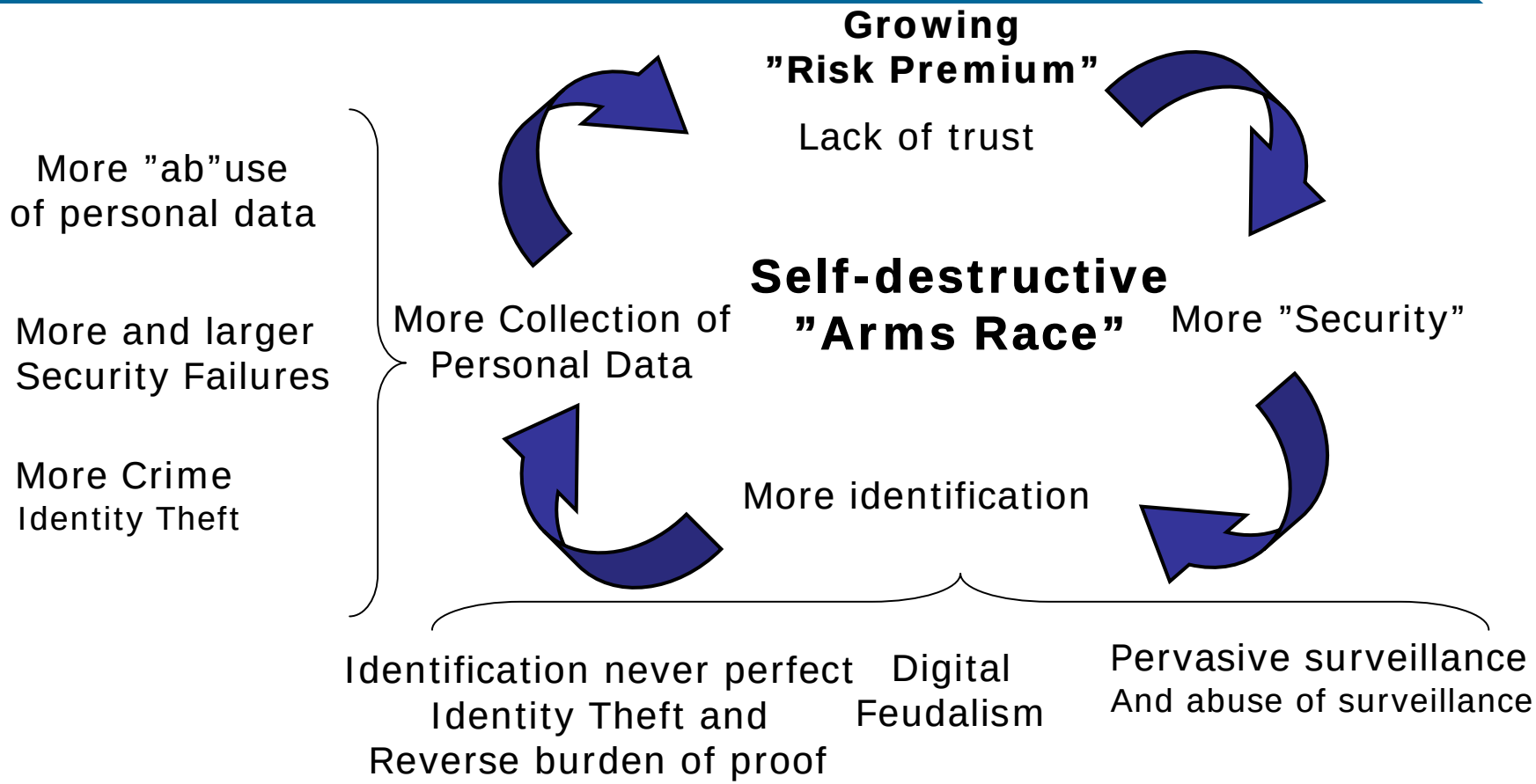
Over time learning will align perception to reality

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

Lack of Control create resistance

The security distrust circle

PRIWAY
Security in Context



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

Security without Privacy? – An illusion

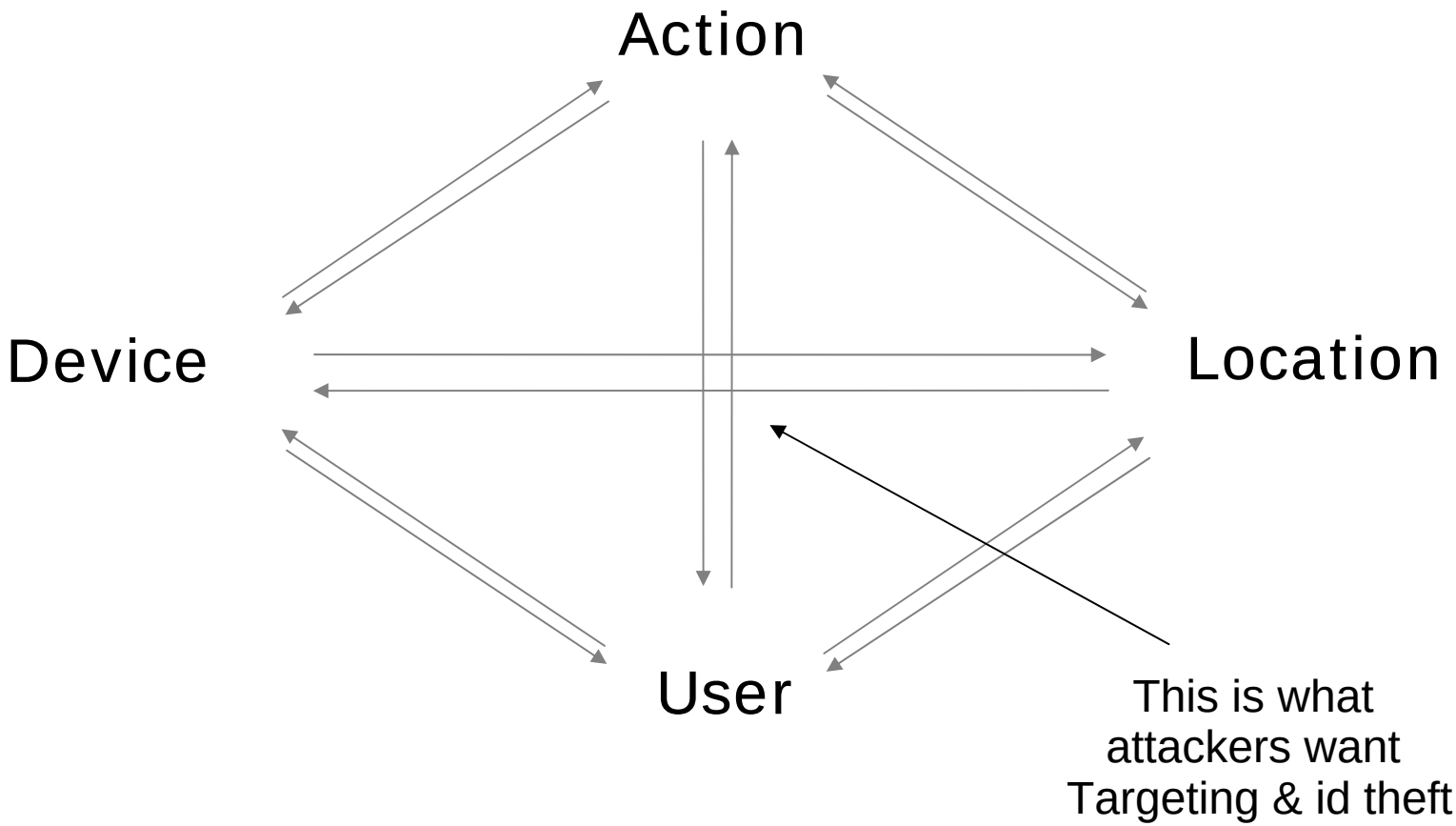
PRIWAY
Security in Context

Reasons for Privacy – Stakeholder security

- SECURITY — Risk reduction, crime prevention
- DAMAGE CONTROL — Dependability, 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

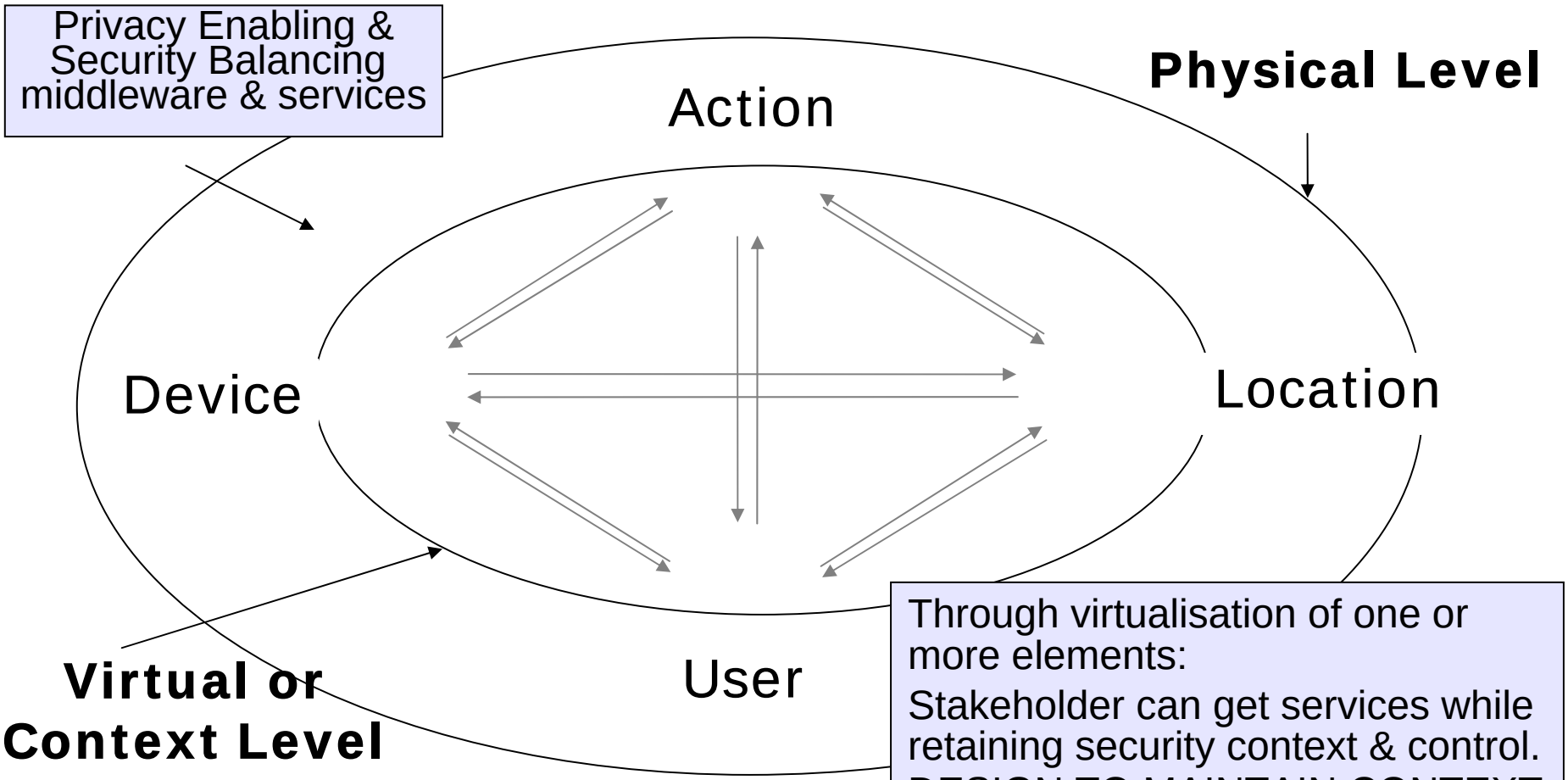
Fribourg Privacy Diamond

PRIWAY
Security in Context



Priway Security Diamond

PRIWAY
Security in Context



Empower the citizen

PRIWAY
Security in Context

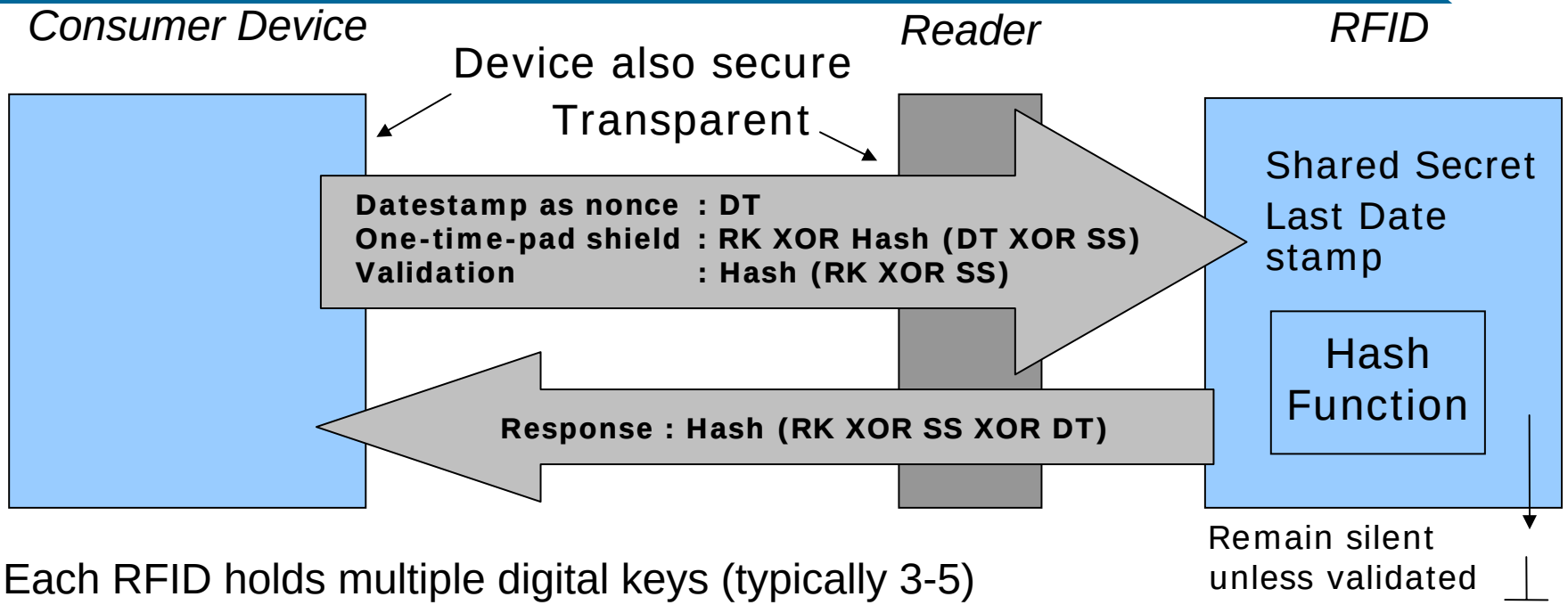
Control should be distributed to those that will suffer from failure

Liability should be distributed to where design is controlled

The usability barrier needs to be pushed by design etc. - we will never have better security than citizens can manage.

Building security into RFID

PRIWAY
Security in Context



- Each RFID holds multiple digital keys (typically 3-5)
- RFID have multiple modes determining response type to a request

Some aspects

- Consumer control new OWNER key (used for Privacy Mode)
- Manufacturer keep Authenticity Key for verifying originality etc.
- Using group keys to narrow in on context – dynamically customised
- Each key can be verified transparently without leaking identifiers

EMPOWERED by ZEROLEAK™

What is achieved?

PRIWAY
Security in Context

- Full virtualisation of both verifier and RFID
  - RFID can operate without leaking information
  - NO IEEE MAC or other persistent identifier
- Consumer get control at purchase
- Strong anti-counterfeit even post-purchase
- Can maintain business confidentiality
- Critical for
  - Home medication (pharmaceuticals in general)
  - Products with counterfitting problems
  - Digitally enhanced products & services
  - Industrial products
  - Solving ”RFID as trigger”-problems military, wearables
- In low-cost implementation compatible with EPC !

RFID wider issues

PRIWAY
Security in Context

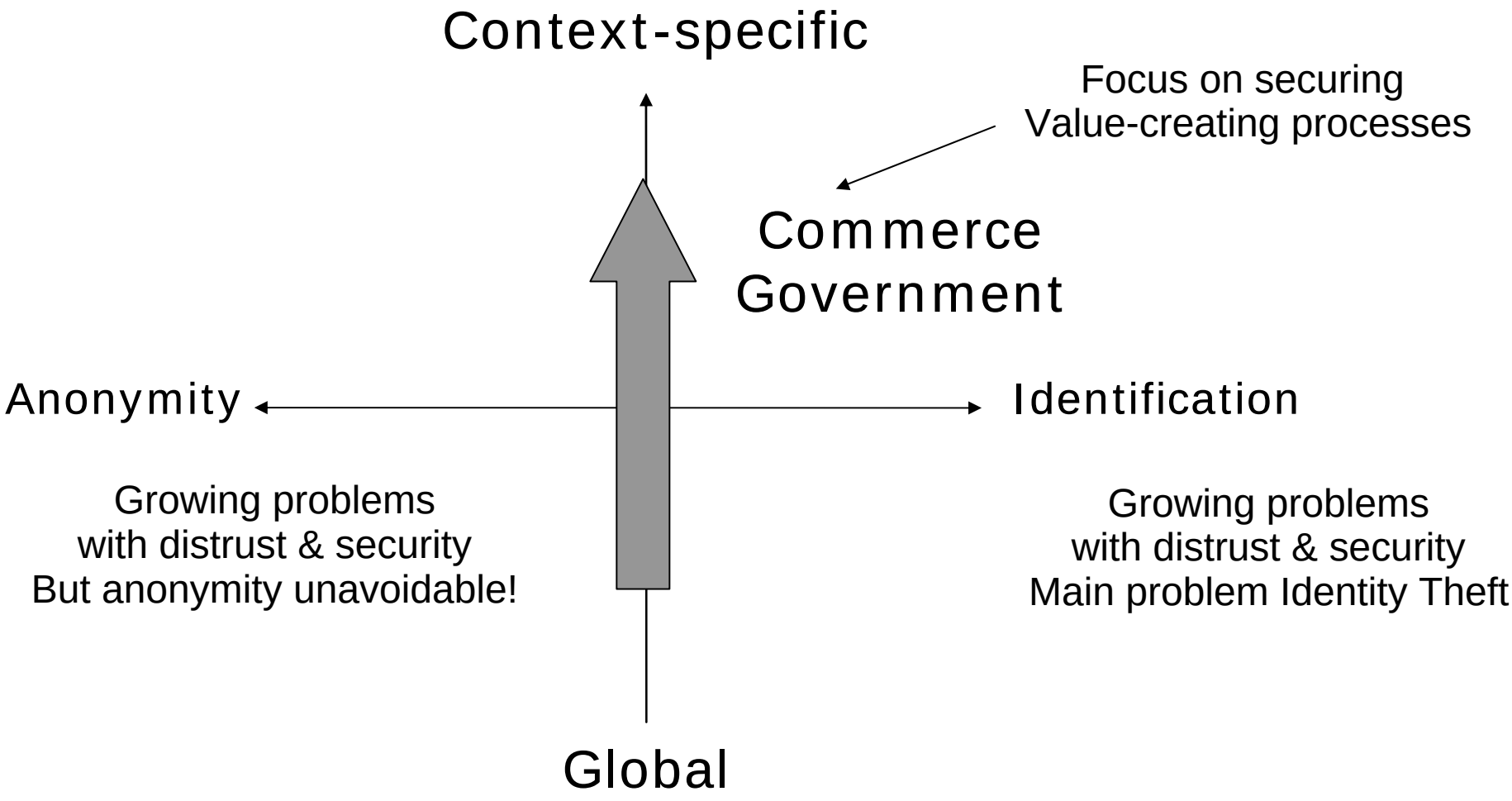
- RFID will be a heterogeneous space - maybe always
  - Many frequencies, different models
  - EPC mainly for retail logistics
- Why ONS? DNS can deliver the same cheaper !
- Most value application require much better security
  - E.g. Pharmaceutical, Branded Goods, Military, Industrial
- Europe is lagging behind
  - Special European needs & opportunities ?

OBS

- RFID unusable for Person Id (payment, access etc.)
  - Open risks of Identity Theft (e.g. Mafia Fraud Attack)
  - Privacy problems create all sort of risks

Think more dimensions

PRIWAY
Security in Context



RFID & The Internet of Things

Citizen Id is context-specific

PRIWAY
Security in Context

- Priway User-centric & anti-identity theft Devices
- Java-card that
  - Detect context BEFORE it assume or create an identity
  - 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 such as a mobile phone extended with Privacy Authentication
  - With anonymous payments incl. anti-laundering & credit
- Many additional aspects
  - *:// . . / / 2/ _ .*

Summary

PRIWAY
Security in Context

- Ambient require new Security Models
  - Growing data needs require stronger security models
  - Prevent criminal targeting & identity theft
- Identity Theft will align Security & Privacy !!
  - Self-protection is critical to trust & system security
  - Key issues are Usability & key management
- Context Security has missing answers
  - Empower the Citizen to secure & build trust
  - Focus on risk reduction – not identification & surveillance
- Research needs? – try asking
  - Which present standards & ICT are sustainable?
  - Why is focus on surveillance instead of security?
  - What does it take to change this?

