Digital Agenda Assembly 2012

Brussels, 21-22 June

Linking Security with Economics

Re-Empower Citizens & Companies to Secure Economic Growth

Stephan J. Engberg
Priway

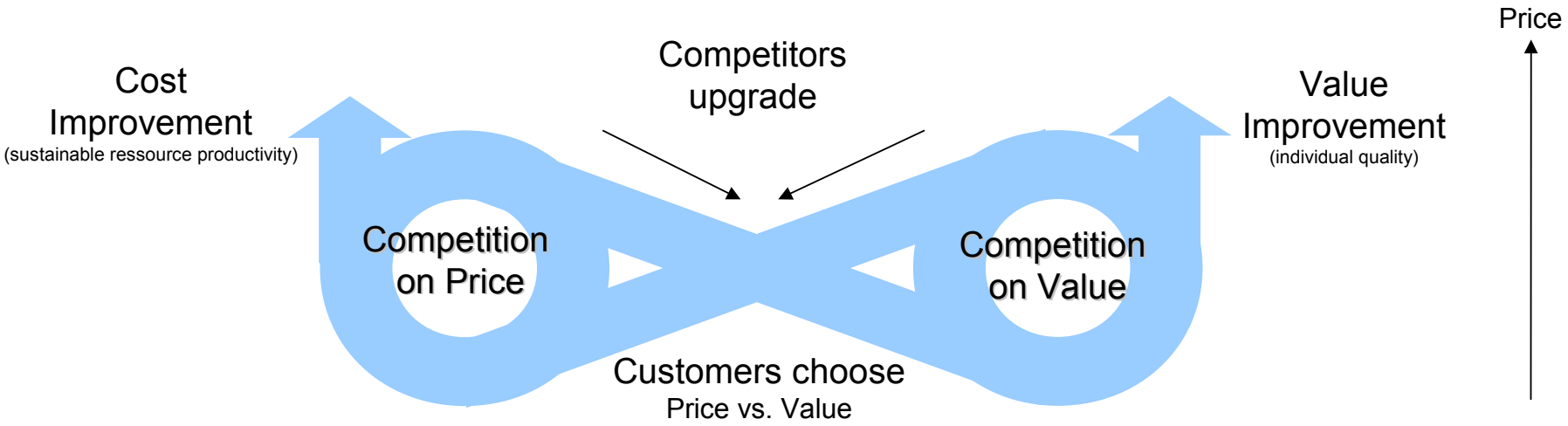
EUROPEAN PARLIAMENT

European Commission

European Economic and Social Committee

EUROPEAN UNION
Committee of the Regions

For markets to create value over time Demand has to control the critical resource !



Digital Agenda problem:

Identification blocking markets by moving control from citizen to infrastructure

Market	Physical Value chain	Digital Value chain
Demand	Next in value chain	End-customer/Citizen
Critical Resource	Money	Personal Data / Keys

Digital Agenda challenge:

How do we ensure control of critical resources remain with citizens !?

Digital value chains control physical value chains
Digital market distortions leads to physical market distortions

Security is key to economics

- Define who has control
- Define the ability to change and customize
- Security by Design

Identification is digital pollution

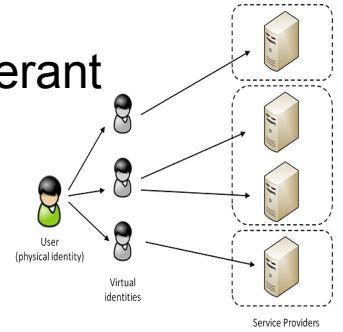
Power and risk concentrate exponentially

Problem: Identification dis-empower

Turns everything into targets
Impossible to secure
Command & Control driven
Destabilizing

Solution : Control at the edge

Control distribution
Risk Isolation & fault tolerant
Demand-driven
Stabilizing



Security barriers for Growth

Public Sector problem
"Managing" Citizens and controlling processes

mutually reinforcing

"Political" legitimization
Commercial control

Private Sector problem
Infrastructure Owning people and controlling processes

Leads to:
Command & Control Economics accumulating inefficiencies

Accumulating ICT & process legacy

Providing less individualized value with more resources

Agree
- they are "trusted"
- problem" is crime and terror
- solution is identification

→ Distorting regulation and infrastructure standards

Regulation prevent security !

Leads to:
Intermediation, concentration, lock-in, technical bottlenecks & market distortions such as frontrunning and trading customers

Preventing competition & innovation

Squeezing more profits out of profiled citizens and commoditized providers

Single market cannot deliver

unless these security problems are resolved!

They are even through identification the source of most security problems!

Any sufficiently advanced cluelessness is indistinguishable from malice
J.P. Clark

Security or Controlware?

Market	Control-ware	Empowering Security
What market buy?	Central Control over people and processes	Distributed Security for growth & Customer Loyalty
Product	Identification, Surveillance, Perimeter Access Control	Built-in security, control distribution, Parametrized & Interoperable identity
Strategic	Power & Short-term Profit	Demand Empowerment & long-term Value Creation & Loyalty
Tactical	Lock-in, prevent competition, compliance through “spin”	Flexibility, Interoperability & Upgrade, Innovation, Adaption/Customization to context & Customer needs, compliance by design
Operational	Optimize control through Identification & surveillance – personal data as an asset and source of Power	Security by Design, minimize stakeholder risks – personal data as a liability and source of distrust
Perceived Barriers	Regulation (Data Protection) Growing security failure Citizen distrust	Regulation (Data Retention & eIdentification) Infrastructure “kartel” standards “Citizen as product” market distortions Complexity
Society value	Negative – market failure	Market enabler

Citizen Empowerment

Free to share throughout value chain
as linking control remains demand-side

Cloud %

Server

Legacy system
Dis-empowering Id

Negotiated
runtime
to fit purpose

Optional
Accountability Proof
for conditional identification
in case of violation

One-way - not linking
multiple transactions
Not a backdoor

Empowering ID
Purpose-specific Contextual Identity
True subset NOT linkable to PKI

Specific Trust
Additional Id

Client

PKI

Citizen Id Card
(Biometric Chip-on-card)

Normative ideal:
Identification reserved for person-to-person
Citizens chose who to trust with specific liability
– not to trust a system or organization

How do we create a Security Market?
We parameterize interoperable identity !!

Identity := A set of optional elements

Security Proofs
- Authentication (recognition)
- Authorization (group membership)
- Accountability (conditional identification)
- Integrity (traceability)
- etc.

Channels
- Payment (e.g. Digital Cash)
- Mobile (e.g device without persistent identifier)
- Postal (e.g. dropbox)
- Digital Post (e.g. email incl address/enc)
- etc.

3rd party Accreditations
- Positive: Statement ("Danish", "Visa OK")
  - Identification (could be encrypted)
  - Tokens (e.g. ticket)
- Negative: Exclusion, Revocations, Convictions

Each Security element of parameterized Identity mapped modeldriven towards Security Objectives according to chosen Assertion Provider

Security Ontology / Objectives
NRL Security Ontology ext.

↓

Security Resolution language
Dynamic negotiation to context @ runtime
E.g. XACML (upgrade)

If <element>.<<Govcert>.<Accountability> >= Govcert.Level_5
and <element>.<Govcert>.<Authentication> >= Govercert.level_2
Then Accept <Element> as Legal Identity

↑

3rd party Assertion providers
BEUC, GOVCERT,
NIST, Industry Ass

Open Data

Open Data %

Cloud %

Server

Co-creation

Client

Data that have not been personal data can be open data !

No “Trusted” Party backdoor or profiling

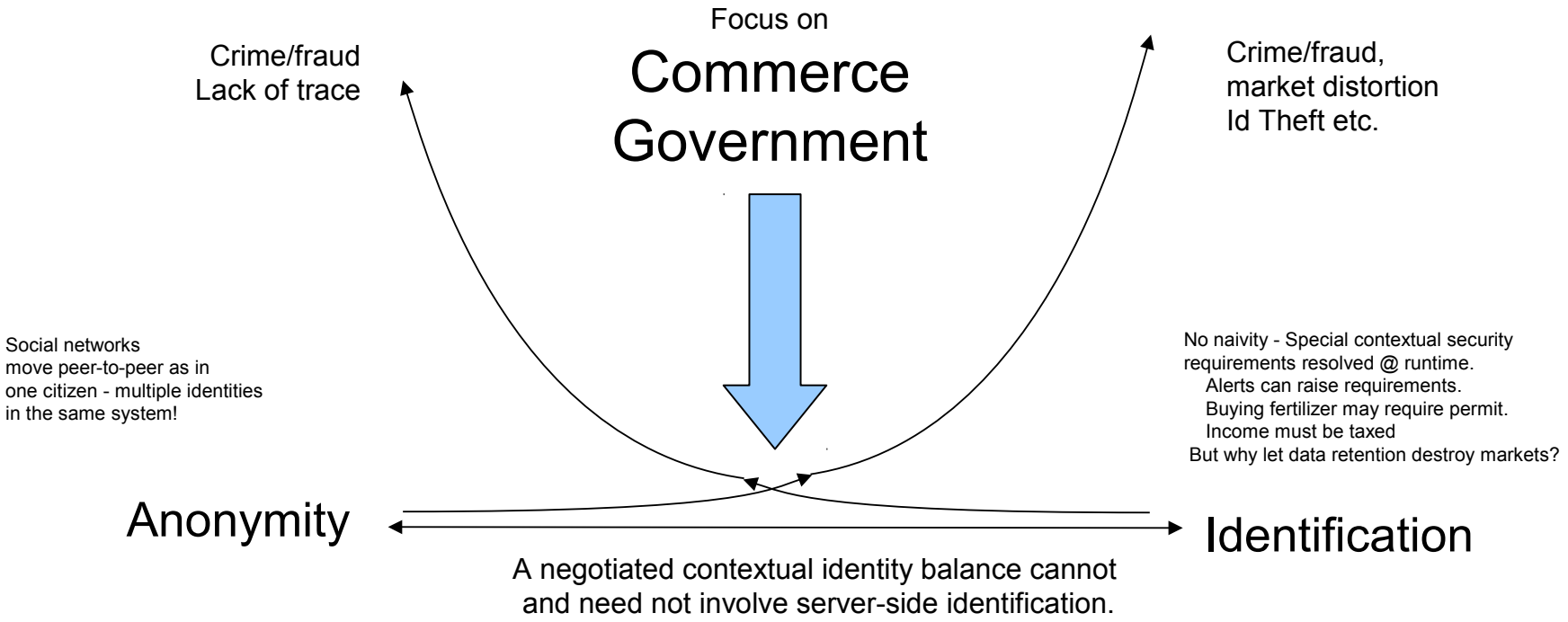
Research can request even intimate details without bureaucratic or non-transparant use of data

Empowering Identity with citizen in control means Service interfaces always open for co-creation but not for intermediation

Horizon 2020 Vision

Re-Empower Citizens & Companies in Single Market through active citizen control of contextual identity & data.

"Your security is limited by the number of isolated identities, your tools can manage."



2020 Vision – Empower the Citizen

To recover economically, we must re-empower the Demand to control the critical resources as requisite to public and private sector economic growth.

Suggested goals for 2020 in order to gradually secure needs-driven innovation:

- National ID 2.0 (Citizen Id) is fully enabled
  - Citizens can trade, reuse data and act purpose-specific trusting to remain control
  - An inclusive Semantic Identity standard in place and security market enabled
  - All infrastructure channels opened and new standards supporting empowerment defined
- Regulation needs to change both to remove barriers and enable
  - Data retention, money-related, e-Identification etc. to accept dynamic Identity
  - Enforce a security split between infrastructure & transaction service providers
  - “Right to transact without identification” but with contextual restrictions
- Driver: No Direct Marketing based on personal data
  - DM based on subscription pull or intra-context push
- Driver: All new or changed Government services empowering
  - Legacy systems gets wrapped and gradually upgraded.

Digital Agenda Assembly 2012

Brussels, 21-22 June

You cannot solve problems with the thinking that created them
Albert Einstein

EUROPEAN PARLIAMENT

European Commission

European Economic and Social Committee

EUROPEAN UNION
Committee of the Regions

Extra slides

For those not present at the workshop,

I have included some additional information.

You might also want to check these links

http://digitaliser.dk/resource/896495

http://www.worldofends.com/

http://googleopoly.net/

http://www.ambafrance-dk.org/spip.php?article3558

http://www.credentica.com/the_mit_pressbook.html

http://www.hydramiddleware.eu/downloads.php?cat_id=2&download_id=48

Trust

The defining characteristic of the untrustworthy

- They try to build trust

The trustworthy don't consider trust

- They avoid creating risks

Intellectuals solve problems; geniuses prevent them.

Albert Einstein

To preserve Data Protection

we need to kill the dichotomy

Difficult choice?

If citizen are identified,

- citizens and counterparts become targets
- no way to secure data or cloud – consent or not
- no way to revoke data in a trustworthy manor
- rapidly escalating identity thef
- no way to know if data are abused
- commercial counterpart are not free to share
  - and if he do, he cannot be secure (intermediation)
- i.e. we cannot build trust even when not sharing data

If citizen are not identified,

- extremely hard to attack the citizen or the counterpart
  - you cannot attack what you cannot target
- no identity theft
- opt-in is implicit, opt-out is guaranteed
- citizen are in control if re-use is in line with consent
- even cloud is secure
- commercial counterpart are free to share
  - and if he do, he is secure
- i.e. trust is almost ensured even when sharing data.

Empowerment begins when

When citizens have CONTROL

- When citizens are exclusively able to link non-related transactions
- When historic data can only reused by the citizens
- When processes are subjected to minimum disclosure

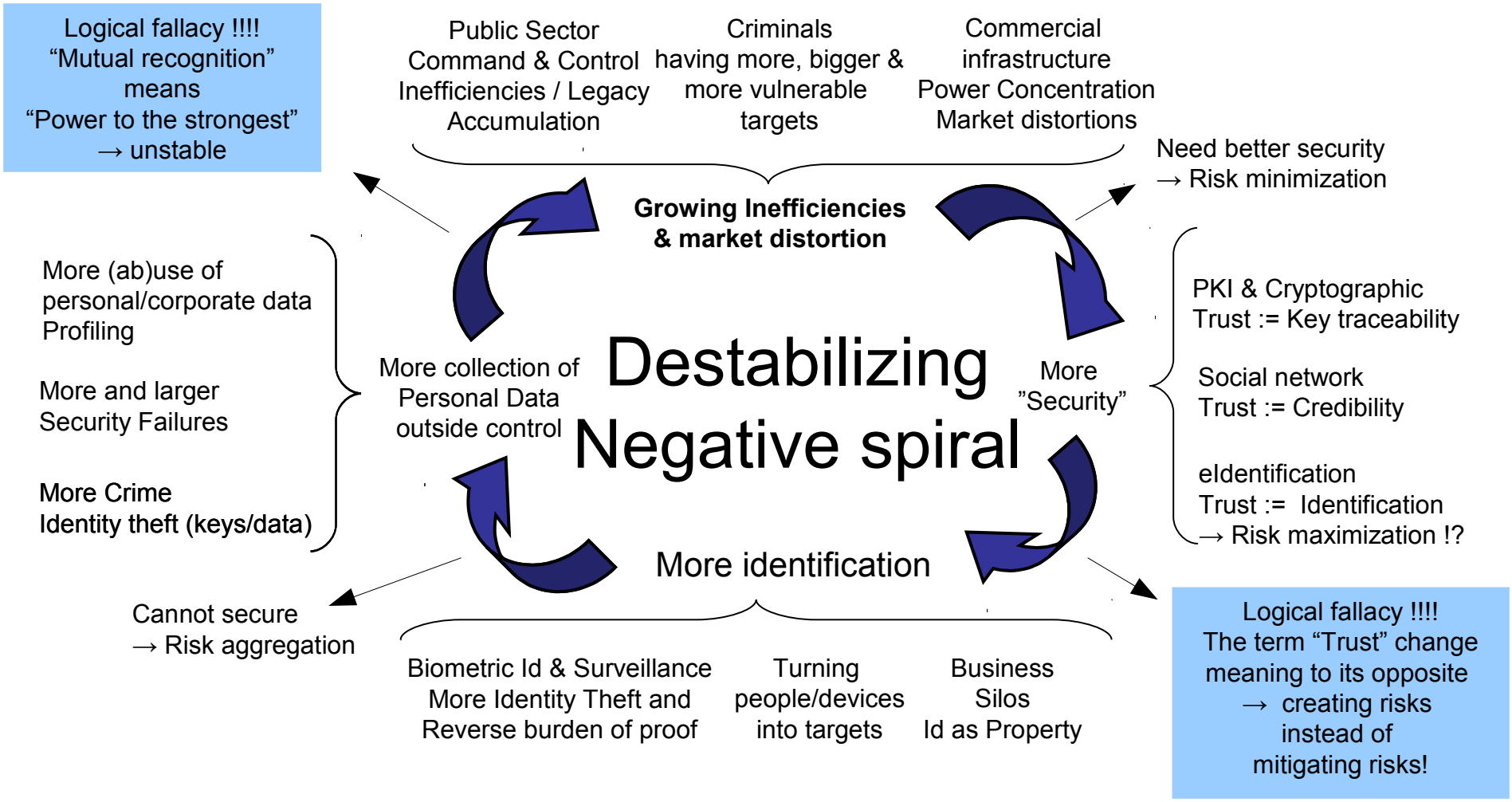
When they can CHOSE

- When regulation or standards don't dictate solutions
- When interfaces are semantically interoperable for new solutions

When they can ACT and TRANSACT

- When you can sign an agreement without identifying
- When you can pay, communicate, trade etc. without linking

When they are able/capable

- When they have the tools and rights to use them
- When they understand they implications

Identification destroy trust !