Covid-19 – the perfect Privacy by Design case
Trustworthy Anonymity as business enabler

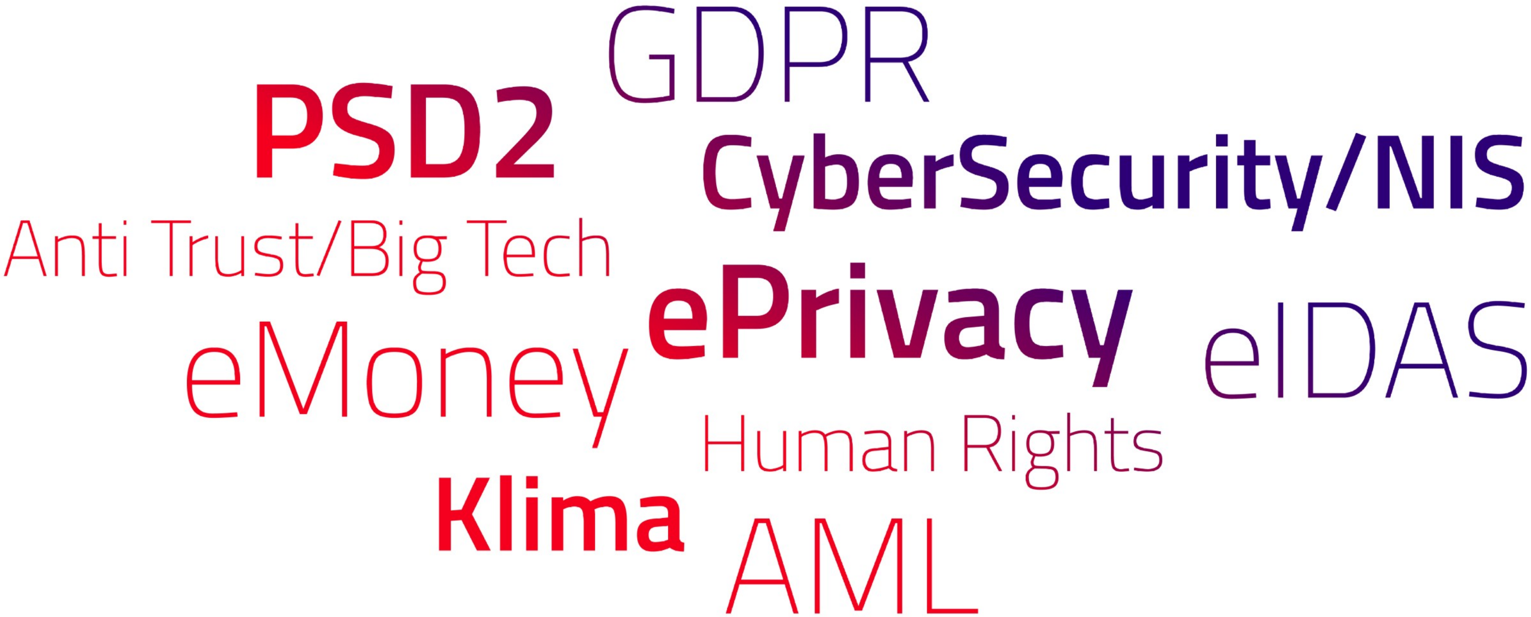
CitizenKey

Fast roll-out, then upgrade

Stephan Engberg, CitizenKey

Many new complex regulation packages

addressing different objectives with apparently inconsistent means
create very complicated operational challenges



The result:
Often leads to ends justifying destructive means with negative externalities that exceed the benefits

GDPR article 25

Data protection by design and by default

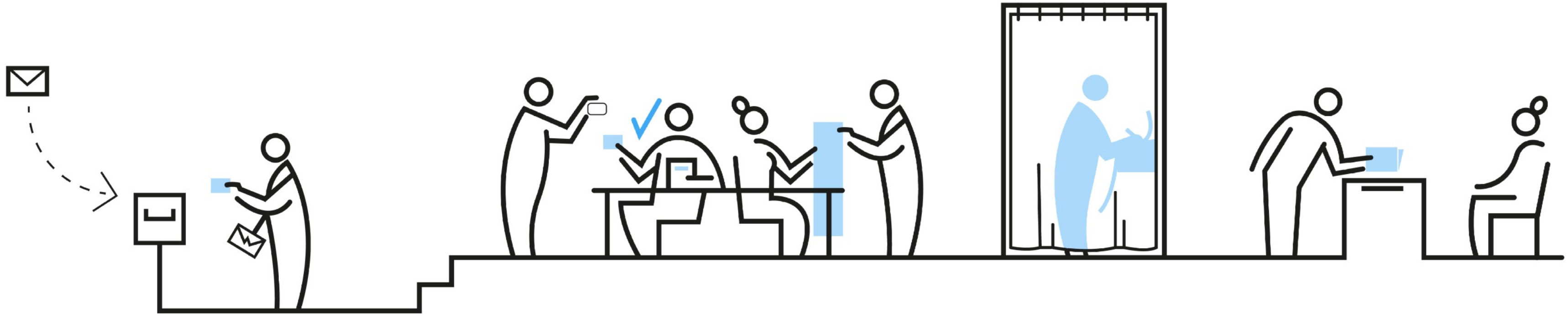
1. **Taking into account the state of the art**, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, **the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation**, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. **The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected**, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Data minimization according to state-of-the-art means:

If you can solve an otherwise legitimate need for data without collecting personal data, you are not allowed to collect personal data !

Elections / Paper ballots – Trustworthy Anonymity in real life



Definitions

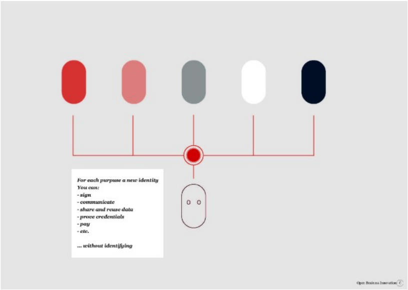
CitizenKey	eIDAS	GDPR
Not Trustworthy Identified in infrastructure Trusted (e.g identified to Appl) Hybrid (mixed, with delegation) Identified	Digital Signature Identification	Data protection by Design Pseudonymized Anonymized Identified
Not Identified Security by Design* Trustworthy Secure Accountable	Identification eID Pseudonymous Signature **) Identification	Identifiable ?? Undefined grey zone ”Not identified but identifiable” Identifiable
Not Accountable Privacy by Design* Trustworthy Anonymous	Identification eID Pseudonymous Signature **) or Not defined under eIDAS/eID	Not Identifiable Anonymous, not covered by GDPR

*) Terminology not defined in GDPR

**) Defined by member states in eIDAS

CitizenKey Five-factor Security

Factor	Basic	Extended
1. Something you are	Biometrics	
2. Something you have	Hardware	
3. Something you know	Password	
4. Purpose-specific keys & identifiers	Zero reuse of keys	Redefines the three first factors
5. Contextual isolation & Customization	Trustworthy spaces	Multi-party Security resolution & data sharing without collecting personal data


For each purpuse a new identity
You can:
- sign
- communicate
- share and reuse data
- prove credentials
- pay
- etc.

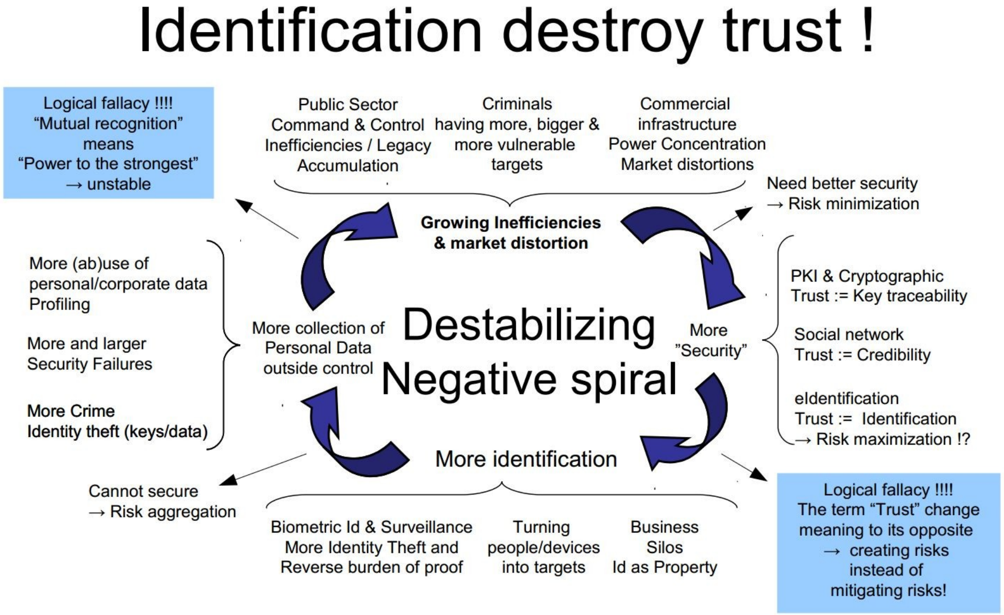
... without identifying

2002: IST Living with Security

”We face an existential choice”

Negative Spiral

Positive Spiral



Identification destroy trust !

Logical fallacy !!!!
“Mutual recognition”
means
“Power to the strongest”
→ unstable

Public Sector
Command & Control
Inefficiencies / Legacy
Accumulation

Criminals
having more, bigger &
more vulnerable
targets

Commercial
infrastructure
Power Concentration
Market distortions

Need better security
→ Risk minimization

Growing Inefficiencies
& market distortion

More (ab)use of
personal/corporate data
Profiling

More and larger
Security Failures

More Crime
Identity theft (keys/data)

More collection of
Personal Data
outside control

Destabilizing
Negative spiral

More
”Security”

PKI & Cryptographic
Trust := Key traceability

Social network
Trust := Credibility

eIdentification
Trust := Identification
→ Risk maximization !?

More identification

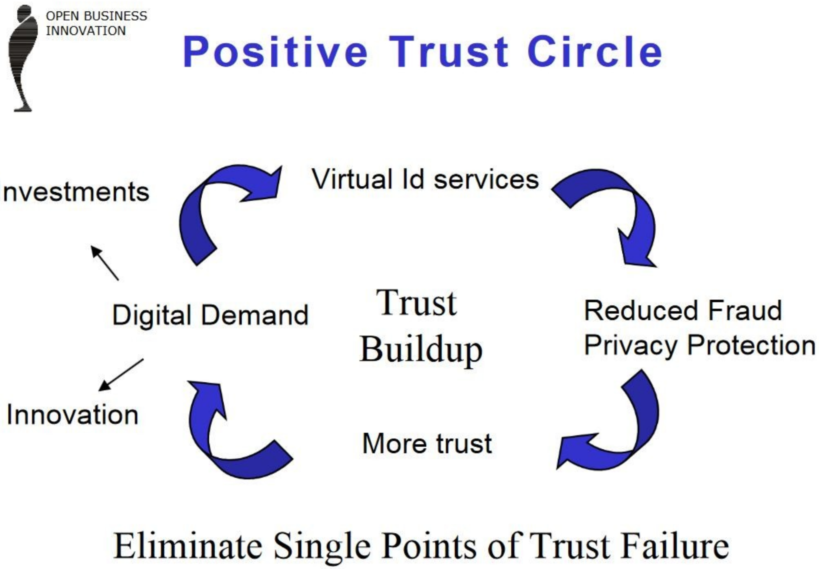
Cannot secure
→ Risk aggregation

Biometric Id & Surveillance
More Identity Theft and
Reverse burden of proof

Turning
people/devices
into targets

Business
Silos
Id as Property

Logical fallacy !!!!
The term “Trust” change
meaning to its opposite
→ creating risks
instead of
mitigating risks!



Positive Trust Circle

Investments

Virtual Id services

Digital Demand

Trust
Buildup

Reduced Fraud
Privacy Protection

Innovation

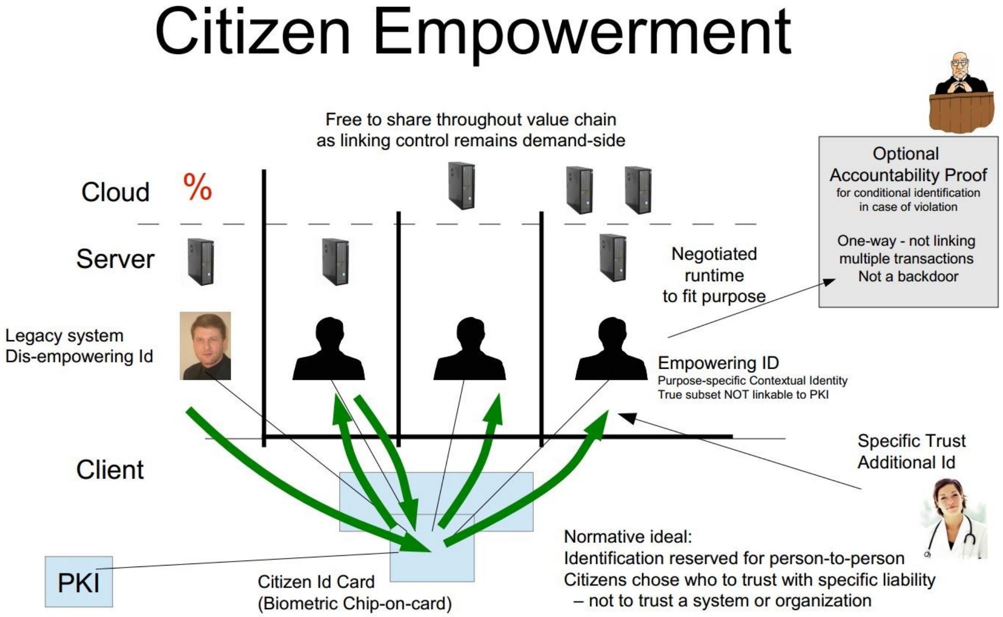
More trust

Eliminate Single Points of Trust Failure

Citizen is a product and object for control

Empowered Citizens are main change agents

2012: EU Digital Agenda
BigData → SmallData



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

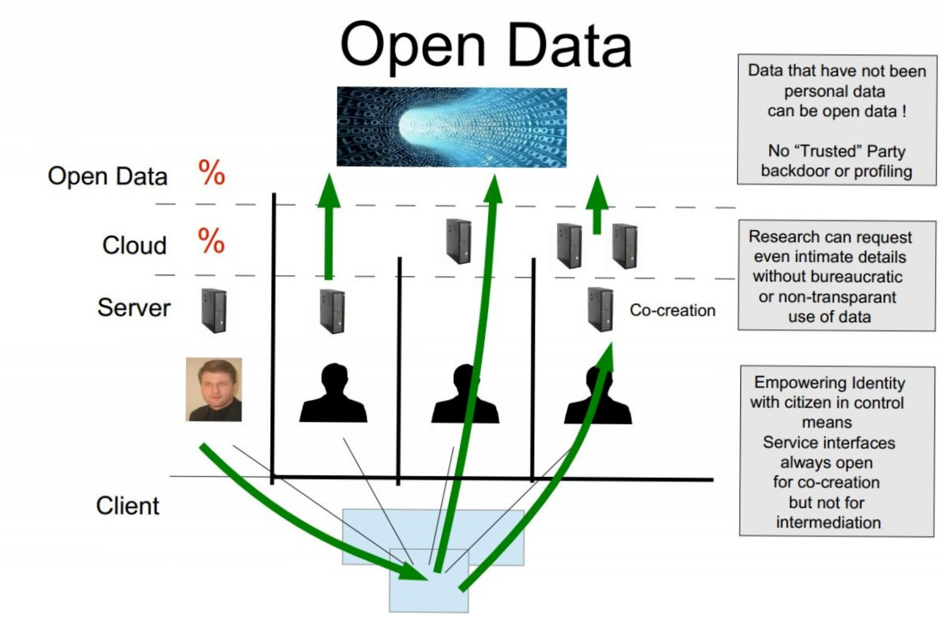
Specific Trust
Additional Id

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



Open Data

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

No “Trusted” Party
backdoor or profiling

Open Data %

Cloud %

Server

Co-creation

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

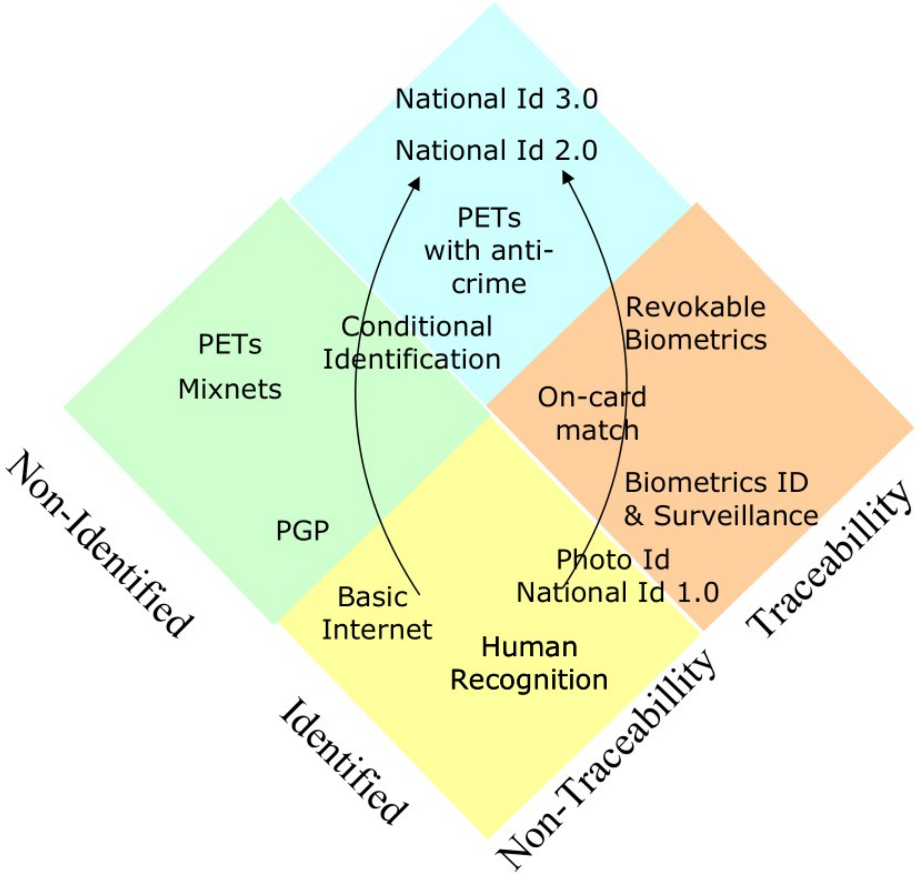
Client

Key control NOT in Smartpones – separate dedicated devices

Priway Identity Model
Roadmap to PETs & Biometrics

PRIWAY
Security in Context

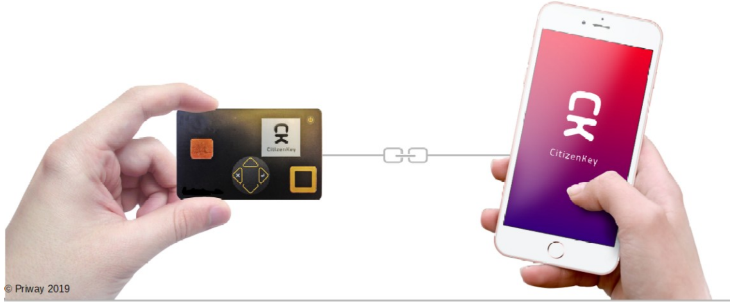
Security for Individual & System



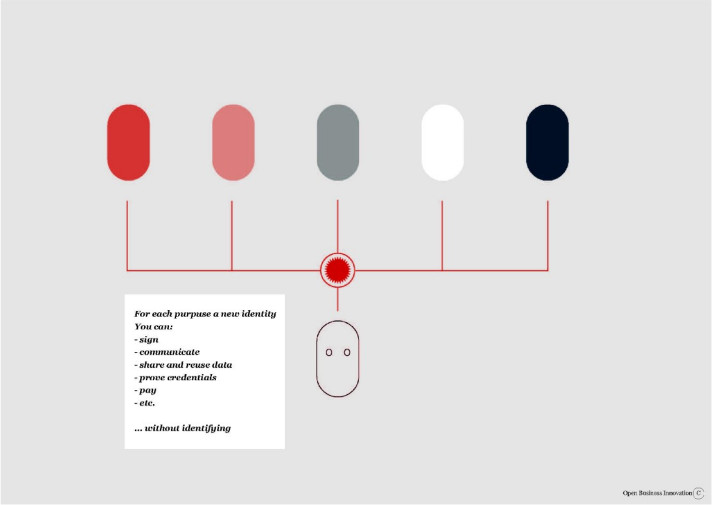
Security against Citizen

© Priway, Maj, 2009 6

Trustworthy COVID-19 data sharing



© Priway 2019



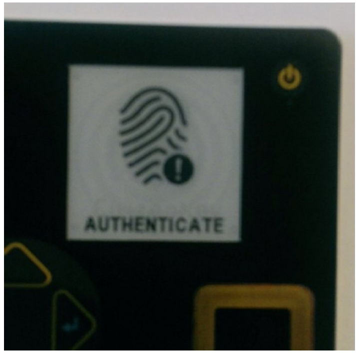
For each purpose a new identity
You can:
- sign
- communicate
- share and reuse data
- prove credentials
- pay
- etc.

... without identifying

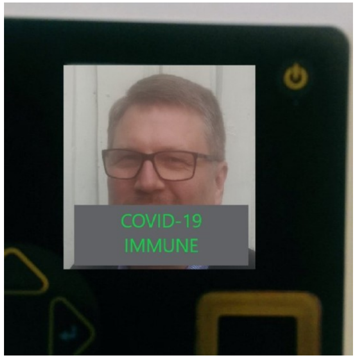
Open Business Innovation

Lab issue
Test results

Trustworthy Identity



On-card visual status



Digital integration

Enabled
Society
Service

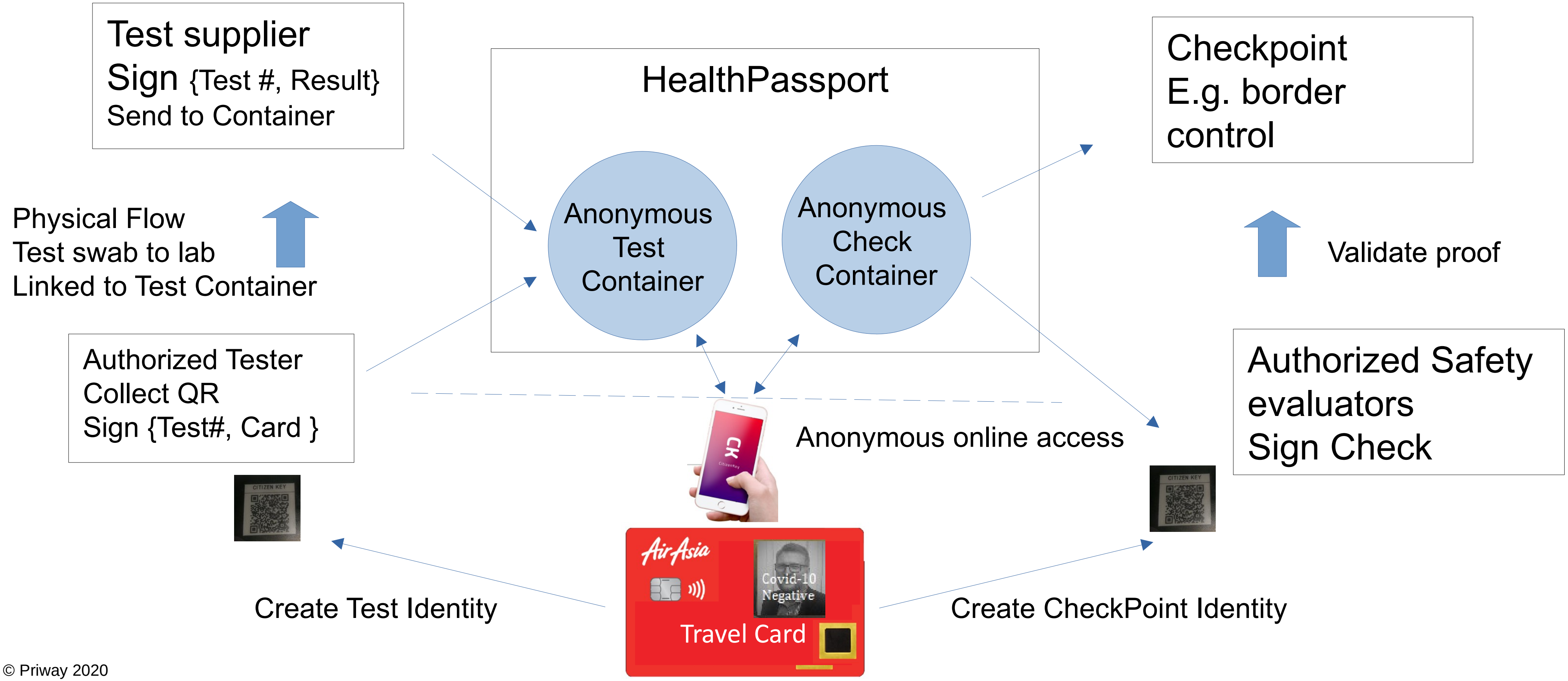
Untested assumptions
prevent problem solution !

Council of Europe
DIGITAL SOLUTIONS TO FIGHT COVID-19 (Oct 12)

”Regardless of the type of test used (viral or antibody) mandatory testing is a highly invasive measure as it involves the use of biometric samples to detect the health status of individuals.”

https://www.coe.int/en/web/portal/-/digital-solutions-to-fight-covid-19-shortcomings-protecting-privacy-and-personal-data

CitizenKey Health Passport



Test supplier
Sign {Test #, Result}
Send to Container

HealthPassport

Anonymous Test Container

Anonymous Check Container

Checkpoint
E.g. border control

Physical Flow
Test swab to lab
Linked to Test Container

Validate proof

Authorized Tester
Collect QR
Sign {Test#, Card }

Anonymous online access

Authorized Safety evaluators
Sign Check

Create Test Identity

Create CheckPoint Identity

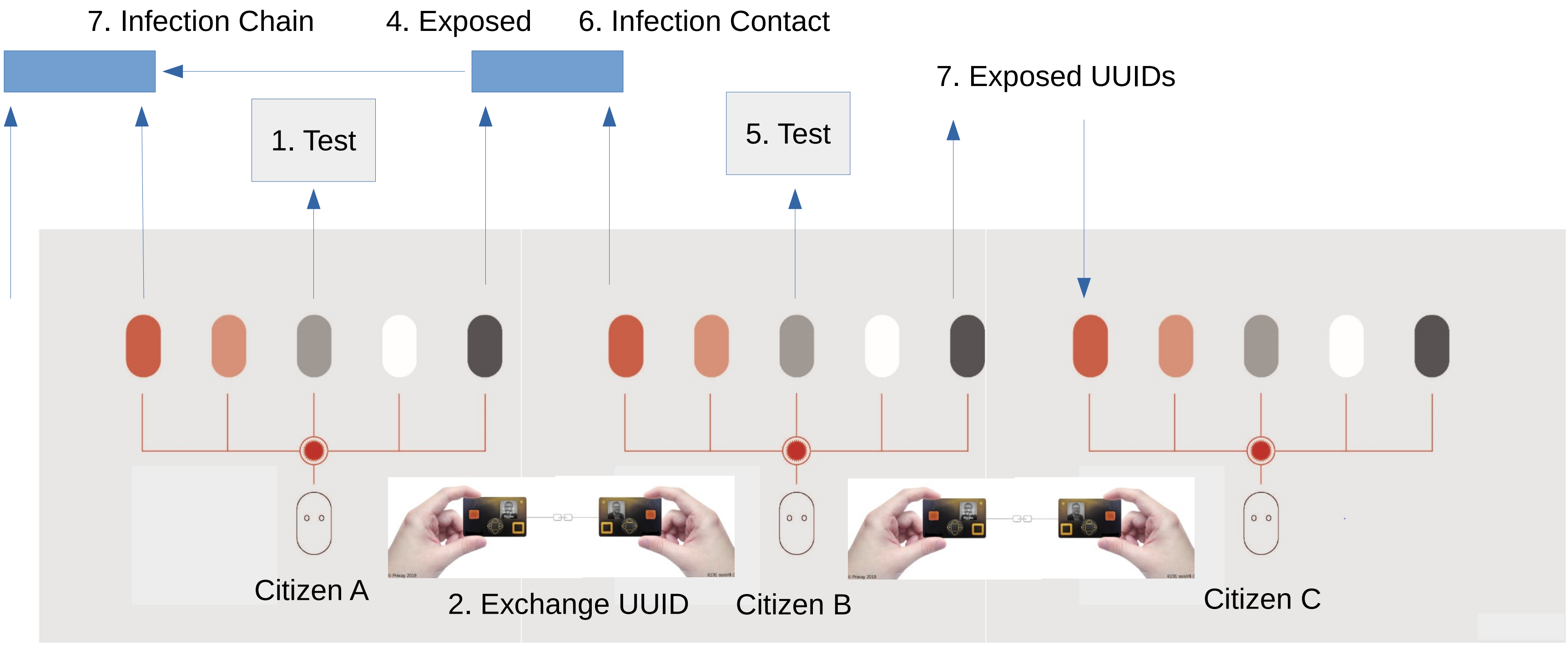
Covid-19

Trustworthy Anonymity as business enabler

- Before Covid-19 we were trying to bring security to Healthcare – research, telemedicine, Trustworthy AI, personal medicine, wearables etc.
- With pandemics we need to bring sensitive health data to security !

	Identified	Trustworthy Anonymous
Data collection	Any testing is collecting DNA, proteins etc.	Main sensitivity problem resolved More testing, more test providers
Data usage	Weak identity → Fraud All checkpoints leak personal data -> resistance & breach. GDPR restrictions	Strong identity → No personal data at Checkpoints – Trustworthy sharing, secure, non-restrictive compliance
Interoperability	Locked to identity model, typical national health infrastructure focus on treatment.	Open model - N:M reuse Citizen “carry” data and proof Citizen can enable secondary use

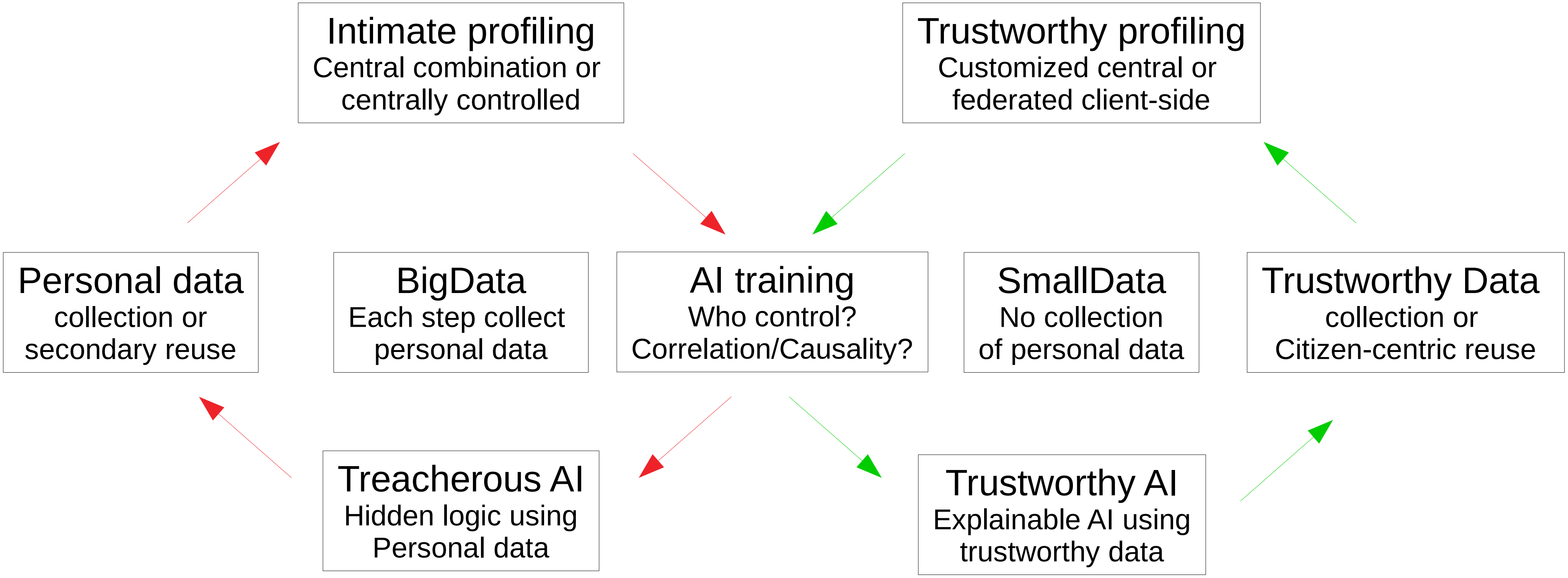
Trustworthy Anomym Covid-19



3. Exchange Health Status i local groups
Mitgate exposure realtime

BigData AI vs. SmallData AI

Negative vs. positive circle



Intimate profiling
Central combination or
centrally controlled

Trustworthy profiling
Customized central or
federated client-side

Personal data
collection or
secondary reuse

BigData
Each step collect
personal data

AI training
Who control?
Correlation/Causality?

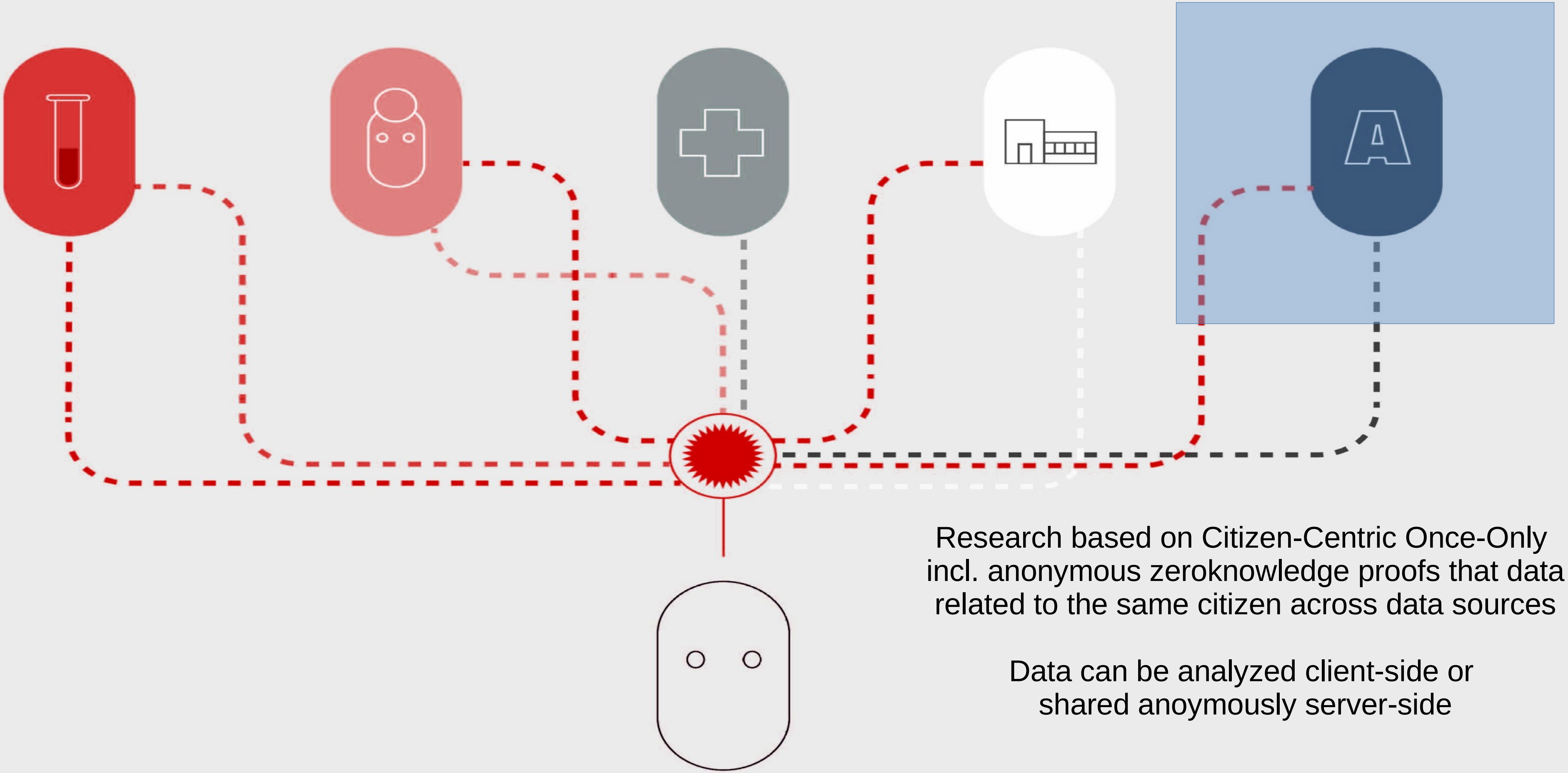
SmallData
No collection
of personal data

Trustworthy Data
collection or
Citizen-centric reuse

Treacherous AI
Hidden logic using
Personal data

Trustworthy AI
Explainable AI using
trustworthy data

SmallData Research Basic



Research based on Citizen-Centric Once-Only incl. anonymous zeroknowledge proofs that data related to the same citizen across data sources

Data can be analyzed client-side or shared anoymously server-side

What did we miss in the first wave?

Issue	Consequence
Trustworthy Anonymous Test	Many resist testing, all testdata vulnerable
Activate the wireless space	Distance resolution pre-infection – e.g. hospitals, Care
Anonymous Contact Points	Privacy by Design support for remembering contacts between strangers (Events, locations etc.)
Proximity testing	Focus was on Central vs. Decentral (smartphone)→BigTech in control Overfocus on distance measurement and time. Better → Dedicated devices so no access to keys
Distributed Infection trace	The focus on Google/Apple decentralized meant we did not enable citizens self-tracing (manual trace on top if needed – not ONLY). E.g. scanning Personal Social network much faster Anonymous Contact Points help Citizens self-trace - scalable
Full Chain support	Need to lean the full chain
SmallData Research	Trustworthy datasharing enable learning without negative spiral

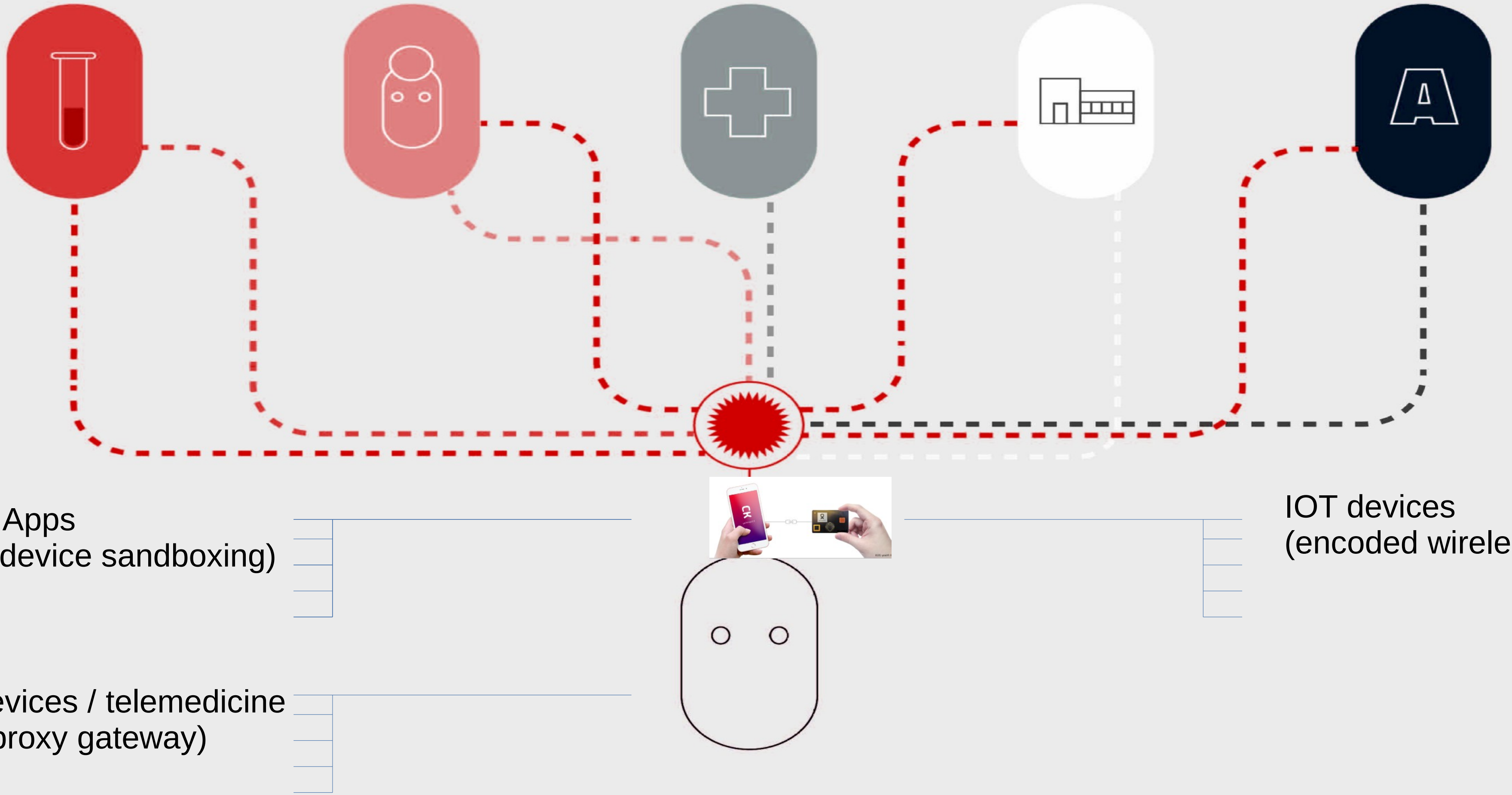
Testing

Treatment
Doctor

Diagnosis
(recruiting clinical trials)

Effects / Sideeffects
(clinical databases)

Treatment
Feedback Loop



Client Apps
(Intra-device sandboxing)

IOT devices / telemedicine
(LAN proxy gateway)

IOT devices
(encoded wireless comm)

EU Digital Strategy

19. februar 2020

An open, democratic and sustainable society: **A trustworthy environment in which citizens are empowered in how they act and interact, and of the data they provide both online and offline.** A European way to digital transformation which enhances our democratic values, respects our fundamental rights, and contributes to a sustainable, climate-neutral and resource-efficient economy.

The **potential of Article 20 of the GDPR to enable novel data flows and foster competition** is recognised in reports for the Commission and Member State governments, not limited to the EU. Yet, as a result of its design to enable switching of service providers **rather than enabling data reuse in digital ecosystems the right has practical limitations.**

These pools may be organised in a centralised or a **distributed way**

In the latter case **the data are not moved to a central place in order to analyse them together** with other data assets. **The analytical tools come to the data, not the other way around. This makes it easier to keep the data secure and to ensure control over who accesses what data for what purposes.**

Secure and universally usable **digital identities are also crucial to enabling individuals' access to and control over their data**.

Trustworthy

Strategic Advisory Board
EU FP7 Security Research Roadmapping

Trustworthy computing: synonymous with "secure and dependable computing."

Dependability: is the ability to avoid failures that are more frequent or more severe than is acceptable.

Trust: accepted dependence.

Dependence: the dependence of system A on system B is the extent to which system A's dependability and security is (or would be) affected by that of System B.

Thus system A:

- **is totally independent of System B if it cannot be affected in any way by System B and its failures** - as well as
- is totally dependent on System B if:
    i. any failure of B causes A to fail, and
    ii. A has no other failures.

Trustworthy Computing

involves absense of dependence
so trust is not even relevant

”Non-interdependence”

”Perimeter security is failing - we have to move to security paradigms based on Security by Design.”

Action points

We missed the first wave for the same reasons Europe has been failing in digital.
GDPR is not about “data protection” but about empowering citizens.
eIDAS is not about Digital Identification, but creating legal structure and digital framework

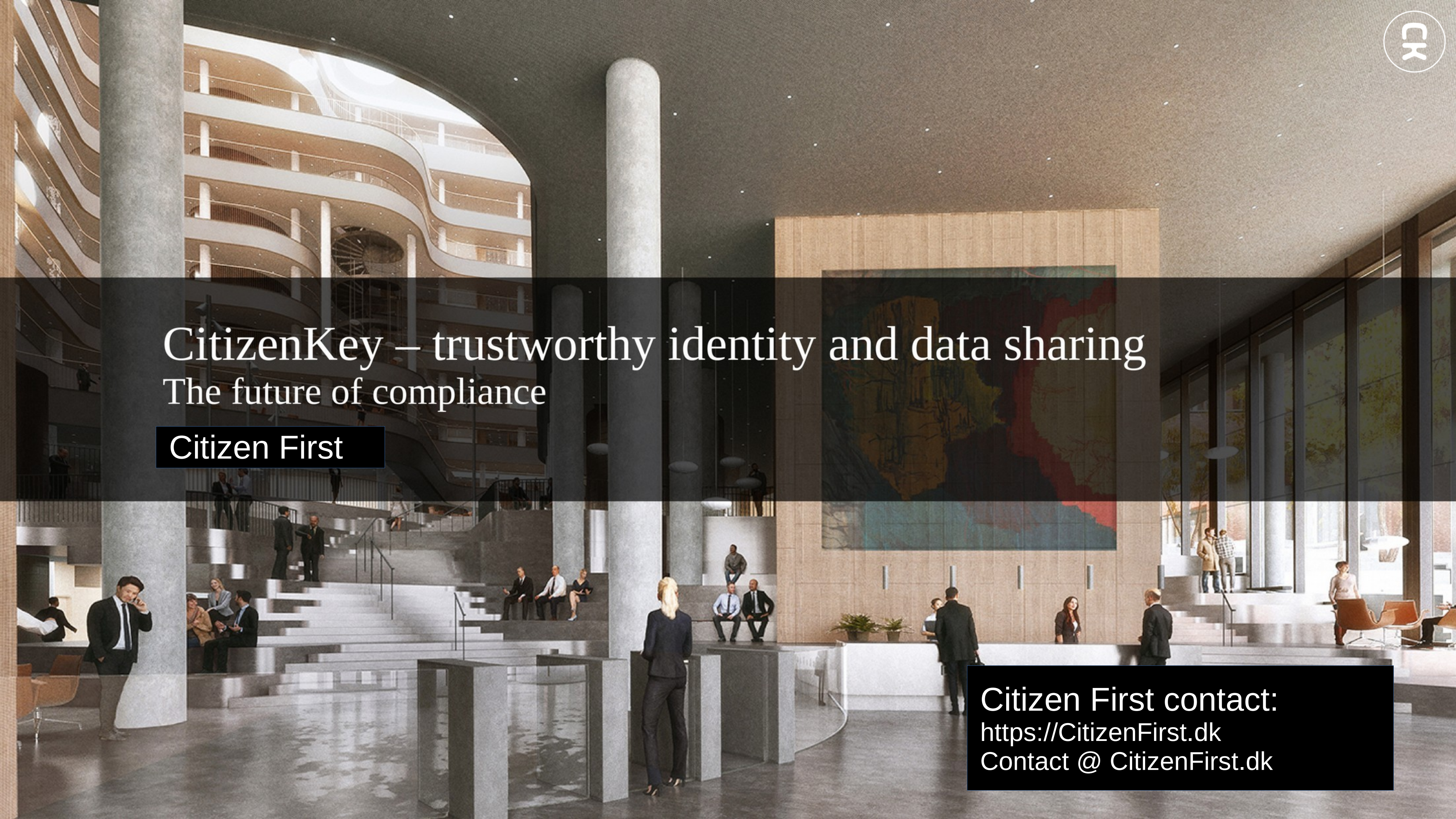
Real test – can citizens get an anonymous test that support operational reopening?
Providing platform for upgrade to Trustworthy Identity for market and democratic recovery

CitizenKey Classic

- Trustworthy Anonymity for Covid-19
  - Global non-profit based in Denmark
- Interim model for fast roll-out
- Gradual upgrade to full model

CitizenKey

- Trustworthy Identity
- Trustworthy Data sharing
- Gradual transformation
- General purpose always customized to context and national jurisdiction/structure



CitizenKey – trustworthy identity and data sharing

The future of compliance

Citizen First

Citizen First contact:
https://CitizenFirst.dk
Contact @ CitizenFirst.dk