Make trustworthy design so data don’t need protection

Aligning eIDAS and GDPR with Trustworthy PKI - the state-of-the-art data minimization requirements to eID / Identity

Stephan Engberg
Priway / CitizenKey
Trustworthy Anonymity is the ansvar

- With Trustworthy PKI, Trustworthy Anonymity is state-of-the-art
- Digital Society works (much better) trustworthy anonymous
- The legal requirement is already in place

Trustworthy = “when you do not need to trust”

Trustworthy :: Non-interdependence
Trustworthy Anonymity is legally required

GDPR main focus is not “data protection”. It is “data minimization according to state-of-the-art” *)

Legal obligation to pursue data minimization in design does not stop until data are Trustworthy Anonymous

In eIDAS, Qualified Pseudonym Signatures are already subset of ”Identification”

*) GDPR article 5.1.C, 25 and 32, Directive on Law Enforcement Article 20, eIDAS art 5 and 24
No need for state or corporate surveillance…

State
eIDAS PKI (Server)
• Trusted Qualified Signatures
• Single Sign-On
• Server-side biometrics

Corporate
Smartphone (BigTech)
• Secure Enclave
• On-phone biometrics
• FIDO (Google Analytics of Id)
• Bad 5G standard (“Trustpid”)
We need Trustworthy PKI

The essence of Trustworthy PKI:
Citizens create and certify new Trustworthy Anonymous Signatures inside a Trustworthy QSCD*) and then customize identity to purpose.
No trusted party.

Within existing standards = already state-of-the-art

Trustworthy QSCD
On-card biometrics
On-card display incl. physical verification
On-card authorization
Can support multiple certification keys
Do not leak identifiers – zero reuse

*) QSCD – Qualified Signature Creation Device – standardized part of eIDAS / ETSI PKI and subject to approval
Case: EU-Login to bootstrap eID must carry

Start as a biometric FIDO-device
This is enrolled as a Trusted Key (as is)

Then you upgrade EU-Login to Trustworthy PKI
Citizen use the EU-Login to create a new identity and verify breeder documents in person. Get a proof e.g. Social Identity. The QSCD verify social identity (but not biometrics) to EU-Login to upgrade assurance.

Ready for Trustworthy Remote On-boarding
Trustworthy PKI extend and works the same as normal Trusted PKI – except no trusted party or backdoor

Identity bootstrap from available and identity integrity grow over time

1. Trustworthy QSCD create key pair
   Get a Root Digital Signature from CA
   You enroll As you would today
   Best effort identity – no change

2. CA return Root Signature Certificate and a shortlived CA Certification key to QSCD

3. QSCD create and certify new Trustworthy Signature
   QSCD create a non-repudiation proof as cross-signing with Digital Signature

4. Non-repudiation Proof is encrypted according to context and shared with other certified data/proofs.
   QCSD as witness in signed XML

Trustworthy Anonymous Qualified Signature

Trustworthy Qualified Signature Customized to context
Case 1: eMobility
(local Trustworthy PKI)
Problems that can be solved with Trustworthy PKI

- ePrivacy/cookies
- Anti-crime / Data Retention – Article 20
- Once Only
- Schrems II
- Anonymous access to political content / legal sentences
- Digital Cash with AML compliance
- Offline identity, credentials and payments.
- Schengen – anonymous check for citizenship/fugitives/asylem
- AML/Privacy in blockchain
- Anonymous data research / AI training
SECURITY
SURVEILLANCE
COMPLIANCE
ANONYMITY
PRIVACY
(citizen security)

SECURITY BY DESIGN
ALLMOST ALL SOCIETY WORK BETTER TRUSTWORTHY

Trustworthy Secure
(Trustworthy Accountability)
Freedom with Accountability

Trustworthy Hybrid
(Intimate sharing with proof)
Patient send datalink to doctor
Citizens share with social group
Citizens share with self / guardian

Trustworthy Restrictions
(Inddirect proof/commitments)
Schengen
Finance KYC/AML
Taxation

Trustworthy Anonymous
(Consentual anonymity)
Elections
Data research/AI training
Searches / access content

SECURITY
SURVEILLANCE
COMPLIANCE
ANONYMITY
PRIVACY (citizen security)
**eIDAS & GDPR already in place**
**Trustworthy PKI re-focus to solve the problems**

<table>
<thead>
<tr>
<th></th>
<th>eIDAS</th>
<th>GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Today</strong></td>
<td>Focus on Trusted or linked identity. Always generate PII</td>
<td>GDPR professionals focus on ”data protection”</td>
</tr>
<tr>
<td><strong>Change</strong></td>
<td>eIDAS/EDPB incorporate Trustworthy Anonymity as ”must-carry” in eID and infrastructure</td>
<td>With Trustworthy PKI, Trustworthy Anonymity with/without Accountability become state-of-the-art requirement</td>
</tr>
<tr>
<td><strong>Tomorrow</strong></td>
<td>Trustworthy security align and upgrade CyberSecurity, Privacy, Compliance and set data free</td>
<td>DPA / GDPR professionals prioritize ”maintaining anonymity” in applications</td>
</tr>
</tbody>
</table>
GDPR do not say citizen control over data is absolute
But secondary objectives used to justify destructive means

<table>
<thead>
<tr>
<th>Primary</th>
<th>Secondary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citizen Security</td>
<td>Law Enforcement</td>
</tr>
<tr>
<td>Citizen Choice</td>
<td>Learning &amp; Research</td>
</tr>
<tr>
<td>Citizen Rights</td>
<td>Taxation</td>
</tr>
<tr>
<td>Market ability to work / competition</td>
<td>Innovation/effectiveness</td>
</tr>
<tr>
<td>Democracy</td>
<td>Social cohesion / Environment</td>
</tr>
</tbody>
</table>

Barriers: Complexity, bad standards, commercial greed, bureaucratic command & control

With Trustworthy PKI, you can solve the secondary objectives Trustworthy anonymously
- even if the secondary objective is mandatory and appear to be in conflict

All the is needed for change is one citizen demanding his right for Trustworthy PKI
But EDPB and DPA need to enforce that right if they want GDPR and free movement to survive
Our own institutions are killing democracy
The case of Denmark

Always linkable Identified
100% Data Retention & BigData
MitID with serverside face recognition
Telco must force identification

Zero security
Mandatory central profiling
No attention to exponential damages

Secondary agenda drive collapse
Bureaucratic Command & Control
Surveillance Capitalism

.. Trustworthy PKI change that
Better solutions without eID Data Retention
Trustworthy Anonymity INSIDE eGov

---

Imagine a country that has...
- Health data that covers all areas of the health sector
- All data to be linked via a unique personal identification number
- High ethical standards and high level of data security
- Many different types of health data and a high degree of detailed data
- A big life science sector

- Unbiased health data on the entire Danish population from cradle to grave
- Health data and socioeconomic data of high quality
- World-class researchers and clinicians
- A structured process to get access to health data
- A range of data services to support you

---

...This is Denmark
CitizenKey - both a road to recovery and to start trustworthy

- CitizenKey is one implementation of Trustworthy PKI
- Main mission – enable Trustworthy Inclusive interoperability
- Role of CitizenKey – trustworthy security as an add-on
  - Acting as a backbone upgrading eID with Trustworthy QSCD / PKI
  - Workarounds to bad standards to maintain trustworthy anonymity
  - Each memberstate will have its own structure under local jurisdiction
  - Five-Factor Security – cybersecurity and compliance WITH privacy
  - Global Id → National Id interoperability → Market recovery
Case 2: Trustworthy PKI enable secondlevel “Wallet” or Agent
Example: Telemedicine IOT or hospitalization agent

Series of event across applications or over time

Alarm -> Response

IRMA, EBSI or other Agent

Data are trustworthy and permanent, but key control change / re-organized

© Priway ApS 2022