EPFL

Overview of eID landscape

Imad Aad
C4DT - EPFL

Center for Digital Trust

29/10/2024

Image credit: kiquebg, Pixabay

IDs going digital...

Why go digital, online?

Advantages of going digital, online: Money

Analog

Digital

Online

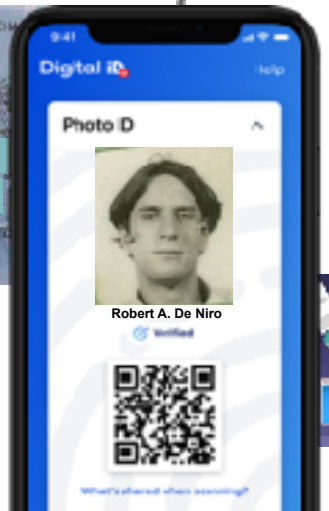
PayPal

TWINT

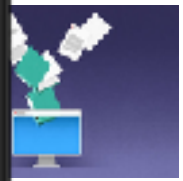
Alipay

Advantages of going digital, online: IDs

Analog

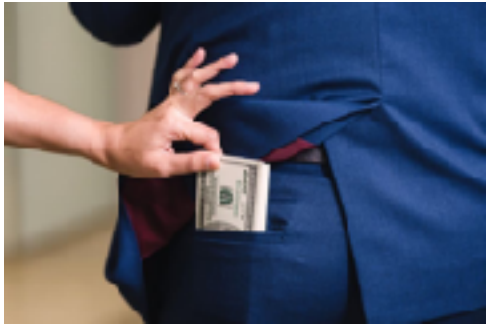


Online



Disadvantages of going online

Analog



Online

TRACES

Image credit: Thinkstock, Getty images

Going digital + online = success?

Among other factors:

- At the right place and at the right time...

  In the 80's: "Why do you need to carry a computer if you have cash?"
  vs.
  Nowadays: "Why do you need to carry cash if you have a smartphone?"

- Simplicity / usability / better government service delivery

- Economic and development potentials

- **Trust** (the system, data protection, no / less fraud)

- **Interoperability**

Outline

- Why go digital?
- Trust x eIDs
- Interoperability x eIDs
- The Swiss eID

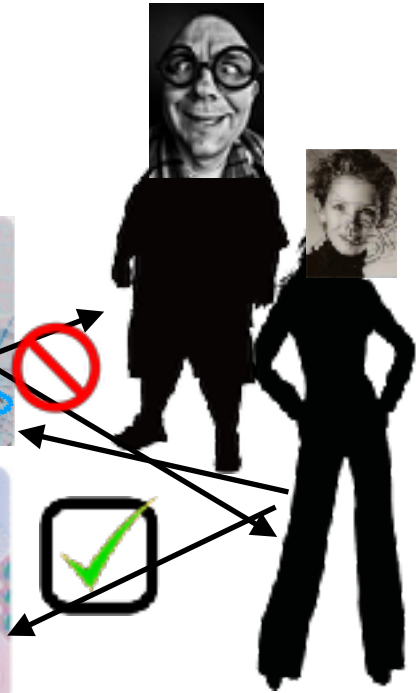
IDs, eIDs... what's the trust model behind?

Physical ID cards

What are their properties and functions?

Her rights

Tamper proof



Obligations

Guarantees

UBS

Certified

Electronic identifiers: ID Provider (IDP)

Certified

!! privacy concerns!!

alexandra.musterfrau@gmail.com
5.10.1982

Her rights

digitec.ch

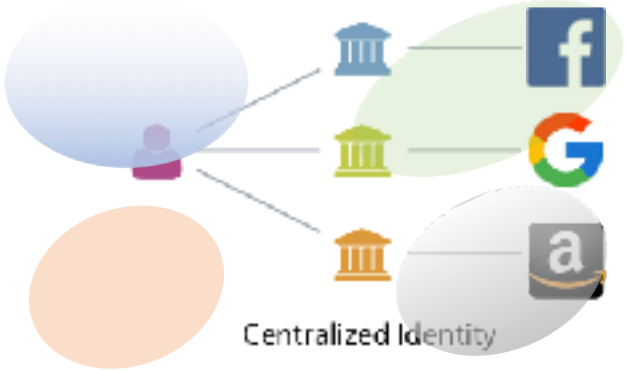
coop

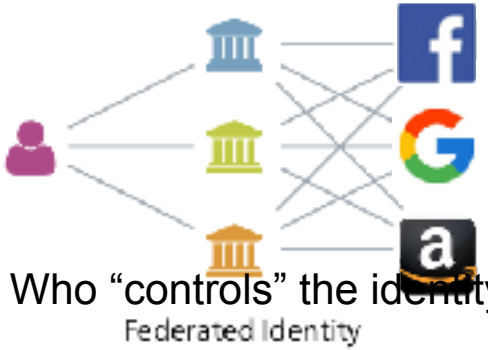
Obligations

Guarantees

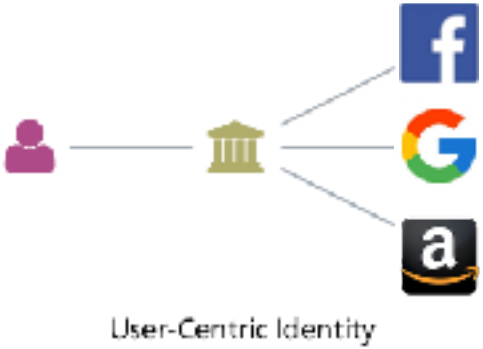
UBS

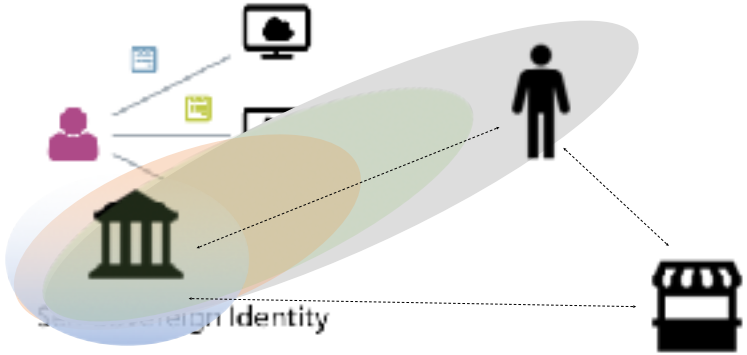
Types of digital identities





Who “controls” the identity and its attributes?

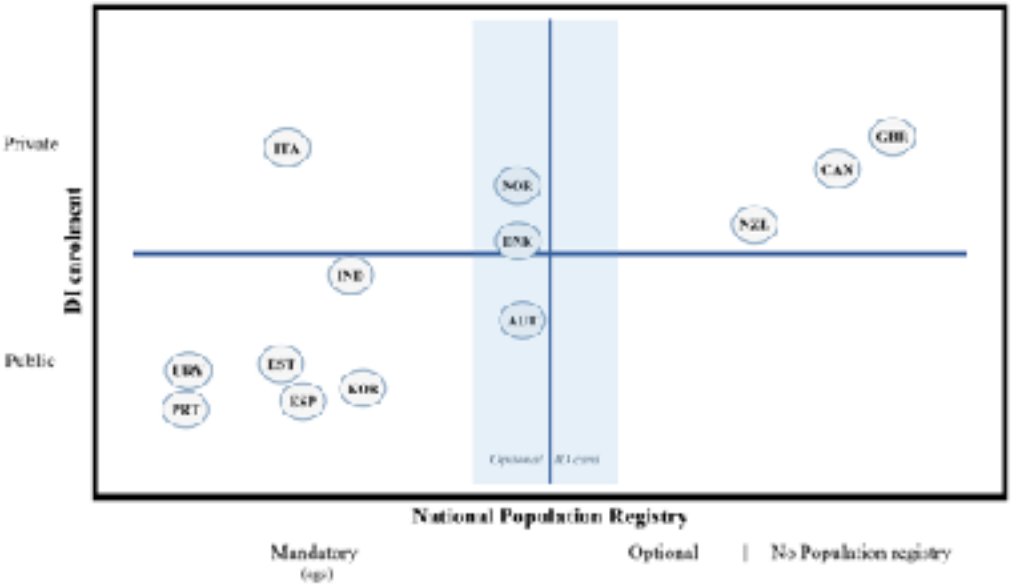




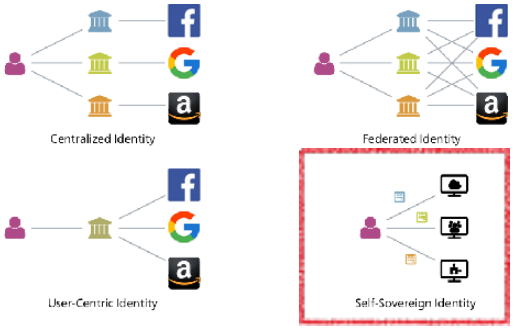
Verifier
Verifiers

OECD Digital Government Studies Digital Government in Chile – Digital Identity

Figure 2.1. Digital ID enrolment and National Population Registers



Self-Sovereign Identities, SSI



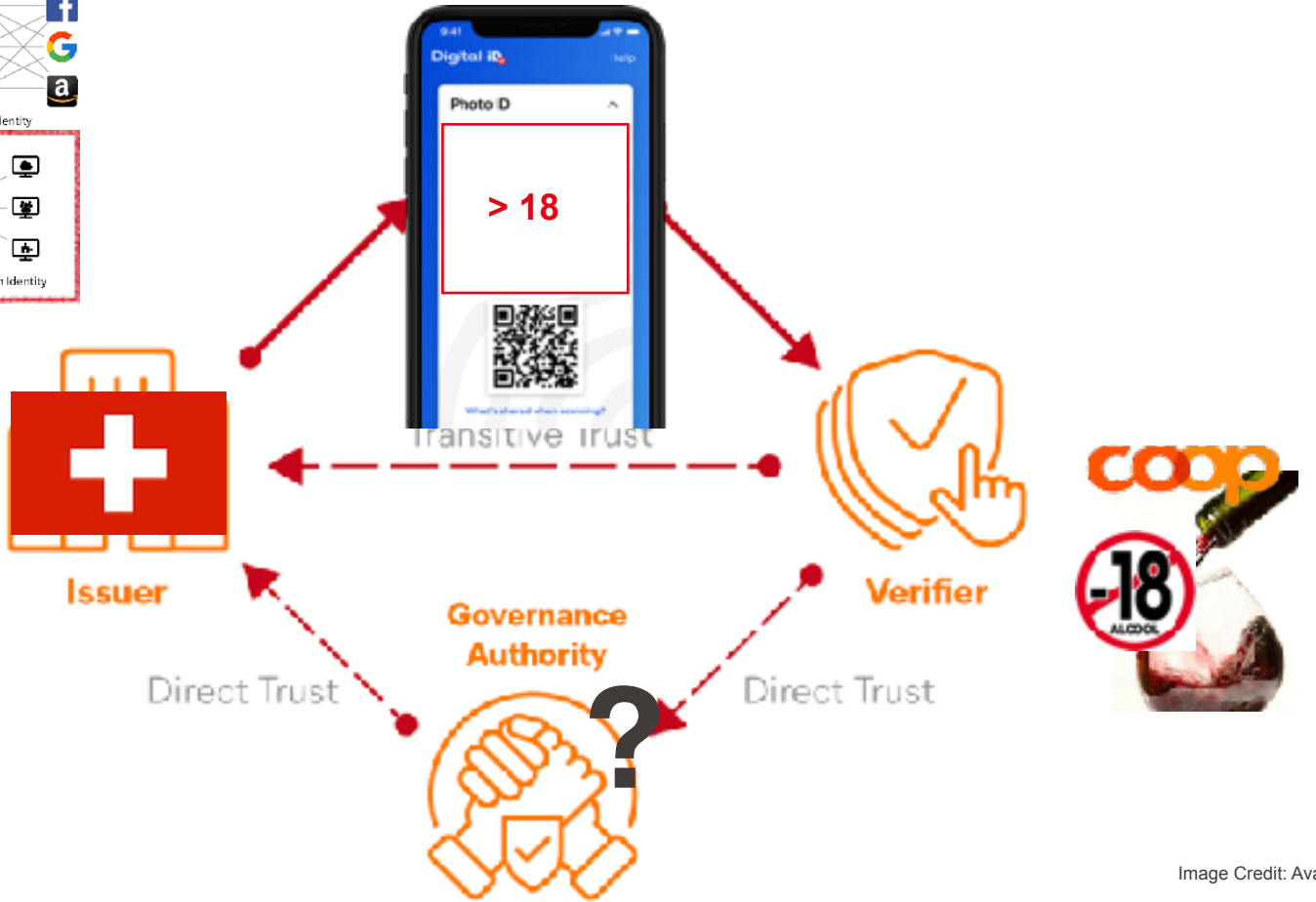


Image Credit: Avast

Self Sovereign IDs, SSI principles

1. **Representation:** An SSI ecosystem shall provide the means for any entity—human, legal, natural, physical or digital—to be represented by any number of digital identities.

2. **Interoperability:** An SSI ecosystem shall enable digital identity data for an entity to be represented, exchanged, secured, protected, and verified interoperably using open, public, and royalty-free standards.

3. **Decentralization:** An SSI ecosystem shall not require reliance on a centralized system to represent, control, or verify an entity's digital identity data.

4. **Control & Agency:** An SSI ecosystem shall empower entities who have natural, human, or legal rights in relation to their identity ("Identity Rights Holders") to control usage of their digital identity data and exert this control by employing and/or delegating to agents and guardians of their choice, including individuals, organizations, devices, and software.

5. **Participation:** An SSI ecosystem shall not require an identity rights holder to participate.

6. **Equity and Inclusion:** An SSI ecosystem shall not exclude or discriminate against identity rights holders within its governance scope.

7. **Usability, Accessibility, and Consistency:** An SSI ecosystem shall maximize usability and accessibility of agents and other SSI components for identity rights holders, including consistency of user experience.

8. **Portability:** An SSI ecosystem shall not restrict the ability of identity rights holders to move or transfer a copy of their digital identity data to the agents or systems of their choice.

9. **Security:** An SSI ecosystem shall empower identity rights holders to secure their digital identity data at rest and in motion, to control their own identifiers and encryption keys, and to employ end-to-end encryption for all interactions.

10. **Verifiability and Authenticity:** An SSI ecosystem shall empower identity rights holders to provide verifiable proof of the authenticity of their digital identity data.

11. **Privacy and Minimal Disclosure:** An SSI ecosystem shall empower identity rights holders to protect the privacy of their digital identity data and to **share the minimum digital identity data required for any particular interaction**.

12. **Transparency:** An SSI ecosystem shall empower identity rights holders and all other stakeholders to easily access and verify information necessary to understand the incentives, rules, policies, and algorithms under which agents and other components of SSI ecosystems operate.

Cryptography Basics

Why do we need encryption?

- CIA
  - Confidentiality
  - Integrity
  - Availability
- +
  - Authentication
  - Non-Repudiation

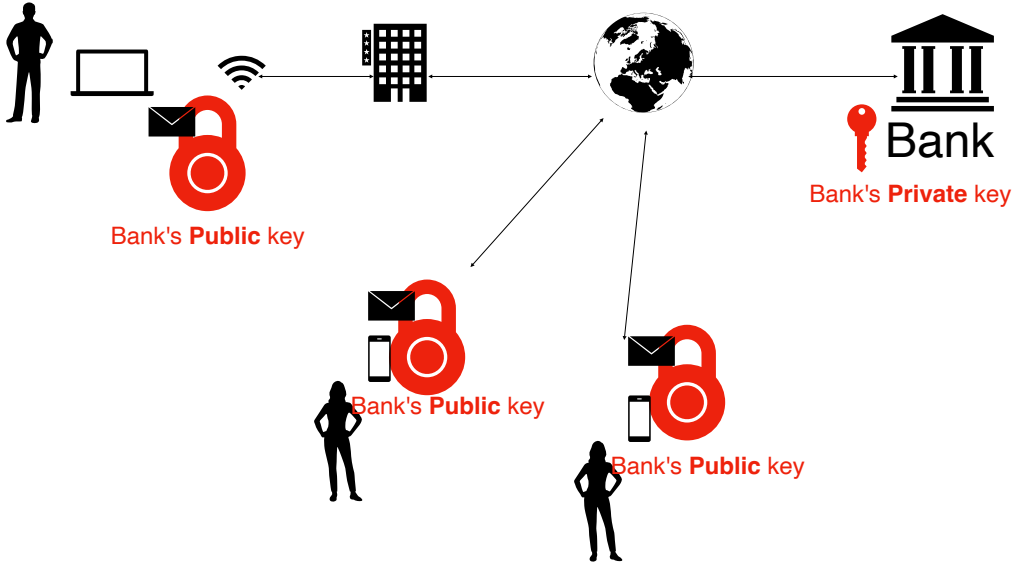
How can we achieve these goals?

(Symmetric) Encryption

This is called <u>symmetric</u> encryption (same secret key for encrypting and decrypting)

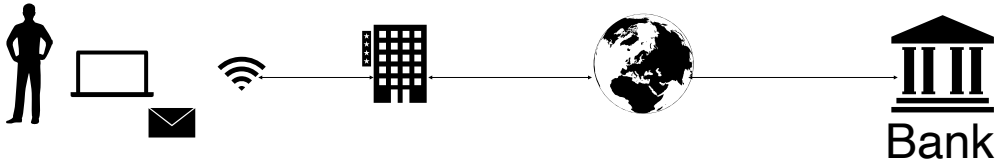
Problem: Need a separate channel for sharing the secret key!

Asymmetric Encryption



Example: https

Encryption and Signing



Encrypt: use Bank's **Public** key → Decrypt: use Bank's **Private** key

CIA: Confidentiality, Integrity

Verify: use Bank's **Public** key ← Sign: use Bank's **Private** key

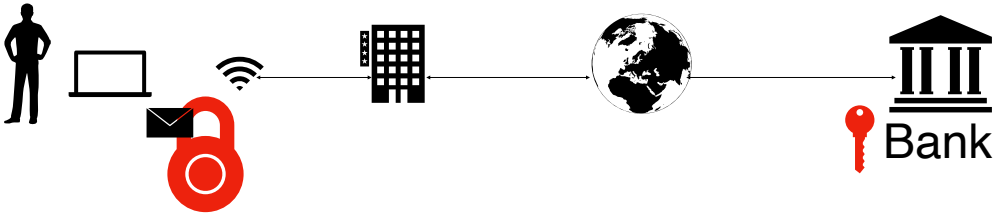
Authentication, non-repudiation

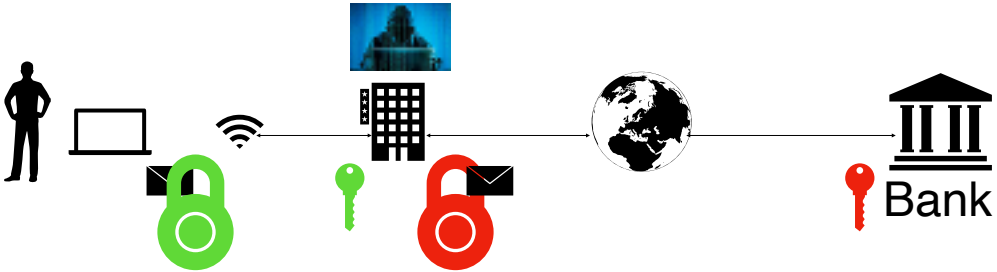
Is that it? No more problems?

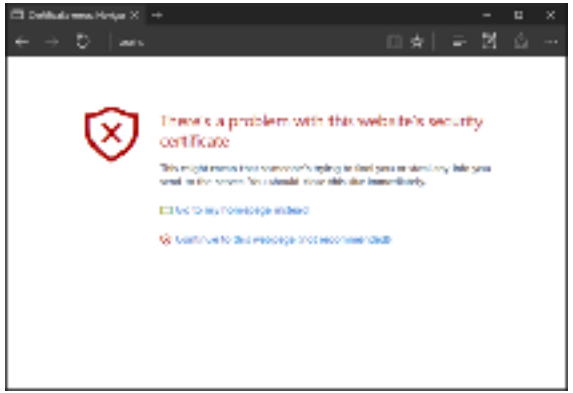
Certificates

Man in the Middle (MITM) problem

Certificates

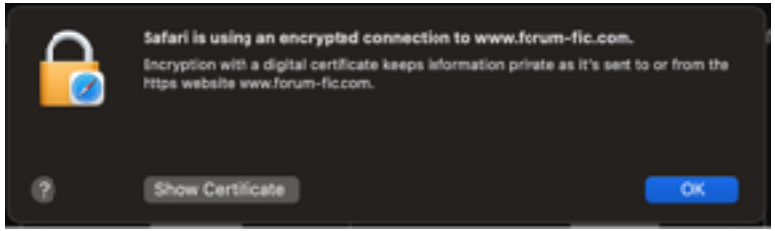


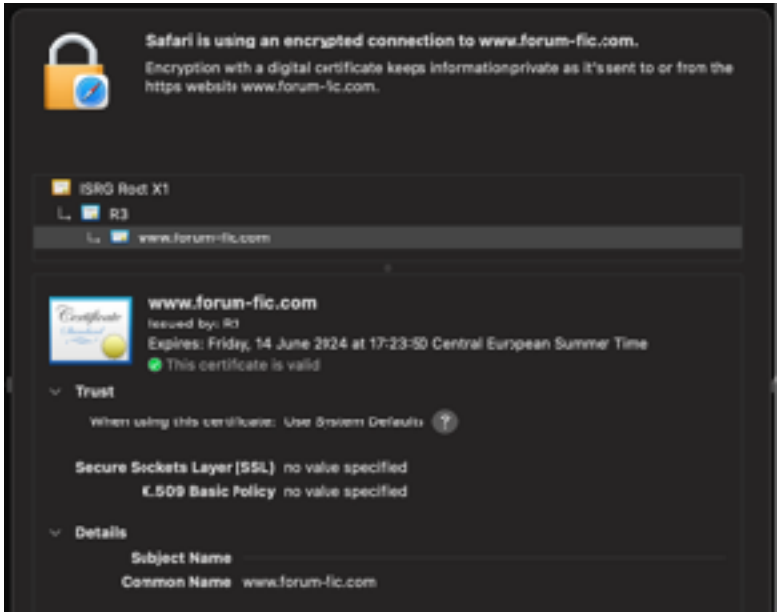




Certificates

- Certify that a given public key belongs to a given domain (domain verification, DV)
- Issued by Certificate Authorities (CAs)
- CAs have "Root Certificates"
- Browsers have a list of "Root Certificates they trust
- Browsers impose their "rules" for trust





Take aways

- You (or your browser) cannot trust everyone who's on the path between you and the server (ex. bank)
- You encrypt end-to-end (http**s**)
- The certificate authority (CA) tells you it's the proper "end" (ex. Bank) you're communicating with
- **You trust the CA**
- **CA can potentially cheat** (ex. by certifying a Man-in-the-Middle)
- **You trust more <u>CA + Browsers</u>**

Where's the state in all of this?!

And then came the QWACs

Qualified
Website
Authentication
Certificates

Credit: securityriskahead.eu

QWACs vs. Traditional (DV) Certificates

	DV Certificates	QWACs
Issued by ...	Certificate Authorities Certificate Transparency, an IETF technical standard that ensures a CA's issuing history can be examined by the public in order to detect malfeasance; WebTrust for CAs audit; ETSI EN 319 411 audit; section 2.2 of the TLS Baseline Requirements	[Qualified]Trust Service Providers ([Q]TSPs) duly certified and audited to ensure they meet the stringent standards established by the regulation.
Certifies that ...	Public key belongs to website	idem + tie to owner org. (EV) "displaying in a user-friendly manner"
Browsers trust ...	Their list of "Root Certificates"	idem + root certif. of member states
Rules of security / trust	Defined by browser makers	Defined by ETSI

QWACs: Motivation

- Strengthen the European position against the market power of powerful internet companies
- Reduce the power of large companies behind major browsers (Google, Apple, Microsoft...)
- Sovereignty
- Financial (est. 247M Euros in 2027)
- [No] increased security?

What's right / wrong?

Credit: securityriskahead.eu

Issues...

- Critics include: Mozilla foundation, EFF, Int'l group of security experts
- The introduction of this text so late in the **legislative process and behind closed doors** is also deeply concerning for democratic norms in Europe.
- While QWACs deliver verifiable identity information, browser certificates secure and authenticate connections to servers. **Treating them interchangeably undermines established best practices** and security mechanisms,
- It seems inevitable that they will have to **create two versions of their software**: one for the EU, with security checks removed. We've been down this road before, when export controls on cryptography meant browsers were released in two versions: strong cryptography for US users, and weak cryptography for everyone else.
- The **owner of a root certificate can intercept users' web traffic** by replacing the website's cryptographic keys with substitutes he controls. Any root certificate trusted by the browser can be used to compromise any website. There are multiple documented cases of abuse, because the security of some certificate authorities has been compromised
- The regulation's technical implementation could serve to expand the **ability of governments to surveil both their own citizens and residents across the EU** by providing them with the technical means to intercept encrypted web traffic. Countries like Kazakhstan, China and Russia have already tried something like this in the past.

QWACs vs. Traditional (DV) Certificates

	DV Certificates	QWACs
Issued by ...	Certificate Authorities Certificate Transparency, an IETF technical standard that ensures a CA's issuing history can be examined by the public in order to detect malfeasance; WebTrust for CAs audit; ETSI EN 319 411 audit; section 2.2 of the TLS Baseline Requirements	[Qualified]Trust Service Providers ([Q]TSPs) duly certified and audited to ensure they meet the stringent standards established by the regulation.
Certifies that ...	Public key belongs to website	idem + tie to owner org. (EV) "displaying in a user-friendly manner"
Browsers trust ...	Their list of "Root Certificates"	idem + root certif. of member states
Rules of security / trust	Defined by browser makers	Defined by ETSI **(Note: ETSI has a WG on Legal Interception)**

Result...

- "The EU wants to force browsers to accept certain certification bodies. In doing so, it intervenes in a system of technical requirements and market economic forces in which there is a lot of need for improvement - but in which a lot can also be broken" [CT magazine]

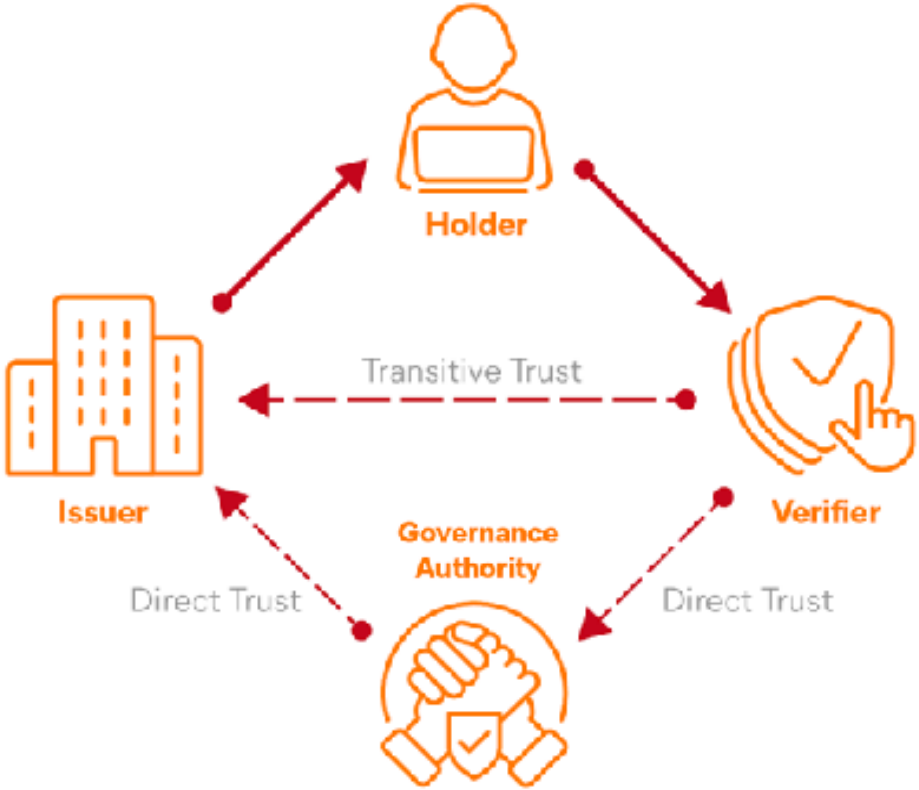
- Outcry by foundations and scientists

- **"Trust the private sector more or less than the authorities?" That is the question**

More on whom to trust...

Trust registries

- Who's allowed to verify?
  - Ex: Discotheque claiming to be a cantonal authority
- Who's allowed to ask for what?
  - Ex: Discotheque asking for diplomas
- Who's allowed to issue what?
  - Ex: Ministry of health issuing driving licenses



All that was about whom to trust

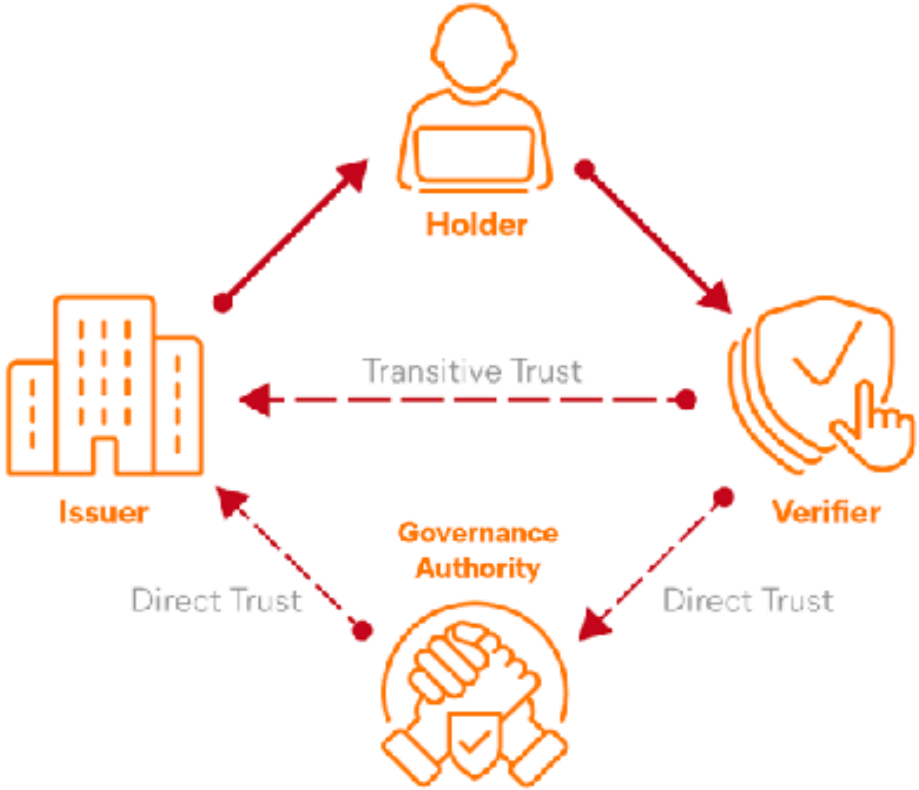
How about **what to share / disclose**?

Privacy issues: Data Minimization

- Selective disclosure
  - how about signature validity?
- Zero-Knowledge Proofs
- Why data minimization?
  - Privacy principles + GDPR; Swiss DPA; eID law...

Privacy issues: [un]linkability

- Holder linkability
- Issuer linkability
- Verifier linkability
- Which signature algo. support this?
  - BBS / BBS+
- Revocation issues?



Challenges and open questions

(Some) **User-related** questions:

- Awareness raising against risks / scams.
- User literacy for being in control.
- Would e-ID custodians help (for "distributed" SSI)?
- Put all the "intelligence" in the wallet?

Short break?

Interoperability

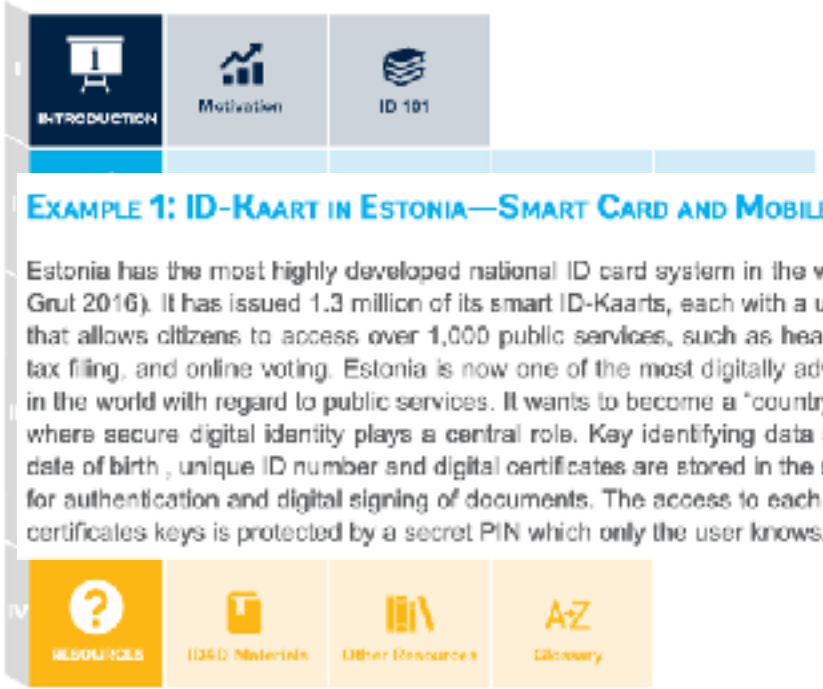
Interoperability issues

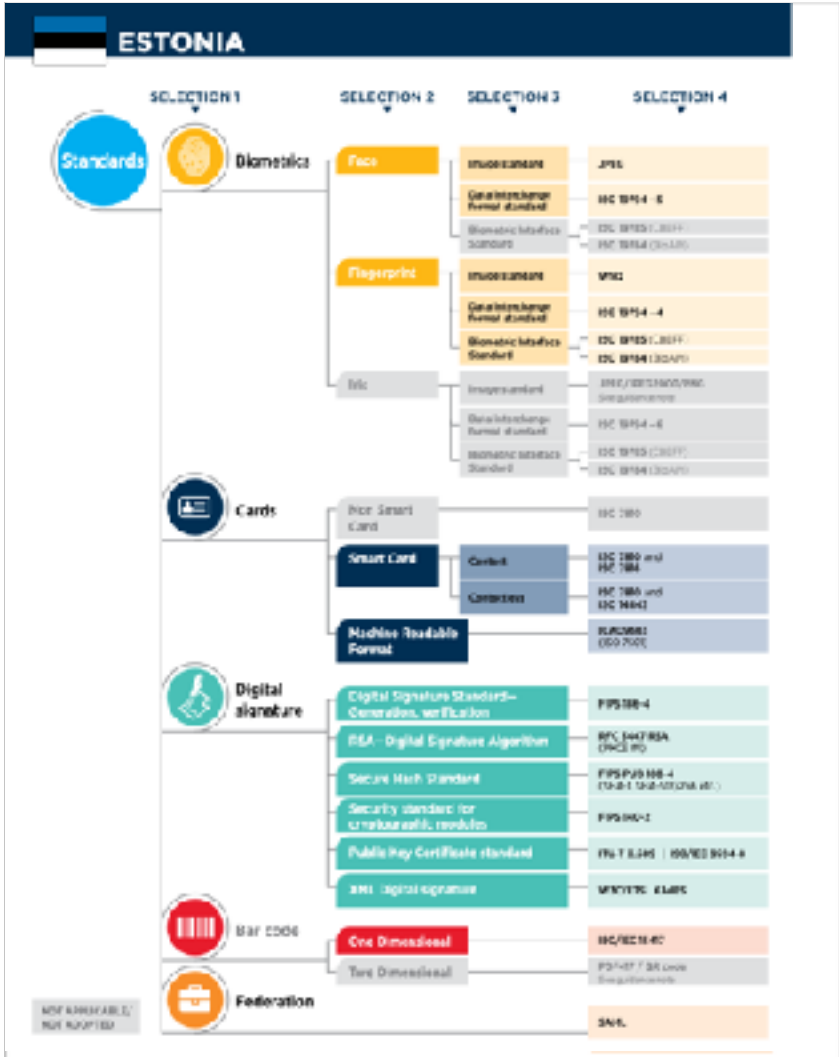
- Technical
  - Solve it in the wallet?
  - More on C4DT's Factory webpage:
    https://c4dt.epfl.ch/article/?cat=10
- Trust Registries
  - Who provides them? Wallet provider? Government?
- Legal
  - ex. Signature qualifications

EPFL

Standards, norms, guidelines...

- World Bank's ID4D Practitioner's Guide





Standards, norms, guidelines...

- NIST Digital Identity Guidelines

SP 800-63-3

Digital Identity Guidelines

SP 800-63A

Enrollment & Identity Proofing

SP 800-63B

Authentication & Lifecycle Management

SP 800-63C

Federation & Assertions

eIDs around the world

eIDAS

(EU ID wallet, ARF)

AADHAAR

MOSIP

China ?

US ? facebook

Google

How does the future look like?

Different regional eIDs

Non-interoperable

Sovereignty issues

Economical issues

Will some dominate the international market, while others remain "regional"?

Dive into the Swiss eID

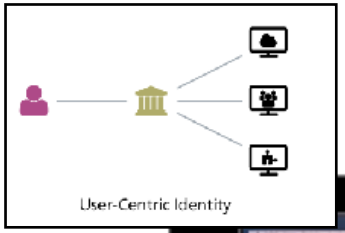
Swiss eID: law

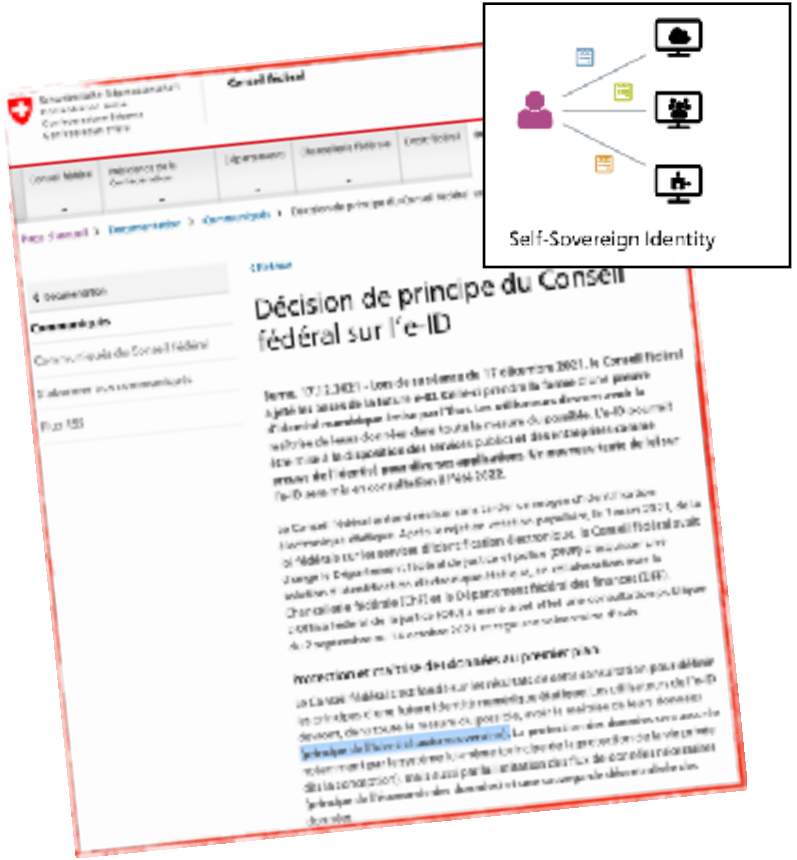
swissinfo.ch

Swiss politics >

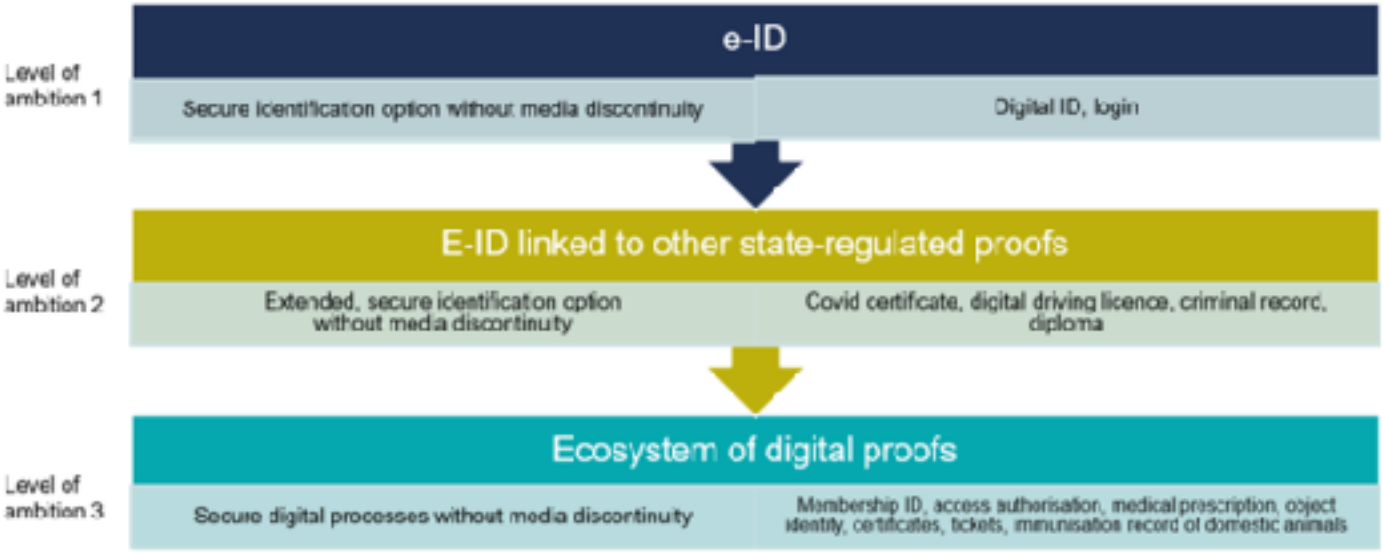
Swiss perspectives in 10 languages

Digital identity scheme shot down by voters over data privacy concerns





Swiss eID: Ambition level



Swiss eID: legal signing?

- No (legal) signing, it's only eID
  - Unlike EU's eIDAS

Fedlex
La plateforme de publication du droit fédéral

Accueil > Recueil systématique > 9 Economie - Coopération technique > 94 Commerce > 943.03 Loi fédérale de la signature électronique (Loi sur la signature électronique, SCSE)

Informations générales

Abrégé SCSE
Décision 19 décembre 2003
Entrée en vigueur 1 janvier 2005
Source RO 2004 5085
Décision abr. 18 mars 2016
Date d'abrogation 1 janvier 2017
Source abr. RO 2016 4651
Langue(s) de la publication DE FR IT

[RS 943.03]

Loi fédérale du 19 décembre 2003 su
domaine de la signature électroniqu

Loi fédérale
sur les services de certi
de la signature électron
(Loi sur la signature électro

Informations générales

Le texte est en vigueur

Abrégé SCSE
Décision 18 mars 2016
Entrée en vigueur 1 janvier 2017
Source RO 2016 4651
Langue(s) de la publication DE FR IT
Chronologie Chronologie
Modifications Modifications
Citations Citations

Outil
Convertisseur de langues

Toutes les versions
01.01.2020 HTML PDF DOC
01.01.2017 PDF

Révisions

943.03

Développer tout | Vue par article | Fermer tout

Loi fédérale
sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques[1]

(Loi sur la signature électronique, SCSE)

du 18 mars 2016 (État le 1er janvier 2020)

[1] Les termes désignant des personnes s'appliquent également aux femmes et aux hommes.

L'Assemblée fédérale de la Confédération suisse,

vu les art. 95, al. 1, et 122, al. 1, de la Constitution[2],
vu le message du Conseil fédéral du 15 janvier 2014[3],

arrête:

[2] RS 101

[3] FF 2014 953

Section 1 Dispositions générales

Art. 1 Objet et but

1 La présente loi règle:

a. les exigences de qualité auxquelles doivent répondre certains certificats numériques et leur utilisation;
b. les conditions auxquelles les fournisseurs de services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques (services de certification) peuvent être reconnus;
c. les droits et les devoirs des fournisseurs reconnus de services de certification;

Swiss eID: other

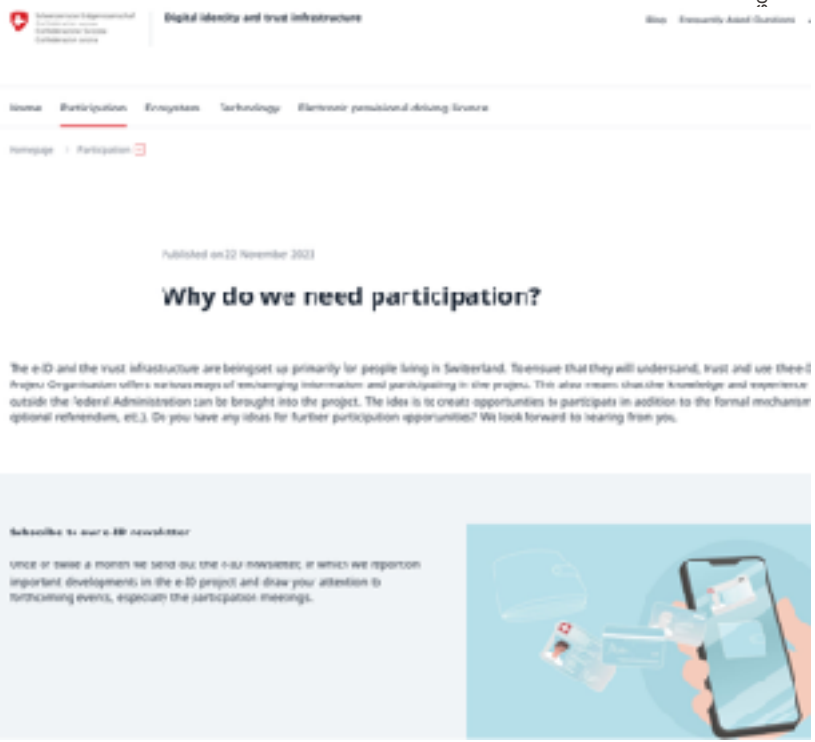
- Not mandatory to have; Mandatory to accept
- Linked to a person or to a device?
  - -> device + secure enclave
    - Social Inclusion?
- No (legal) signing, it's only eID
  - Unlike EU's eIDAS
- EU compatible?
  - How about BBS/BBS+ / ZKP etc.?
- + digital wallet
- Note: Don't confuse eID with online logins

Swiss eID: other

- FOITT's sandbox(es)

- Expected to be launched in 2026

- Follow the news / join participation meetings: https://www.eid.admin.ch/en/why-do-we-need-participation



EPFL

Thank you!

imad.aad@epfl.ch

c4dt.epfl.ch

@C4DT_EPFL

/company/c4dt-epfl/

EU Regulations, eIDAS

- The eIDAS Regulation evolved from **Directive 1999/93/EC, which set a goal that EU member states were expected to achieve in regards to electronic signing**.
- The directive also **allowed each member state to interpret the law** and impose restrictions, thus preventing real interoperability, and leading toward **a fragmented scenario.**
- In contrast with this directive, **eIDAS ensures mutual recognition** of the eID for authentication among member states, thus achieving the goal of the **Digital Single Market**.
- eIDAS is primarily **designed to tackle identification** challenges experienced by **digital <u>public</u> services**.
- Yet, Member States are also encouraged to **support the voluntary reuse of eIDAS-based eIDs by the private sector**.

EU Regulations, eIDAS

The Regulation provides the regulatory environment for **the following important aspects** related to electronic transactions:

- Digital identity: a European-wide framework for digital authentication of citizens, with legal validity. **Nine principles** of EU digital identity have been defined: **user choice, privacy, Interoperability and security, trust, convenience, user consent and control proportionality, counterpart knowledge and global scalability.**

- Advanced electronic signature: An electronic signature is considered advanced if it meets certain requirements:
  - It provides unique identifying information that links it to its signatory.
  - The signatory has sole control of the data used to create the electronic signature.
  - It must be capable of identifying if the data accompanying the message has been tampered with after being signed. If the signed data has changed, the signature is marked invalid.
  - There is a certificate for electronic signature, electronic proof that confirms the identity of the signatory and links the electronic signature validation data to that person.
  - Advanced electronic signatures can be technically implemented, following the XAdES, PAdES, CAdES or ASiC Baseline Profile (Associated Signature Containers) standard for digital signatures, specified by the ETSI.

- Qualified electronic signature, an advanced electronic signature that is created by a qualified electronic signature creation device based on a qualified certificate for electronic signatures.

- Qualified digital certificate for electronic signature, a certificate that attests to a qualified electronic signature's authenticity that has been issued by a qualified trust service provider.

- Qualified website authentication certificate, a qualified digital certificate under the trust services defined in the eIDAS Regulation.

- Trust service, an electronic service that creates, validates, and verifies electronic signatures, time stamps, seals, and certificates. Also, a trust service may provide website authentication and preservation of created electronic signatures, certificates, and seals. It is handled by a trust service provider.

EU Regulations, eIDAS

- The regulatory obligations and security needs to which they are subject in terms of identity verification have placed **banks and financial institutions in a strategic position**.
- More and more institutions are exploring how they could leverage the procedures that they have put in place to verify customers' identity for other parties by **acting as identity providers**.
- eIDAS-based eIDs offer the possibility to provide a strong authentication of users (natural and legal persons), based on ID information endorsed by governmental authorities across Europe.

- List of