



Digital Identity

Jon Ølnes
Tribe Lead / Product Manager
Signing and Trust Services
Signicat

Finse Cyber Security Winter School
2022.04.26



Disclaimer

Please note that this presentation is for information purposes only, and that Signicat has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation.

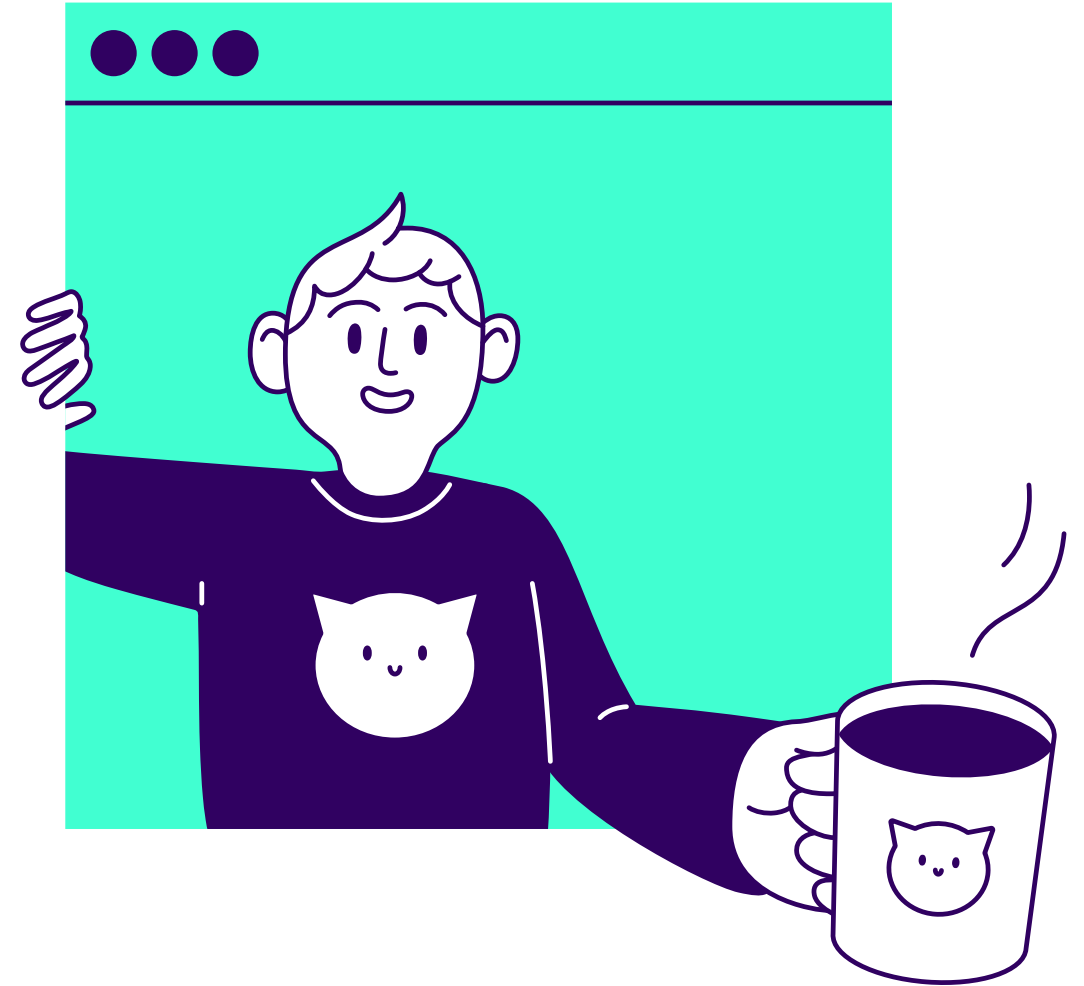
The future strategy and possible future developments by Signicat are subject to change and may be changed by Signicat at any time for any reason without notice. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. Signicat assumes no responsibility for errors or omissions in this document.

Agenda

1. What is (digital) identity?
2. Personal devices
3. The big techs and profiling
4. States and (digital) identity
5. Electronic proof of identity (eID)
6. Levels of assurance (LoA)
7. Identity management (the traditional way)
8. Self-sovereign / decentralised identity
9. The European Digital Identity Framework (AKA the EU Wallet)
10. Signing (EU example)
11. Identity proofing (EU example)
12. Regulating identity (eIDAS, EU example)
13. The eIDAS revision (proposal) including the wallet



About Signicat



A European leader



Roots in the leading identity regions

Nordics & Benelux
HQ in Trondheim, Norway



About 400 identity experts



Full cross-border digital identity journey

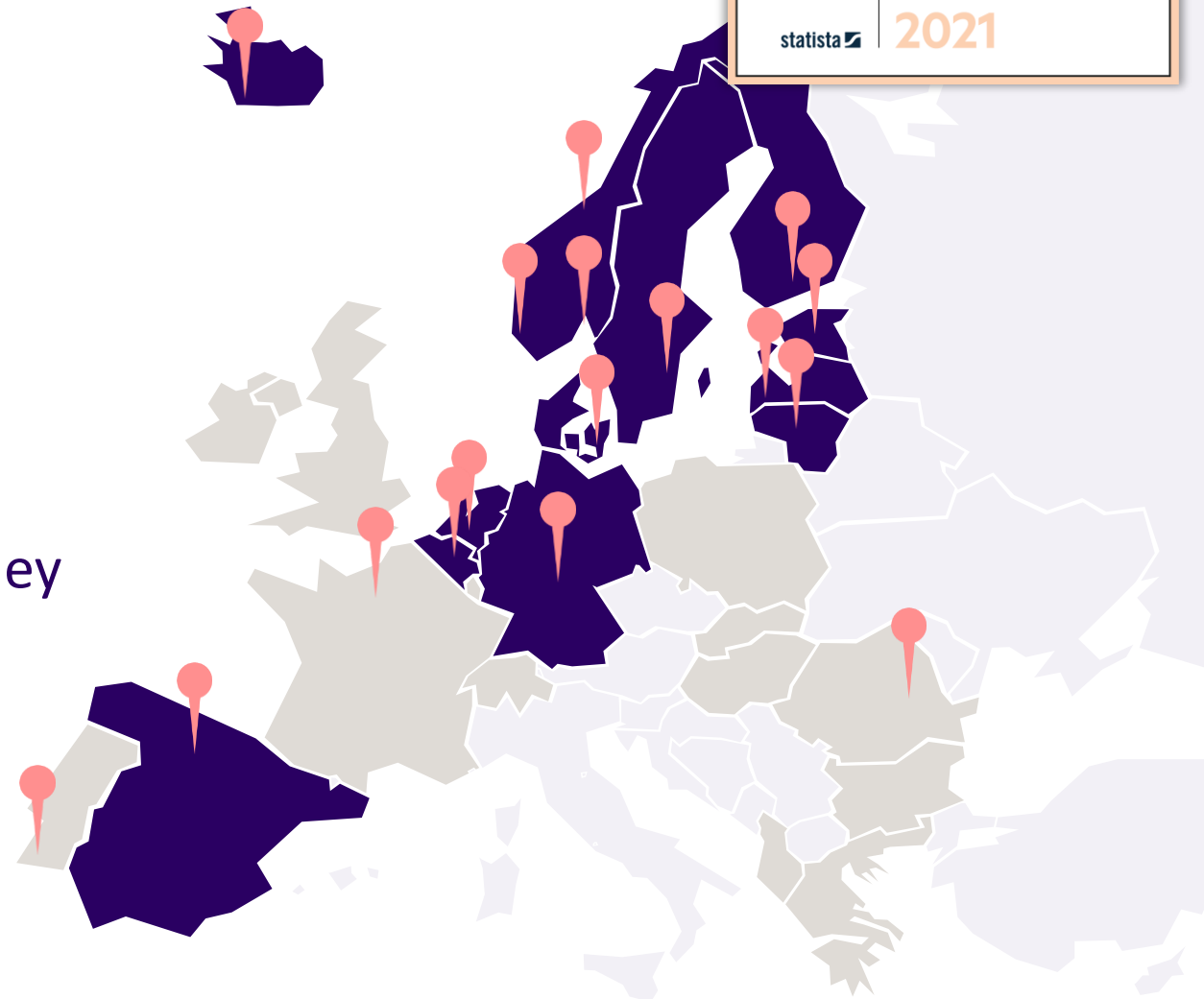


40% Y2Y Growth



The highest eID coverage

>30 eID integrations



Signicat and subsidiaries

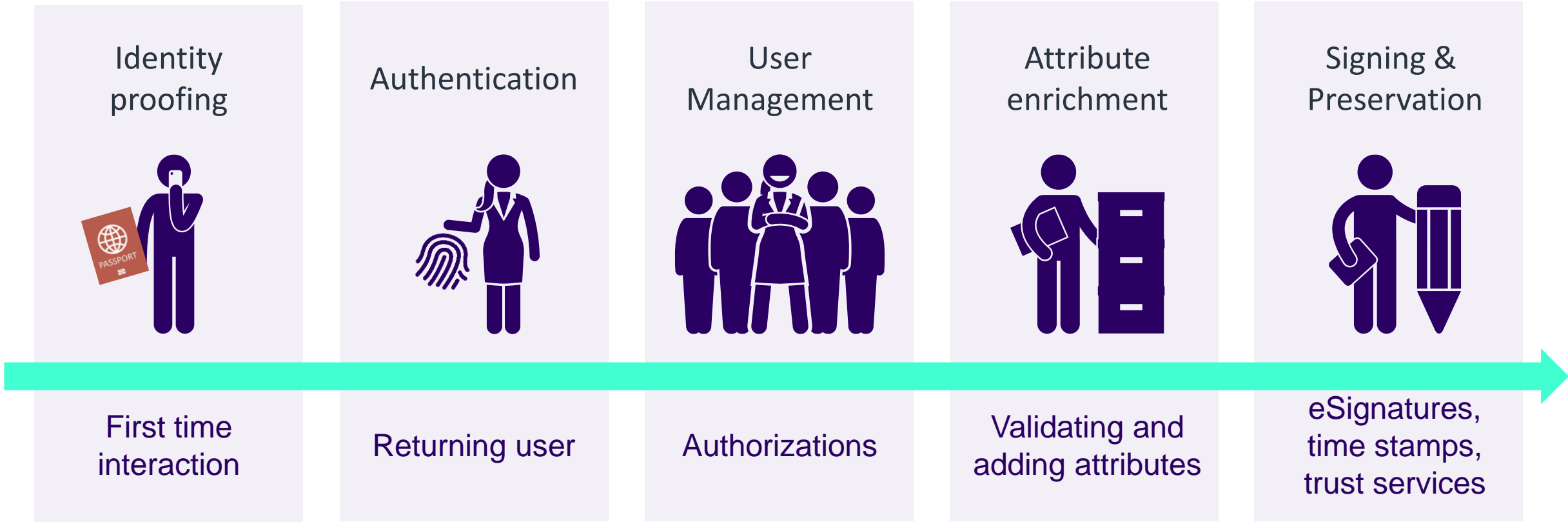
- Strong market footprint
- Light market footprint
- Office



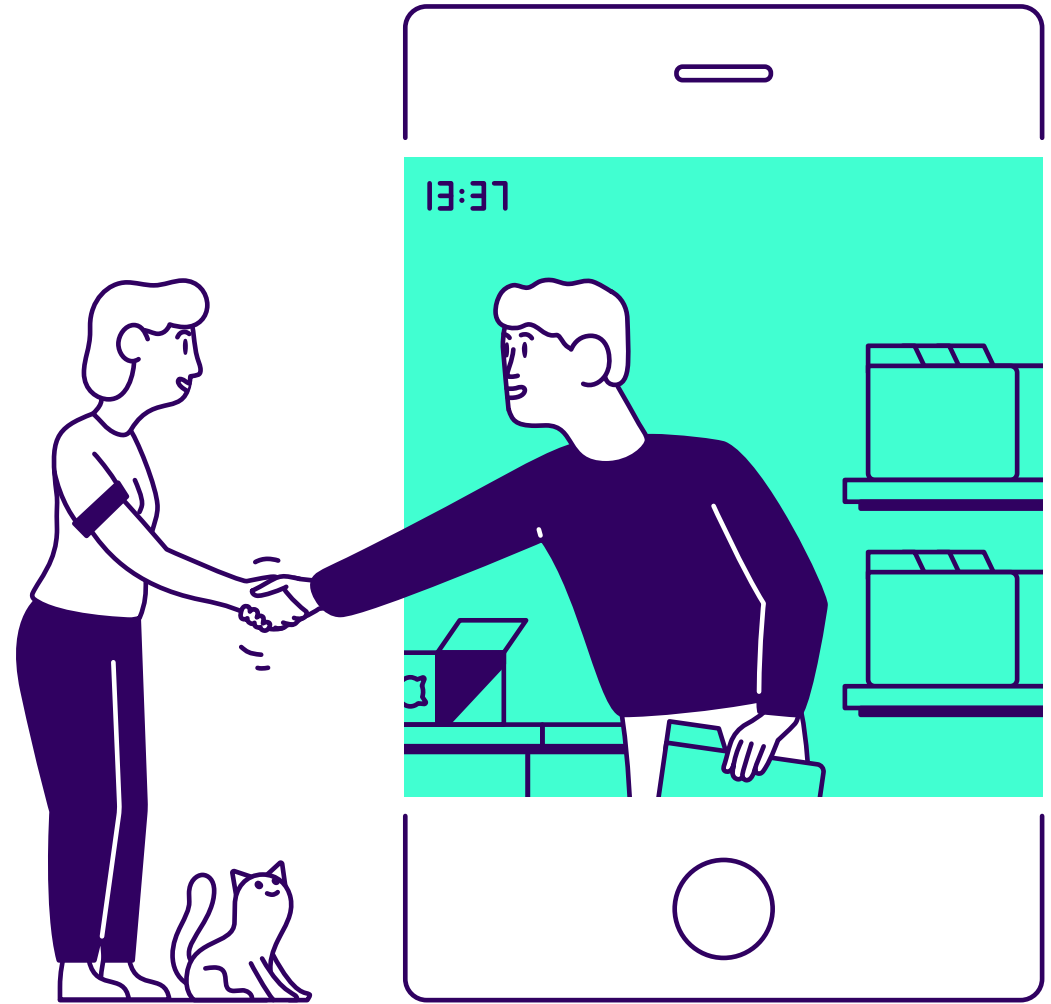


Identity lifecycle

SaaS provider
Mainly white-labelled
Customer's look and feel



What is (digital) identity?



Your identity – everything about you



Identity may be the way you perceive yourself

But in this context how you are perceived by others and perceived «by society»

Your digital double – digital identity

Truths

Lies & rumours

What you publish about yourself

What others publish about you

Newsfeeds and social media

Public registers

Health information

And much more...



Identification

- name
- age
- address
- national ID number
- much more...



Persistence of information

Whatever information is «in the wild» on Internet remains there

The mistaken posts you made

The false rumours and the impersonations

Maybe fading over time but not disappearing



One digital identity or many?

Digital identity will evolve
Metaverse is one direction

My opinion: **You have only one digital identity** – everything that can be linked to you as a physical person

Borderline cases of “identity” shared between persons can exist, e.g. game character controlled by multiple players





Personas – different aspects of your double



The tax-payer



The shopper



The traveller



The professional



The banker



The dater



The patient



... and many more

Identity, privacy, and security

Identity = societal, political, psychological, behavioural aspects

> **Privacy** = legal aspect, the right to own information and to protect it

> **Security** = technical and organisational aspects

Identity is a human right
Identity depends on privacy, but is more

Privacy is about data protection
Privacy depends on security, but is more

Digital identity is based on security technology and trustworthy actors.

Is identity a security topic?

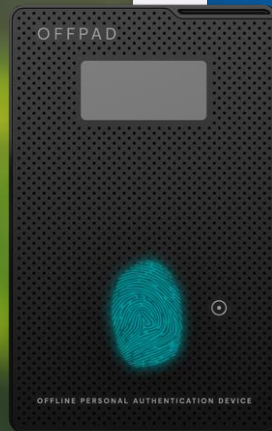
- Depends on point of view, but identity >> security
- Identity solutions should start from useability, not security
 - Identity is about letting people in, not about keeping people out
 - Identity solutions must be secure!
- Digital identity relies on security technology



Personal devices



Link between physical and digital identity



The tax-payer



The shopper



The traveller



The professional



The banker



The dater



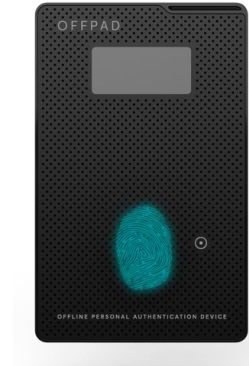
The patient



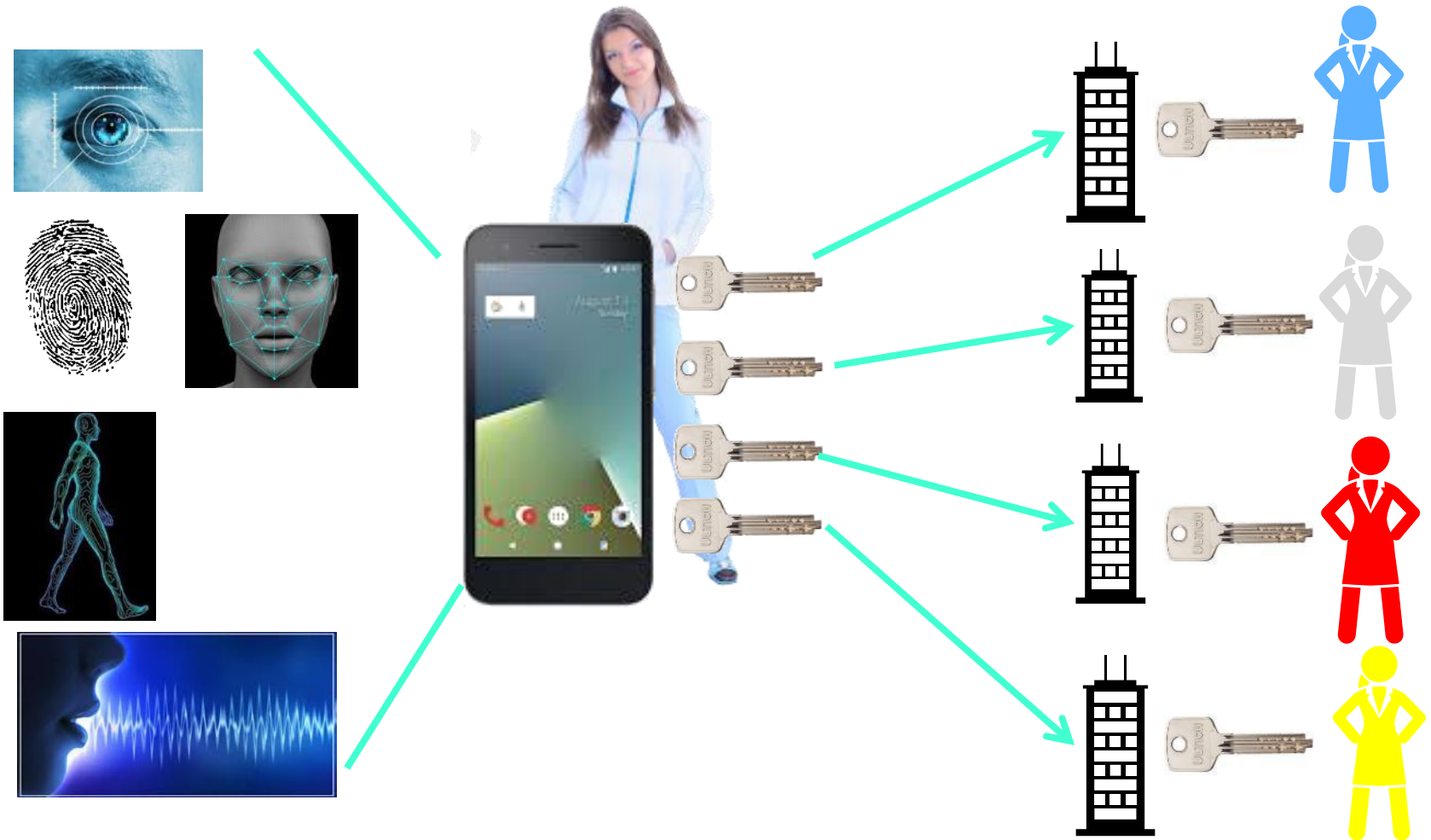
... and many more

What we really need

- A personal device bound to you as an individual
 - That can do crypto processing (which humans cannot)
 - That represents you
 - That does not put extra stress on the user
- The device must protect your identity
 - Which most devices do not today
 - Information on all your personas passes through the device
 - The device shall not spy on you
 - Software installed on it shall not be allowed to spy on you
 - Nor reveal information to other parties outside of your control
- The device should be the first line of defense for digital identity



How the device might represent you



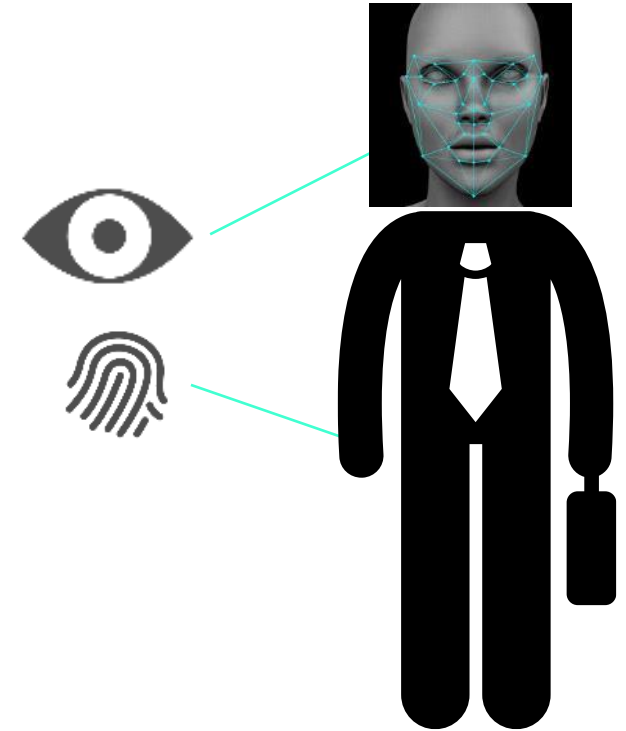
Different personas

Targeted identity

fido[™]
ALLIANCE

Accessing devices: biometrics

- Can be made very secure
- Easy for user, nothing to remember
- **Requires a trusted environment**
 - Fresh measurement from a trusted sensor
 - Never assume biometric info to be secret
 - Must protect against copy and replay attacks

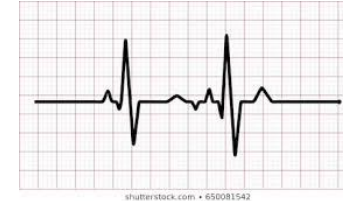
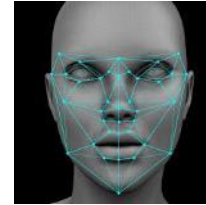


Biometrics on mobile devices

A dozen different mechanisms

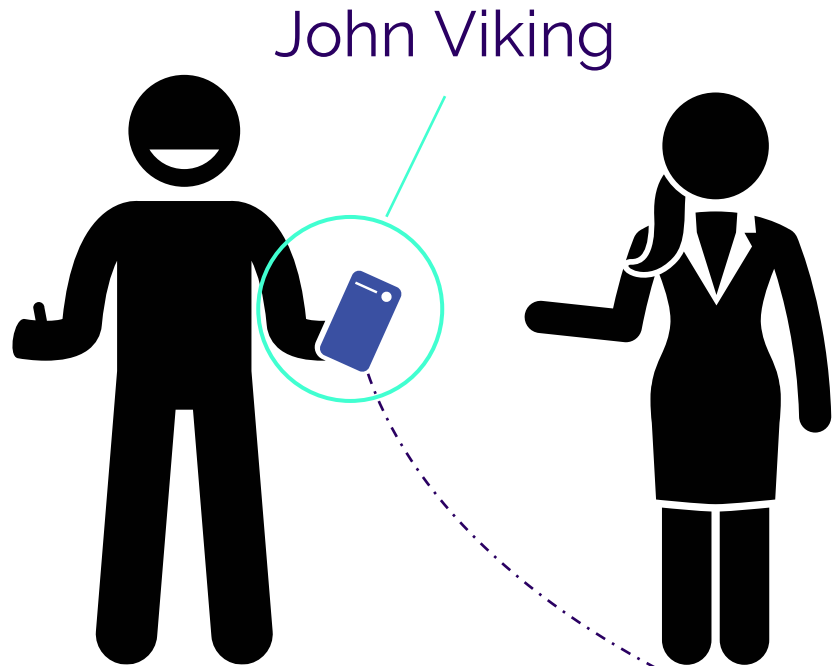
Physiological biometrics

Behavioural biometrics



Are mobile devices trusted environments?

Device may “know” that it is in your possession



Not John Viking

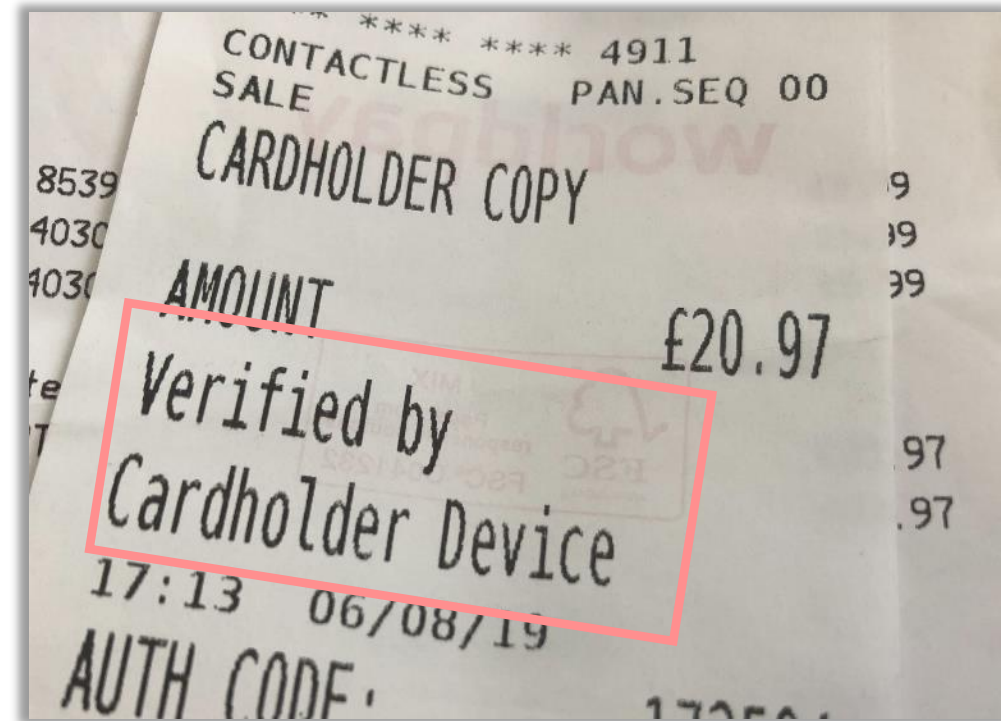


Example Apple Pay with watch



PIN at first use

Then no need for PIN as long as watch remains on wrist

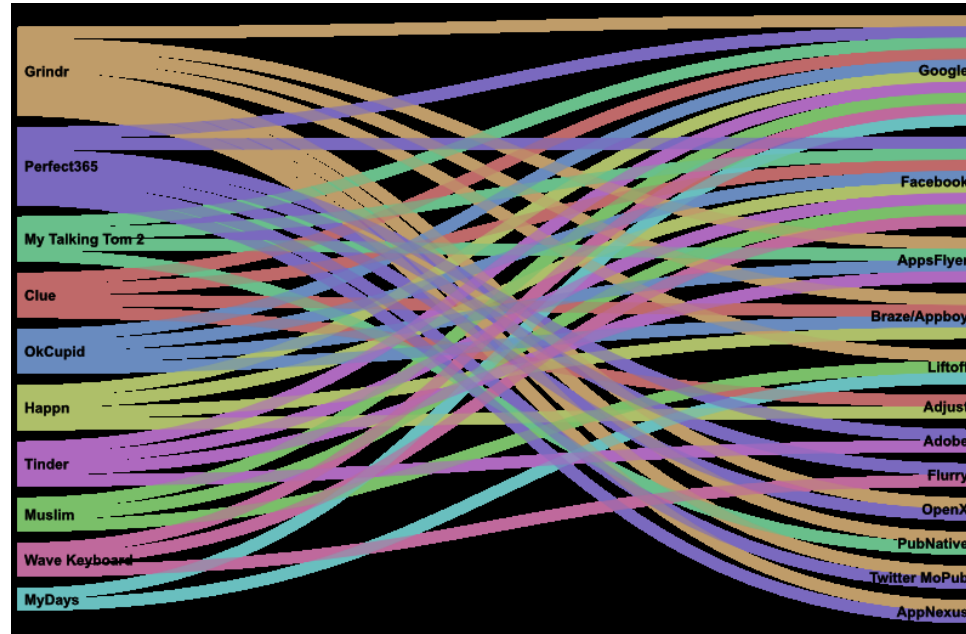


Apps spy and share your information



OUT OF CONTROL

How consumers are exploited by the online advertising industry
14.01.2020



Norwegian Consumer Council
with mnemonic

Apps should be the second line
of defence for digital identity

Apps request wider
permissions than needed

Apps may collect info that
is not declared

Apps share your info with
their providers

Apps share your info with
third parties

Third parties can correlate
info across sources

Online communication tools
send sound to server even
when microphone is «muted»

The big techs and profiling

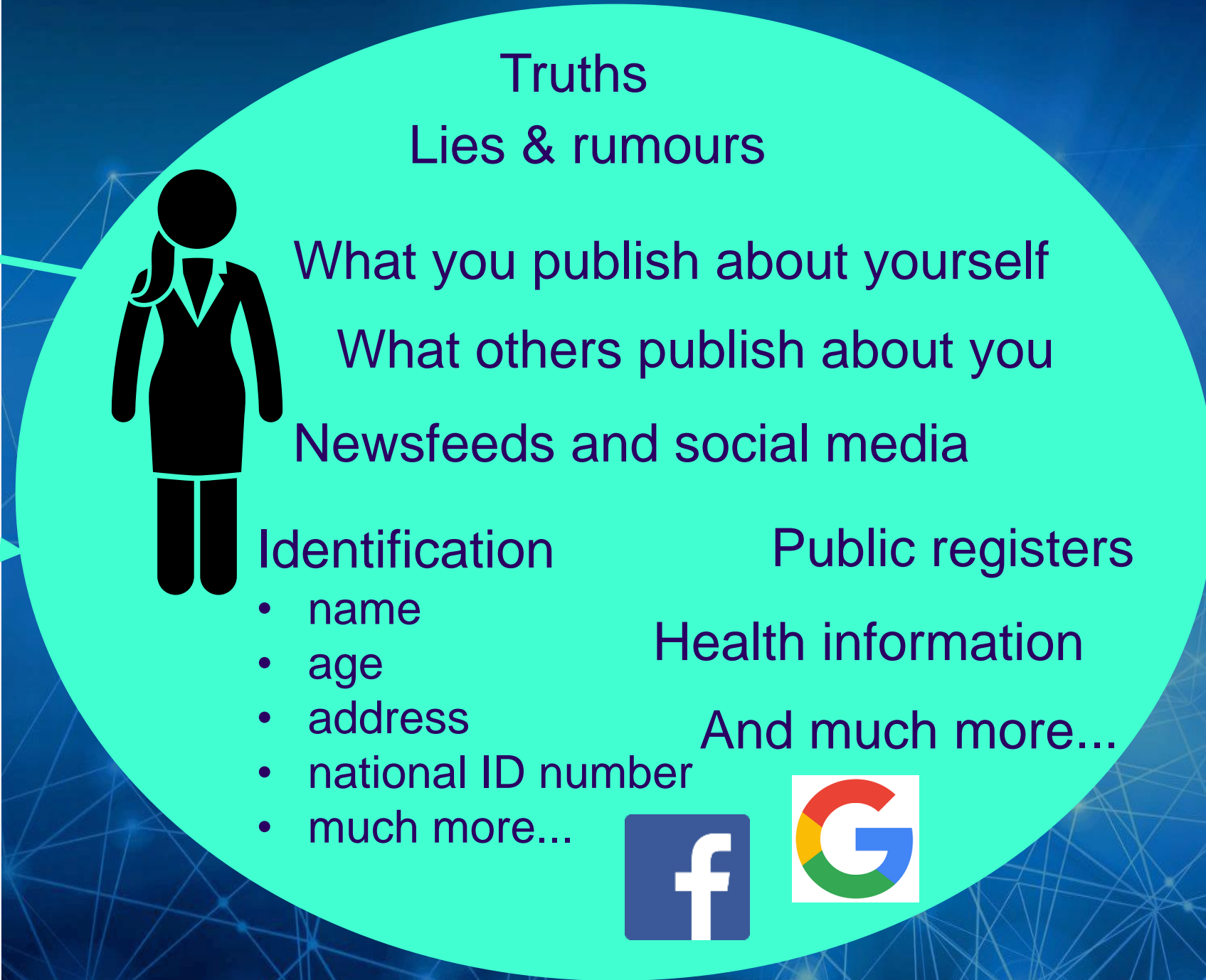


The business model of Facebook, Google etc.

Commercial, political and other actors



Feedback loop changes your identity



The business model of the big techs

- Gather as much information as possible about you
- Make profiles of you
- Sell use of profiles to whoever provides «content»
- Ensure content is visible to the correct profiles
- **You will only get «correct content» according to your profile**
- The easy ones like books and music
 - Discover more that you probably will like
 - ... but you do not get exposed to new music styles
- The difficult ones like news and politics
 - Get more content reinforcing your previous (weak?) biases
 - ... and never get exposed to alternate viewpoints
- **The result is an amplifying feedback loop**

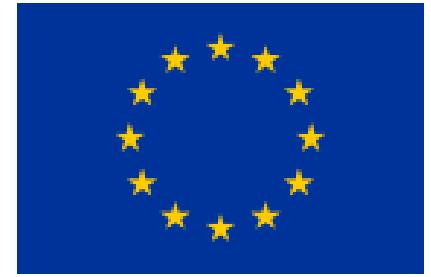
You are NOT Facebook's and Google's customer
You are their product



- This is not merely «data protection»
- It is about changing people's identity
- **Effects pose fundamental threats to societies**

Regulation is required
Perhaps profiling must be made illegal?

The EU is the regulator of the world



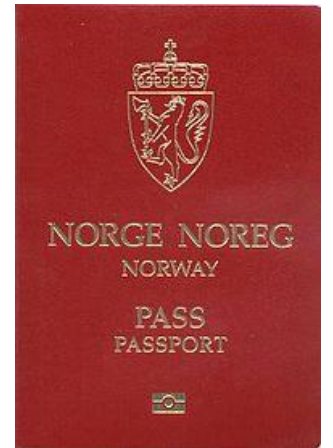
- GDPR on privacy
- eIDAS on electronic identity and trust services
- Digital Markets Act on preventing large market players from abusing their power
- Digital Services Act on illegal content, transparent advertising and disinformation
- Many other countries adopt similar regulations

States and (digital) identity



Your official identity is national

- Every human is (supposed to) have a nationality
 - State of citizenship and residency
 - Rights and obligations in states
 - States are sovereign and act individually

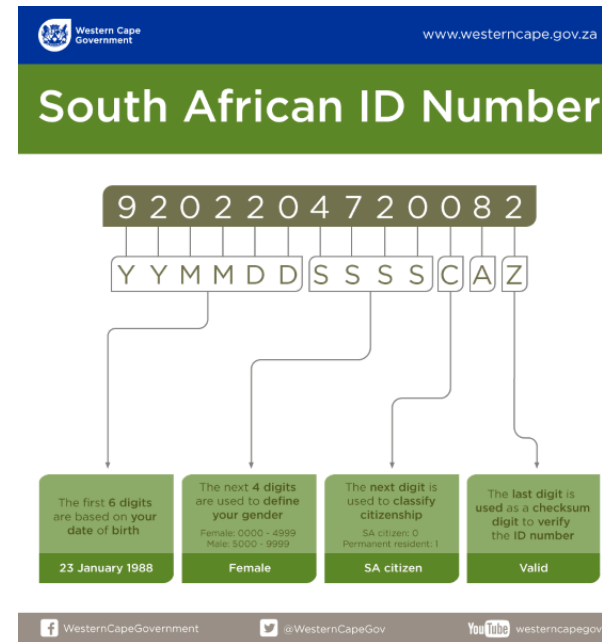


- There is no such thing as an EU identity

Identity for private sector need not be tied to nationality

How do states keep track?

- **National identity numbers**
 - In some countries
- **Mandatory ID-cards**
 - In some countries
- **Population registers**
 - In some countries
- **Other means, or hardly**
 - In some countries



Requires reliable and trusted state infrastructure

Leave no-one behind, nationally

Not everybody has a bank account

Or even a national ID number



Government responsibility to ensure everybody is included!



Leave no-one behind, globally



About 1 billion people do not have an official proof of identity
May not obtain banking services, health care, education, voting...



Sierra Leone: Biometrics and blockchain mean just a thumbprint can open a bank account

UNICEF urges methodical and wholistic approach in Africa's race for digital identity



India: World's largest biometric ID system

Kenya: Building refugee IDs with blockchain

African Union to Consider Good Digital Identity Principles at Summit

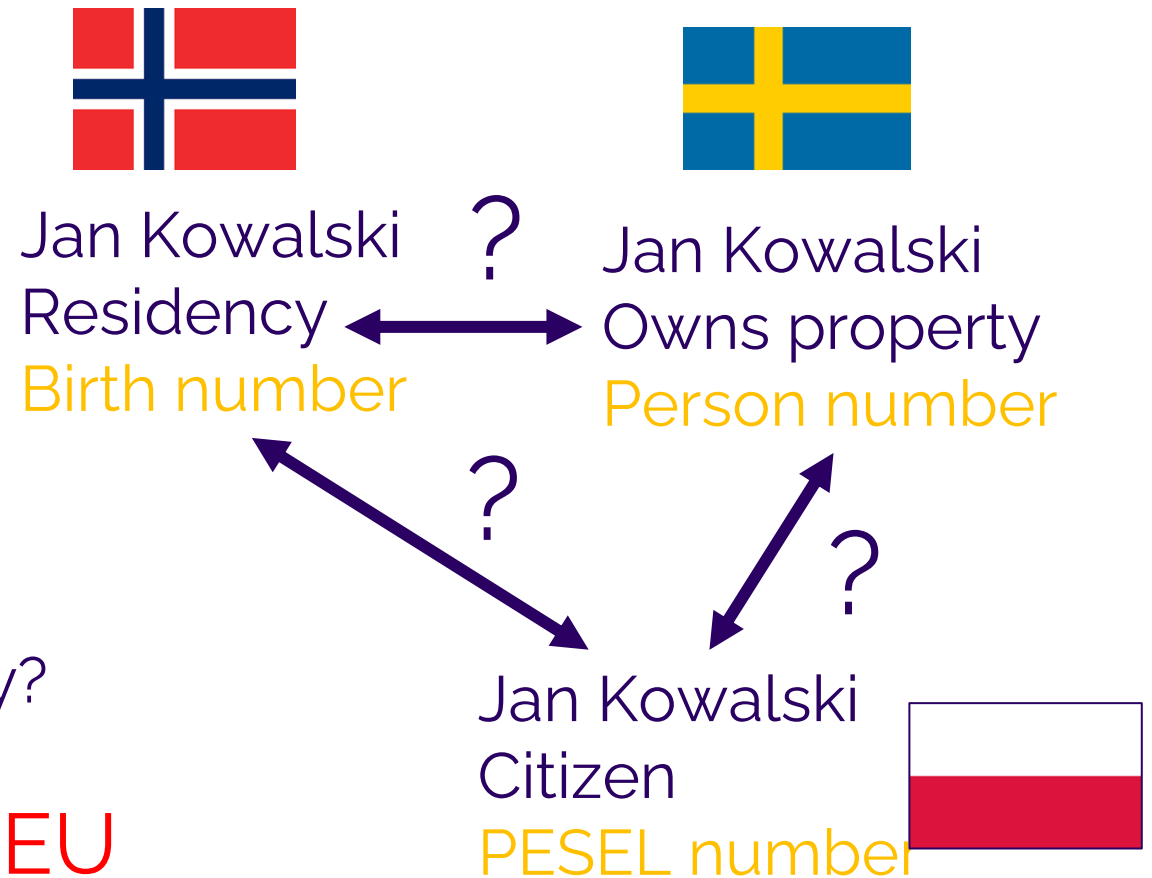
Linking national identities?

National identity defined by citizenship, residency, rights, and obligations

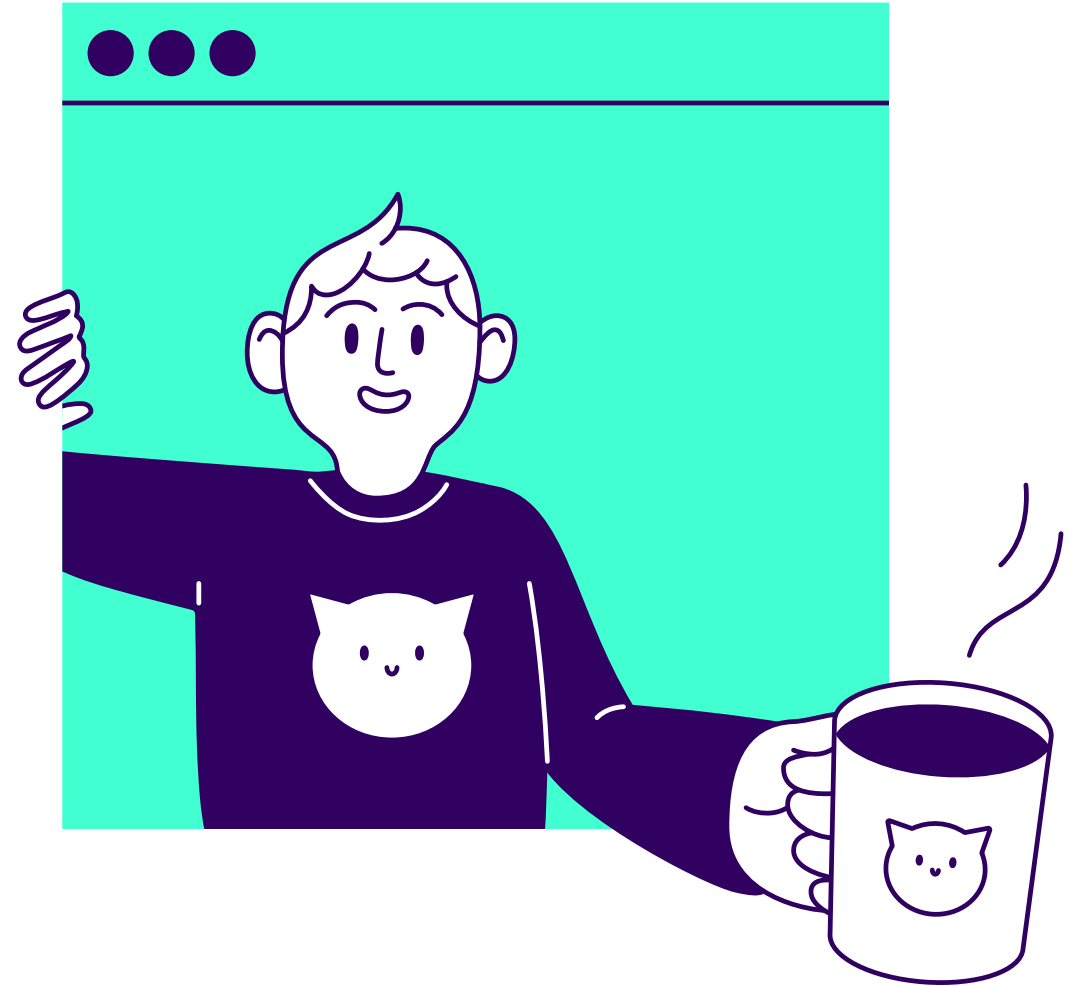
How do we link national identities cross-border?

What about countries that cannot (really) even identify their own residents uniquely?

To what extent is a common EU identity concept desired/needed?



Electronic proof of identity – eID



eID, digital way of proving your identity

Trust that the person is who they claim to be

«Identity» is official, national identity or can be other persona, unique in the given context

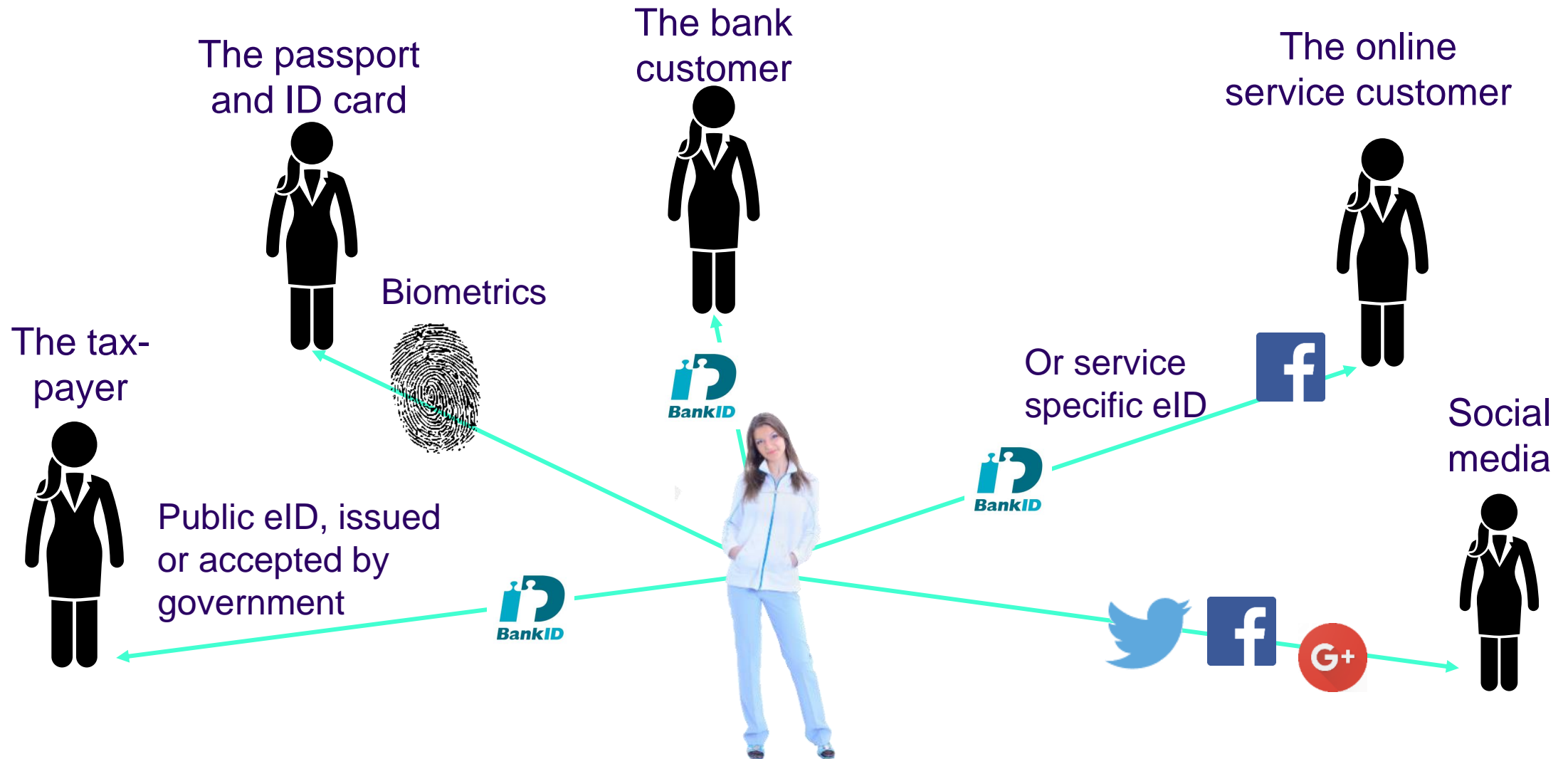


Digital counterpart to a physical identity method

bank ID



The link between you and a persona



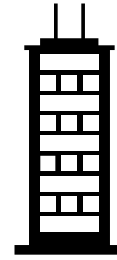
Public, reusable, national eID

Sort of «last year's trend»



Consumers

One eID for most purposes



Service providers

One eID to integrate



Society

Well-known, reliable eID

Combine with register systems where **service providers** look up further identity information

Most countries have nothing like this today

Potential downsides

- Monopoly, closed business models
- No cross-border solution
- Privacy, tracking of use
- No targeted eID – same information to all



The Nordics is in the lead

How to build national eID

1. The government does it all

- Model in many countries – government does not trust private actors
- Downsides: eID may not be available or used by private sector, deployment is not triggered by government services alone

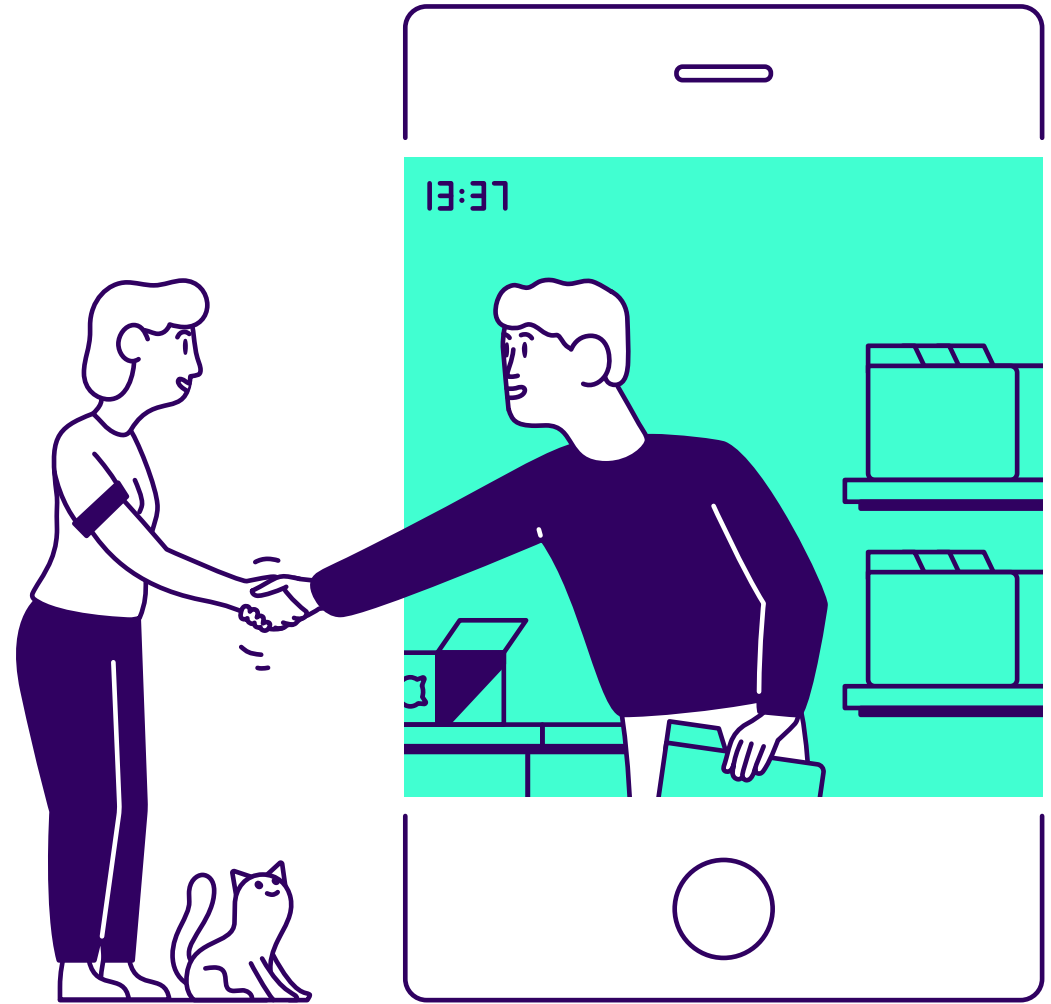
2. Public – private partnership

- Government contracts a commercial actor to do eID
- Denmark: Public procurement for MitID in co-operation with banks

3. Government trusts private actors

- Government sets rules for acceptance of commercial eIDs
- Norway, Sweden, Finland: eIDs issued by banks
- Downside: You need a bank account to get a national eID

Levels of assurance (LoA)



Classifying eIDs in discrete quality classes

NIST Special Publication 800-63

Revision 3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-63-3>

COMPUTER SECURITY



NIST Special Publication 800-63-3

Digital Identity Guidelines

- Frameworks define 3-4 levels
- E.g. the EU (eIDAS) 'low' 'substantial', 'high' levels
- Only some alignment between frameworks
- Non-government frameworks also exist



9.9.2015

EN

Official Journal of the European Union

L 235/7

COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502

of 8 September 2015

on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

Aspects of LoA classification

1. Application and registration
2. Identity proofing and verification
3. eID means characteristics and design
4. Issuance, delivery, and activation
5. Suspension, revocation, and re-activation
6. Renewal and replacement
7. Authentication mechanism
8. Management and organisation (of provider)
 - General provisions
 - Published notices and user information
 - Information security management
 - Record keeping
 - Facilities and staff
 - Technical controls
 - Compliance and audit

EU/eIDAS framework example

Some frameworks add IdP and federation as aspects (e.g NIST)

Most frameworks require full compliance with all requirements. Some allow «minuses» weighted towards «pluses» for other aspects

The LoA level applies to all attributes conveyed.
Is this always feasible?
Are all attributes always similarly assured?

Identity management (traditional way)



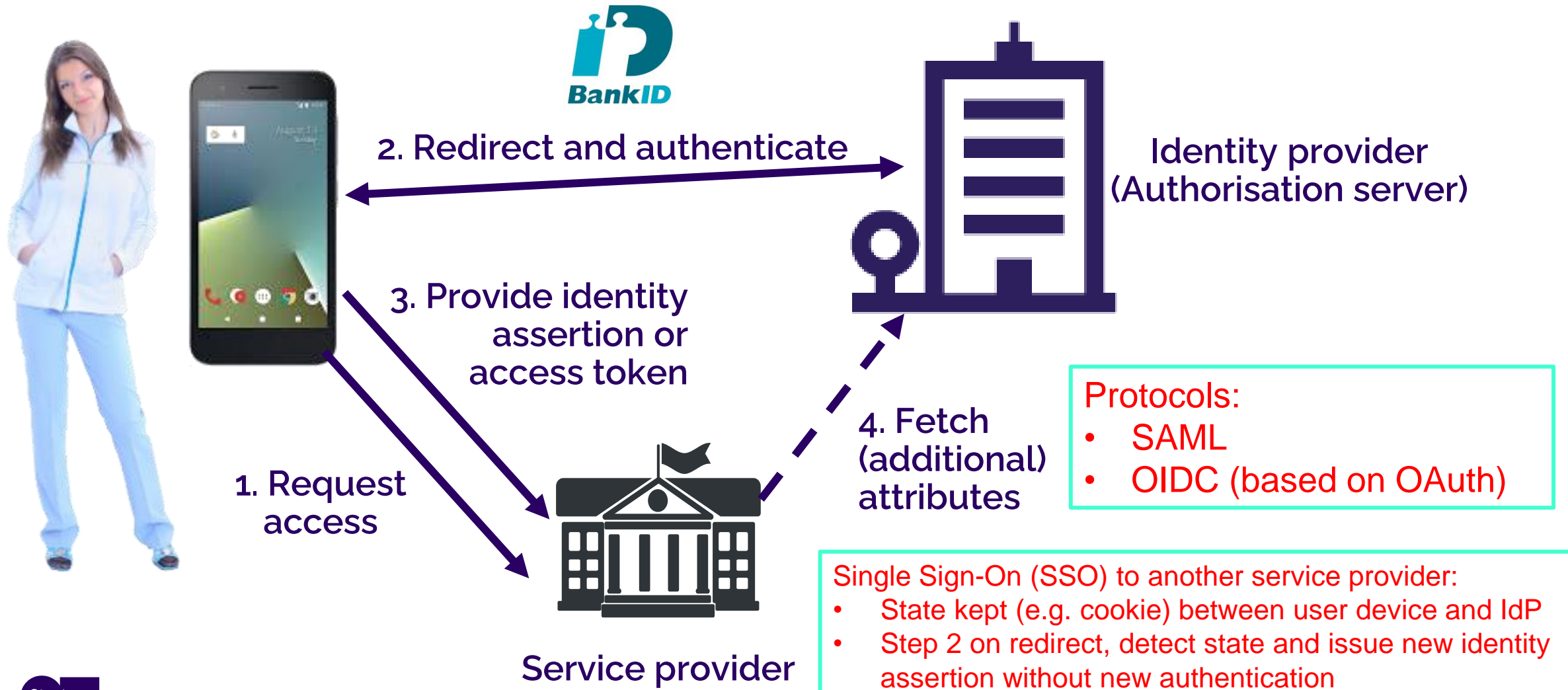
Some concepts

Not too formal

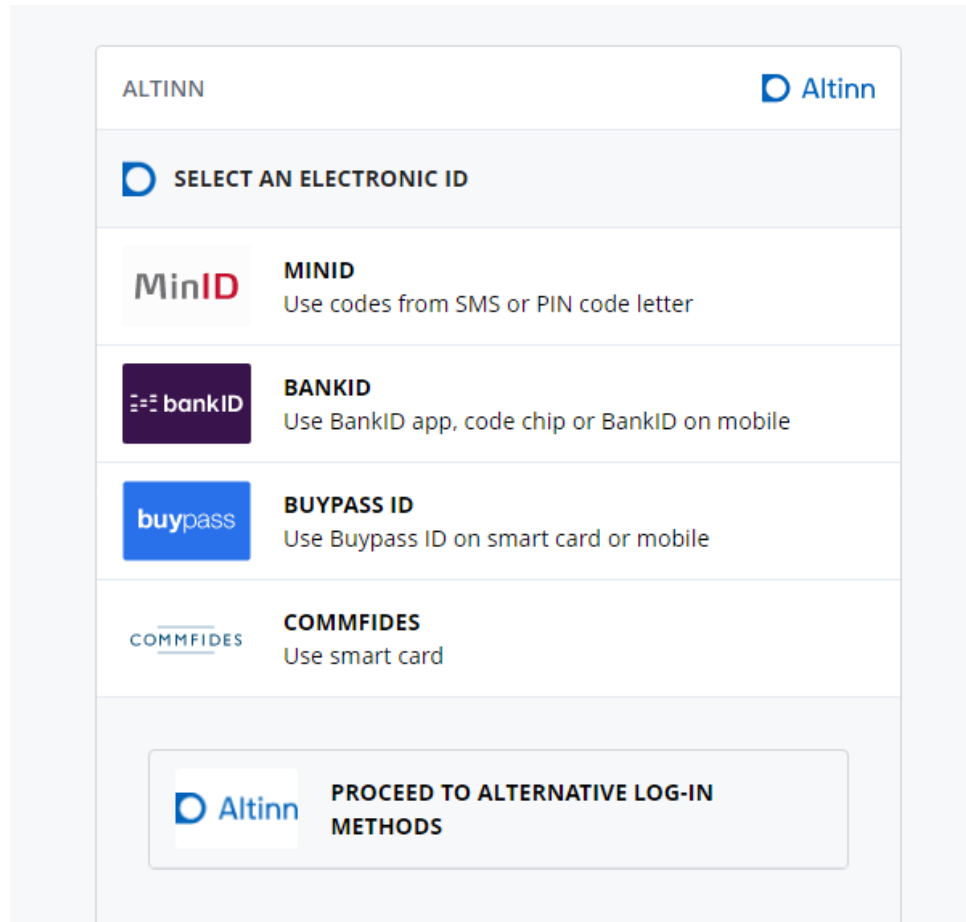
There is not one generally accepted set of terms

- **Attribute:** an identity property that can be assigned a value
- **Person identification data:** set of attributes that uniquely identifies a person or entity in a given context
- **Claim:** statement that a person or entity makes about itself or another subject (about attribute values)
- **Assertion:** proof of correctness of claim issued by an entity trusted by the receiver of the assertion
- **IdP (Identity Provider):** issuer of assertions
- **Authentication:** the act of proving unique identity (in the given context)
- **eID (electronic identity/identification):** material and/or immaterial unit containing person identification data and which is used for authentication for an online service
- **eID scheme:** governance model and technical specifications allowing interoperability between eID means from different eID providers
- **Identity federation:** trust and interoperability between IdPs

Identity provider model (simplified)



The broker model – many eIDs in one API



The screenshot shows the Altinn login interface. At the top left is the text 'ALTINN' and at the top right is the Altinn logo. Below this is a header section with the Altinn logo and the text 'SELECT AN ELECTRONIC ID'. The main content area lists five options for electronic IDs, each with a logo, a title, and a description:

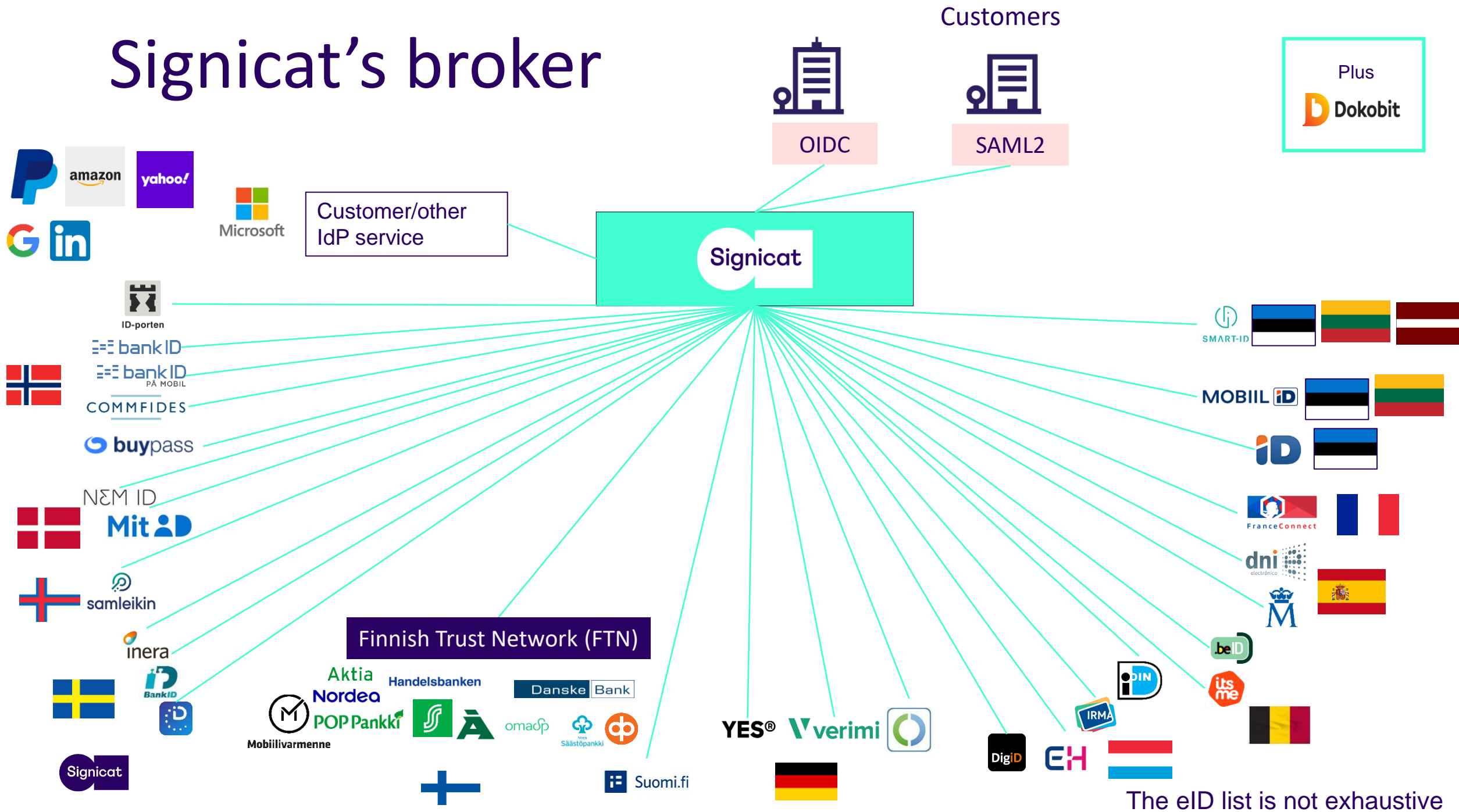
- MinID** (MINID): Use codes from SMS or PIN code letter
- bankID** (BANKID): Use BankID app, code chip or BankID on mobile
- buypass** (BUYPASS ID): Use Buypass ID on smart card or mobile
- COMMFIDES** (COMMFIDES): Use smart card

At the bottom of the list is a button with the Altinn logo and the text 'PROCEED TO ALTERNATIVE LOG-IN METHODS'.

- Service providers make one integration to an IdP
- OIDC or SAML2
- IdP shows selection menu and runs authentication
- Uniform result back to service provider

ID-porten, IdP/broker for Norwegian public sector

Signicat's broker



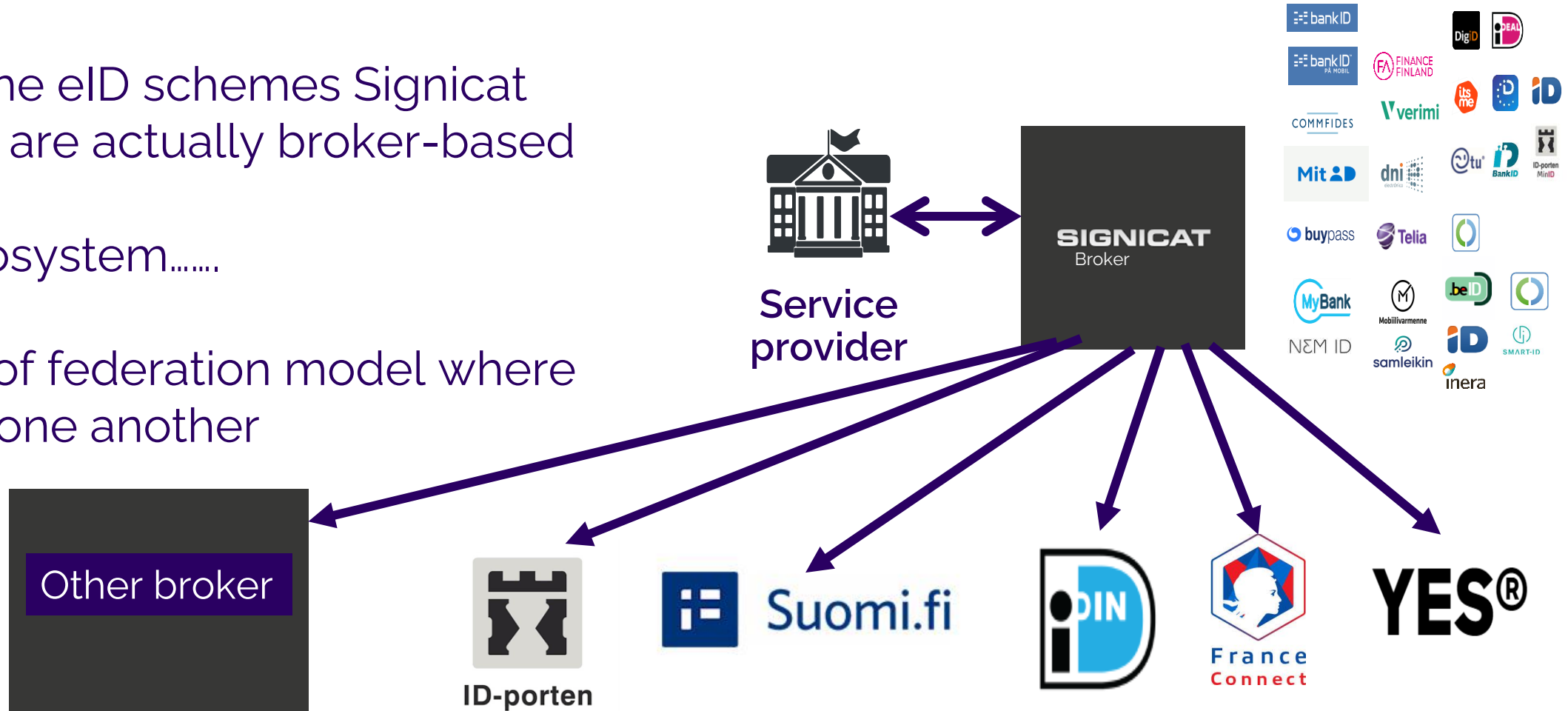
The eID list is not exhaustive

Brokers may be chained

Some of the eID schemes Signicat integrates are actually broker-based

It is an ecosystem.....

One type of federation model where IdPs trust one another



Self-sovereign / decentralised identity



The identity wallet

Identification could be by
Decentralised Identifiers (DID)

W3C[®]



Concept

Decentralized identity – no centralized repository of identity information

I am in control of my identity data

I decide what to share with whom

SSI

Self-Sovereign Identity





No-one owns the
data store

I'm the only one with
the access-key

Confidential info cannot be placed on a
distributed ledger – eventually the crypto
will become insecure

Only validation information can go on the
distributed ledger

SSI can be built without
distributed ledger

SSI

Self-Sovereign Identity



Kim Cameron's

Laws of Identity

1 User Control and Consent

Technical identity systems must only reveal information identifying a user with the user's consent.

3 Justifiable Parties

Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

2 Minimal Disclosure for a Constrained Use

The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.

4 Directed Identity

A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

5 Pluralism of Operators and Technologies

A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

6 Human Integration

The universal identity metasytem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

7 Consistent Experience Across Contexts

The unifying identity metasytem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

SSI adheres to these (but there are issues)

Traditional eIDs are all good for #7 and may cover more

Social media IDs are good for #7

The issues for «pure SSI»

1. User experience and reliability
 2. Business model for involved actors
 3. Interoperability
- No-one questions the principle of SSI(?)
 - Practical implementation may need concessions
 - A system may work perfectly well “in the lab” but fail when it is exposed to “real life”

Are people reliable?

We forget

We lose things

We are careless

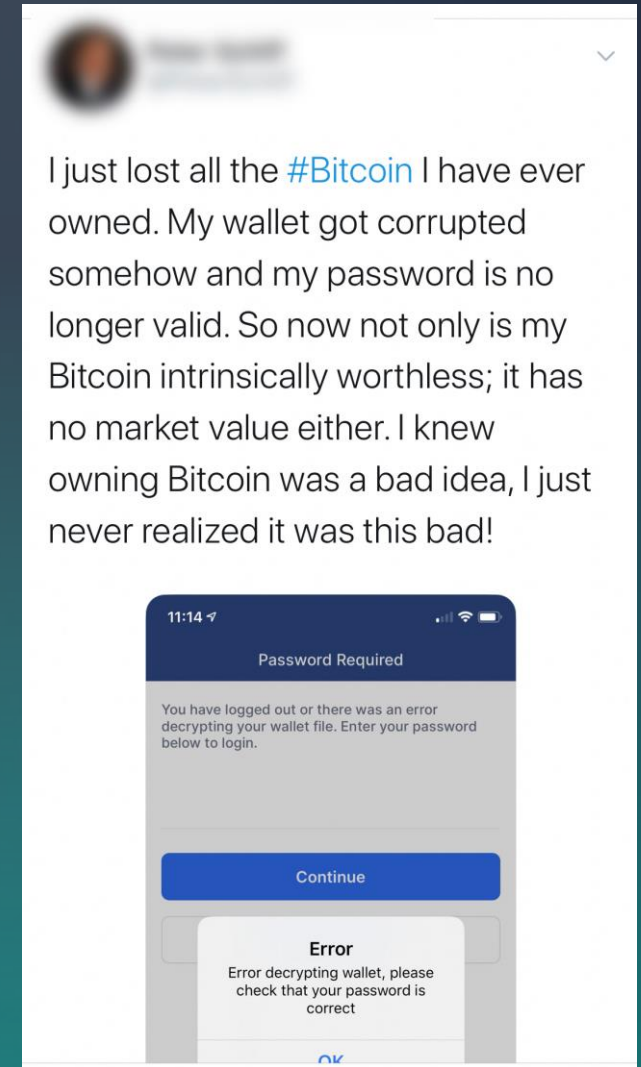
Can we manage our SSI all alone?

Will 20 % of SSIs be lost?

20 % of all bitcoins are lost

<https://www.investopedia.com/news/20-all-btc-lost-unrecoverable-study-shows/>

People want
somebody to call
when they have a problem



Twitter 2020-01-19

Business model

- **In any public identity ecosystem, all roles must have a viable business model**
 - Either roles must receive payment, or be government funded
 - Liability comes with a cost
 - As does operation of the systems
- **This is not specific to SSI but may be more difficult for SSI**

Interoperability

- **An eID scheme cannot be designed assuming it is the only one around**
 - eID schemes must co-exist or even better be interoperable
 - SSI in society must co-exist with traditional eIDs
 - Brokers should be allowed to integrate SSI-schemes (some SSI purists do not like the broker role)
- **There is a lot of attention on interoperability of SSI schemes**



The European Digital Identity Framework

AKA the EU Wallet



European Digital Identity Wallet anchored at top of EU

The Commission will soon propose a secure European e-identity. One that we trust and that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves what data and how data is used.

- Ursula von der Leyen, President of the European Commission
- Statement at the "state of the Union" speech, 16th September 2020

Motivation:

- Strengthen the internal market
- More efficient government
- Strengthen the EU (cross-border) perspective
- Fight "big techs" – one of several initiatives

Objectives for monitoring:

- Provide access to eID means for all EU citizens
- Increase cross-border recognition and acceptance of eID scheme, with an ambition to reach universal acceptance
- Stimulate adoption by the private sector and the development of new digital identity services



Legislative means

Revision of the eIDAS regulation

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

European Digital Identity Framework with toolbox

COMMISSION RECOMMENDATION of 3.6.2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework

Coordination with other legal initiatives such as Digital Services Act and Digital Markets Act

They are serious about this....

Call for large-scale pilots

- Call for large-scale pilots, deadline **17. May** (may be prolonged)
 - Deployment of the EU Digital Identity Wallet (37 MEuro)
 - EBSI services (European Blockchain Services Infrastructure) (15 MEuro)
 - Blockchain standardization (1 MEuro)
 - AI security in law (5 MEuro)
- At least 4 pilots on the Wallet
- 50 % contribution from EU, same amount added by participants
- Digital Europe programme – this is not research
- Only “wallet responsible” agencies in Member States can submit applications
- Both public and private sector participants

The immediate effect

Enormous increase in interest
in SSI, distributed identity and
wallet-based systems

The first examples of
useful SSI/wallet schemes
were already launched



What is the EU Wallet?

- A **level high** eID that can be used nationally and across borders
- Issued based on national identity documents/procedures
- Providing basic identification of official identity
- Providing attributes and attestations in addition to or instead of basic identity
- Enabling use for qualified electronic signatures
- Full user control on release of information («**SSI inspired**»)
- **Government responsibility, issued nationally, eID still a national competence:**
 - a) By government itself
 - b) On behalf of government (public procurement)
 - c) By private actors approved by government



Means a wallet provider cannot operate cross-border
And a commercial provider has limited opportunities except with c)

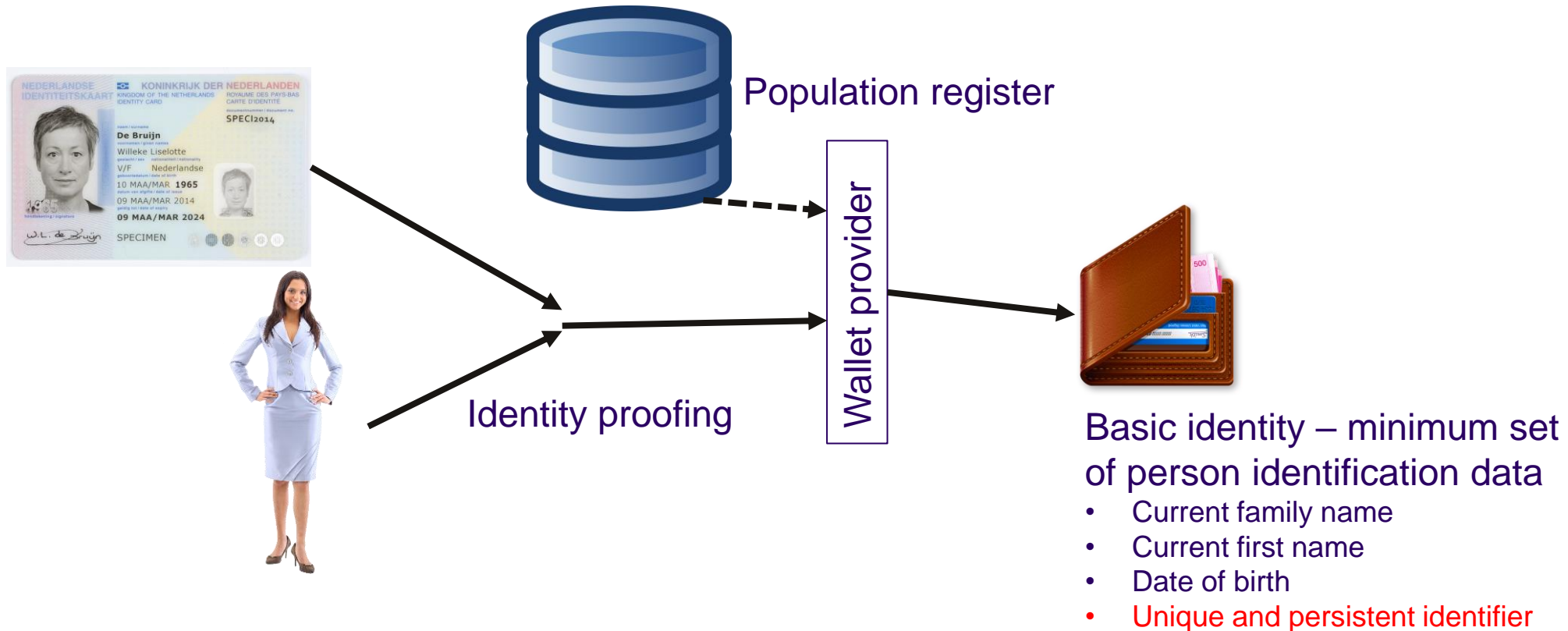
Some technical issues

- Few (but some) standards to build on – depending also on what you mean by «standard»
- Mobile/app as user device – access to secure element, what about ubiquitous access?
- Emphasis also on offline use
 - Clarification, handover only – the wallet and the receiver may be required to have network access
- All interactions through wallet, external interfaces responsibility of wallet provider
 - User control plus scaling («back channels» to information sources not needed)
- Common «toolbox» to be developed – mandatory for all wallets
 - First draft version issued late February
 - Technical architecture, reference model, standards – but zero technical content in first version
 - “Reference implementation” to be developed – dispute on whether this will be mandatory (hopefully not) or only an offer

Where will wallet acceptance be mandated

- Public services, cross border
- Private service providers required to use strong user authentication
 - Transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education, telecommunications
- Very large online platforms as defined by Digital Services Act – meaning the “big techs”
- More can be added

Initiating the wallet

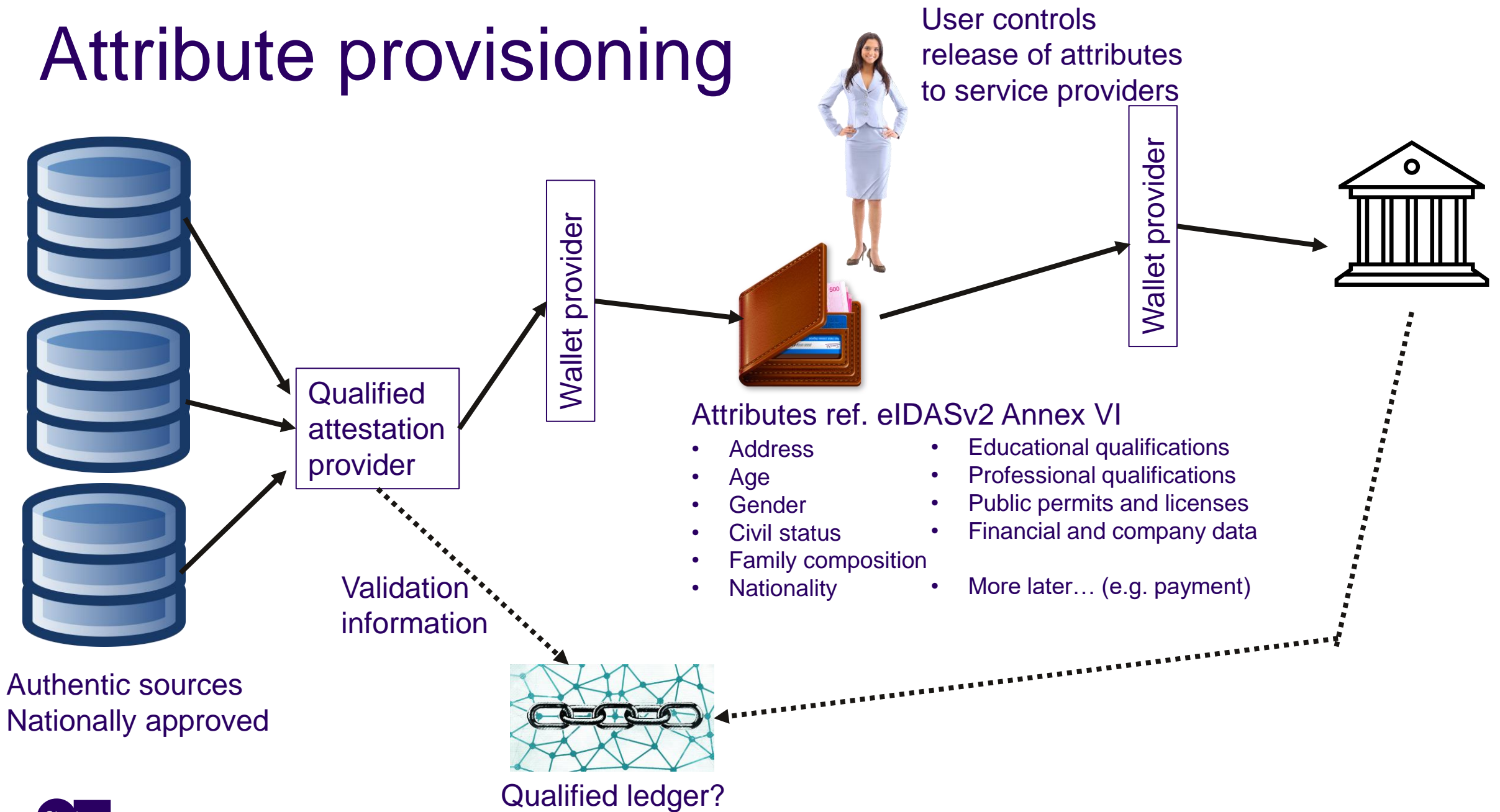


New requirement with eIDASv2 and possibly a controversial issue

Wallet provider is

- Government or someone on behalf of govt.
- Commercial provider approved at **national** level

Attribute provisioning



Some relevant specifications for wallet

Wallet use of trust services
Attribute attestation



Open ID Connect



CC protection profile for wallet
European citizen card
European breeder documents



Verifiable credentials
Decentralized Identifiers (DID)



ISO/IEC 18053-5 Mobile driving license
Identity management standards
Biometric security standards
Cryptography



National and EU
pilots and projects

NIST identity framework?



Risks and opportunities

Will the wallet happen? **YES**
Will it be a success? **Who knows**

One extreme: EU Wallet is hardly used – other eIDs prevail

Middle situation: EU Wallet is one of several eIDs

Other extreme: EU Wallet becomes the only eID in Europe



Successful eID deployments are almost always public-private co-operation, mainly financial industry



Will these be forced out of business?
Competition law, state subsidies?

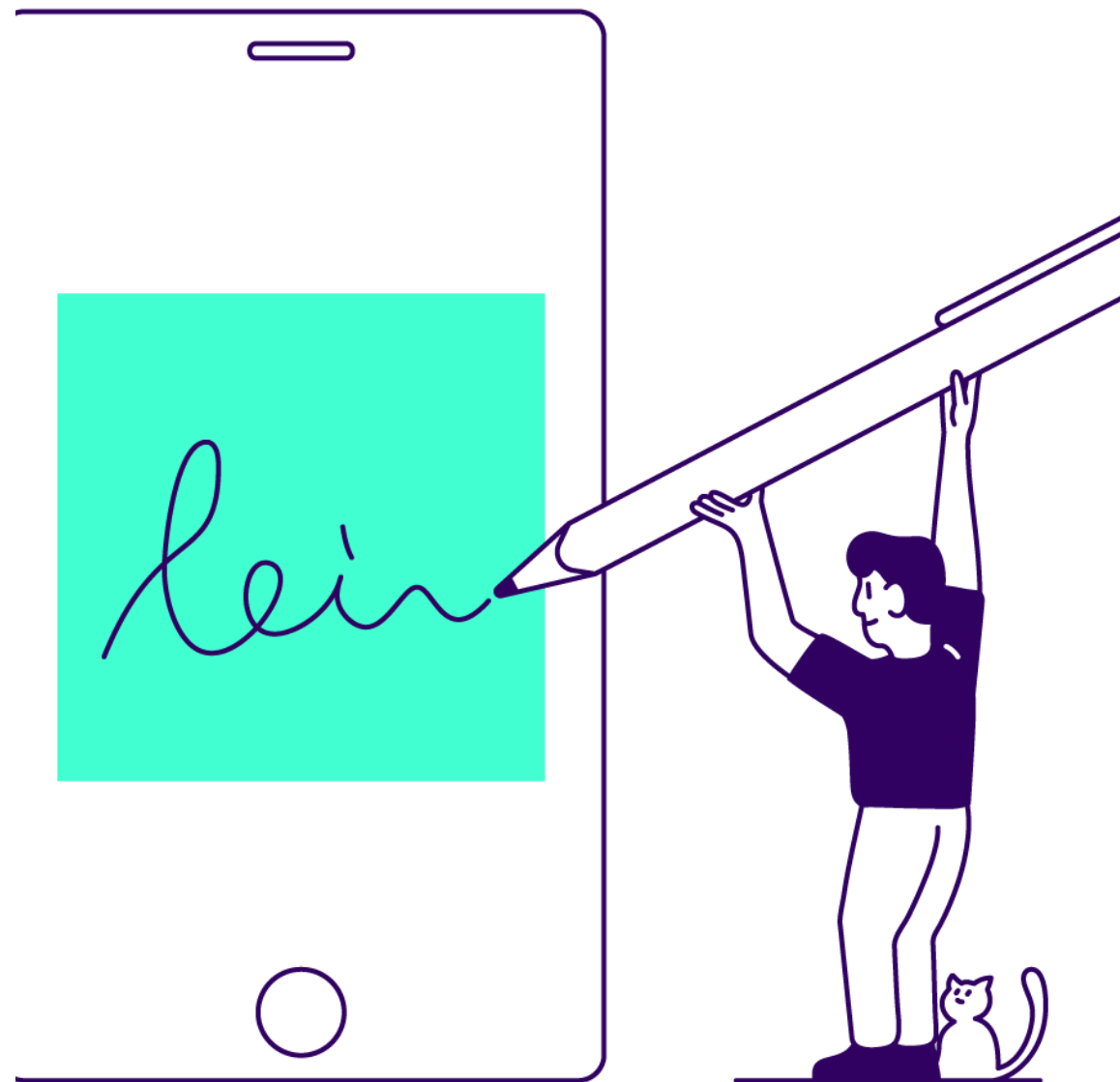
Business model?

- User does not pay, but service providers will
- How are all actors (e.g. attribute provider) paid?
- Business for wallet provider?

Evident risks:

- Government priority on getting wallet in place?
- Wallet is voluntary for users
- Governments are notoriously bad at sales and marketing
- Proposed timeline way too optimistic

Signing (EU example)



Electronic signature policy: The what, why, who, and how

- One always signs as part of a (business) process
- Specifying signing for a process means:
 - **What to sign** (what documents at what steps of the process)?
 - **Why** (legal and other implications of signatures)?
 - **Who** (competence or role of signers)?
 - **How** (signature level, formats and other technicalities)?
- A specification of what, why, who and how is a **signature policy**
- Signature policy can be implicit in process description or explicit (a document)

Approaches at regulating signing

- EU: Focus on strength of mechanism
- US: Focus on the intent of the signers, then «anything goes»
- UN UNCITRAL model law on electronic signatures, more towards the EU approach
- Laws are as starting point technology neutral
- Might in reality point at specific technology (e.g. PKI)



- **Electronic signature**: legal term for the act of signing
- **Digital signature**: technical term for a specific use of public-key cryptography

Electronic signatures in the eIDAS regulation

- Three (or four) “levels” of signature/seal

- Electronic Signature/Seal (ES) – “anything goes”
- Advanced Electronic Signature/Seal (AES)
- Advanced Electronic Signature/Seal with qualified certificate (AES/QC)
- Qualified Electronic Signature/Seal (QES)



Sign



Seal

Natural person Legal person

AES defined in eIDAS Article 26:

- (a) it is uniquely linked to the signatory;
- (b) it is capable of identifying the signatory;
- (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
- (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

QES is AES with two extras:

- Identity assessed by qualified certificate
- Private key protected in QSCD (Qualified Signature Creation Device)

Must rely on public-key cryptography and PKI (today)

QES as a common denominator

- eIDAS defines signature levels, not the signature level required for different purposes
- Such requirements are set by national, sectorial law, occasionally by EU regulations/directives
 - Different countries, different requirements
 - “For any purpose, one is likely to find at least one country requiring QES”
- QES is the highest level, guaranteed compliance and cross-border use
 - There is a push for QES by the EU and many Member States
 - Nationally, AES or even ES can work perfectly well in many countries

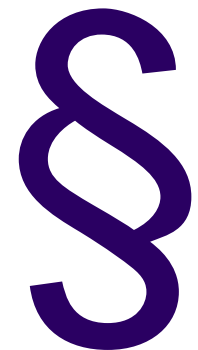
In Europe, seamless signing means seamless QES



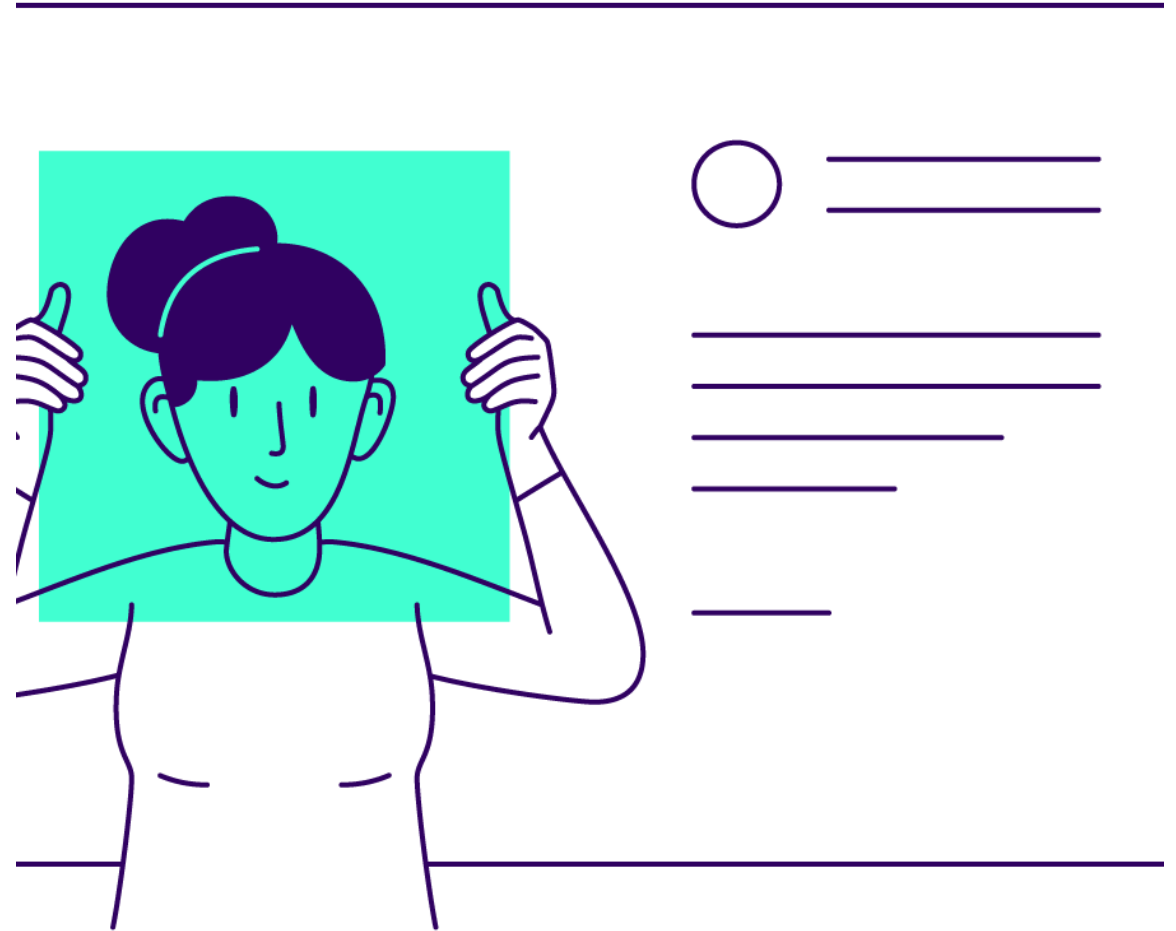
The misconception of «legally binding»

- **A priori, any electronic signature is binding** (eIDAS Article 25.1)
 - Compliance requirements may demand a specific signature level
 - E.g. requiring QES for a purpose
 - Non-compliant signatures **may** be considered as non-binding
- **The legal binding of any signature can be disputed**
 - If a court believes that the signer did not intend to sign, not even a QES will be legally binding
 - Signer is tricked, fooled or threatened to sign
 - Signer did not understand the process or the implications of signing
 - Signer signed something else than the intended content
- **QES is guaranteed compliant but not guaranteed legally binding**

eIDAS Article 25.1:
An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures

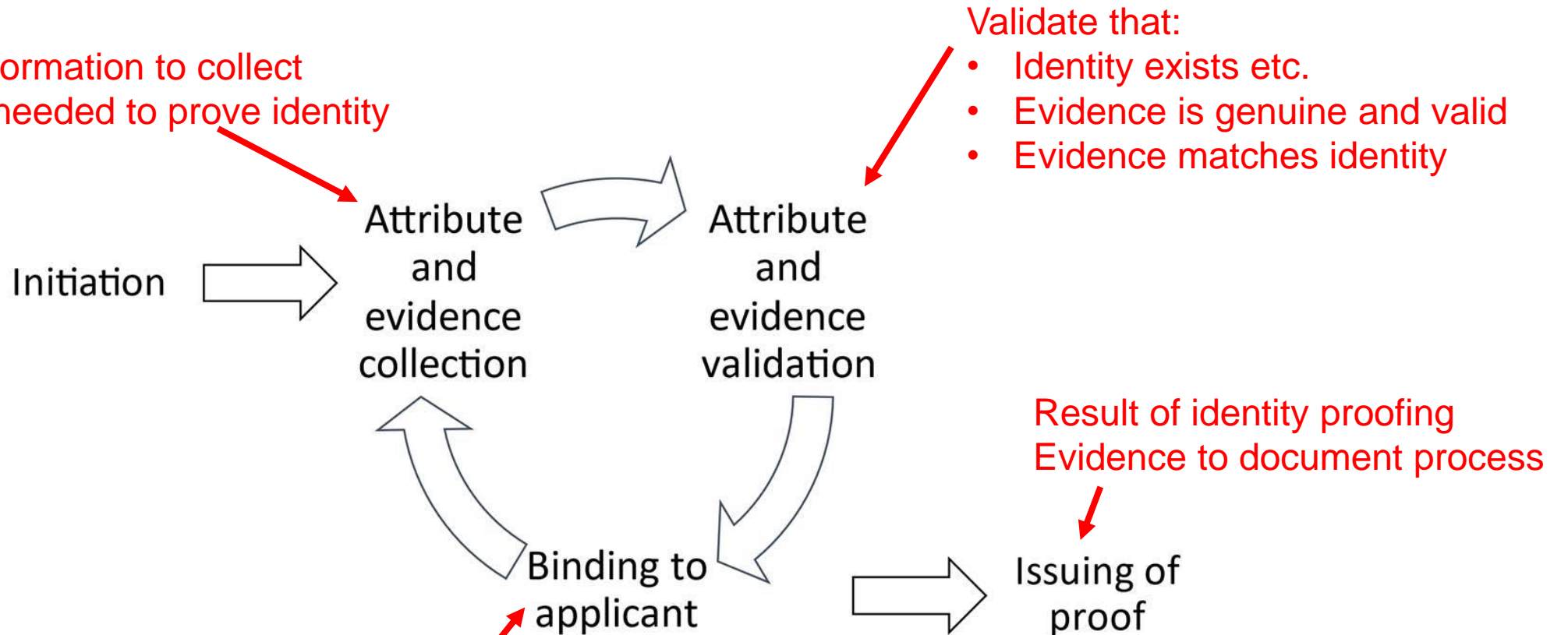


Identity proofing (EU examples)



The identity proofing process

The identity information to collect
The evidence needed to prove identity



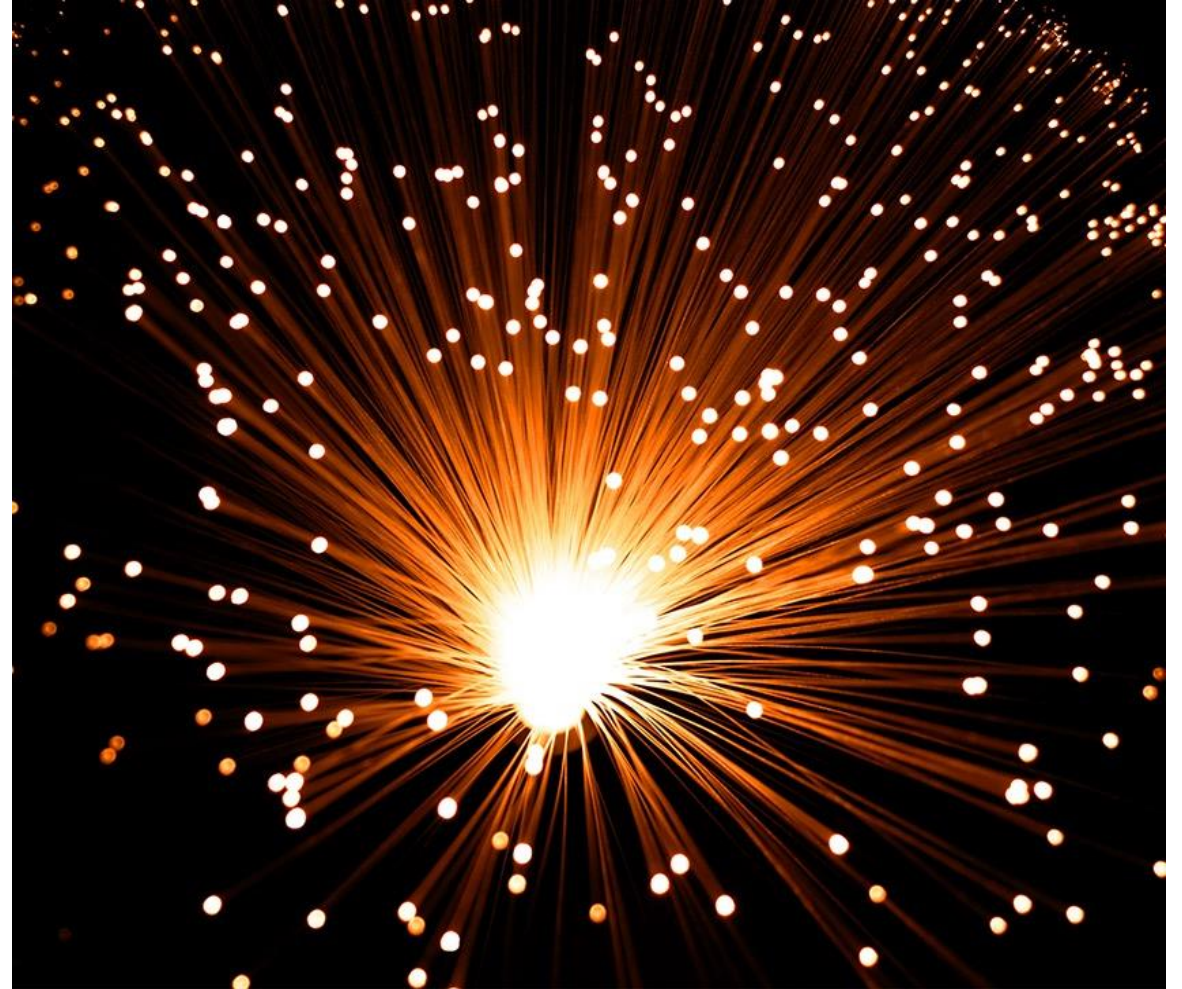
When identity documents are used:

- Manual face verification
- Biometric face verification

Let us look at current status of three areas in EU

... and the resulting chaos

1. Financial services according to AMLD5
2. Issuing of eID
3. Issuing of qualified certificates according to the eIDAS Regulation



AMLD5 is a directive

- implemented differently in different Member States

AMLD5 Article 13.1(a):

identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means, relevant trust services as set out in *[the eIDAS Regulation]* or any other secure, remote or electronic identification process **regulated, recognised, approved or accepted by the relevant national authorities;**

Example Nordics:

- Norway requires eID "high" and eID "self-declared" according to national rules
- Sweden/Denmark/Finland all have only eID "substantial" available, plus uncertain if foreign "eIDAS notified" eIDs can be accepted for financial services in Norway
- => Norwegian service provider cannot onboard users from other Nordic countries



Issuing of eID

... is national and governed by the Member States

No-one issues an eIDAS eID. One issues a **nationally approved eID** that may then be «eIDAS notified» as a cross-border eID for public services

eID approved against national assurance level framework with **national rules for identity proofing**. National frameworks may or may not be aligned with eIDAS assurance levels. **May contain rules for remote identity proofing – or not.**



Issuing of eIDAS qualified certificates

... the infamous eIDAS Article 24.1, four ways of identity proofing

- a) Physical presence
- b) eID means at substantial and high, issued on basis of physical presence
- c) Certificate of qualified electronic signature/seal (issued according to a or b)
- d) **Other means recognised at national level to provide equivalent assurance to physical presence**

Which means? Passport office, bank branch, lottery commissioner, ...? **National rules can apply.**

But the LoA specification (CIR (EU) 2015/1502) does not require physical presence, not even for high

OK – you already got one, and need another

Equivalent to what (see above)?
Some Member States have adopted (different) rules, most have no national rules leaving this space open

ETSI standards for trust services are equally vague in their identity proofing requirements

ETSI TS 119 461 Policy and security requirements for identity proofing of trust service subjects

Strictly speaking for trust services only but should be applicable to other areas

- Issuing of qualified certificate == eID substantial (eID high based on standard should be possible)
- Current EBA consultation on identity proofing for financial services suggests lower level, but that can still be influenced

Standard defines one Baseline level of identity proofing sufficient for qualified trust services – level can be reached in various ways

Authoritative evidence – at least one of these must be used

- Physical identity document – passport or national identity card
 - Use for physical appearance
 - Use with remote scanning and validation (video capture of document required)
- Digital identity document – read from NFC chip of passport or national identity card
 - Use with physical appearance and specialized equipment (ala border control)
 - Remote reading from chip with validation of signature on document
- eID used in an authentication protocol
- Digital signature with identity certificate



 bankID

 buypass

 COMMFIDES

Supplementary evidence (can be authoritative regarding identity information)

- Trusted register (e.g. a population register or business register)
- Proof of access (in particular to bank account)
- Documents and attestations (important for legal persons)

Use cases:

- Physical presence
- Attended remote (physical presence at a distance)
- Unattended remote (can be automated with digital identity document)
- eID for authentication
- Digital signature with certificate

Some highlights – the consensus in ETSI

- Remote identity proofing
 - Remote capture of facial image of applicant requires video sequence – photo not sufficient
 - Digital identity document required for automated processing – validate signature on document, face biometrics against high resolution reference picture from document
 - Physical identity document scanning requires real-time video sequence – photo not sufficient
 - Manual validation of physical document allowed, combined manual and machine learning technology recommended
 - Requirements for both manual face verification and automated face biometrics
- Requirements for manual processes including physical presence
 - Training, face comparison, document validation

Moving forward in the finance area

- EU Digital Finance Package launched September 2020:
- Digital Finance Strategy, 4 priorities:
 1. Remove fragmentation in the digital single market
 2. Adapt the EU regulatory framework to facilitate digital innovation
 3. Promote data-driven innovation in finance by establishing a common financial data space
 4. Address the challenges and risks associated with digital transformation

Digital Finance Strategy and KYC (1)

- remove fragmentation in the digital single market by defining a new AML framework **enhancing the financial service providers' ability to authenticate the identity of the customers** and defining by means of **technical standards** of the European Banking Authority **identification and authentication elements for customer on-boarding purposes.**
- By 2024, the EU should implement a **sound legal framework enabling the use of interoperable digital identity solutions** to access financial services based on **more harmonised anti-money laundering (AML)** and a revised eIDAS Regulation. It should **enable customer data to be reused subject to informed customer consent**

Digital Finance Strategy and KYC (2)

- *ensuring greater convergence on the elements related to identification and verification needed for onboarding purposes [...] without the need to apply different processes or comply with additional requirements in each Member State, therefore making it easier to identify customers and check their credentials. [...] this could be done by stating what ID documents are needed to establish a person's identity, and by clarifying which technologies can be used to check ID remotely*

Timeline and likely actions

- **2018-2020: EU expert group on KYC in financial services**
 - Status report on KYC in EU Member States, Study on reuse of KYC information
- **Q3 2021: Publication of European standard**
 - ETSI TS 119 461 Policy and security requirements for identity proofing of trust service subjects (formally scope is only trust services but use for other purposes possible)
- **Q4 2021: EBA request for input on guidelines on harmonisation of KYC**
 - Can the ETSI standard be made relevant?
- **2021-2022/23: Revision of the eIDAS Regulation on eID and trust services**
- **2024: EU legal framework enabling use of interoperable digital identity solutions (for KYC) building on the revised eIDAS**
 - Allowing reuse of customer data based on user consent
- **2024/25: AML Regulation (common EU law) to replace AML Directive**

Moving forward in trust services

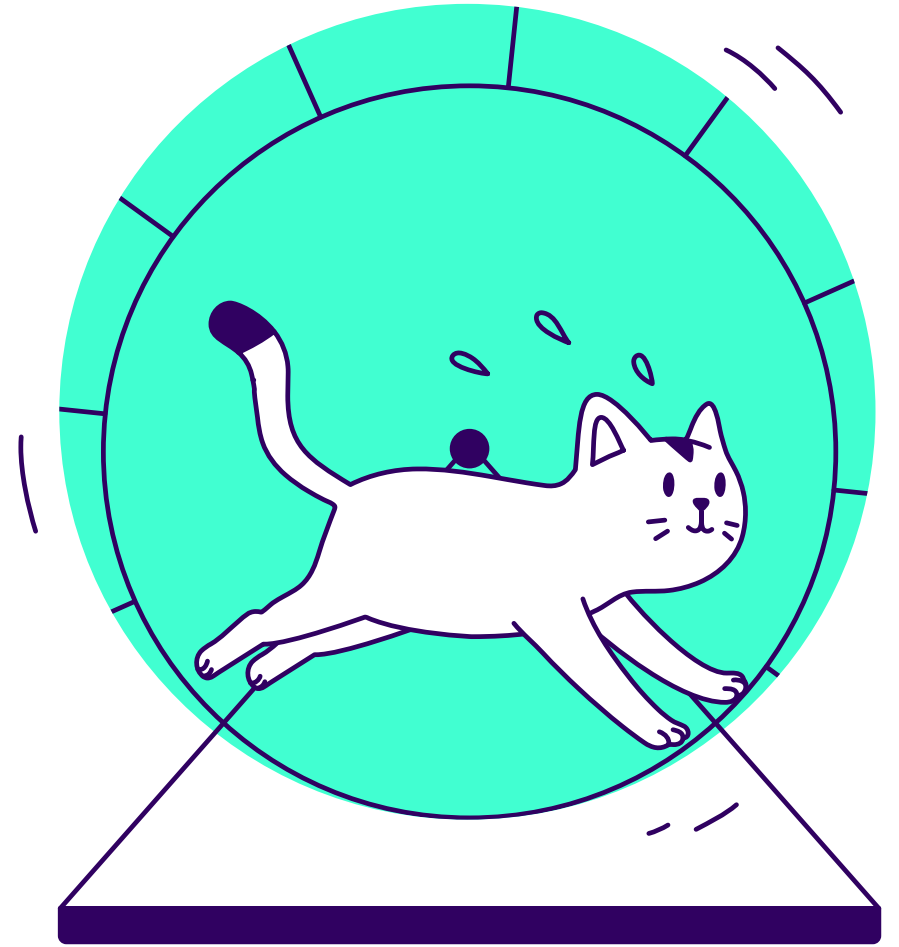
- **Proposal for revised eIDAS changes Article 24.1 (issuing of Q-cert)**
 - Physical presence
 - Notified eID at Substantial or High (the notified requirement may not be well thought.....)
 - Qualified attestation of attribute or certificate of qualified signature/seal
 - Other identification methods that ensure a **high level of confidence** (confirmed by an auditor)

- Commission shall provide an implementing act pointing to specification of identity proofing for «other methods», **should refer to ETSI TS 119 461**

Moving forward in eID

- Less clear, but the eID area is «in play» with the «European digital identity wallet» introduced by proposed revised eIDAS
- The standard can be used
 - Directly for issuing of eID Substantial?
 - Additional profiling to reach eID High?

Regulating identity, (eIDAS, EU example)



What is eIDAS?

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC



eIDAS-
compliant

Covers three topics:

1. eID
 2. (Qualified) trust services
 3. Legal provision for acceptance of electronic documents
- **Legal text, not a technical specification**, in principle technologically neutral
 - European technical standards produced to meet eIDAS requirements

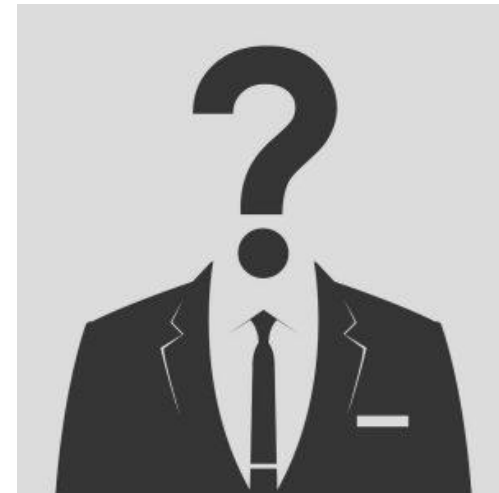


Revision of eIDAS in progress

- Draft revised Regulation published June 2021
- Changes expected from comments by Member States and others
- Expected to be approved ~~early/mid~~ late 2022

eIDAS eID – today

- Only covers cross-border eID and only for public services
- Identity and eID are national and governed by the states
- eIDs notified by governments for x-border use
- Public services required to accept foreign, notified eIDs
- “eIDAS infrastructure” with national nodes exist



Trust services in eIDAS

- **Founded on treaty on the internal market**
- **Commercial services cross-border**
- **Closed set of services:**
 - Certificate issuing (e-signature, e-seal, website)
 - Validation of e-signatures and e-seals
 - Preservation of e-signatures and e-seals
 - Time-stamping
 - Electronic registered delivery
 - (Signing – cannot be qualified)

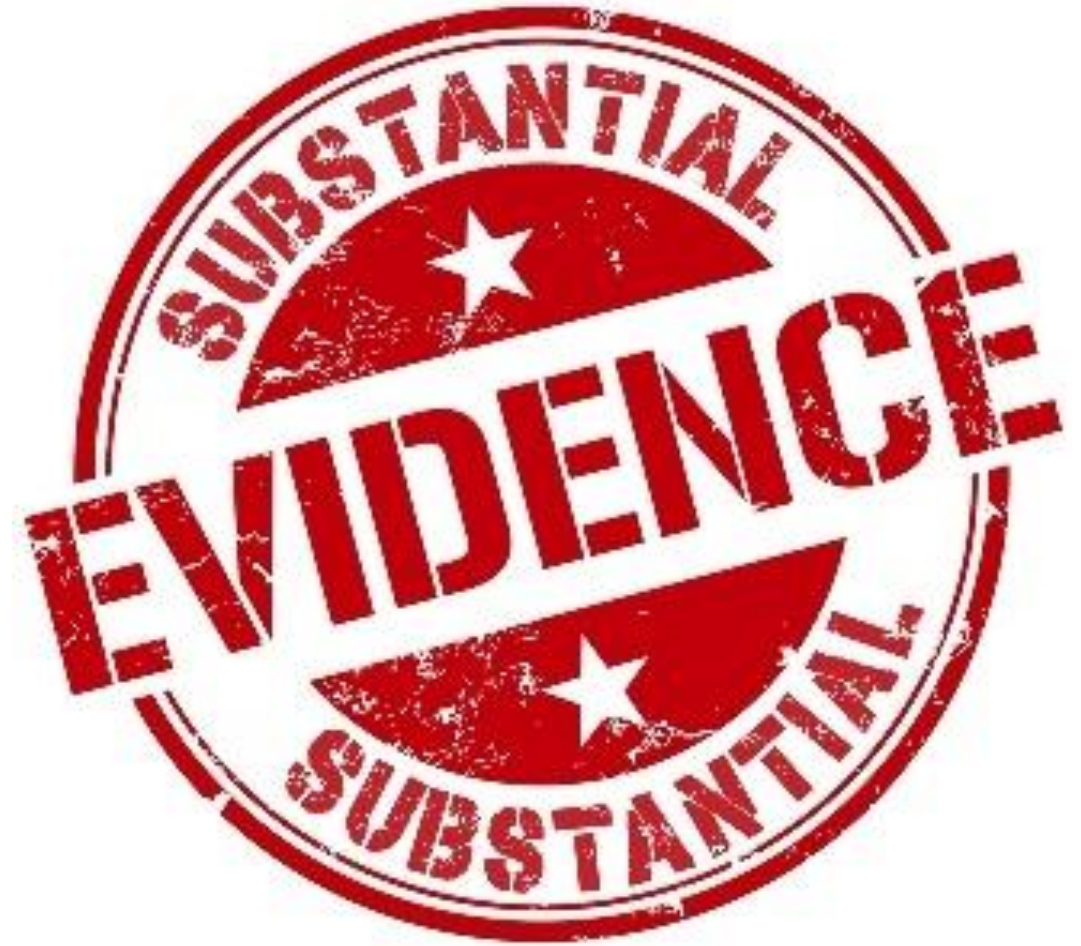
- **Qualified trust services**
 - Fulfilling eIDAS requirement
 - Audited and supervised
 - Highest level possible
 - “Guaranteed acceptance”
- **Non-qualified**
 - Few eIDAS requirements
 - Light-weight supervision
 - No guaranteed acceptance

- **Publication on qualified services in the EU Trusted List system**



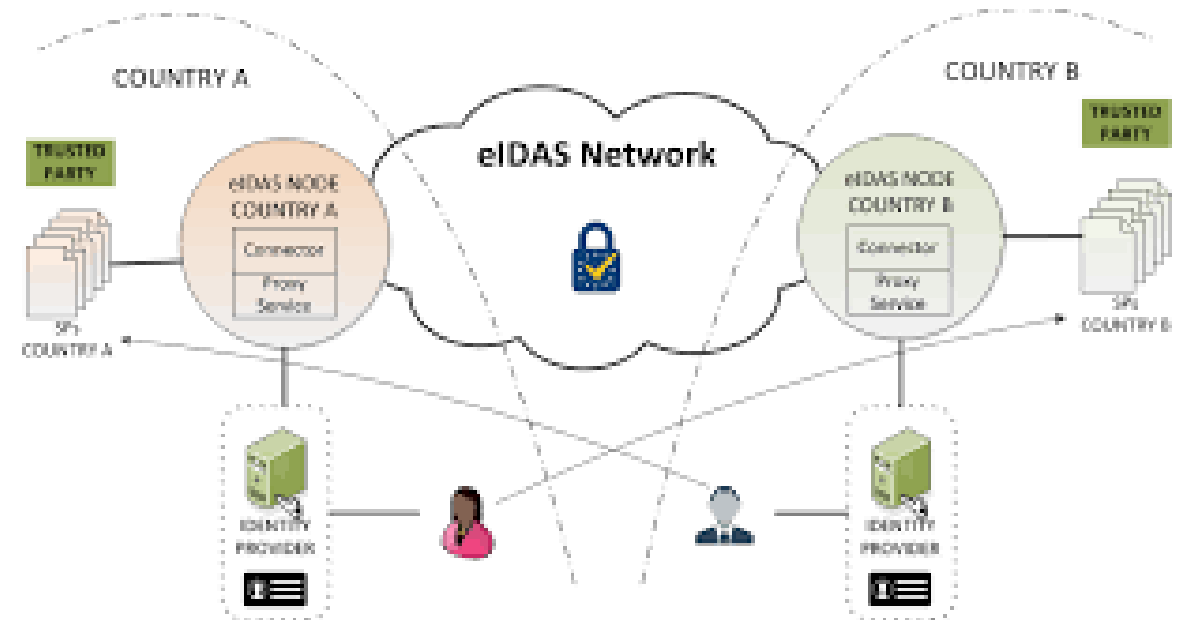
eIDAS eID – what has worked

- Alignment of national eID levels of assurance (LoA)
 - **Substantial** and **high** as pan-European reference levels
- Attention on the role of eID and cross-border acceptance



eIDAS eID – what has not worked (or hardly)

- **The notification system**
 - Only some countries notify
 - Minimal practical effect
- **The eIDAS infrastructure**
 - Works, but old-fashioned
 - Not available to private sector
 - In practice not used
- **Lack of eID deployment and/or use at national level**
 - Will not work cross-border if it does not work nationally



Overall, eIDASv1 eID has largely failed

Trust services – what has worked

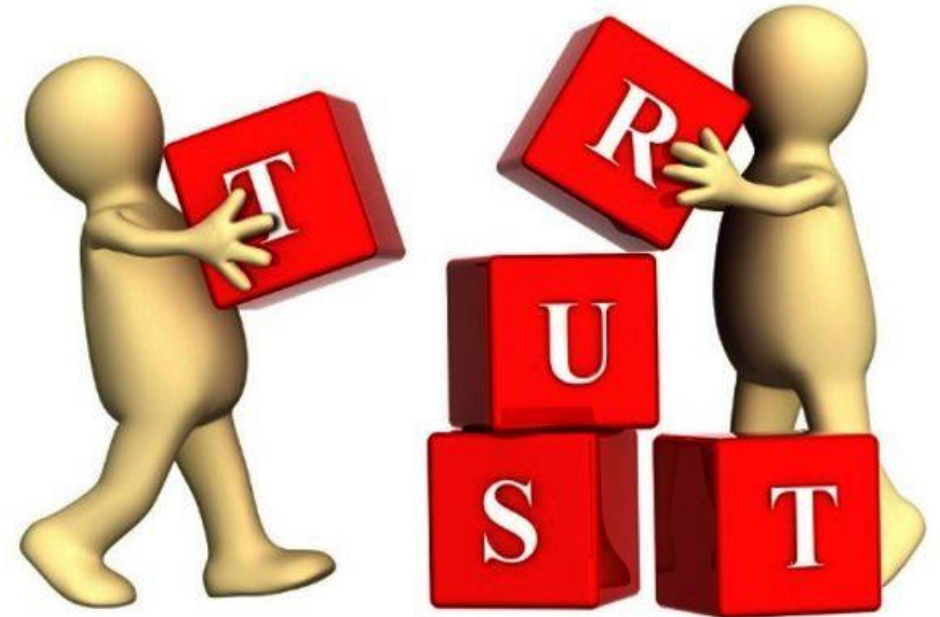
Alignment of Qualified across Member States



- Not perfect but pretty well
- With standards as firm base
- Well established conformity assessment

Trust services – what has partly (or not) worked

- **Cross-border service provisioning**
 - Not much but slowly evolving
- **Qualified as a concept**
 - Still the ultra-secure and expensive option
- **Trusted Lists**
 - Works only for specialized software and services
- **Deployment and use (national/international)**
 - Can only be achieved if seen together with eID



Overall, eIDASv1 trust services is not a failure but also not a great success

eIDAS, implementing acts and standards

Possibilities for delegated and implementing acts



29 pointers to delegated/implementing acts

Some state Commission shall implement, other state may implement

8 acts decided

Delegated and implementing acts apply for all Member States

European and international standards



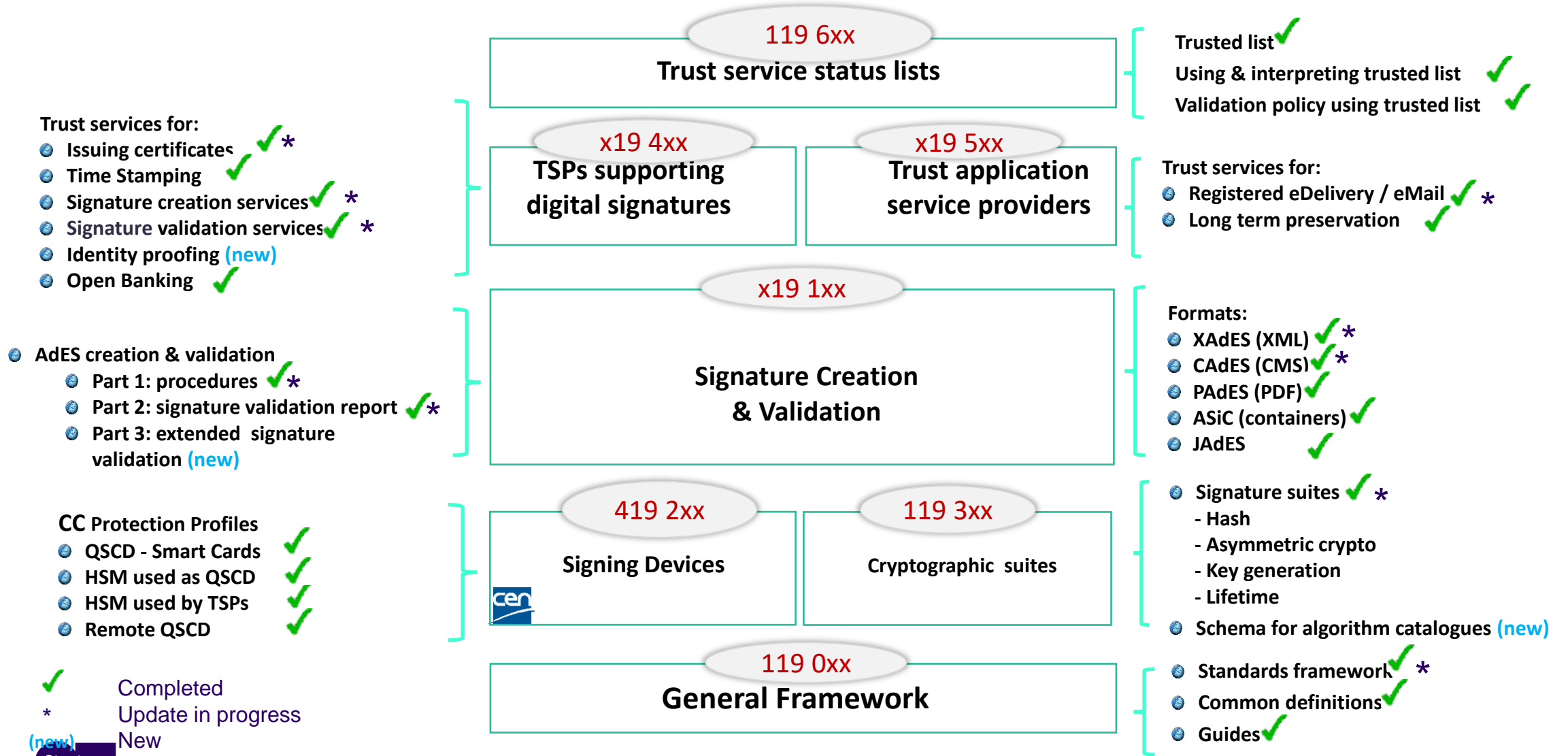
Few or none relevant standards from these bodies on eID

ETSI and CEN has Commission mandate to develop standards for trust services

Implementing acts for trust services can to a large degree only point to standards

1. **Comitology decision** – expert committee develops (technical) specifications approved by Commission. Mostly for eID.
2. **Reference standards** where use implies “presumption of compliance”. No standard can be mandatory. For trust services.
3. **No implementing act** but **guidelines**, e.g. by ENISA, as “soft measure”. Used for both eID and trust services.
4. **Do nothing** (now). Either because no useful standard exists (yet) or to let the market decide. Used for some trust services.

Framework for standardisation for Digital Signatures and Trust Services



- Trust services for:
- Issuing certificates ✓ *
 - Time Stamping ✓
 - Signature creation services ✓ *
 - Signature validation services ✓ *
 - Identity proofing (new)
 - Open Banking ✓

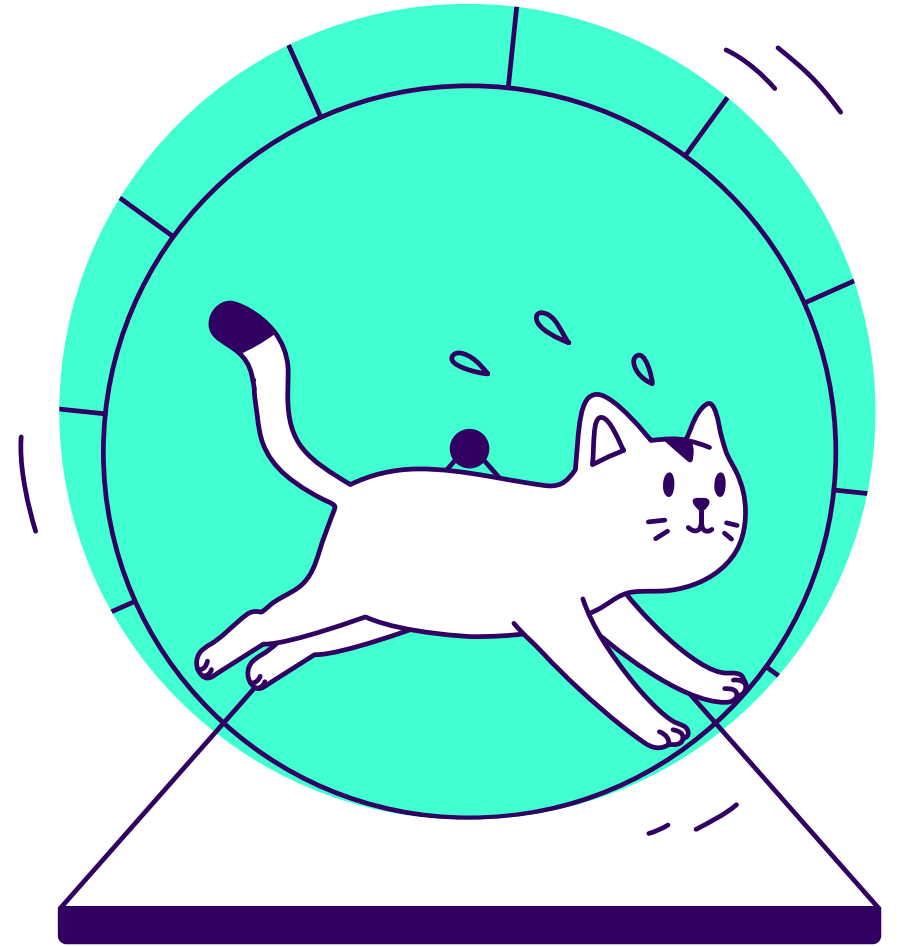
- AdES creation & validation
 - Part 1: procedures ✓ *
 - Part 2: signature validation report ✓ *
 - Part 3: extended signature validation (new)

- CC Protection Profiles
- QSCD - Smart Cards ✓
 - HSM used as QSCD ✓
 - HSM used by TSPs ✓
 - Remote QSCD ✓

✓ Completed
* Update in progress

(new) New
Signicat
ETSI

The eIDAS revision (proposal) including the wallet



Changes in eIDAS eID

- Introduction of the «European Digital Identity Wallet»
- Requirement to include a unique and persistent identifier in the minimum set of person data
 - Even for countries that do not use a national identity number
 - To be able to link identities cross border
- Easier procedures for notification by Member States (certification)
- Member States must notify at least one eID / eID scheme for cross-border use
 - The EU Wallet is one – must be notified
 - National identity cards – what we use for identity proofing
 - Other eIDs issued by government, issued on behalf of government, or approved by government (as today)
- eID is still a national competence
 - But much further towards EU harmonisation
 - Many wanted «eID as a trust service» to place eID issuing in the open market
 - Presumably Member States could not accept that

eIDAS revision – trust services

New (qualified) trust services added

- Electronic attestation of attributes
- Recording of data into an electronic ledger
- Electronic archiving of documents
- Management of remote e-signature/-seal creation devices

Relevant for the EU Digital Identity Wallet

Proposal to place qualified trust services under the upcoming NIS2 Directive

Proposal that Commission **shall** provide implementing acts – mostly pointers to standards

Within ETSI's standardisation mandate
Work starting now on new trust services
Remote signing covered by existing standards



eIDAS revision and standardisation



- European digital identity wallet – standardisation by «the toolbox»
- Electronic attestation – profiles for signing and validation and more
- Archival – ISO standards and more exist, may be need to «EU'ify», in case ETSI
- Electronic ledger – standardisation likely needed, ETSI has started some work
- Remote signing finally a qualified trust service on its own!
- Policy and security standards – revision due to NIS2 requirements?

Attestation of attributes

Trust service provider (a commercial actor) signing declaration on attributes from authentic sources

- 'authentic source' is a repository or system, held under the responsibility of a public sector body or private entity, that contains attributes about a natural or legal person and is considered to be the primary source of that information or recognised as authentic in national law;

Minimum set of attributes must be available from each Member State

Interface to the EU Wallet required

Risks:

- To what extent are “authentic sources” for these attributes available?
- Potentially huge standardisation effort on syntax and semantics of attributes

(Qualified) Electronic ledger

There are initiatives piloting a pan-European ledger system

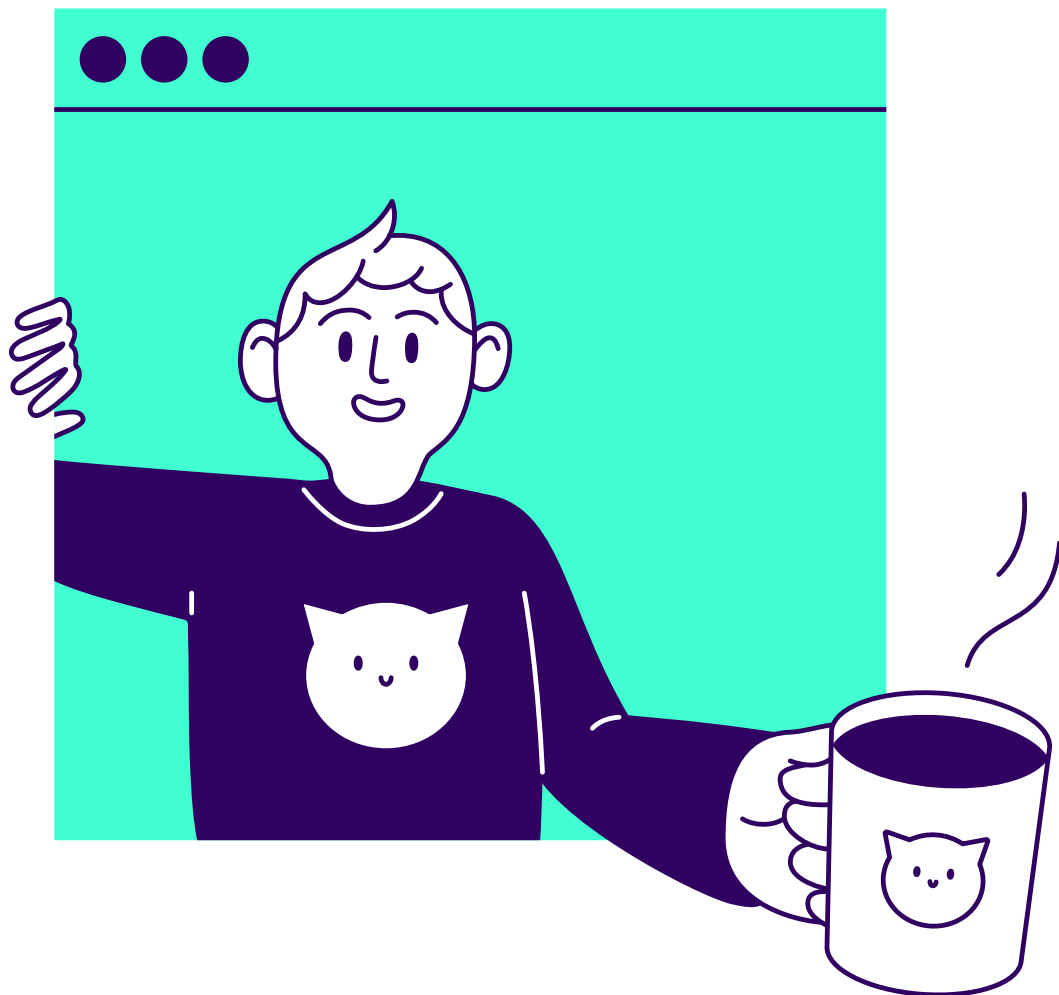
- European Blockchain Services Infrastructure (CEF Digital)

Remove reliance on cryptocurrency ledgers and similar systems

Qualified electronic ledger as a trust service

- Qualified ledger created by one or more qualified trust service providers – commercial services
- Presumption of uniqueness and authenticity of the data contained, of accuracy of date and time, and of the sequential chronological ordering

It is likely that the EU Wallet will use (or may use) ledger to store validation information



Thank you!

Jon Ølnes

Product manager trust services

jon.olnes@signicat.com

+47 478 46 094