Lecture series: Data Science in Action
University of Mannheim
Mannheim Center for Data Science
12 October 2023

Digital Identity

Jessica EYNARD
Assistant Professor in Law
University of Toulouse Capitole
Jessica.eynard@ut-capitole.fr

ENGAGE·EU
EUROPEAN UNIVERSITY

UNIVERSITÉ TOULOUSE 1 CAPITOLE
INSTITUT DE DROIT PRIVÉ

Partenaires de plusieurs projets européens :

- ✓ Projet H2020 Legality Attentive Data Scientists (LeADS), H2020-MSCA-ITN-2020.
- ✓ Projet Horizon Europe Data Usage Control for empowering digital sovereignty for All citizens (DUCA)
- ✓ Projet EU Check

I-NOTION OF DIGITAL IDENTITY

INFORMATIONAL SELF-DETERMINATION

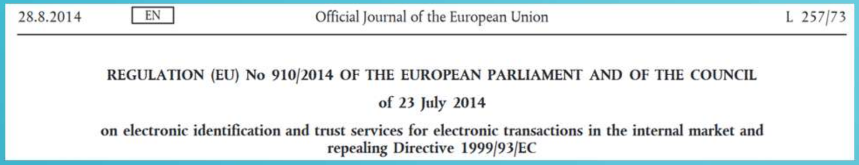
Identity + Digital

ELECTRONIC IDENTIFICATION

DIGITAL IDENTITY

Self-sovereign (Digital) identity (SSI)

PRESENT



28.8.2014 EN Official Journal of the European Union L 257/73

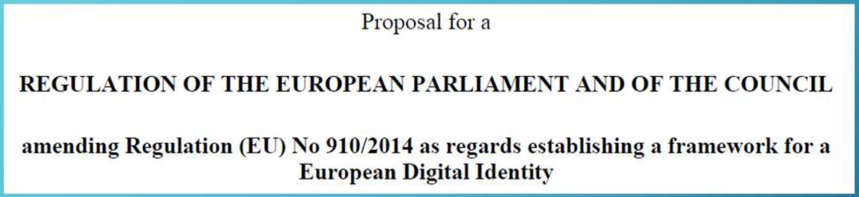
REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 July 2014

on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

Purpose: mutual recognition of cross-border identification methods within the Union, with public services

FUTURE



Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

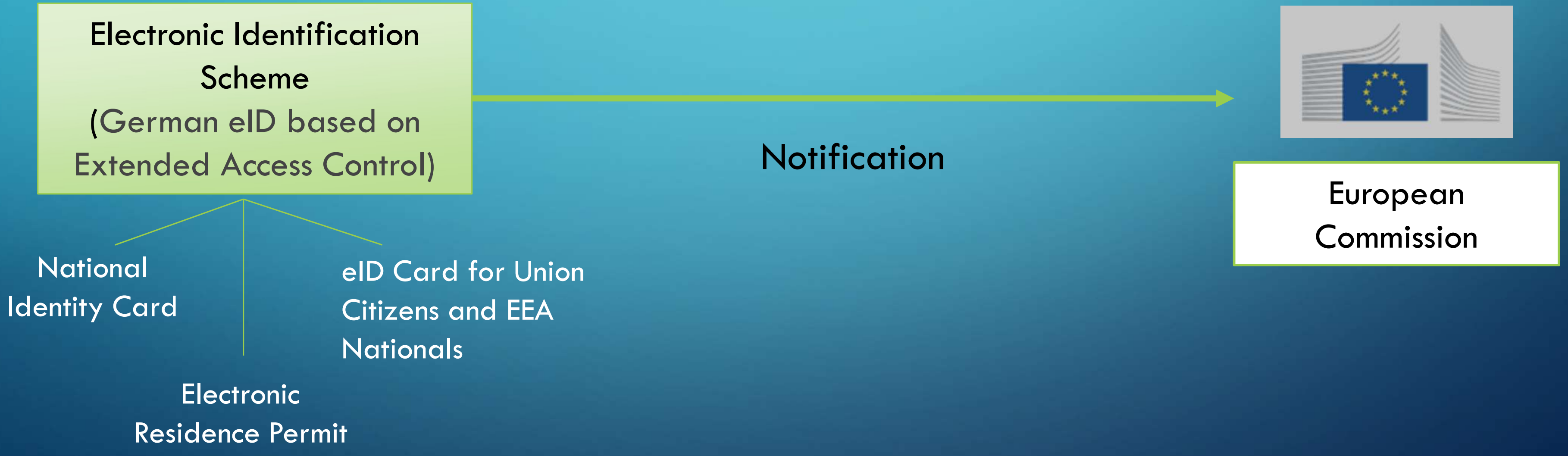
Purpose: cross-border identification with public and private operators,
under the user's control

Electronic Identification → Digital Identity

1) ELECTRONIC IDENTIFICATION

Art. 3 eIDAS : ‘electronic identification’ means the process of using personal identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person.

→ Creation of an Electonic identification scheme (EIS) enabling the issuance of identification means (ID Card, Passport, …)



Electronic Identification Scheme (German eID based on Extended Access Control)

Notification

European Commission

National Identity Card

Electronic Residence Permit

eID Card for Union Citizens and EEA Nationals

Designing the identification process (Electronic Identification Scheme)

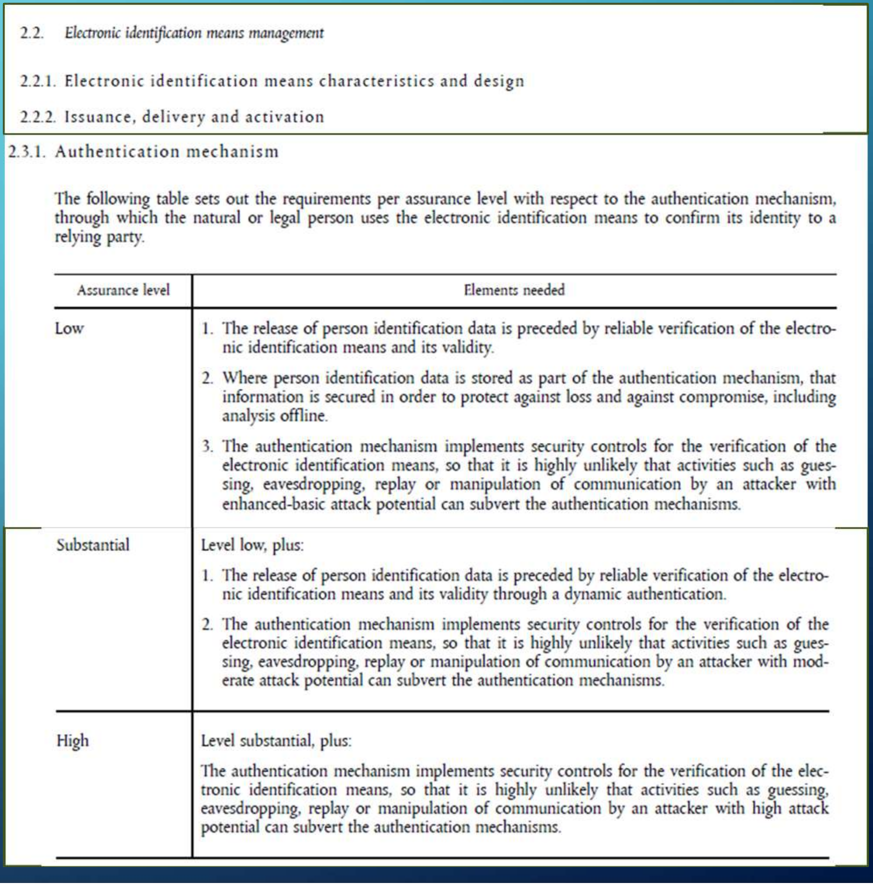
IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014

- ➢ To determine at each stage of the process (from the request for the issuance of the means, through authentication, to its revocation) which <u>**technical standards**</u> to implement to ensure the chosen level of guarantee (low, substantial, high)

(a) **assurance level low** shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, <u>the purpose of which is to decrease the risk of misuse or alteration of the identity</u>;

(b) **assurance level substantial** shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, <u>the purpose of which is to decrease substantially the risk of misuse or alteration of the identity</u>;

(c) **assurance level high** shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the <u>purpose of which is to prevent misuse or alteration of the identity</u>;



2.2. *Electronic identification means management*

2.2.1. Electronic identification means characteristics and design

2.2.2. Issuance, delivery and activation

2.3.1. Authentication mechanism

The following table sets out the requirements per assurance level with respect to the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party.

Assurance level	Elements needed
Low	1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity. 2. Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline. 3. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.
Substantial	Level low, plus: 1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication. 2. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.
High	Level substantial, plus: The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.

CONCLUSION ON ELECTRONIC IDENTIFICATION

Within the framework of the eIDAS regulation on electronic identification, **the focus is on the technical aspects of identification and not on the person**. This text organizes a secure identification pathway, without considering the person as a decision-maker regarding the data that enable him/her to be identified.

⇒**The person is only considered through the justification elements that he/she must provide at each stage of the identification scheme.**

Evolution with the Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, 3rd of June, 2021.

2) TOWARDS A SELF-SOVEREIGN DIGITAL IDENTITY

October 2020 : the European Council invites the European Commission to present a proposal on European digital identification aimed at establishing "an EU-wide framework for secure electronic public identification (e-ID), including interoperable digital signatures, which enables people to exercise control over their identity and data online and provides access to public, private and cross-border digital services" (Conclusions adopted by the European Council at its extraordinary meeting on October 1-2, 2020, EUCO 13/20, CO EUR 10, CONCL 6, n°14)

March 2021 : the European Commission publishes a communication in which it states that, "by 2030, the EU framework should have led to the widespread deployment of a user-controlled trusted identity, allowing every citizen to control his or her own interactions and presence online", (A digital compass for 2030: Europe charts the digital decade, March 9, 2021, COM(2021) 118 final, p. 13 et 14)

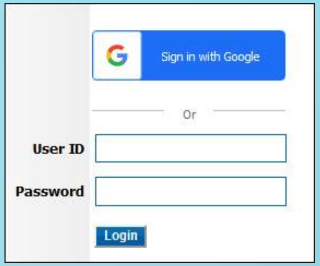
June 2021 : publication of a proposal for a regulation amending Regulation (EU) No 910/2014 as regards the establishment of a European framework for a digital identity, (June 3, 2021, COM(2021) 281 final).

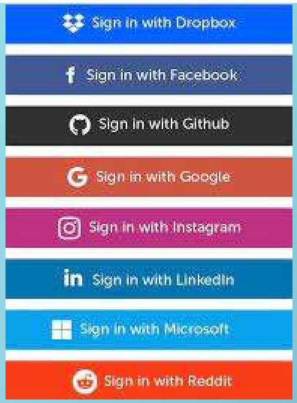
- ➢ The term "digital identity" is used expressly
- ➢ Objective: to give individuals full control over the data they share => the individual is at the heart of the system. We thus move from electronic identification to digital identity. As the latter is controlled by the individual, we speak of a self-sovereign digital identity

Peter Steiner, *The New Yorker, July 5, 1993*

"On the Internet, nobody knows you're a dog."

How the hell does Facebook know I'm a dog?





<u>Administrative</u> control by multiple, federated authorities

=> To prevent from using the same login/password for many websites but data exploitation

Device identification

Centralised identity

Federated identity

Self-sovereign identity

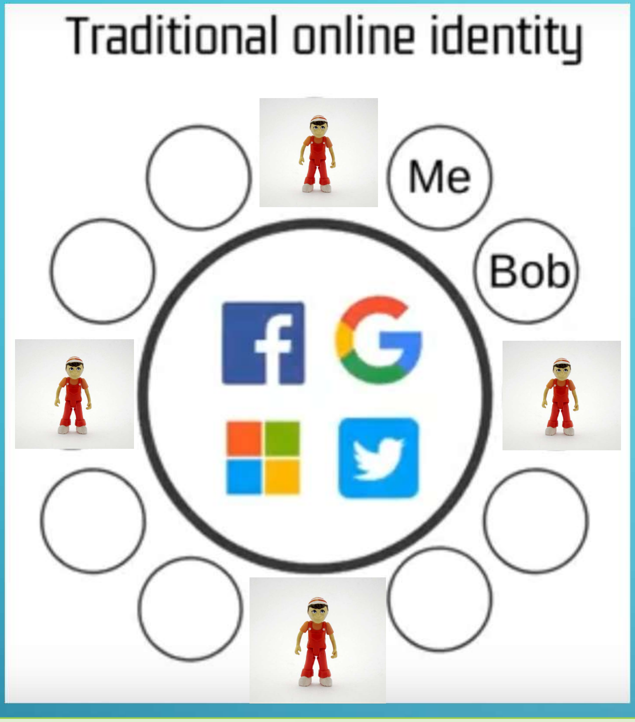
<u>Administrative</u> control over the data by a single authority/entity

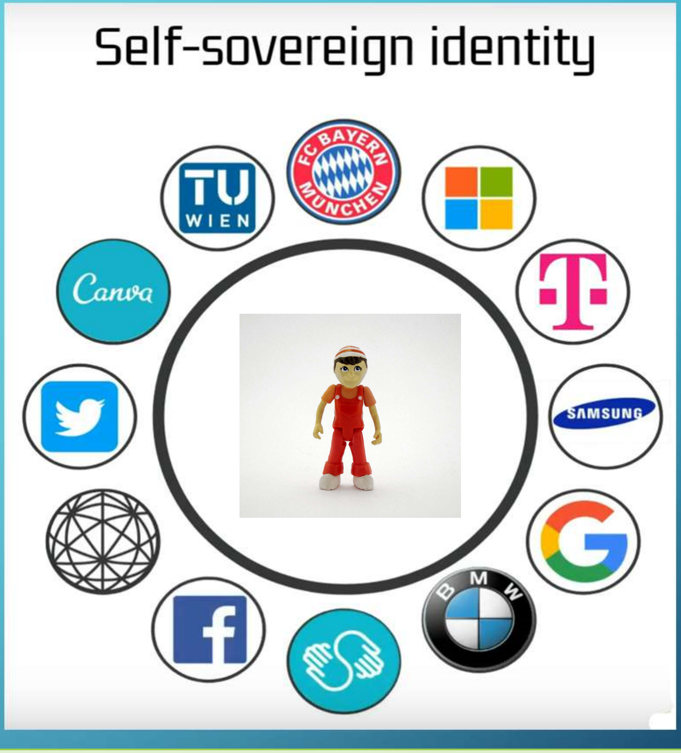
(ex : e-commerce site)

<u>Individual</u> control across any number of authorities

=> Rather than just advocating that users be at the center of the identity process, **self-sovereign identity requires that <u>users be the rulers</u>** of their own identity

SSI Amabassador, **An introduction to Self-Sovereign Identity**, https://www.youtube.com/watch?v=djhYZZ3CkuM





Each person has **various profiles held by the various companies** with which they have come into contact.
They may become "captive" to a company through which they regularly identify themselves and which collects information about them at each identification

The person is at the center of the system enabling him to decide what data to provide to whom and how it can be used + traceability

DEFINITION of SSI

- No legal definition

- **Sovereignty** applies in principle to a natural or legal person. It refers to the exclusive power exercised by a State, an organ or a monarch, without being subject to any control. The notion is also used in law to refer to the sovereign decisions of judges, to indicate that these decisions are not subject to review by the Supreme Court.

Applied to identity, sovereignty could therefore mean that the identity provided by a person at the time of identification is not subject to any control by the person receiving the information. However, this is not the case, and sovereignty here seems more to reflect the power that the individual holds over his or her identity, and the fact that he or she is not subject to any control over the choices he or she makes when deciding whether or not to share information.

In doctrine, it **"aims to preserve the right to selective disclosure of different aspects and components of one's identity, in different domains and contexts" and that it refers to the idea that "individuals should retain control over their personal data and, to some extent, over the representations of their identities (or personas) within a particular identity management system"**

(F. WANG, P. DE FILIPPI, « Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion », 20 février 2020, p. 9, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3524367).

It is therefore a matter of giving the individual the possibility to determine and control who can access what information about him or her

Does self-sovereign identity then amount to informational self-determination?

In doctrine, it "**aims to preserve the right to selective disclosure of different aspects and components of one's identity, in different domains and contexts" and that it refers to the idea that "individuals should retain control over their personal data and, to some extent, over the representations of their identities (or personas) within a particular identity management system**"

(F. WANG, P. DE FILIPPI, « Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion », 20 février 2020, p. 9, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3524367).

It is therefore a matter of giving the individual the possibility to determine and control who can access what information about him or her

Does self-sovereign identity then amount to informational self-determination?

NO

- **Informational self-determination: legal control over its information by the person => GDPR**
- **Self-sovereign identity: legal and technical control => without technical control, there is no sovereignty, only a piecemeal control that can be summarized as informational self-determination.**

Questions :

1) Can a self-sovereign digital identity really exist? = Is the individual capable of achieving this sovereignty?

2) Is a self-sovereign identity desirable? = Doesn't this mean putting the risks and therefore the responsibility on the shoulders of the individual and, as a result, removing the responsibility from the identity provider?

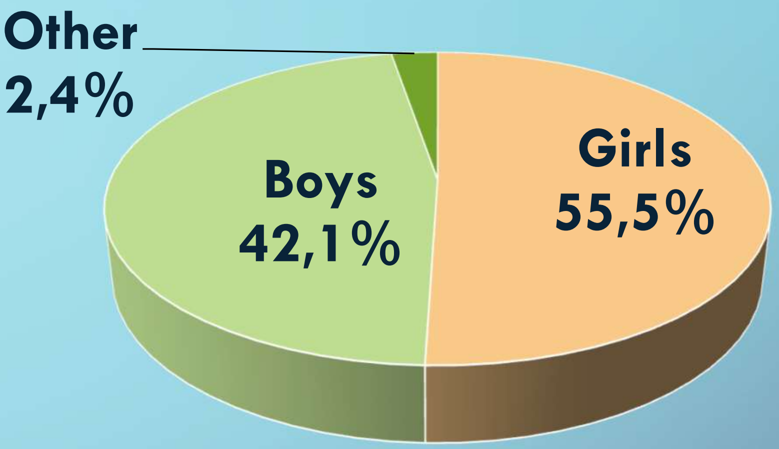
3) What identification scheme should be recommended to achieve this identity or to come as close as possible to it?

II-LEGAL FRAMEWORK OF DIGITAL IDENTITY

Questionnaire Survey

371 students

17-22 years old

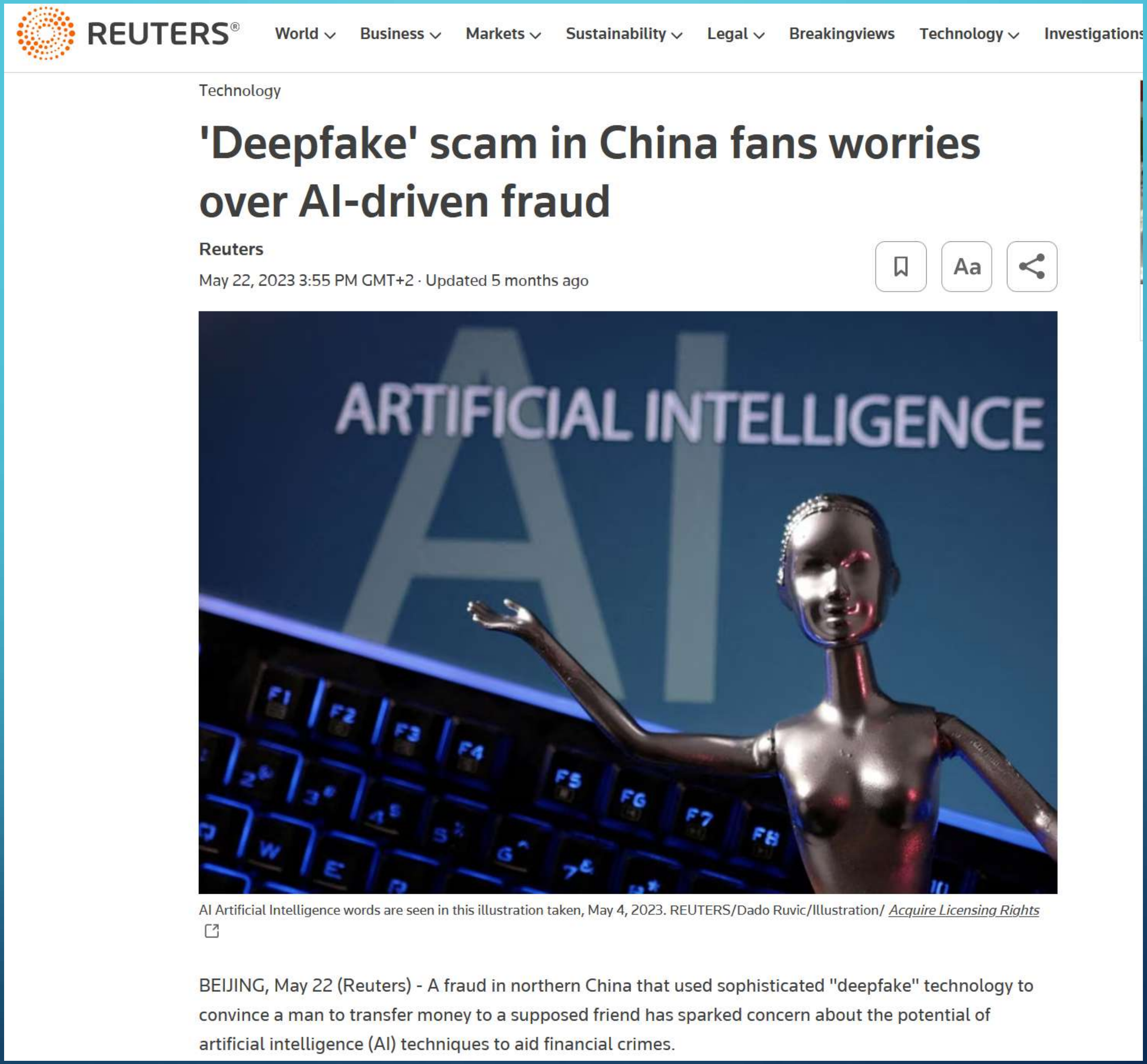


The most popular mean of identification	**Login and password**	**70%**
	Facial recognition	18%
	Digital print	9%
Use of … to sign in online (multiple choices question)	**Biometric Data**	**89%**
	Plug-in « sign in with » Facebook or Google	76%
	France-Connect	16%
	Blockchain	8%

- **Choice of the identification mean:**
  - ➢Practical aspects
  - ➢Knowledge of the mean
- **Reasons for no use of a mean:**
  - ➢Preference for **another mean of** identification
  - ➢Desire to **limite the informations** on the Internet
    - ✓Fear of data manipulation
    - ✓Fear for privacy

Several concerns … including	
Feel like online sites know me well	66%
On the Internet, I feel like I'm being watched	64%
On the Internet, I'm worried about my privacy	42%

Drawbacks for all the means studied



Technology

'Deepfake' scam in China fans worries over AI-driven fraud

Reuters

May 22, 2023 3:55 PM GMT+2 · Updated 5 months ago

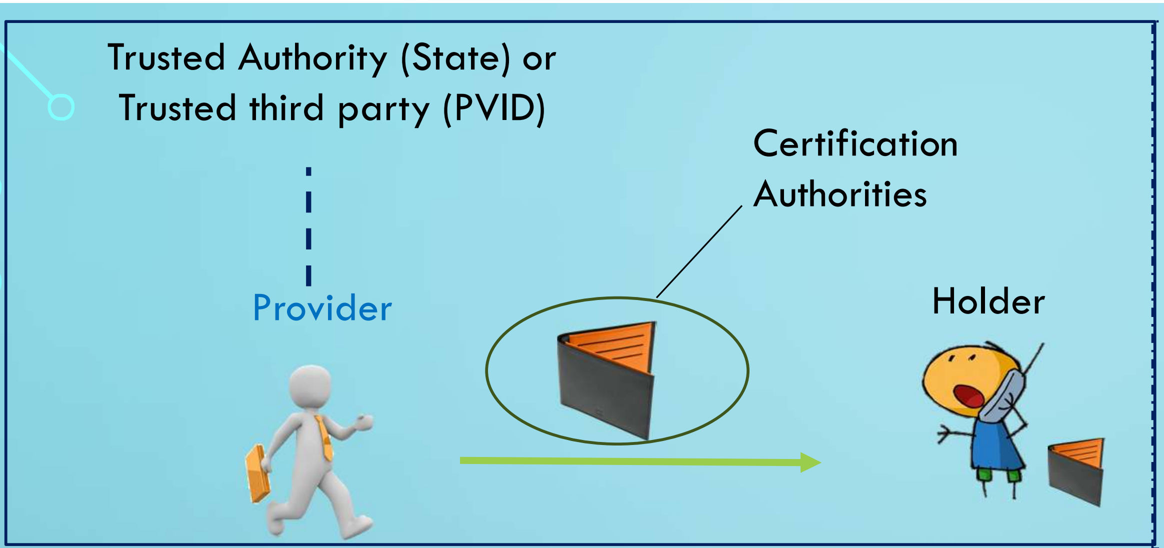
AI Artificial Intelligence words are seen in this illustration taken, May 4, 2023. REUTERS/Dado Ruvic/Illustration/ *Acquire Licensing Rights*

BEIJING, May 22 (Reuters) - A fraud in northern China that used sophisticated "deepfake" technology to convince a man to transfer money to a supposed friend has sparked concern about the potential of artificial intelligence (AI) techniques to aid financial crimes.

EXAMPLE: THE EUROPEAN DIGITAL IDENTITY WALLET(S)

- **Mandatory issuance** for all Member States within 12 (or 24 months ?) of the regulation's entry into force
- Purpose: **to identify oneself, share attributes and sign** with a qualified electronic signature
- Content: **personal identification data, attributes (driver's license, diploma, ...), electronic signature**
- **Used on a voluntary basis** but obligation for the major platforms to accept it when the person wants to identify itself with this wallet

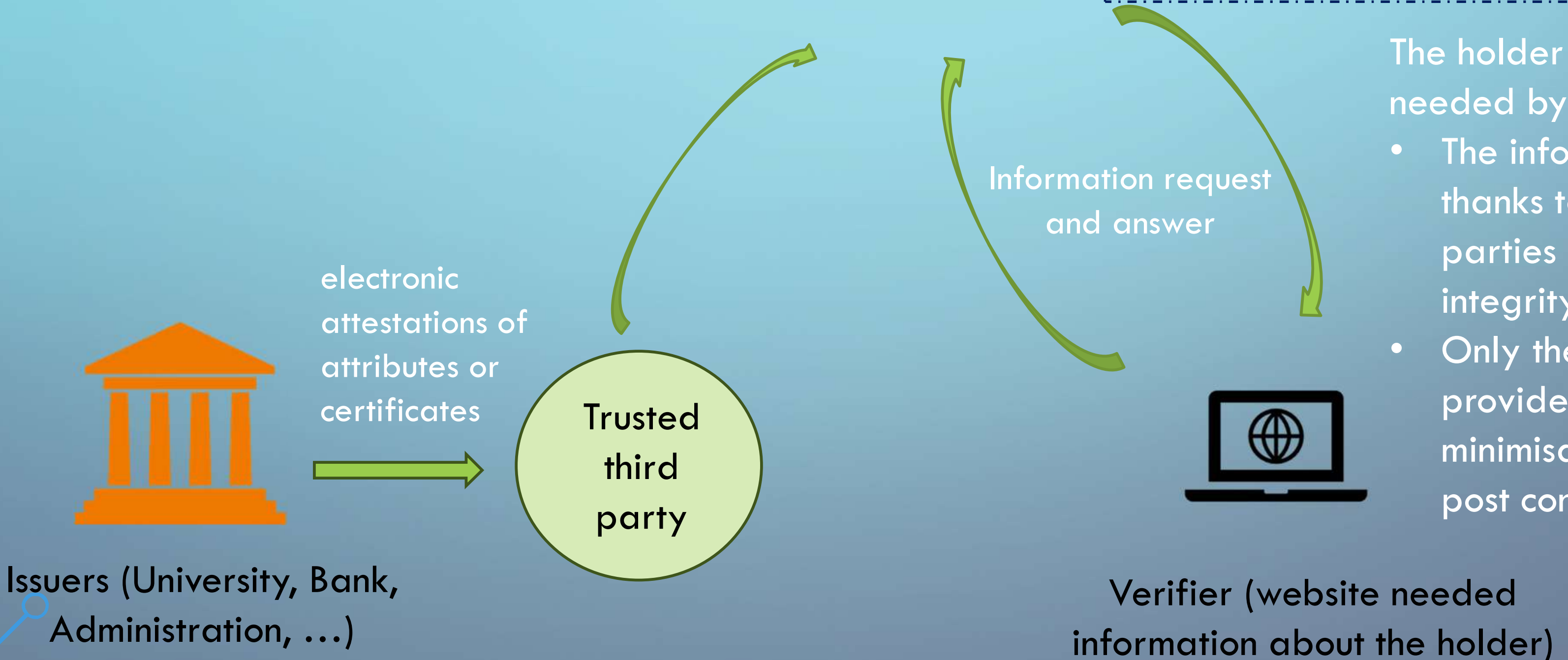
Electronic identification Scheme



A high level of guarantee is required from the electronic identification scheme enabling the issuance of the wallet

- ➢ Intervention of the State issuing an Id Card (reliable document) for example or of a certified third party
- ➢ The provider can be the Member States directly or an entity with the intervention of the Member State
- ➢ Certification of the wallet

Usse of the wallet scheme



The holder provides the information needed by the verifier :

- The information should be reliable thanks to the intervention of trusted parties (authentification + integrity)
- Only the information needed is provided (principle of minimisation/confidentiality) => ex post control measures ?

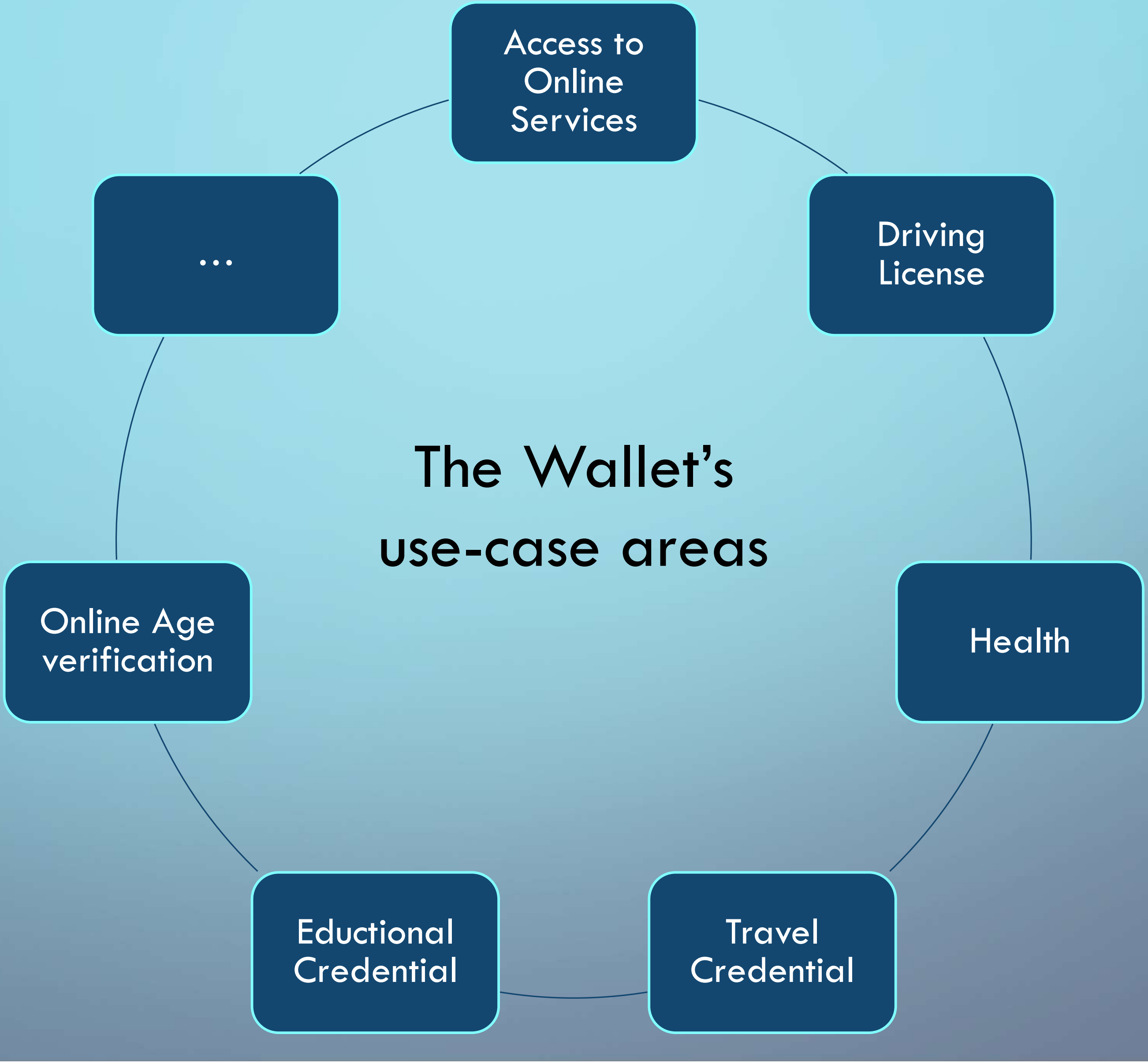
- ✓ The wallet is free of use for the holder
- ✓ Normally, the provider is not allowed to exploit the data generated by the use of the wallet

=> what is the business model of the providers ?

> *“The issuer of the European Digital Identity Wallet shall not:*
> *- collect information about the use of the wallet which are not necessary for the provision of the wallet services,*
> *- combine person identification data and any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by this issuer or from third-party services which are not necessary for the provision of the wallet services, unless the user has expressly requested it”*

- ✓ **Use of a unique identifier?** (to be checked as the last draft agreement doesn’t refer to a unique identifier but requires from the Member State concerned to ensure unequivocal identity matching for natural persons using notified electronic identification means or European Digital Identity Wallets

The Wallet's use-case areas



Access to Online Services

Driving License

Health

Travel Credential

Eductional Credential

Online Age verification

…

TO BE CONTINUED …

THANK YOU

Jessica Eynard

Jessica.eynard@ut-capitole.fr