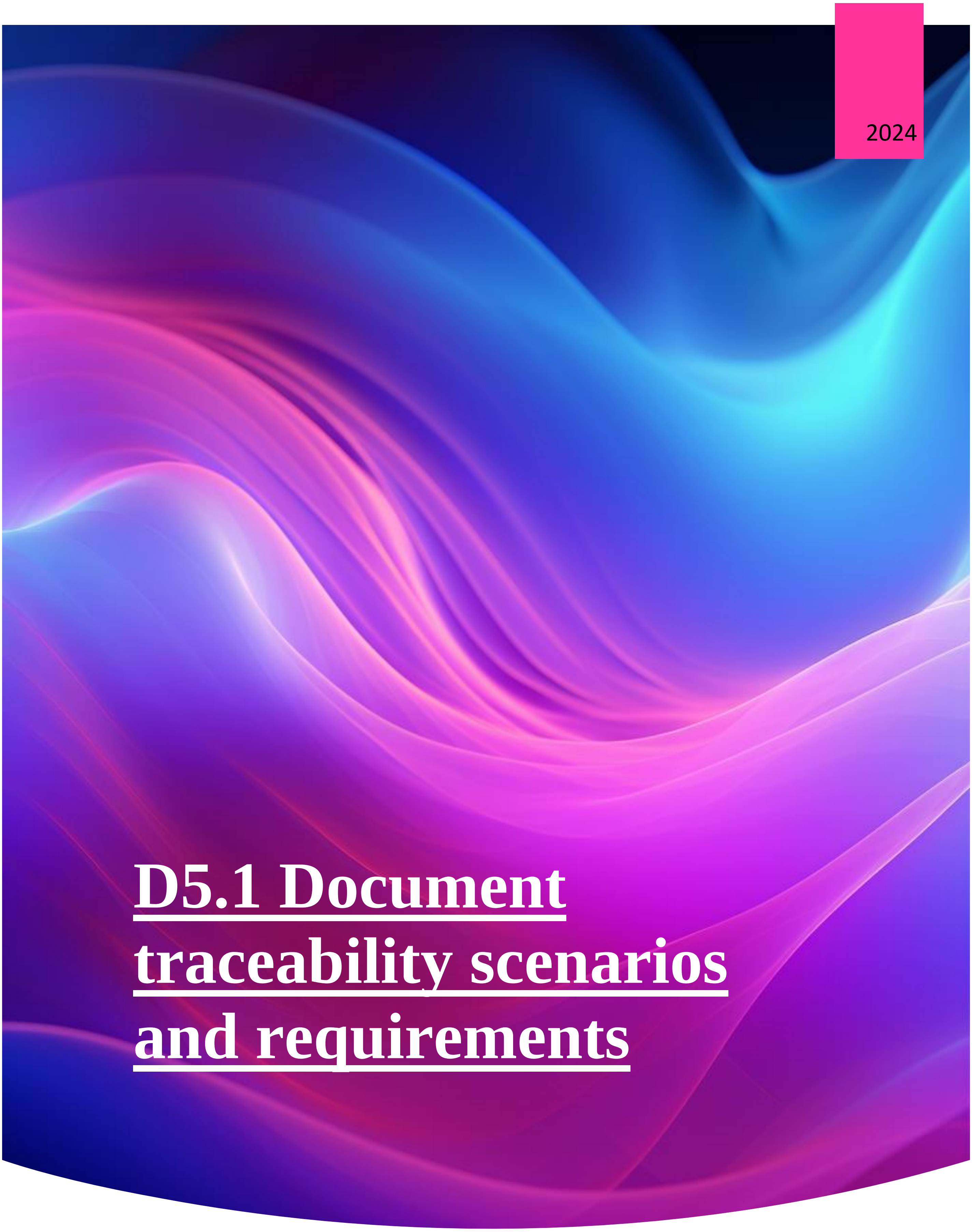


2024

# D5.1 Document traceability scenarios and requirements

This project has received funding from the European Union’s DIGITAL programme under grant agreement No 101102743

| | |
|---|---|
| **Project Title** | **TRACE4EU** |
| **Grant Agreement No.** | Grant agreement No 101102743 |
| **Deliverable Title** | **D5.1 Document traceability scenarios and requirements** |
| **Version** | 1 |
| **Deliverable nature:** | Report (R) |
| **Dissemination level: (Confidentiality)** | Public (PU) |
| **Responsible Partner** | INFOCERT |
| **Authors** | DIGICITI, GOLDMAN, RBI, TU Berlin |
| **Contributors** | **Yiorgos Antoniou (GOLDMAN), Giancarlo Degani, Davide Porro (INFOCERT), Patrick Erbke (TU Berlin), Philippe Rixhon (DIGICITI), KAROLJ SKALA (RBI)** |
| **Reviewers** | |

Change Log

| Date | Editor/Reviewer | Version | Activity |
|---|---|---|---|
| 10/10/2023 | Giancarlo Degani | 0.1 | Initial Version |
| 9/11/2023 | Davide Porro | 0.2 | Infocert contribution |
| 14/11/2023 | Patrick Erbke | 0.3 | TU Berlin contribution |
| 20/11/2023 | Philippe Rixhon | 0.4 | Digiciti contribution |
| 12712/2023 | Karolj Skala | 0.5 | RBI contribution |
| 22/01/2024 | WP1 | 0.6 | Quality Check |
| 25/01/2024 | Marco Crabu | 1 | Final Version |

# Executive summary

Through domain knowledge, technological expertise, and commitment to decentralization of its consortium members, TRACE4EU project aims to contribute significantly to the broader adoption of EBSI in various sectors. This will be achieved by strategically leveraging EBSI features to demonstrate its adaptability and effectiveness in addressing five contemporary high-value digital challenges: professional credentials, academic publishing, secure document and messaging delivery, and customer identity verification.

This D5.1 deliverable describes five distinct use cases, each corresponding to the aforementioned digital challenges: Open Rights Data Exchange, Resume Credentials, Democratizing Academic Publishing, Electronic Registered Delivery, Know Your Customers. These use cases highlight the versatility and efficiency of EBSI in revolutionizing data management and secure transactions, thanks to its provided advantages in terms of Transparency and Immutability, Enhanced Security, Trust and Accountability, Fraud Reduction, and Interoperability with existing systems.

For each use case, detailed descriptions of the implemented process, functional and technical requirements are provided.

Finally, and equally importantly, inside each use case thorough consideration will be given to incorporating the relevant European regulations and technical standards, such as eIDAS, ETSI, ISO, etc., into the services provided by EBSI, thereby strengthening EBSI's support for legal aspects as well.

# Table of contents

# 1 Introduction

In today's digital age, the need for transparency, security, and accountability in document tracing has never been more critical, making blockchain-led document tracing not merely a technological advancement; but a strategic direction of evolution in the rapidly changing digital world.

The business value that a blockchain ledger like EBSI can provide in document tracing, is multifaceted and transformative. It promises to offer unprecedented levels of transparency, security, trust, and efficiency while reducing the risk of fraud and ensuring compliance.

More specifically, a blockchain based ledger like EBSI can provide many advantages in tracing in terms of:

- Transparency and Immutability
    - Blockchain technology, known for its decentralized and tamper-proof nature, introduces an unprecedented level of transparency and immutability in tracing. This immutability ensures that once an information is recorded on the blockchain, its authenticity and integrity are preserved, reducing the risk of fraud and disputes.
- Enhanced Security
    - Blockchain leverages advanced cryptographic techniques to secure data, ensuring that only authorized parties can access and modify information saved in it.
- Trust and Accountability
    - Blockchain's distributed ledger ensures trust and accountability in tracing. Participants within the blockchain network can verify the authenticity of transactions without relying on intermediaries, reducing the need for third-party validation.
- Fraud reduction
    - Blockchain technology has the potential to virtually eliminate document fraud. By offering a transparent and tamper-proof ledger, with both the approaches, in-chain and off-chain, businesses can ensure that documents, such as certificates, contracts, and financial records, are genuine and have not been altered.
- Interoperability with existing systems
    - Blockchain technology is inherently interoperable, allowing organizations to integrate their document tracing systems with existing databases and software.

Finally, but not less important, a blockchain based ledger like EBSI can simplify auditing and compliance processes because regulators, auditors, and internal compliance teams have in the decentralized/distributed ledger a unique access point to the events connected to the history of documents, ensuring that all requirements are met. This reduces the administrative burden on organizations and minimizes the risk of non-compliance.

The 5 pilots of TRACE4EU, Open Rights Data Exchange, Resume Credentials, Democratizing Academic Publishing, Electronic Registered Delivery, Know Your Customers, described in the following of this deliverable, aim demonstrate concretely and in real cases the advantages of using EBSI ledger in the tracing processes.

# 2 Implementation and piloting of Open Rights Data Exchange application

## 2.1 Introduction

The creative industries represent more than 5% of EU GDP and more than €750 billion in yearly revenues. They depend on trusted copyright data to protect and monetise their digital assets. The management, licensing, enforcement, and remuneration of copyrights and related rights require real-time access to reliable, exhaustive, current, and interoperable rights data:

- contents and parties must be identified,
- one must know who did what and who owns what, as well as
- the standard terms & conditions to use a particular content.

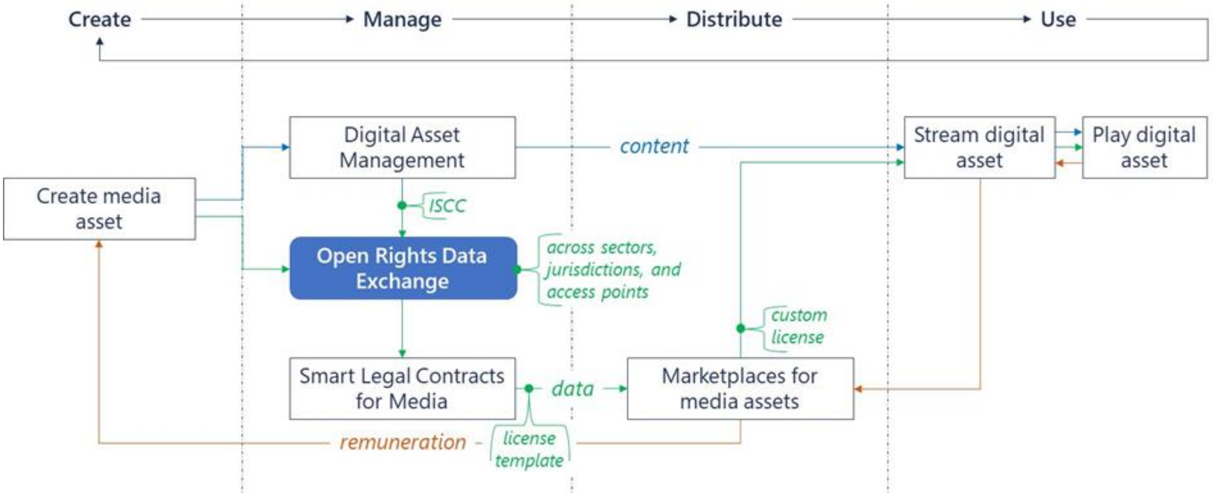


***Figure 1: Context of the Open Rights Data Exchange (ORDE)***

This rights management information should be available across sectors, jurisdictions, and access points. Therefore, we suggested opening the rights data framework – the set of rules, technologies and institutions that frame data management practices in the creative industries. And then, building an Open Rights Data Exchange to intermediate trusted rights management information between stakeholders.

Three **themes** are the large focus areas that span Digicti's organisation –

1) **Facilitate** a fair, appropriate, proportionate, and transparent remuneration of creators and rightsholders,
2) **Provide** real-time access to reliable, exhaustive, current, and interoperable rights management information,
3) **Leverage** open data, once-only principle, and self-sovereign identity.

## 2.2 Scenarios

**Five initiatives** are the collections of epics that drive towards the Open Rights Data Exchange (ORDE) –

1) **Locate**: the necessary functionality for users to find the ORDE, that should become a destination just like Wikipedia and IMDb are destinations for somebody searching for a film or an actor,
2) **Access**: the necessary functionality for users to assess the benefits offered by the ORDE and join it as active participants,
3) **Declare**: the necessary functionality for users to list media assets,
4) **Store**: the necessary functionality for the ORDE to store the immutable binding between content and declarer, related public metadata and related private metadata,
5) **Search**: the necessary functionality for users to find what they are looking for and to be alerted as soon as what they are looking for would become available.

The Open Rights Data Exchange is a two-sided marketplace of trusted rights data. On one side, it allows rightsholders to register their rights and receive a registration token – an attestation/certificate of machine-readable rights data. On the other side, it gives online platforms and other rights users real-time access to reliable, exhaustive, current, and interoperable rights data.

**Generic rights holders' scenario: Registration / Initiatives: Locate, Access, Declare and Store**

Creators, rightsholders, or intermediary declarers register rights related to a media asset either by using a webform or an API linking their catalogue with the ORDE.

The registration process counts 5 steps:

1) The declarer uploads a media file, i.e., a manifestation of a work, and the media file is fingerprinted, typically with the International Standard Content Code (ISCC),
2) The declarer enters rights management information about the work and the parties involved,
3) The declarer enters geolocated royalty splits related to the work and standard terms and conditions related to the use of the work,
4) The timestamped immutable binding between declarer's ID and media file fingerprint is stored on a blockchain network. It points to a set of public metadata stored on the InterPlanetary File System (IPFS). This public set of metadata can include the address of a set of private metadata stored at the declarer's location of choice, and
5) The ORDE issues a registration token.

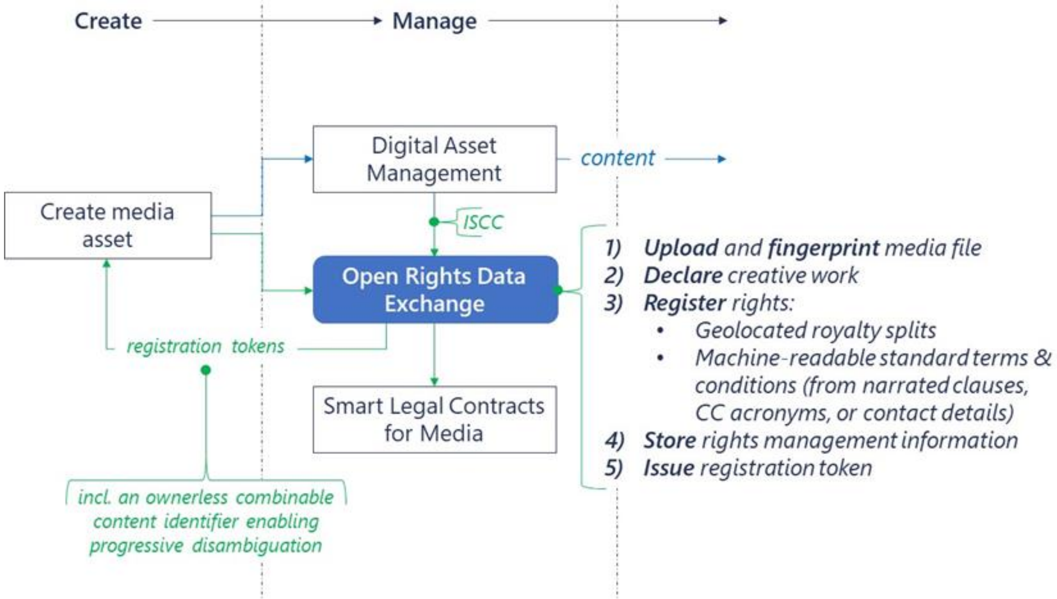

Create
Manage
Digital Asset Management
content
Create media asset
ISCC
Open Rights Data Exchange
registration tokens
Smart Legal Contracts for Media
incl. an ownerless combinable content identifier enabling progressive disambiguation
1) Upload and fingerprint media file
2) Declare creative work
3) Register rights:
• Geolocated royalty splits
• Machine-readable standard terms & conditions (from narrated clauses, CC acronyms, or contact details)
4) Store rights management information
5) Issue registration token

*Figure 2: The 5 steps of the rights registration process*

**Generic rights users’ scenario: Query / Initiatives: Locate, Access, and Search**

Rights users, e.g., streaming platforms or film producers looking for music to be used in their creations, query the ORDE using a webform or an API linking their databases with the ORDE.

**A specific rightsholders’ use case: AI & Copyright**

Creative sectors may now claim their (new) rights vis-à-vis online aggregators and give or withhold their consent for the test and data mining systems training Large Language Models. In the European Union, one counts three types of requirements based on recent regulations such as the EU directive 2019/790 on copyright (Articles 3 and 4 on text and data mining) and the Artificial Intelligence Act –

- **Information**: standardise interoperable identifiers and opt-out declarations
- **Traceability**: identify content that has been created or modified by AI
- **Transparency**: document the training and generation algorithms used to produce AI-generated content

## 2.3 Functional requirements

There are 3 ways for Digiciti to share the ORDE application scenario with the TRACE4EU consortium to validate the EBSI architecture and identify eventual missing components:

- **Minimum**: we share media files, rights metadata, and business logic for WP2 and WP5 to conduct tests.
- **Medium**: minimum, plus we share an example of our hybrid storage of rights data (immutable binding of content and declarer's identifiers on a blockchain, pointing to the ISO Dublin Core of metadata stored on IPFS, pointing in turn to more metadata stored anywhere) for WP2 and WP5 to conduct tests with us aiming at exploring decentralised identifiers, verifiable credentials and cross-ledger interoperability.
- **Maximum**: medium, plus we leverage eIDAS and EBSI SSI developments.

The sequence Minimum - Medium - Maximum could be adopted during the prototype phase (January - December 2024).

The readiness of APIs and the advances in (a) **cross-ledger interoperability**, (b) **self-sovereign identity**, and (c) underlying components to assure **provenance and authenticity** can help us leverage EBSI in our pilot.

The translation of narrated standard terms and conditions into **machine-readable clauses** would allow an immediate use of such terms and conditions in smart contracts and pave the way to a faster, simpler, more transparent, and more affordable licensing of copyrights and related rights. See also Figure 3.

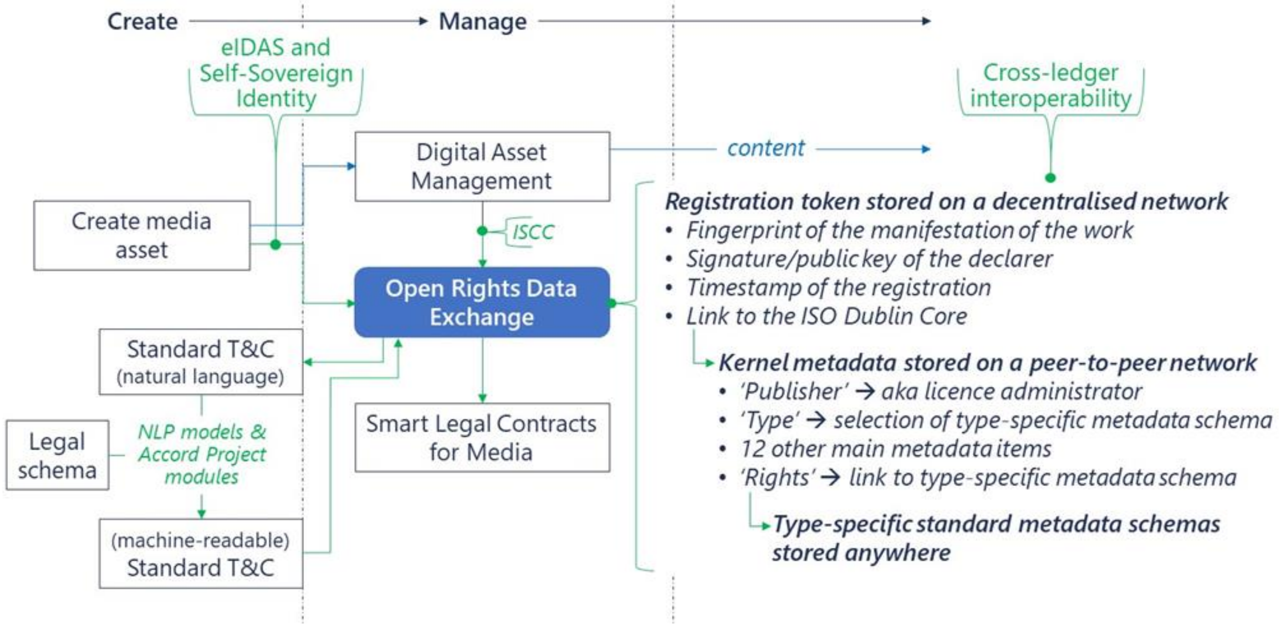

Create
Manage
eIDAS and Self-Sovereign Identity
Cross-ledger interoperability
Digital Asset Management
content
Create media asset
ISCC
Open Rights Data Exchange
Registration token stored on a decentralised network
• Fingerprint of the manifestation of the work
• Signature/public key of the declarer
• Timestamp of the registration
• Link to the ISO Dublin Core
Kernel metadata stored on a peer-to-peer network
• 'Publisher' → aka licence administrator
• 'Type' → selection of type-specific metadata schema
• 12 other main metadata items
• 'Rights' → link to type-specific metadata schema
Type-specific standard metadata schemas stored anywhere
Standard T&C (natural language)
Smart Legal Contracts for Media
Legal schema
NLP models & Accord Project modules
(machine-readable) Standard T&C

***Figure 3: Storage of rights management information***

We foresee the need for (1) **standardisation** and liaisons between EBSI and ETSI, ISO, ITU, and W3C, and (2) **interoperability** with DLT systems based on Directed Acyclic Graphs, e.g., IOTA Foundation and Hedera Hashgraph.

We expect the TRACE4EU architecture team (a) to let us know what features/components required by our plan are available or not, and (b) to help us leverage the existing ones.

## User eXperience

The ORDE must be easily **discoverable** on the Internet among other ways through Search Engine Optimisation.

The access to ORDE can be **plugged in** other applications.

The user experience includes interactive tutorials about “you”, “your work”, “your rights”, and “your rights data”. See DGA Art. 12m: A provider offering services to data subjects shall act in the data subjects’ best interest where it facilitates the exercise of their rights, in particular by **informing** and, where appropriate, **advising** data subjects in a **concise**, **transparent**, **intelligible** and **easily accessible manner** about intended data uses by data users and standard terms and conditions attached to such uses before data subjects give consent.

## User Interface

The user interface must be self-explanatory, fool proof, and available in multiple languages.

Rights data must be read, added, modified, or deleted depending on permissions and the timing of these actions.

The ORDE must be a one-stop-shop and help rightsholders –

- get party identifiers such as ISNI, IPI, IPN, ORCID, etc.
- get content identifiers such as ISBN, DOI, ISRC, ISWC, EIDR, ISAN, etc.
- register their rights with collective management organisations.

Rights data can be declared and searched manually (i.e., contribution by contribution) or automatically through APIs (i.e., in bulk).

**Output**

Rights registrations must suffice to parametrise smart legal contracts, therefore one must:

- represent rights through a semantics such as the W3C **Open Digital Rights Language** that allows to disambiguate rights, permissions, obligations, prohibitions, actions, terms, conditions, and licences,
- represent the **granularity of permissive actions** (e.g., in the UK music industry: reproduction, distribution, rental, adaptation, performance, communication, and making available),
- represent the **granularity and interdependence of media assets**, whereby the complex and dynamic structure of a media product can be represented by a bill of contributions, that can then be handled by an indexed or graph database,
- comply with the **regulations on smart contracts** which must be human-readable, amendable, and revocable and should support the proportional and transparent remuneration of creators and rightsholders, and
- comply with the General Data Protection Regulation (GDPR) and also protect trade secrets, which will be done through an appropriate structure of data storage and access permissions.

**The ORDE will be operated as a Data Intermediation Service regulated by the EU Data Governance Act. It must comply with the conditions stipulated in Article 12 - Conditions for providing data intermediation services.**

**Transparency**

The ORDE will not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users and will provide these data intermediation services through a specific legal entity.

The **commercial terms**, including **pricing**, for the provision of data intermediation services to a data holder or data user will not depend upon whether the data holder or data user uses other services provided by the ORDE or by a related entity, and if so to what degree the data holder or data user uses such other services.

The data collected with respect to any activity of the ORDE for the purpose of the provision of the data intermediation service, including the date, time and geolocation data, duration of activity and connections to other natural or legal persons established by the person who uses the ORDE, will be **used only for the development of that data intermediation service**, which may entail the use of data for the **detection of fraud or cybersecurity**, and will be **made available** to the data holders upon request.

The ORDE will ensure that the procedure for access to its service is **fair**, **transparent** and **non-discriminatory** for both data subjects and data holders, as well as for data users, including with regard to **prices** and **terms of service**.

**Interoperability**

The ORDE will facilitate the exchange of the data in the format in which it receives it from a data subject  or a data holder, will **convert** the data into specific formats only to enhance interoperability within and across sectors or if requested by the data user or where mandated by Union law or to ensure **harmonisation with international or European data standards** and will offer an opt-out possibility regarding those conversions to data subjects or data holders, unless the conversion is mandated by Union law.

The service may include additional specific tools and services to data holders or data subjects for the specific purpose of facilitating the exchange of data, such as **temporary storage**, **curation**, **conversion**, **anonymisation** and **pseudonymisation**, such tools being used only at the explicit request or approval of the data holder or data subject and third-party tools offered in that context not being used for other purposes.

The ORDE will take appropriate measures to ensure **interoperability with other data intermediation services**, inter alia, by means of commonly used **open standards** in the sector in which the service operates.

**Security**

The ORDE will have procedures in place to **prevent fraudulent or abusive practices** in relation to parties seeking access through its service.

The ORDE will put in place adequate technical, legal and organisational measures in order to prevent the transfer of or access to **non-personal data** that is unlawful under Union law or the national law of the relevant Member State.

The ORDE will take necessary measures to ensure an appropriate level of security for the storage, processing and transmission of non-personal data, and Valunode will further ensure the highest level of security for the storage and transmission of **competitively sensitive information**.

The ORDE will without delay **inform** data holders in the event of an unauthorised transfer, access, or use of the non-personal data that it has shared.

**Reliability**

The ORDE will, in the event of its insolvency, ensure a reasonable **continuity of the provision of its service** and, where its service ensures the storage of data, will have mechanisms in place to allow data holders and data users to obtain access to, to transfer or to retrieve their data and, where its service is provided between data subjects and data users, to allow data subjects to exercise their rights.

The ORDE must be **scalable** to ensure a reasonable continuity of the provision of the service.

**Data location**

When the ORDE provides tools for obtaining consent from data subjects or permissions to process data made available by data holders, it will, where relevant, specify the third-country jurisdiction in which the data use is intended to take place and provide data subjects with tools to both give and withdraw consent and data holders with tools to both give and withdraw permissions to process data.

**Log record**

The ORDE will maintain a logged record of the data intermediation activity.

## 2.4 Technical requirements

**General considerations**

**Self-sovereign identity integration:** Integration with the EBSI self-sovereign identity / digital wallet application chosen by the TRACE4EU consortium.

**Blockchain integration:** Integration with the EBSI blockchain infrastructure chosen by the TRACE4EU consortium.

**Types of data:** Any digital content or media files, i.e., manifestations of creative works.

**Metadata:** Identification metadata, rights metadata, descriptive metadata, usage metadata, and administrative metadata. Identification of contents and parties, timestamps, KYC, rights management information including info about content, parties, royalty splits, and standard terms and conditions.

**Protocol:** So far, we use Polygon on-chain, and IPFS and private metadata stores off-chain.

**Interoperability:** With the Ethereum Virtual Machine.

**APIs and integration:** APIs with repositories of large rightsholders and large rights users, APIs with standardisation bodies.

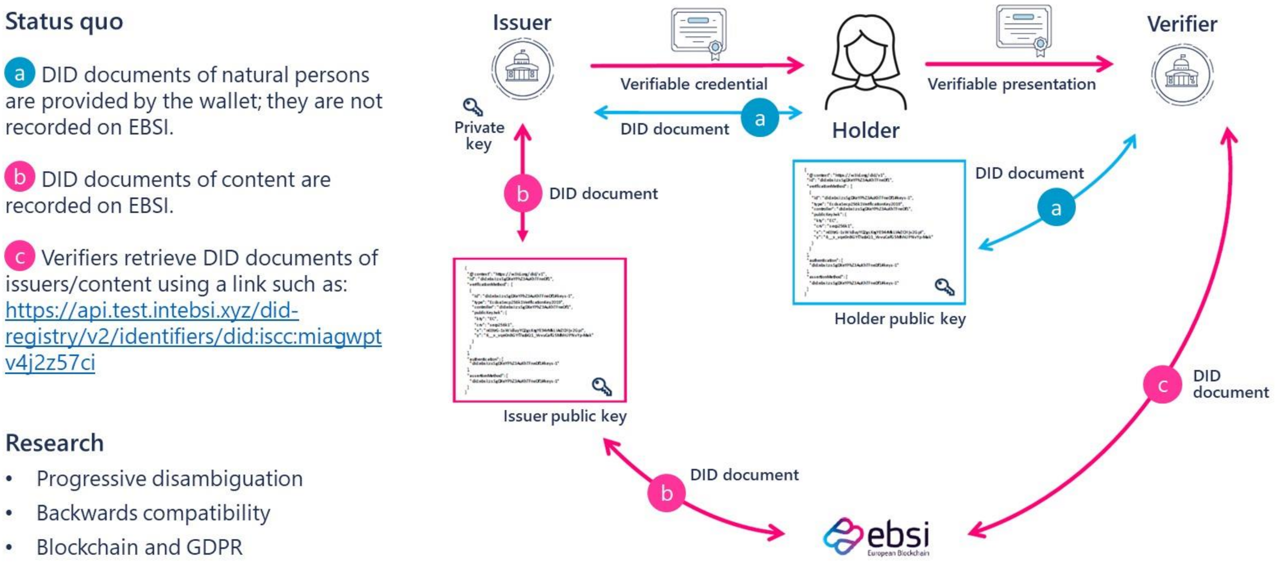
**Compliances:** The ORDE must comply with the GDPR, apply KYC procedures, and align with the copyright-related *Acquis Communautaire* and the Data Governance Act.

**On-chain vs. off-chain:** On-chain: immutable binding between content and declarer's identifiers, timestamp, and related IPFS address. Off-chain: public metadata on IPFS pointing to private metadata stored where the declarer wants it to be stored.

**Decentralised identifiers (DIDs)**

The rights management information stored in the **ORDE must trustworthily identify content and parties**. Previous attempts to centralise/federate the issuance of (analogue) identifiers and the storage of rights data have failed. The ORDE must make use of decentralised identifiers.

W3C: "Decentralised identifiers (DIDs) are a new type of identifier that enables verifiable, decentralised digital identity. A DID refers to any subject (e.g., a person, organisation, thing, data model, abstract entity, etc.) as determined by the controller of the DID. In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralised registries, identity providers, and certificate authorities. Specifically, while other parties might be used to help enable the discovery of information related to a DID, the design enables the controller of a DID to prove control over it without requiring permission from any other party. DIDs are URIs that associate a DID subject with a DID document allowing trustable interactions associated with that subject".



Status quo

a DID documents of natural persons are provided by the wallet; they are not recorded on EBSI.

b DID documents of content are recorded on EBSI.

c Verifiers retrieve DID documents of issuers/content using a link such as: https://api.test.intebsi.xyz/did-registry/v2/identifiers/did:iscc:miagwptv4j2z57ci

Research

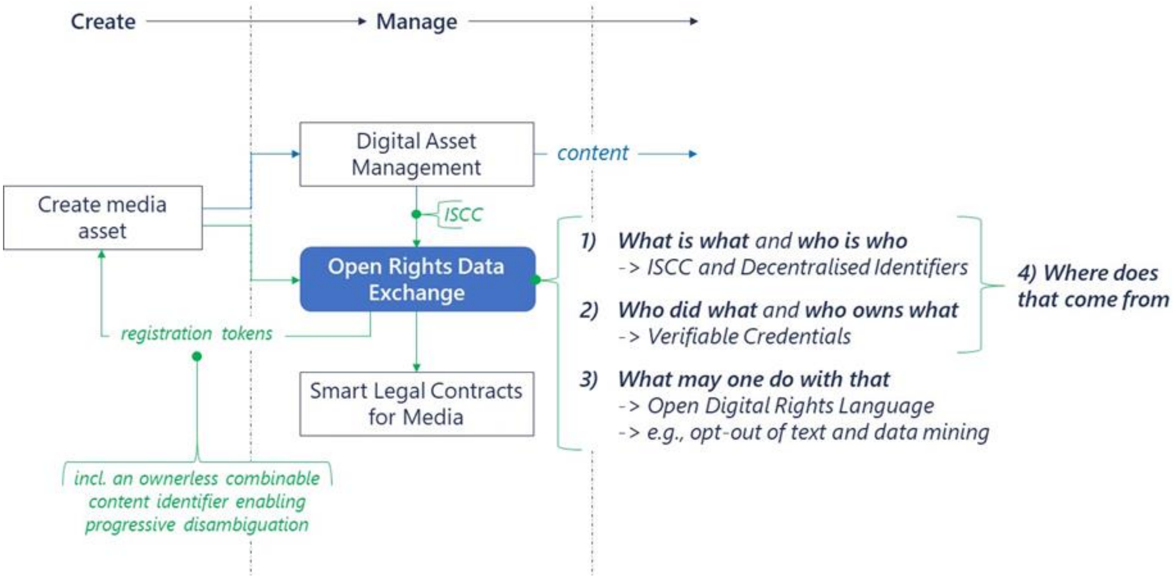
- Progressive disambiguation
- Backwards compatibility
- Blockchain and GDPR

*Figure 4: Decentralised identification*

See https://github.com/w3c/did-spec-registries/pull/465 about the ISCC as a DID.

**Progressive disambiguation**

A DID URL extends the syntax of a basic DID to incorporate other standard URI components such as path, query, and fragment to locate a particular resource – for example, a cryptographic public key inside a DID document, or a resource external to the DID document. Could this open the door to progressive disambiguation through multilayered DIDs?



Create
Manage
Digital Asset Management
content
Create media asset
ISCC
Open Rights Data Exchange
registration tokens
Smart Legal Contracts for Media
incl. an ownerless combinable content identifier enabling progressive disambiguation
1) What is what and who is who
-> ISCC and Decentralised Identifiers
2) Who did what and who owns what
-> Verifiable Credentials
3) What may one do with that
-> Open Digital Rights Language
-> e.g., opt-out of text and data mining
4) Where does that come from

*Figure 5: ORDE questions, decentralised identifiers and verifiable credentials*

**Verifiable credentials**

The **ORDE must also trustworthily validate** authorship **claims** (who did what: e.g., Paul McCartney wrote “Hey Jude”) and ownership claims (who owns what: e.g., MacLen (Music) Limited owns the rights related to “Hey Jude”). The ORDE must make use of verifiable credentials.

W3C: “A verifiable credential can represent all of the same information that a physical credential represents. The addition of technologies, such as digital signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts.

Holders of verifiable credentials can generate verifiable presentations and then share these verifiable presentations with verifiers to prove they possess verifiable credentials with certain characteristics.

Both verifiable credentials and verifiable presentations can be transmitted rapidly, making them more convenient than their physical counterparts when trying to establish trust at a distance”.

## Backwards compatibility

A particular attention must be given to the backwards compatibility between the ORDE, its decentralised identifiers and their multi-layered structure, its verifiable credentials, and its hybrid storage architecture, on one hand, and the current rights and royalty system deployed in the creative industries, on the other hand.

The larger the backwards compatibility, the easiest the progressive adoption by the media & entertainment ecosystem.

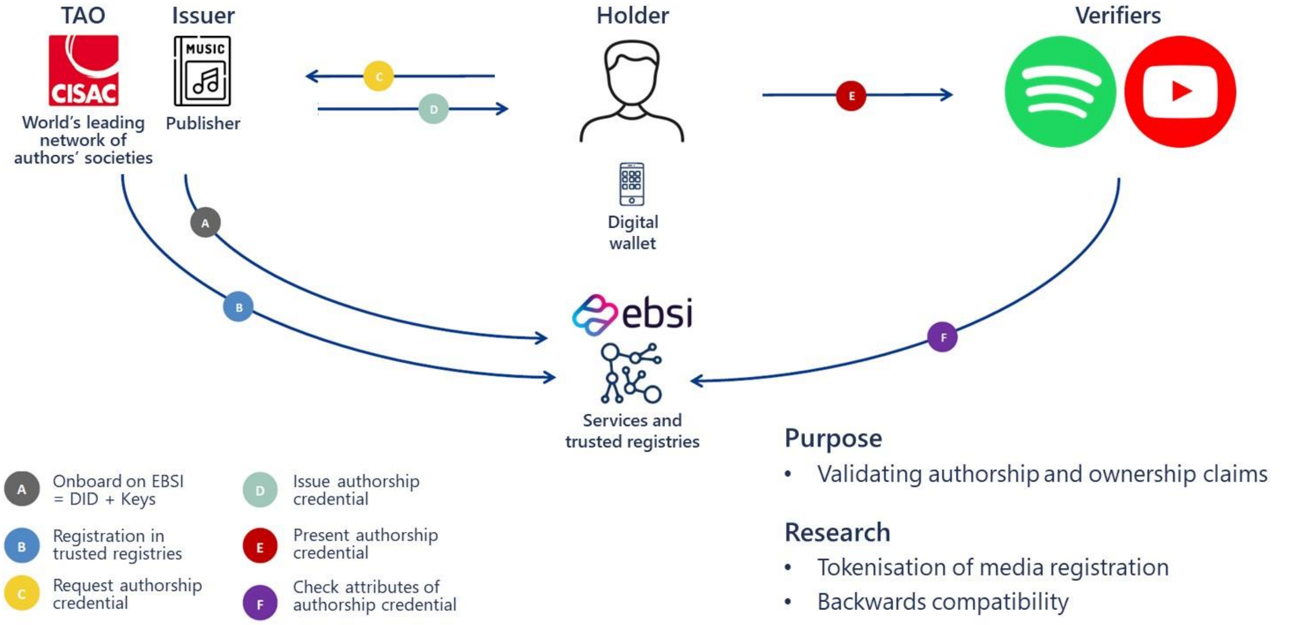

TAO
Issuer
Holder
Verifiers
CISAC
World's leading network of authors' societies
MUSIC
Publisher
C
D
E
Digital wallet
A
B
F
ebsi
Services and trusted registries
Purpose
• Validating authorship and ownership claims
Research
• Tokenisation of media registration
• Backwards compatibility
A Onboard on EBSI = DID + Keys
B Registration in trusted registries
C Request authorship credential
D Issue authorship credential
E Present authorship credential
F Check attributes of authorship credential

*Figure 6: Verifiable credentials*

## The AI & Copyright use case

The ORDE must address questions raised by the emergence of Large Language Models and the deployment of Generative AI applications:

- What is what, and who can tell,
- Who is who, and who is accredited to claim work authorship or right ownership,
- What may one do with what, and how can an author or rightsholder opt-out of text and data mining, and
- Where does that content come from.

The opt-out declaration must be:

- machine-and-human-readable-readable,
- based on open standards,
- inseparably bound to the content (i.e., resilient to content sharing),
- resilient to manipulation (i.e., resilient to the stripping of watermarks or metadata),
- able to provide verifiable attribution (e.g., using digital signatures or verifiable credentials), and

timestamped.

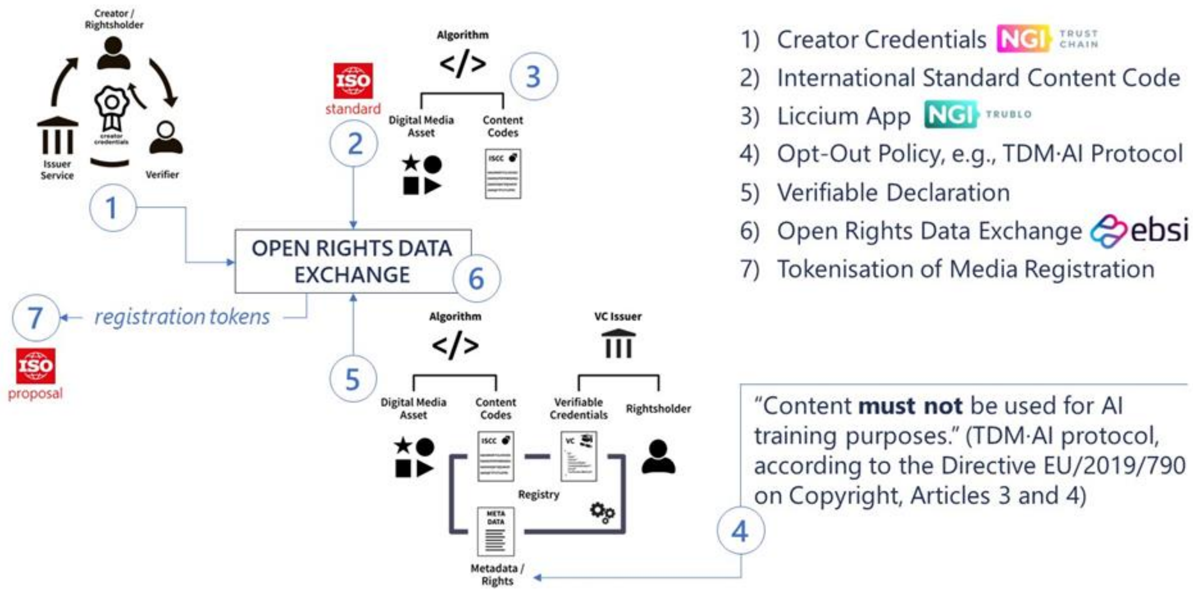

Creator / Rightsholder
creator credentials
Issuer Service
Verifier
1
ISO
standard
2
Algorithm
</>
3
Digital Media Asset
Content Codes
ISCC
OPEN RIGHTS DATA EXCHANGE
6
7
registration tokens
ISO
proposal
5
Algorithm
</>
VC Issuer
Digital Media Asset
Content Codes
Verifiable Credentials
Rightsholder
ISCC
VC
Registry
META DATA
Metadata / Rights
4
1) Creator Credentials NGI TRUST CHAIN
2) International Standard Content Code
3) Liccium App NGI TRUBLO
4) Opt-Out Policy, e.g., TDM·AI Protocol
5) Verifiable Declaration
6) Open Rights Data Exchange ebsi
7) Tokenisation of Media Registration
"Content **must not** be used for AI training purposes." (TDM·AI protocol, according to the Directive EU/2019/790 on Copyright, Articles 3 and 4)

***Figure 7: European developments addressing the AI & Copyright Use Case***

Besides TRACE4EU, the European Commission Next Generation Internet initiative (NGI) is co-funding NGI Trublo and its project Liccium App, which helps creators to inseparably bind public and verifiable claims to their content, and NGI TrustChain and its project Creator Credentials, that can help identify creators and rightsholders and create trust in claims and attributions. Integrating the NGI prototypes with the TRACE4EU development seems to be a promising starting point to technically develop a standardised opt-out mechanism.

The envisaged integration would rely on open standards – ISO standards and W3C recommendations. Not only does the European TDM·AI protocol compare favourably with other related initiatives, but it can even be combined with them.

## Standardisation of the registration token

We proposed to ISO/JPEG NFT to standardise the registration token. Based on the identified JPEG use cases, an initial set of JPEG NFT requirements have been identified and organised in the following main categories:

**Compatibility**: the standard shall comply with the JPEG Systems framework and should retain backwards compatibility. It shall also align with JPEG Trust and more specifically with its requirements.

**Metadata descriptions**: the standard shall provide means to identify, authenticate and describe involved actors while considering privacy of individuals. It shall provide means to identify and describe media assets and to signal IPR information related to media assets.

**Metadata embedding and referencing**: the standard shall provide means to embed relevant metadata descriptions into media assets and/or to link relevant metadata descriptions to media assets. It shall consider privacy of individuals and locations as well as trade secrets, provide means for identification of media assets and related NFTs, and support searchability of NFTs and associated media assets.

**Provenance, authenticity and integrity**: the standard shall provide means to trace the provenance of NFTs. It shall provide means to assess the authenticity and integrity of the media asset referred to by NFTs.

**Media asset registration format**: the standard shall provide means to register media assets and related NFTs while building up on existing standards of identifiers, metadata sets, and metadata exchanges.

**Management of intellectual property rights**: the standard shall facilitate the copyright declaration and micro-licensing of media assets, and the IP protection of the NFT itself.

# 3 Implementation and piloting of Resume Credentials application

## 3.1 Introduction

In the Trace4EU research project, a key area of focus will be aligning Trace4EU's resume credential development with the standards set by the Europass CV and European Learning Model v3. The Europass CV, a widely recognized and accepted standard across the EU, will benchmark our verifiable credential development process. We will analyze the structure, content, and user interface of the Europass CV to ensure our resumé credentials meet similar standards of clarity, professionalism, and user-friendliness. This alignment will enhance the interoperability of our credentials within the European job market, thereby increasing their utility and acceptance.

**Stakeholders:**

In the context of the Trace4EU project's Resume Credentials application, the roles of issuer, holder, and verifier are integral to the digital credential ecosystem:

- Issuer: The issuer is the entity that creates and issues digital credentials. In the scenario outlined, issuers would be educational institutions like universities that issue diplomas or organizations that issue working certifications (verifiable credentials/claims). They are responsible for ensuring that the credentials accurately represent the achievements or qualifications of the holder. The issuer must also ensure that the credentials are issued securely, allowing for later verification by relying parties. The trustworthiness of issuers will be guaranteed by an EBSI backed registry filled and managed by the relevant ministers of the European countries (according to the country specific accreditation procedures). (The issuer could be an employer validating a professional experience of the holder)
- Holder: The holder is the individual who has been issued the digital credential. A holder stores his/her credentials in his/her digital wallet and, through the digital wallet functionalities, generates a verifiable presentation of them when needed. The holder controls his/her credentials, sharing them with verifiers for specific purposes, such as job applications. Holders can also self-claim specific skills and request institutions and organizations to generate a Verifiable Credential attesting such a self-made claim. This procedure might involve a third-party helper application or service to select the correct schema for the requested Verifiable Credential; however, no third party will come in possession at any time of the Verifiable Credential issued, as it will always be directly sent from the issuer to the holder wallet.
- Verifier: The verifier is the entity that needs to check the validity of a digital credential presented by the holder. This could be a potential employer or another institution that requires proof of the holder's qualifications or skills. The verifier confirms that the credentials are authentic, have not been revoked, and were indeed issued by the claimed issuer.

## 3.2 QTSP & eIDAS Compliance

In the given scenario, the Qualified Trust Service Provider (QTSP) could act in several roles:

As an issuer, if they provide Qualified Attestatiosn of Attributes to e.g. resume credentials or QTSP for issuance of qualified certificates for qualified electronic signatures, seals or timestamps. ce

As a verifier, when they need to validate the credentials presented to them. For instance, a QTSP might be called upon to verify the signature on a digital document to ensure its integrity and the signer's identity.

As a trusted intermediary, providing services that underpin the trustworthiness of the entire system. QTSPs can offer timestamping, validation, and preservation services for digital certificates and signatures. The last ones ensure the long-term validity and integrity of the credentials in the ecosystem.

In the digital credentials ecosystem,  in order to achieve the eIDAS C0mpliance of EBSI  the QTSP especially on Qualified Attestations of Atrributes operates in close collaboration with the authentic source so e.g. the university  which contains the data base for diploma or other resume credentials as defined in eIDAS 2.0.

In any case the compliance on eIDAS 2.0 and the Architecture and Reference Framework as well as the implementing acts has to be achieved.. ,

## 3.3 Scenarios

This section details the scenarios related to the resumé credential use case. The interaction with QTSP is special case of the scenarios and would mean that the QTSP will be integrated in the roles mentioned in section 3.2.

**Collecting credentials**

Two different credential types issued by an organisation attesting an attribute about the subject. An example is the university issuing a diploma, or a training organisation issuing an achievement credential. (the employer attesting the facts about the subject, holding the defined position during a certain period of time)

1. Self-claimed skills, such as good team player, communication skills, level of strengths in a programminng language, etc., which can be confirmed by other persons (WoT).
2. Formal skills like e.g. certain diploma, examinations etc.

The first credential type is issued in the well-known way, for example, whenever a student wants to get their diploma credential, they have to request it at the corresponding university and follow the provided process. The issued credential is received in the wallet and stored there. The same process also applies to other credential types such as upper-secondary school certificates.

For the second credential type, they can be created and counter confirmed using the resume credential web service.

**Creating Resume credential**

A user that wants to use the resume credential service has to register at this service. Next, they can start to create the resume credential with the following steps.

For any type 1 credential (defined above), the user self claims their achievements such as university degrees etc. including all necessary information for example, graduated in computer science from TU Berlin in 2023.

The same process is applied for type 2 credentials. Additionally, credentials of type 2 can be confirmed by other members of the resume credential platform by signing the claimed statement.

This way, the user can create a full resume reflecting the professional carrer including education.

**Share resume credential**

A use case could be that a person is searching for a job on an online portal on the laptop (cross device flow). After finding an interesting one, the user decides to apply. There are several options available to apply for the job including one namely “apply via Resume Credential”. The user select this option and is being redirected to the Resume Credential web service.

At this service, the user is able to see what data are requested in order to apply for the job. In this case, the user already has all the data asked by the portal as well as respective verifiable credentials for the asked data in his wallet.

Next, the user selectively chooses what data he wants to submit to the job portal, and which ones he wants to keep from sending. Furthermore, the user add additional data such as softs kills that might be relevant but were not directly requested. After selecting all the data that the user wants to share he presses next. In the next step, the web service creates the template of the VP request (could also just be forwarding a list of credential types) to the relying party.

The relying party receives the VP request template and creates the actual OIDC VP request (needs to be singed by the requester). The user is being redirected to the job application website (could be the job portal or directly the organisation where the user wants to apply). A QR code is presented which the user scans using his wallet, and thus, initiates the OIDC4VP flow. The wallet receives the request for sharing data from the user, and the user, again, has the choice to select what data are going to be revealed to the relying party and which one won't. After selecting the data to be shared, the user gives explicit consent to share this data by pressing next/send/ok. A verifiable presentation is created and sent to the relying party (the VP is signed by the users private key).

Finally, the relying party receives the VP and can now, validate the individual credentials including revocation checks if necessary.

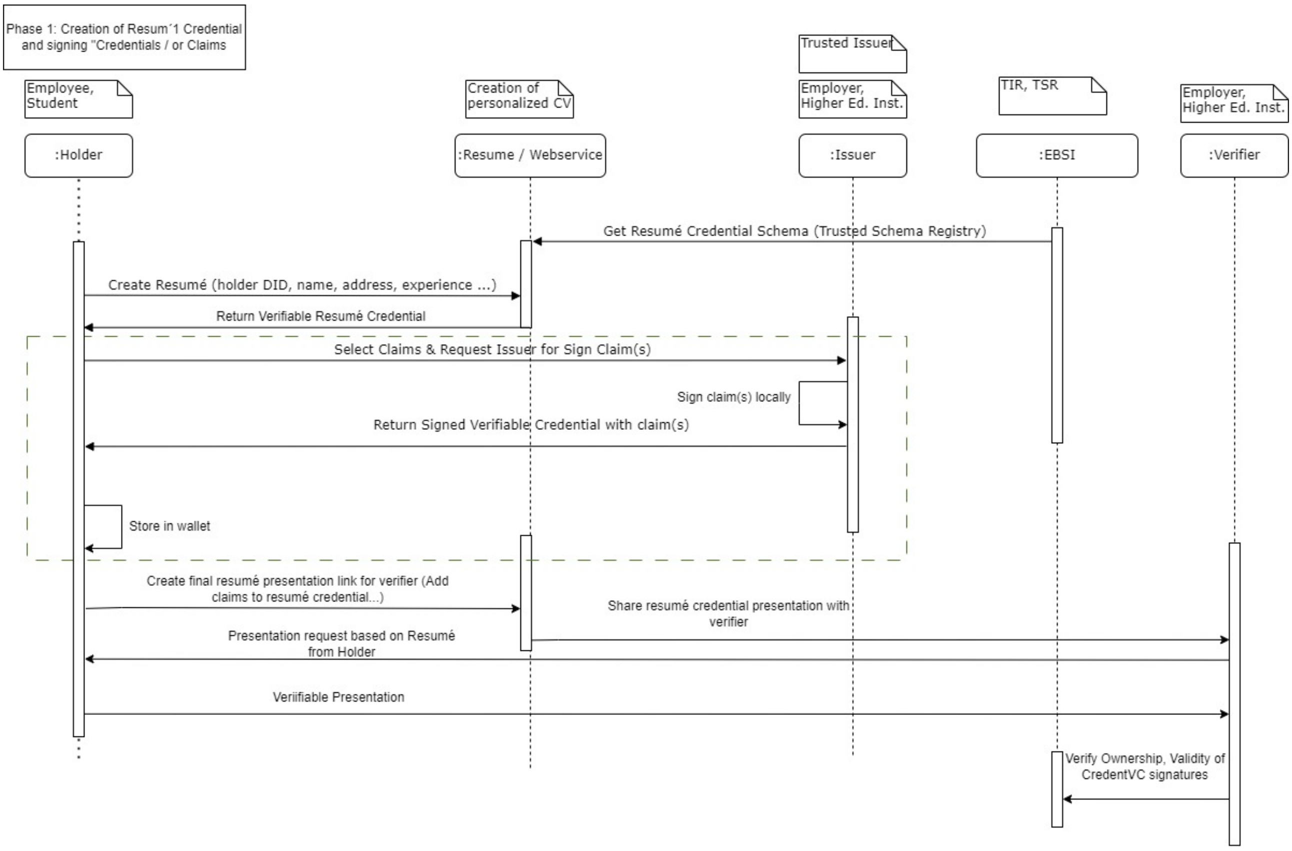

Phase 1: Creation of Resum´1 Credential and signing "Credentials / or Claims
Employee, Student
:Holder
Creation of personalized CV
:Resume / Webservice
Trusted Issuer
Employer, Higher Ed. Inst.
:Issuer
TIR, TSR
:EBSI
Employer, Higher Ed. Inst.
:Verifier
Get Resumé Credential Schema (Trusted Schema Registry)
Create Resumé (holder DID, name, address, experience ...)
Return Verifiable Resumé Credential
Select Claims & Request Issuer for Sign Claim(s)
Sign claim(s) locally
Return Signed Verifiable Credential with claim(s)
Store in wallet
Create final resumé presentation link for verifier (Add claims to resumé credential...)
Share resumé credential presentation with verifier
Presentation request based on Resumé from Holder
Veriifiable Presentation
Verify Ownership, Validity of CredentVC signatures

*Figure 7: Sequence diagram initial draft (not final)*

**Publish resume?**

Ideas:

- Should be users be able to advertise themselves by making this resume public (thinking of the LinkedIn use case)
- Publish to other platforms? Social media such as linkedin
  - Link to other platforms?

In the context of a resumé credential service, the user can disseminate their resumé across the World Wide Web, either in a temporally bounded manner or on a permanent basis. This dissemination process involves the user's discretion in selecting specific subsets of their resumé for publication. Additionally, the resumé credential service facilitates the integration of the resumé information with various online platforms, notably professional networking sites like LinkedIn. Publishing is a passive mode of information dissemination, in contrast to the proactive nature inherent in sharing mechanisms delineated in the previous section. The distinction lies in the user's engagement level: publishing entails a broader, less targeted audience reach, while sharing is directed toward specific entities or platforms.

**Benefits**

- Resume always available
- Easily updatable and usable
- Resume credential service (RCS) does not have the actual VCs (data minimization)
- RCS establishes connection between holder and RP
- RCS forwards/generates VP request template
- RCS offers the feature to attest skills of others (technical details tbd)
- RCS could be integrated in other services such as Europass or LinkedIn
- Data are verifiable by the RP

- Todo:
- Abstract architecture overview of Stakeholder and their relations
- Sequencediagram (seperate scenarios to above mentioned

## 3.4 Functional requirements (

The functional requirements for the Resume Credentials application within the Trace4EU project are delineated as follows:

1. Credential Collection and Verification: The application shall enable the collection of two distinct types of credentials: organization-issued and self-claimed, with the latter subject to peer confirmation within the platform.
2. User Registration and Credential Creation: Users must register with the service, after which they can create and self-claim educational and professional achievements with type 1 and 2 credentials. In the case of Type 1 credentials issued by entities directly, the issuer must be able to add the information to the web service. In the case of type 2 credentials, the user must be able to request attestations (credentials) from the corresponding educational institution or organization.
3. Credential Sharing: Users shall be able to share their credentials with prospective employers through a cross-device flow, ensuring selective data disclosure and consent-based sharing of verifiable presentations.
4. Privacy and Data Minimization: The resumé service shall not retain actual verifiable credentials (VCs) but will establish a secure connection between the holder and the relying party (verifier).
5. Credential Verification: The system shall provide functionalities for data verification by verifier, including revocation checks, thereby ensuring the reliability of the shared credentials.

6. Resumé Credential Publication: Users can make their resume credentials public for broader visibility, similar to the LinkedIn model, with features enabling time-bound or permanent publication options.
7. Integration with External Platforms: The system could support linking or referencing credentials to external platforms, enhancing users' ability to leverage their credentials across various professional networks.
8. Optional - Interoperability with Europass CV and European Learning Model v3: The system shall support the integration of resume credential structures that align with the Europass CV format and the European Learning Model v3, promoting seamless cross-platform utility.

## 3.5 Technical requirements (

The technical requirements for the Resume Credentials application are specified as follows:

1. Standards Compliance: The application complies with standards such as the European Learning Model v3, the ESCO ontology, EQF level, and the International Standard Classification of Education (ISCED).
2. API Development: APIs will be developed to integrate the resume credential service with external platforms, including but not limited to educational institutions and professional networking sites.
3. Security: Implement robust security measures to protect user data and credentials from unauthorized access and ensure the credential-sharing process's integrity.
4. User Interface: Develop a user interface consistent with the Europass CV's clarity and professionalism, ensuring an intuitive experience for users when creating and sharing resume credentials.
5. EBSI Integration: The application utilizes EBSI for the immutable recording of credential verification and sharing events, providing a transparent and tamper-proof system.
6. Data Portability: Support for data portability, allowing users to transfer their credentials between different platforms and services.
7. Digital Wallet Compatibility: Ensure compatibility with digital wallets for storing and managing resume credentials, allowing users to maintain control over their personal information.
8. Interoperability: To the extent feasible, the application will be compatible with different digital identity frameworks and technologies, including EBSI, eIDAS2-compliant wallets, and others.

**Standards / Input:**

Further considered standards within the analysis period:

- ELM v3 : https://europa.eu/europass/en/news/upcoming-launch-european-learning-model-v3
- The ESCO ontology: https://ec.europa.eu/esco/lod/static/model.html (Vasilios)

ESCO (European Skills, Competences, Qualifications and Occupations) is the European multilingual classification of Skills, Competences, Qualifications and Occupations. The ESCO ontology can be used by online platforms for services like matching jobseekers to jobs on the basis of their skills, suggesting training to people who want to reskill or upskill etc. ESCO provides descriptions of 3008 occupations and 13.890 skills linked to these occupations, translated into 28 languages.

ESCO is organised in three pillars: the occupations pillar; the knowledge, skills and competences pillar; the qualifications pillar.

Occupations are defined as a ‘set of jobs whose main tasks and duties are characterised by a high degree of similarity’. ESCO is strongly interlinked with the latest version of the International Standard Classification of Occupations (ISCO). Each occupation is therefore mapped to an ISCO code. Whereas ISCO has only 4 levels of occupations, ESCO provides a more detailed classification.

The skills pillar provides a comprehensive list of knowledge, skills and competences. The skills pillar contains 13,890 concepts structured in a hierarchy which contains four sub-classifications: Knowledge, Language skills and knowledge, Skills, Transversal skills.

The skills pillar distinguishes between i) skill/competence concepts and ii) knowledge concepts by indicating the skill type. There is however no distinction between skills and competences.

Qualifications are the formal outcome of an assessment and validation process which is obtained when a competent body determines that an individual has achieved learning outcomes to given standards. Information on qualifications at European level is displayed in Europass. Qualifications in ESCO come from national qualifications databases of Member States that are included in National Qualifications Frameworks that have been referenced to the European Qualifications Framework (EQF). The EQF provides a common reference framework which assists in comparing the national qualifications systems, frameworks and their levels.

# 4 Implementation and piloting of Democratizing Academic Publishing application

## 4.1 Introduction

Democratizing academic publishing is a project which aimed to improve current publishing and reviewing processes by making it transparent and trustworthy using blockchain technology.

The goal of the project is to ***create a democratic, trustworthy, and efficient platform for academic open access publishing*** in order to strengthen the European Research Area, and Open Research Europe, and to strengthen the academic communication and transfer of knowledge. Since knowledge and information represent strategic power, the goal of DAP is to ***give authors, researchers, and the public*** more ***control over scientific knowledge and information***, improve research practices, and prevent research integrity violations, such as those seen in the proliferation of open access "predatory" publishers.

A major social impact of the DAP project will be the seamless inclusion of citizen scientists, and specifically retired and other institution-less researchers and scientists, advancing the knowledge transfer and enhancement.

## 4.2 Scenarios

Author submits his document to review system. Reviewers are able to read the document metadata, and to decide if they will accept to review it or not. When they accept they can read the document, and submit their decision. If the document needs changes, the author will resubmit and the process will be repeated. This process is equivalent to the  usual reviewing process, the difference being automatisation and usage of blockchain to keep metadata. Blockchain will ba also used to pay reviewers and authors for their participation. Reviews will be rated and their rating will produce metrics which will help during the reviewer selection process. Peer reviewers, including the author, provide valuable feedback through the DAP platform, contributing to the manuscript's refinement. All active participants in DAP, i.e. those which contribute to the system (e.g. authors, reviewers, infrastructure providers etc.) are appropriately rewarded by DAP fully fungible tokens named Ergions.

## 4.3 Functional requirements

Functional requirements for the DAP (Democratic Academic Publishing) platform outline the specific features and capabilities that the system must possess to meet its objectives. Below are some functional requirements for DAP:

1. **User Registration and Profiles:**
   - Users should be able to register on the platform using the Scholarly Wallet.
   - Each user must create a profile with essential information, including their academic credentials, areas of expertise, and contact details.
2. **Role Assignment:**
   - Users should have the flexibility to choose one or more roles (Author, Reviewer, etc.) within the DAP ecosystem.
3. **Content Submission:**
   - Authors must be able to submit research papers, articles, and related content to the platform

4. **Open Peer Review:**
    - DAP should support open and competitive peer review processes.
    - Reviewers, including the authors themselves, should be able to provide feedback and critiques through the platform.
5. **Publication Workflow:**
    - The platform must have a streamlined workflow for manuscript publication, including editorial reviews, revisions, and final publication steps.
6. **Content Accessibility:**
    - Published content should be openly accessible to the public, adhering to the principles of open access publishing.
7. **Scholarly Wallet Integration:**
    - The Scholarly Wallet should seamlessly integrate with various user actions, such as content submission, and participation in peer review.
8. **Reward System:**
    - DAP should support the distribution of rewards in the form of DAP FTs (Ergions) to users based on their contributions within the ecosystem.
9. **Blockchain Integration:**
    - The platform should integrate blockchain technology for secure and transparent record-keeping of user interactions, reviews, and publication histories.
10. **Search and Discovery:**
    - Users should be able to search for content based on keywords, authors, topics, and other relevant criteria.
11. **Notification System:**
    - DAP should provide a notification system to inform users about updates, comments, reviews, and other relevant activities.
12. **User Interaction and Engagement:**
    - The platform should facilitate user interactions through comments, ratings, and discussions on published content.
13. **User  Management:**
    - Users should be able to manage their roles, areas of interest, and personal information
14. **Analytics and Reporting:**
    - DAP should provide analytics and reporting tools to track the impact and reach of published content, as well as user engagement metrics.
15. **Data Security and Privacy:**
    - The platform must prioritize data security and user privacy, adhering to relevant regulations and standards.
16. **Feedback Mechanism:**
    - Users should have a mechanism for providing feedback, reporting issues, and suggesting improvements to the platform.
17. **Support for Machine Intelligence:**

- Provisions should be in place to accommodate Machine Intelligence texts and reviews for knowledge extraction.

These functional requirements are ess0ential for the DAP platform to operate efficiently, provide a user-friendly experience, and achieve its goals of democratizing academic publishing and fostering collaboration within the scientific community.

## 4.4 Technical requirements

These are preliminary technical requirements for a prototype, which will have to be expanded and adapted in the future of DAP establishment.

- Access to BESU nodes and EBSI test/production nodes is essential for seamless integration with the blockchain network.
- Documentation for EBSI web services, covering aspects such as creating wallets, authentication, and contract deployment, is crucial for developers to understand and implement blockchain functionalities.
- In the absence of other available options, an IPFS (InterPlanetary File System) local instance needs to be set up. IPFS facilitates decentralized file storage and retrieval, ensuring data availability and resilience.
- A local relational database server is required to store and manage data efficiently. This relational database system supports the structured storage of information, contributing to the overall functionality of the prototype.
- To host the web application for publishing and reviewing, a local web server such as Apache is necessary. The web server should have PHP support to enable the execution of dynamic web pages and interactions with the backend.
- Additionally, a web service needs to be implemented on the local web server, orchestrating all processes on the blockchain or database. This centralizes the functionality and ensures seamless communication between the web application and blockchain. Service needs java runtime environment to function properly.
-

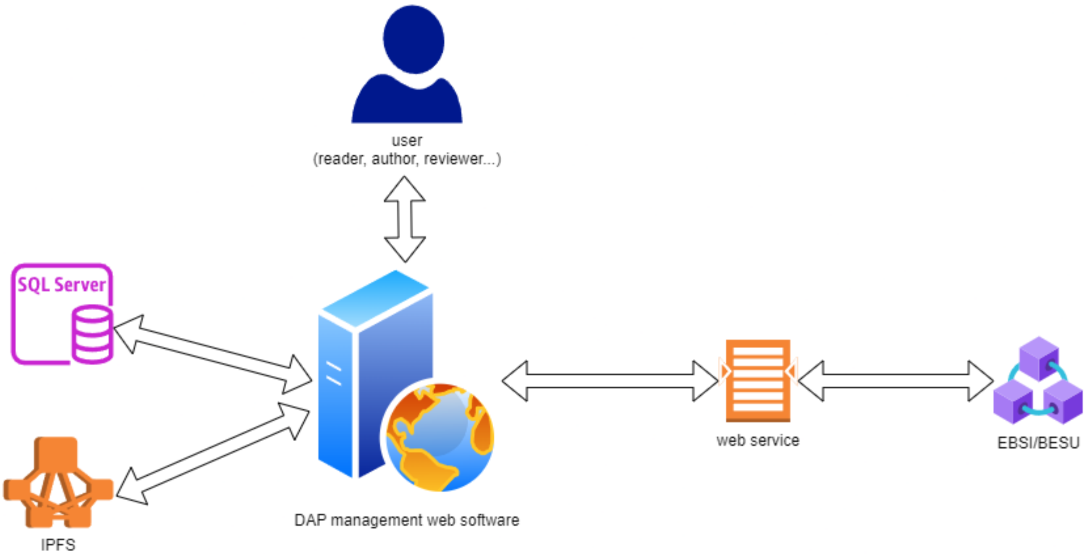


***Figure 8:*** **Block schema of DAP ecosystem**

# 5 Implementation and piloting of Electronic Registered Delivery Application

## 5.1 Introduction

The secure exchange of electronic documents and data is a cornerstone of modern business and government operations, especially critical in an era where digital transformation has reshaped the way we conduct business, enforce contracts, and interact with governments.
The lighthouse guiding in Europe is the eIDAS Regulation, which came into effect in July 2016. It is a pivotal piece of legislation within the European Union (EU) that seeks to establish a uniform framework for electronic transactions and digital identity across member states. At its core, eIDAS aims to create a legal environment where electronic transactions can enjoy the same legal recognition as traditional paper-based processes, thereby fostering trust and interoperability across borders. A key element of eIDAS is the implementation of robust electronic identification, authentication, and trust services that underpin the security and reliability of electronic communications.
Electronic Registered Delivery (ERD) is regulated by a section of the eIDAS regulation, primarily by the articles 43 and 44. The regulation addresses the fundamental need to ensure the confidentiality and integrity of electronic documents and their non-repudiation, meaning that the sender cannot deny having sent the document. ERD systems compliant with eIDAS offer a technical framework for transmitting electronic data and documents in a manner that is both secure and legally binding.
By leveraging digital signatures, time-stamping, and secure transmission channels, ERD systems are highly reliable means of delivering electronic documents while maintaining their legal integrity.
THe requirements on ERD were not changed in eIDAS 2.0 only implementing acts will become mandatory.

## 5.2 Scenario

John, an executive at a multinational company based in France, needs to send a contract proposal to their business partner, Sarah, who works at a partner organization in Germany.
The contract proposal outlines the terms of a new joint venture and must be sent securely.

By utilizing the Electronic Registered Delivery system, John and Sarah successfully exchange the contract proposal in a secure, efficient, and secure manner, eliminating the need for paper-based documentation and ensuring the confidentiality and integrity of the contract in their cross-border business transaction.

To do it they will execute the following steps:

**Step 1- Document Preparation**:

John begins by preparing the contract proposal on his computer.
He ensures that the document is in digital format and includes all the necessary terms, conditions, and signatures required for a valid contract.

**Step 2 - Digital Signatures:**

John adds his digital signature to the document using a cryptographic key issued by a trusted certificate authority. This signature ensures the document's authenticity and non-repudiation.

**Step 3 - Accessing the Electronic Registered Delivery Service**:

John logs into his company's secure online portal, which offers access to the Electronic Registered Delivery service.
The portal is compliant with eIDAS and ensures secure access.

**Step 4- Document Upload**:

Within the portal, John initiates the process of sending the document using the Electronic Registered Delivery service. He uploads the contract proposal, which is automatically encrypted to protect its confidentiality.

**Step 5 - Recipient Verification**:

John enters Sarah's ERD address and other contact information, ensuring it's accurate. The system may also ask for additional authentication or verification, such as a one-time passcode or security question, to confirm the recipient's identity.

**Step 6 - Timestamping**:

The system records a timestamp with the exact date and time of submission. This timestamp is crucial for legal purposes and serves as evidence of when the document was sent.

**Step 7- Secure Transmission**:

The Electronic Registered Delivery system uses a highly secure and encrypted channel to transmit the document to Sarah's designated email address. The system provides end-to-end encryption, safeguarding the document from unauthorized access during transit.

**Step 8 - Confirmation of Receipt**:

Once the document is successfully delivered to Sarah's ERD address, the system sends a confirmation to John, indicating that the document has been received. The confirmation may include a delivery receipt with the timestamp.

**Step 9 - Recipient Authentication**:

Sarah receives an email notification with a link to access the document. To ensure her identity and prevent unauthorized access, she may be required to authenticate herself using a secure login or a one-time passcode.

**Step 10 -Document Review and Acceptance**:

Sarah reviews the contract proposal, once satisfied, she digitally signs the document using her own trusted cryptographic key. Her digital signature is added to the document.

**Step 11 - Acknowledgment of Acceptance:**

The system generates an acknowledgment that Sarah has accepted the document, which is then sent back to John, by Sarah confirming that the document has been accepted and signed by the recipient.

The entire process, from document preparation to final acceptance, if it complies with the legal requirements established by eIDAS on electronic signatures and ERD**,** guarantees both parties that the electronic contract exchanged is the one legally valid.

## 5.3 Functional requirements

The functional requirements of the Electronic Registered Delivery application represent the characteristics to be satisfied by the ERD system produced in TRACE4EU, below a numbered list of the main ones:

**1 – Document Confidentiality and Integrity:**

Electronic Registered Delivery prioritizes the confidentiality and integrity of electronic documents, ensuring that sensitive information remains secure and unaltered during transmission on its secure channels. This is achieved through robust encryption, digital signatures, and timestamping mechanisms, which collectively safeguard the content of the documents from unauthorized access and tampering.

**2 - Non-Repudiation:**

One of the central tenets of Electronic Registered Delivery is non-repudiation. This means that once a sender electronically delivers a document using this system, they cannot deny having sent it. Digital signatures and secure transmission methods provide concrete evidence of the sender's identity, thereby preventing disputes and ensuring accountability.

**3 - Cross-Border Compatibility:**

In the European digital space and market, where cross-border interactions are commonplace, Electronic Registered Delivery becomes especially vital. It ensures that electronic documents can traverse national boundaries while still adhering to legal requirements, thereby fostering the European digital single market.

Test

**4 - Efficiency and Cost Savings:**

Electronic Registered Delivery streamlines processes by eliminating the need for physical documents and paperwork. This not only enhances efficiency but also reduces costs associated with paper-based communication and document storage.

**5 - Interoperability:**

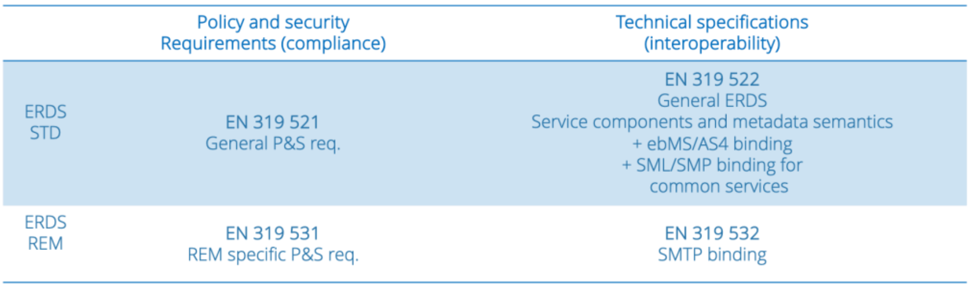
Interoperability is a cornerstone of eIDAS, and Electronic Registered Delivery is designed to seamlessly integrate with various eIDAS-compliant services, such as electronic signatures and electronic seals. This ensures that different electronic trust services can work together, further promoting cross-border digital transactions.

## 5.4 Technical requirements

In the follow, by points, listed the additional technical requirements will be satisfied by the ERD system of the TRACE4EU initiative:

**1 - Compliance to EU technical standards.**

In addition to support the articles 43 and 44 of eIDAS Regulation, an ERD system must be compliant with the TC ETSI prepared standards for Electronic Registered Delivery Services (ERDS) and Registered Electronic Messaging (REM) listed in the following figure 1 :



| | Policy and security Requirements (compliance) | Technical specifications (interoperability) |
|---|---|---|
| ERDS STD | EN 319 521<br>General P&S req. | EN 319 522<br>General ERDS<br>Service components and metadata semantics<br>+ ebMS/AS4 binding<br>+ SML/SMP binding for common services |
| ERDS REM | EN 319 531<br>REM specific P&S req. | EN 319 532<br>SMTP binding |

*Figure 9: ETSI standards for ERD*

Moreover, additional standards that will be considered are:

TS 119 524 - Testing Conformance and Interoperability of Electronic Registered Delivery Services

TS 119 534 - Testing Conformance and Interoperability of Registered Electronic Mail Services

TR 119 500 - Business Driven Guidance for Trust Application Service Providers

**2 - Integration with the EBSI blockchain**

Integration of the TRACE4EU's ERD system with the EBSI blockchain to provide business value to the ERD Systems, as required by the grant agreement.

### 3 - Efficient utilization of the EBSI blockchain

The balancing between decentralization and scalability is the main key to preventing blockchain performance bottlenecks. Specifically, performance problems originating from uses of the blockchain that conflict with the intrinsic technical characteristics of the blockchain itself, can originate really poor performance of the system.
For example, in an ERD system these could happen if the blockchain is used as a normal storage, like a database managed by a modern DBMS, saving everything inside its blocks. For these reasons Off-Chain approaches will be preferred over In-Chain ones.

### 4 - Modular "Track on Block chain" sw component

The "tracking on blockchain" functionalities will be encapsulated in an independent software component, clearly separated by the rest of the ERD system by specific interfaces, to facilitate its reuse by EBSI
Moreover, it will be evaluated also the possibility to implement it using smart contracts to facilitate its deployment in the EBSI block-chain based infrastructure.

### 5 – Support of one-to-many communication

The ERD system is going to manage not only communication from one sender to one receiver but also from one sender to many receivers.

# 6 Implementation and piloting of Know Your Customer (KYC tool) application

## 6.1 Introduction

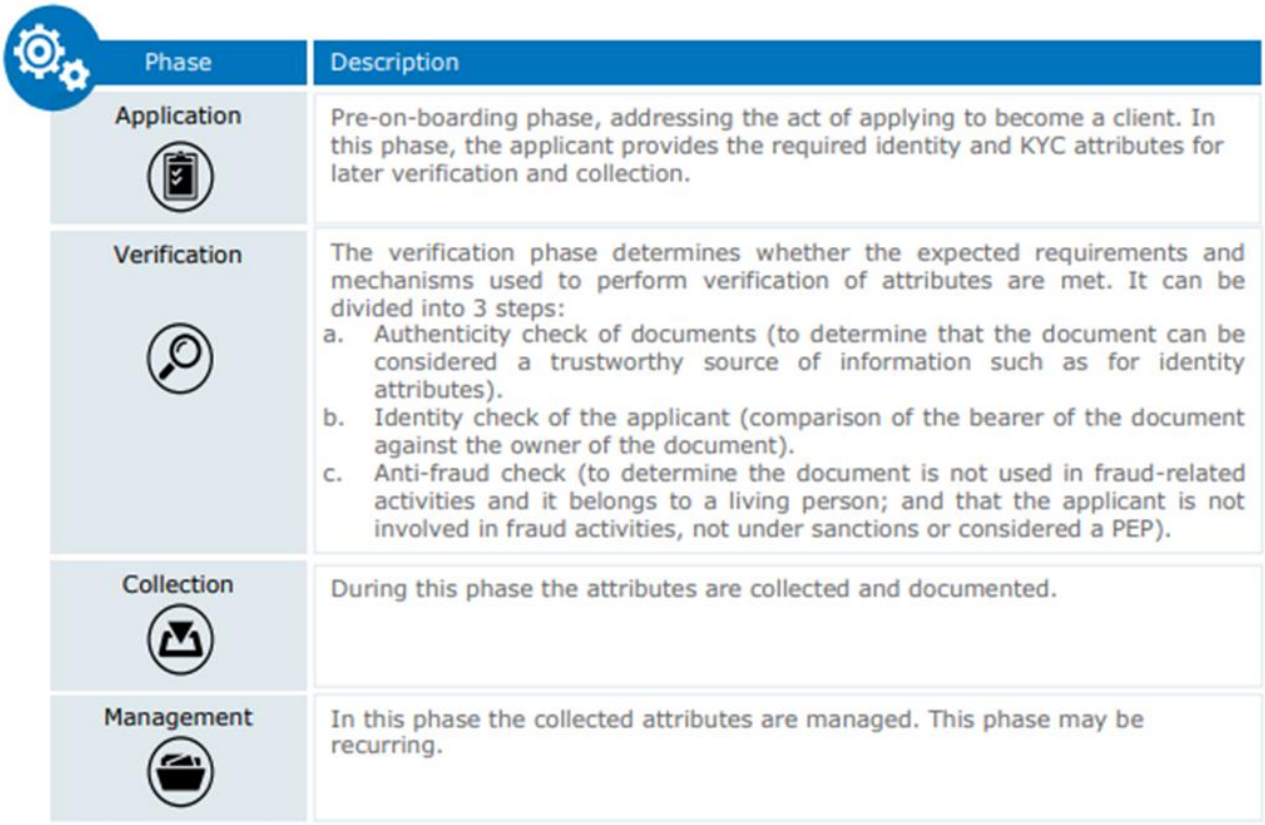
### On-boarding processes, requirements, and regulation

KYC is a procedure to identify and verify a customer's identity. The process consists of a series of checks implemented in the first stage (on-boarding) of the relationship with the client to verify that he is who he says he is, considering his identity documents and his personification.

The on-boarding process implements the requirements and procedures used by financial institutions for the enrolment of potential clients. For the purpose of the Use Case, the on-boarding process was divided into the following four process phases: -

Application, Verification, Collection and Management, described in more detail in the Table1 below. Note that the Collection and Verification can be performed as a single phase, denoted as 'verify while collect'.

**Table 3. The phases of on-boarding**



| Phase | Description |
|---|---|
| Application | Pre-on-boarding phase, addressing the act of applying to become a client. In this phase, the applicant provides the required identity and KYC attributes for later verification and collection. |
| Verification | The verification phase determines whether the expected requirements and mechanisms used to perform verification of attributes are met. It can be divided into 3 steps:<br>a. Authenticity check of documents (to determine that the document can be considered a trustworthy source of information such as for identity attributes).<br>b. Identity check of the applicant (comparison of the bearer of the document against the owner of the document).<br>c. Anti-fraud check (to determine the document is not used in fraud-related activities and it belongs to a living person; and that the applicant is not involved in fraud activities, not under sanctions or considered a PEP). |
| Collection | During this phase the attributes are collected and documented. |
| Management | In this phase the collected attributes are managed. This phase may be recurring. |

[1.] Source: Study on eID and digital onboarding: mapping and analysis of existing onboarding bank practices across the EU (A study prepared for the European Commission DG Communications Networks, Content & Technology by PWC)

### Legal obligations

The banking/financial sector is obliged to implement compliance processes to address concerning security, know-your-customer, strong authentication of parties and interoperability, e.g. as provided under the Directive (EU) 2015/849 (4th Anti-Money Laundering Directive, denoted as '**4AMLD**') which is the main instrument, along with its subsequent amendments, the 5th Directive (EU) 2018/843 ('**5AMLD'**) and the 6th Anti-Money Laundering Directive (EU)2018/1673 ('**6AMLD**').

With a strict application as of January 10, 2020, 5AMLD establishes the reference framework for electronic KYC (Know Your Customer) processes in Europe and enables financial companies to provide services in a digital single market with 508 million consumers. Barriers to doing business in multiple industries and markets were removed.

Another important obligation relevant to any KYC process, is compliance with the Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

For a detailed description of Current legal and regulatory requirements for on-boarding please refer to Appendix 1 – Current Legal and Regulatory Requirements.

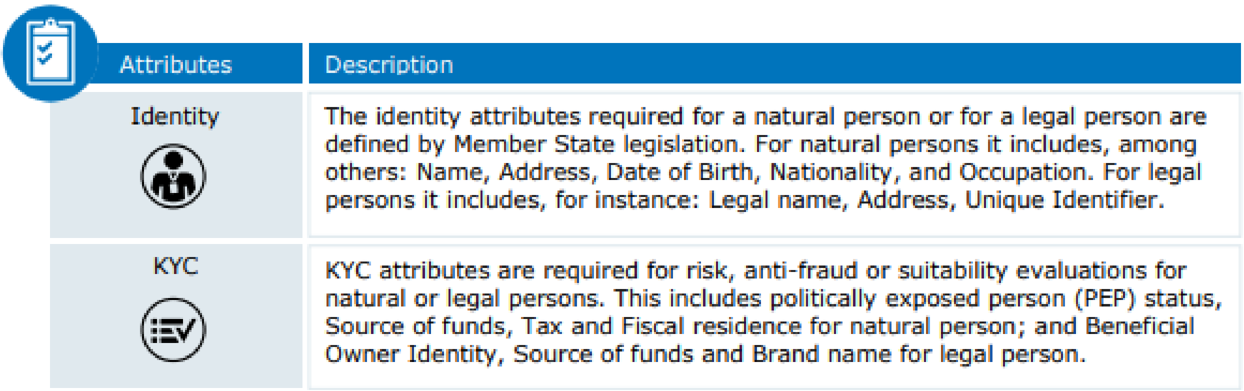
### Affected Parties

- • Financial institutions
- • Virtual currencies
- • Anonymous prepaid cards
- • Digital wallet services
- • Gambling services
- • Letting agents
- • Art dealers

### Required attributes.

The different required attributes are distinguished as two types: identity and KYC related attributes, as defined in table2 below. For a detailed description of individual attributes, please refer to Appendix 2.

**Table 2. The phases of on-boarding**



| Attributes | Description |
|---|---|
| Identity | The identity attributes required for a natural person or for a legal person are defined by Member State legislation. For natural persons it includes, among others: Name, Address, Date of Birth, Nationality, and Occupation. For legal persons it includes, for instance: Legal name, Address, Unique Identifier. |
| KYC | KYC attributes are required for risk, anti-fraud or suitability evaluations for natural or legal persons. This includes politically exposed person (PEP) status, Source of funds, Tax and Fiscal residence for natural person; and Beneficial Owner Identity, Source of funds and Brand name for legal person. |

Attributes typically consist of ID attributes like name, first name, date, and place of birth, etc.

Additional attributes could be the tax address, jurisdiction, or contact details. It is important to differentiate between the identity datasets themselves and the information which is used to verify information about oneself.

It is believed that better portability of data attributes could be facilitated using an off-chain architecture. This would also fit in context of GDPR where the data subjects have more control over their data. Access to the data in the off-chain structure can only be given by the data subject him/herself.

### The Cyprus Government's Strategic objectives – EBSI KYC UC.

To enable the CY government to assess and seize the DLT opportunity, to drive the right level of awareness and clarity concerning the technology, in the context of fostering and utilising innovation for the benefit of the economy.

This strategic objective is in line with Cyprus' vision to be one of the leading international centres for innovation and growth, where innovators abiding to the regulatory framework can flourish.

Government's Priorities:

- Prepare an enabling legislative framework.
- Enhancing the application of technology by the government and the private sector.
- Promoting DLT in the financial sector.

### Opportunities and Challenges

- Collaborative Learning / sharing experiences
- Implications of off-chain / on-chain transactions
- Interoperability: Integration and architecture requirements for integration with EBSI as well as domestic Blockchain needs to be considered. Important to understand the interoperability with existing infrastructure.
- Selecting the appropriate frameworks: Since we might need in the future to apply Blockchain in other sectors we need to study which framework offers easier integration to other problems of interest. For example, we might proceed with land registry and in the future, we consider to apply Blockchain in tax authorities - we need to ensure integration and linkage is feasible.
- Compatibility with other niche technologies: Before we consider a possible design of a Blockchain solution for a particular domain we need to ensure that our design can facilitate other technologies to be applied such as Artificial Intelligence, Machine Learning etc. Since Blockchain is about data verification and agreement we need to make sure that our infrastructure design facilitates exploitation of data for other purposes such as automation, data analytics, machine learning etc. To understand better the suitability of EBSI as a DLT application framework.

## 6.2 Scenarios

The KYC Tool scenario covers EU citizens submitting their KYC (Know Your Customer) documents to banks and/or other financial or administrative institutions. The scenario applies to all EU countries that require identifying customers as part of their AML regulatory framework implementation.

Currently KYC process are mostly executed manually, in-person, using wet-ink signed or notarized documents and repetitive, whether a new customer opens an account or requests new financial services/facilities. Maintaining personal details updated is also necessary (every 2-3 years).

## Existing KYC process

- customer submits KYC documents to his bank
- Bank verifies documents and approves customer

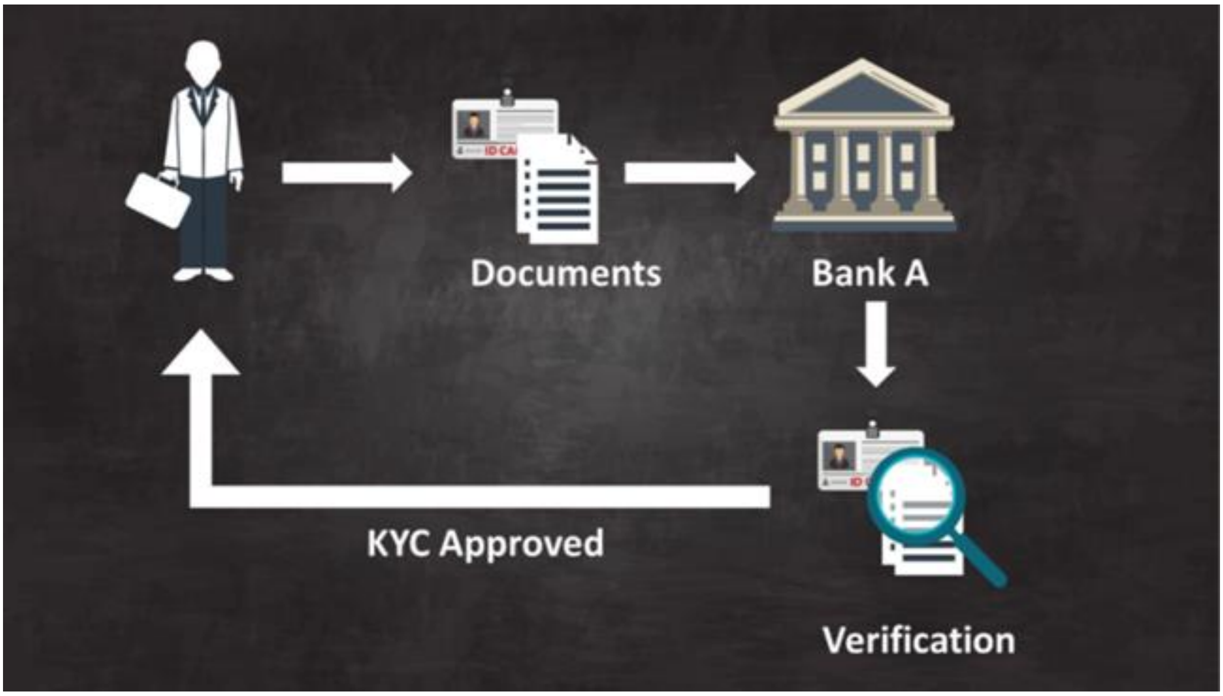


*Figure 10: Existing KYC process*

## The problem

customer needs to repeat the process, e.g., documents submission and verification for every other bank he wishes to do business with.

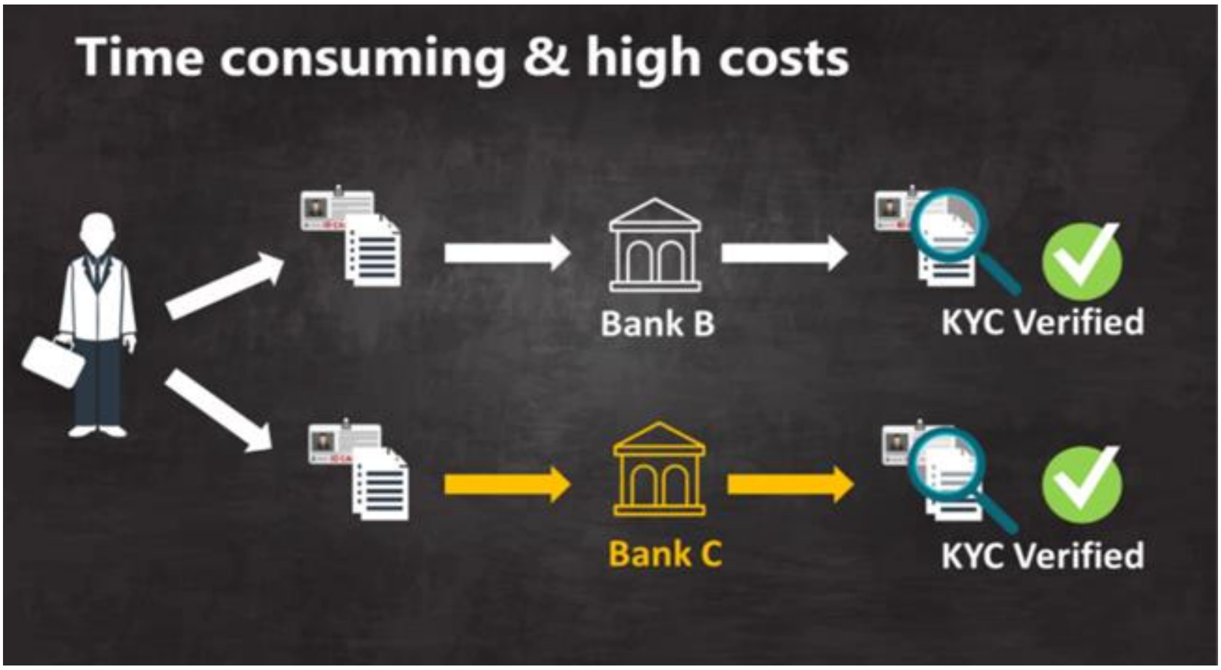


*Figure 11: The problem*

The KYC Tool aims to simplify the KYC process and to reduce the customer's time-consuming and cost-intensive identification. New services for KYC processes will be required to be implemented by EBSI.

## EBSI Solution - Overview

- customer submits KYC documents only once.
- KYC encrypted docs kept in off-chain EBSI storage.
- encrypted key to decrypt the docs kept in on-chain EBSI.

## Aligned with GDPR

- right to anonymity
- right to be forgotten (erase)

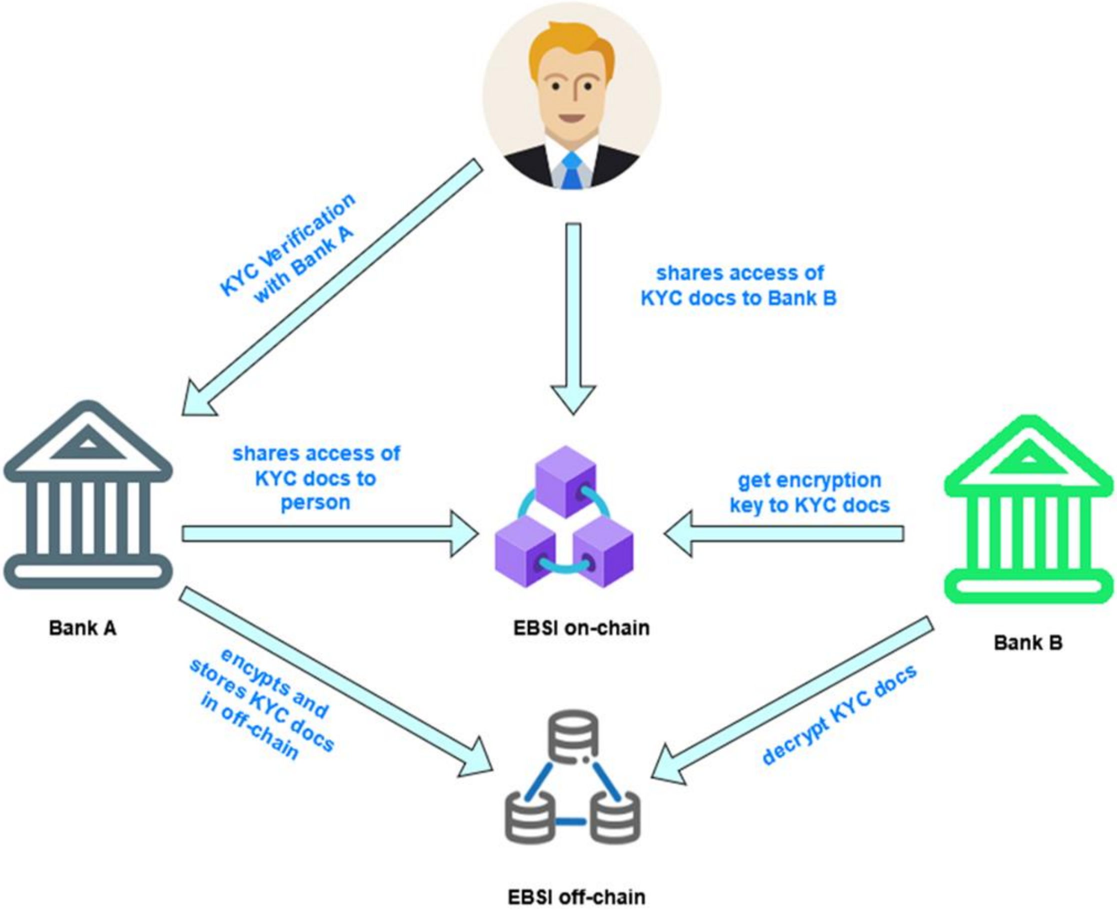

KYC Verification with Bank A
shares access of KYC docs to Bank B
shares access of KYC docs to person
get encryption key to KYC docs
Bank A
EBSI on-chain
Bank B
encypts and stores KYC docs in off-chain
decrypt KYC docs
EBSI off-chain

*Figure 12: KYC process*

The proposed KYC scenario aligns with GDPR requirements. Personal data will be kept encrypted in off-chain storage and the owner of the encryption key will share the key with an institution via the on-chain EBSI network, encrypted with the institution's public key.

The KYC tool will allow an EU citizen to submit his personal documents securely and digitally to e.g., a bank, which will validate them and then store them encrypted in a preservation storage. The bank will also store the encryption key on EBSI. The citizen will then be able to make his KYC docs available to any other bank or institution by sharing with them the encryption key via the EBSI network.

## Basic Scenario (EBSI)

### *Step-1*

1. customer submits KYC documents to Bank A
2. Bank A verifies docs, encrypts them with a key and stores them in off-chain.
3. Bank A encrypts the encryption key with the customer's public key and puts it on on-chain. It also includes the **hash** of the **un-encrypted** docs and the status "**Verified by Bank A**".

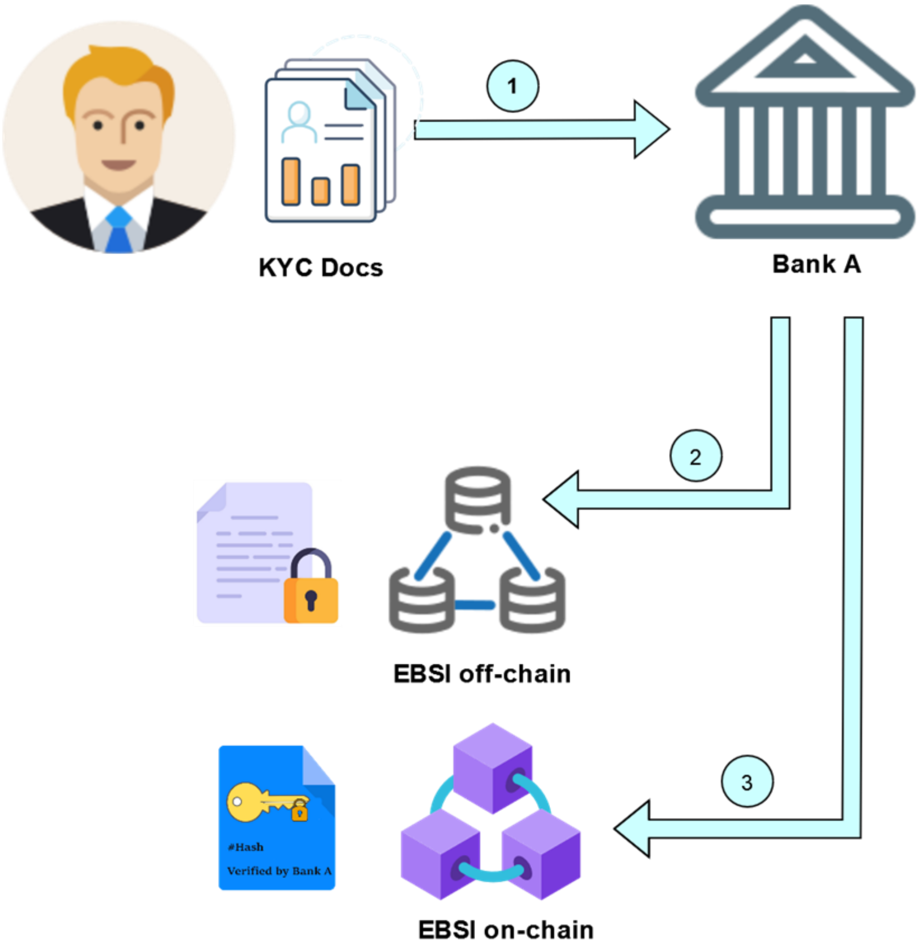


*Figure 13: Basic Scenario*

### *Step-2*

1. Customer gets encryption key, decrypts the docs and encrypts again using a new encryption key.
2. Customer encrypts the key using Bank A's and Bank B's public keys and puts them on on-chain.
3. Bank B gets the encryption key from on-chain using their private key.
4. Bank B **decrypts** KYC docs off-chain. Bank B **verifies** the docs have not been changed using the **#Hash** in the two blocks. Bank B knows docs have already been verified from Bank A (previous block).

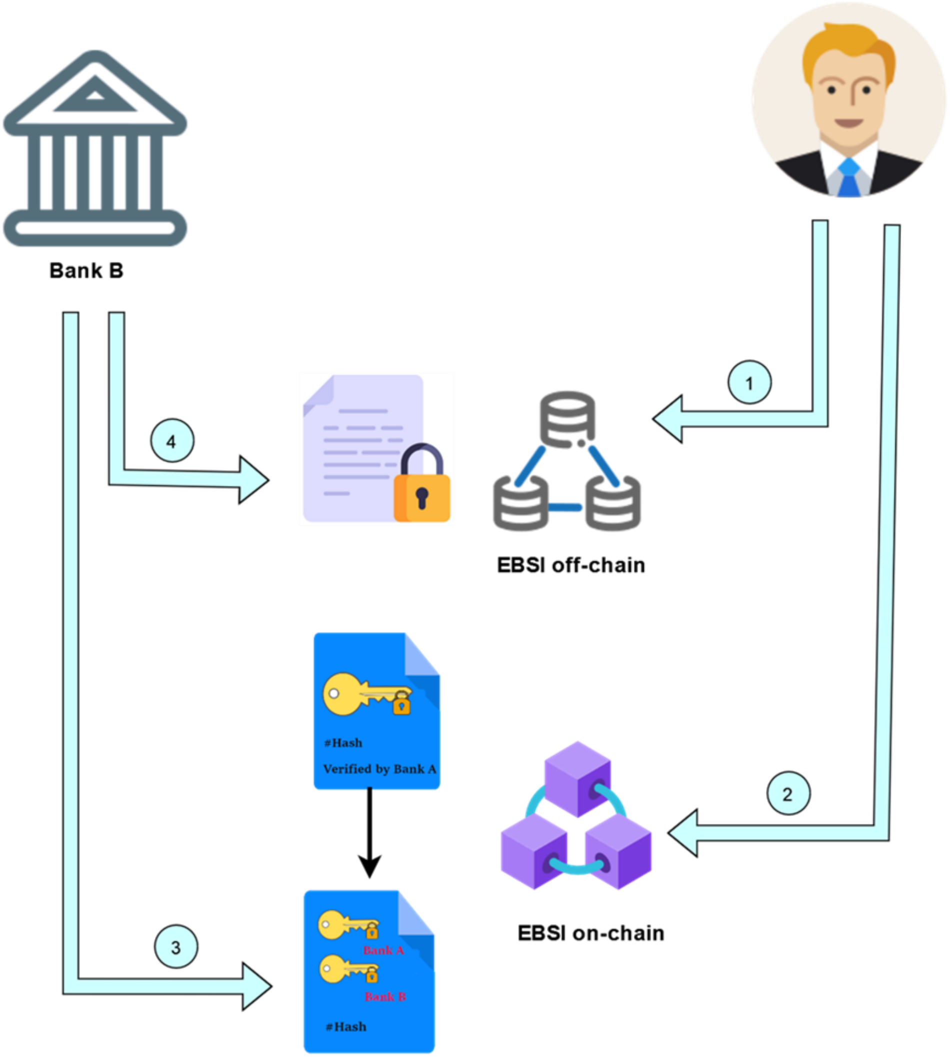


*Figure 14: Basic Scenario*

## 6.3. Functional requirements

Facilitating the digitalization of the KYC process between Natural Persons and Financial Institutions. Our Use Case will be covering the development of an EBSI-based "process tool" that can be used to facilitate the automation of the KYC process. The Scenario will not be covering the execution full KYC process, especially the Identification part which most likely lies within the eIDAS boundaries - for the sake of the UC scenario execution we will be most likely utilizing the EBSI VC-ID (SSI) implementation.

**Identity Verification:** Reliably verify new customers across the globe across a broad range of countries, languages, and ID types.

**Liveness Detection (“**anti-spoofing”**):** Prevent evolving and sophisticated spoofing attempts to assume another individual’s identity.

**Seamless and speedy user/customer Experience:** Verify customers across devices via a native mobile/web application. Streamline the user journey with a simple, fast, and compliant onboarding experience.

**KYC process digitalization (eKYC)**

eKYC is the expression used to describe digital KYC processes. eKYC means the remote, paperless process that minimizes the costs and traditional bureaucracy necessary in KYC processes.

Falsification of identity, signatures and phishing is very common. To ensure that eKYC processes meet the same safety standards as traditional ones of identification and face verification, companies must implement electronic identification processes with high levels of safety and reliability, in absolute compliance with the rules set in 5AMLD and eIDAS2 regulations.

Compliance with the current Regulatory and Legal/Industry framework (see Appendices 1 and 5) relevant to the KYC process is a major requirement.

For Details on Identity and KYC Attributes required by current verification mechanisms, please refer to Appendices 2, 3, and 4.

## 6.3 Technical requirements

### General Considerations

1. **EBSI Integration:** Trusted Issuers  back/front-end systems integration with EBSI. The application utilizes EBSI to record credential verification and sharing events, providing a transparent and tamper-proof system.
2. **Data reusability:** Allowing users to share their data with different financial service providers.
3. **Digital Wallet Compatibility:** Ensure compatibility with digital wallets for storing and managing KYC personal data, allowing users to maintain control over their personal information.
4. **Interoperability:** EBSI, eIDAS2-compliant wallets, ???.
5. **Security:** Implement robust security measures to protect user data  from unauthorized access and ensure the data-sharing process's integrity.
6. **MetaData/off-chain:** Documents containing encrypted evidence of personal data associated with the KYC process.
7. **Data/on-chain:** Identification of documents, encryption keys, hash, status, timestamps,…
8. **Off Chain Storage** setup and management (Cloud/physical, Database, API???).

### Identification of Actors and relationships mapping

| Actor | Role | Accredited to | Accredited by | Additional Information |
|---|---|---|---|---|
| Ministry of Finance (MOF) | Root TAO | • **Accredit** CBC **to issue KYC-VCs** | | |
| Central Bank of Cyprus (CBC) | Trusted Issuer | • **Issue KYC-VC** to banks and other FIs | MOF | |
| Hellenic Bank (HB) | [Bank A] | • Use KYC-VC to get access to EBSI T&T service | CBC | Creates and delegates access of empty KYC header to citizens.<br>Manual Verification, Add/Update Timestamp of verified documents in Ledger.<br>Use of PKI for doc decryption |
| Bank of Cyprus (BoC) | [Bank B] | • Use KYC-VC to get access to EBSI T&T service | CBC | Creates and delegates access of empty KYC header to citizens.<br>Manual Verification, Add/Update Timestamp of verified documents in Ledger.<br>Use of PKI for doc decryption |
| Citizen (Wallet Holder) | KYC Data subject | | | provides encrypted data documents, and delegates access to banks, FIs |

*Figure 15: Actors and roles*

## KYC Trust Chain

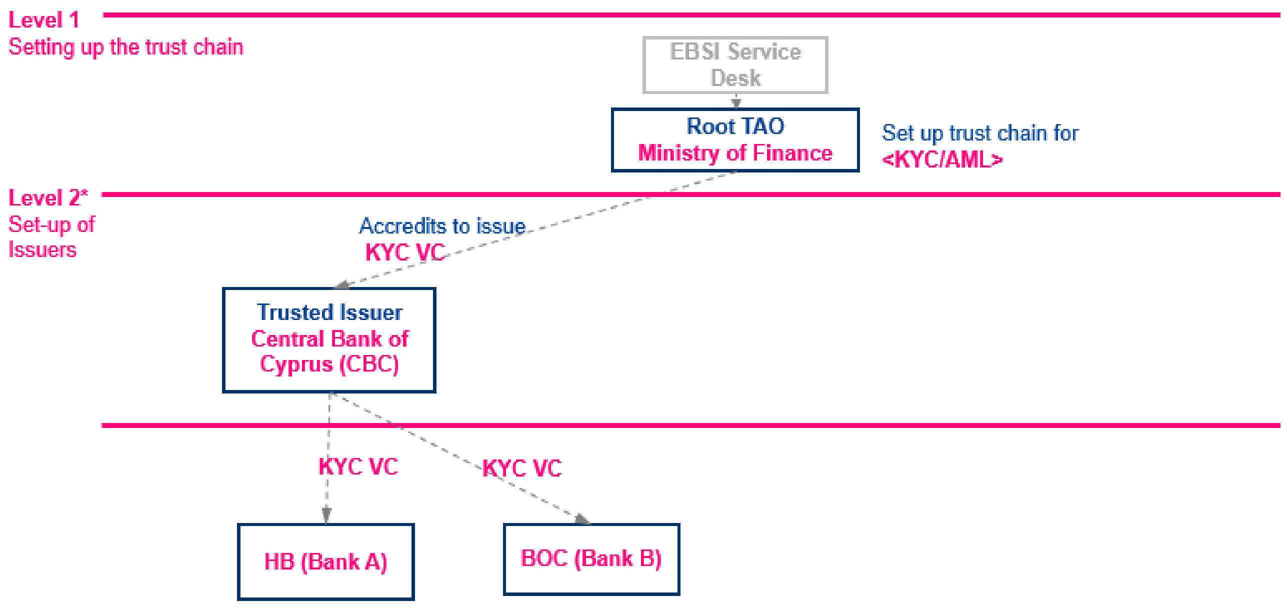


*Figure 16: trust chain*

## Flow diagram utilising EBSI's Track and Trace (T&T) new functionality – preliminary*

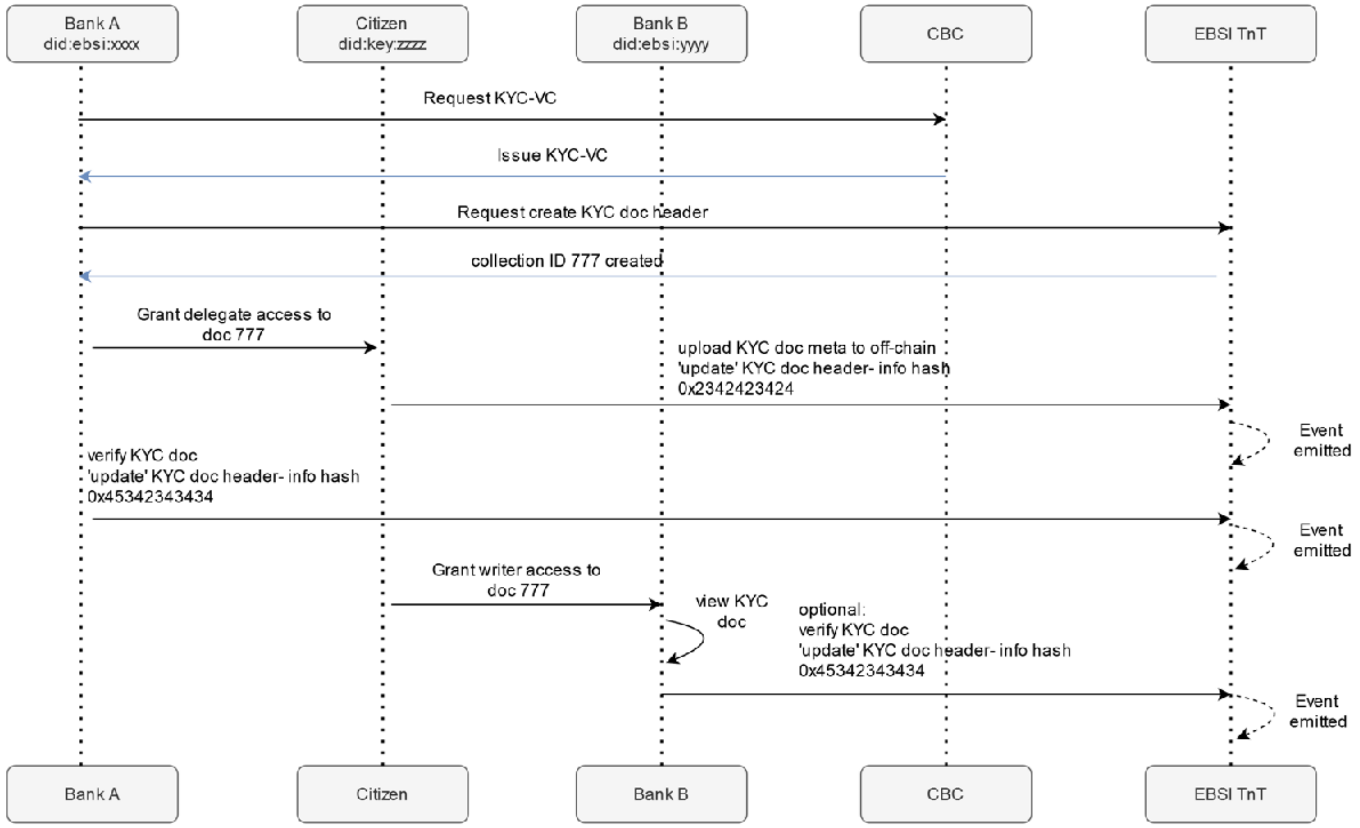


***Figure 16: Flow with EBSI T&T api***

*preliminary, as far as the final design/implementation is concerned, as the EBSI's T&T functionality/specs are still under development.

- Citizen creates a wallet and its associated DID.
- Citizen requests an KYC doc header from Bank A using his DID
- Bank A creates a KYC header in T&T and delegates access to a citizen
- Citizen encrypts KYC docs and uploads to off-chain storage. updates KYC header in T&T with the encryption key encrypted with bank's A public Key.
- Bank A decrypts and verifies KYC docs and updates KYC header in T&T
- Citizen gives access to Bank B after adding the encryption key encrypted with Bank's B public key in KYC header.
- Bank B views KYC doc and optionally re-verifies.

# APPENDIX 1 – KYC, Current Legal and Regulatory Requirements

Financial institutions apply several AML requirements identified in local AML legislations which are developed in line with the Financial Action Task Force (FATF) Recommendations; the Directives 2005/60/EC12 (hereafter denoted as '3AMLD'); and the Directive 2006/70/EC13.

Prior requirements to customer due diligence (CDD) is to establish a business relationship only with identified natural or legal persons. Strong identification as well as verification of the provided information should be performed irrespective of the on-boarding method, namely: face-to-face or remotely.

The common due diligence measures include:

- identification of the natural and legal person on the basis of documents and data submitted; and verification of the submitted information on the basis of information obtained from a reliable and independent source.
- identification and verification of the legal representative and the right of representation.
- identification of the beneficial owner, based on information provided for onboarding or obtained from another reliable and independent source; and
- obtaining information on the purpose and nature of the business relationship or transaction.

The enforcement of the due diligence measures is required for completing the onboarding process since the relationship with the financial institution cannot be established in the following cases:

- an anonymous or unidentified person; or
- a person that fails to submit sufficient information required for customer due diligence, e.g., identity information; or
- a failure of the veracity or authenticity of the documents or data.

On the subject of remote on-boarding, common AML requirements are that financial institutions shall take extra CDD steps to compensate the associated risk by applying additional due diligence measures (i.e. enhanced customer due diligence, EDD). The additional measures usually are:

- obtaining additional supporting evidence (e.g. a certified copy of an identity document) allowing to confirm the identity of the person;
- the first payment must be from a client account in the European Union; or
- receiving a validation of the client's identity by a third party (financial institution).

Some Member States allow the use of electronic identification means for remote on-boarding, providing a possibility for eIDAS to be used in the future to support the on-boarding. However, there is no common approach applied in the surveyed Member States on which electronic identification means are accepted and what are the requirements to these. Also, the process differs per Member State. For electronic verification of identity, the financial institutions can perform on-boarding themselves or use a third-party provider.

To understand where an electronic means and a digital process can support AML requirements for collection and management of information, the current recordkeeping requirements as per AML legislation were studied. The following approach is commonly required by local AML regulations within the majority of Member States:

- At on-boarding of natural persons, an officer of the financial institution shall make a copy of the page(s) of a government issued document submitted for identification which contains the identity attributes and a photograph.

- At on-boarding of legal persons, copies of government issued documents submitted for identification and verification (including documents required for identification and verification of beneficial owners) as well as for establishment of business relationship should be collected.
- The document storage period is defined on national level and can vary among Member States. But based on the FATF Recommendations it should not be less than 5 years after termination of a business relationship.

The usage of technologies, such as computer network access to electronic databases, video conference on-boarding or eID solutions, allowed for remote on-boarding by the AML legislation, lead to divergent cases of record-keeping observed in Member States which are presented in Annex II.

### 4AMLD, 5AMLD, 6AMLD

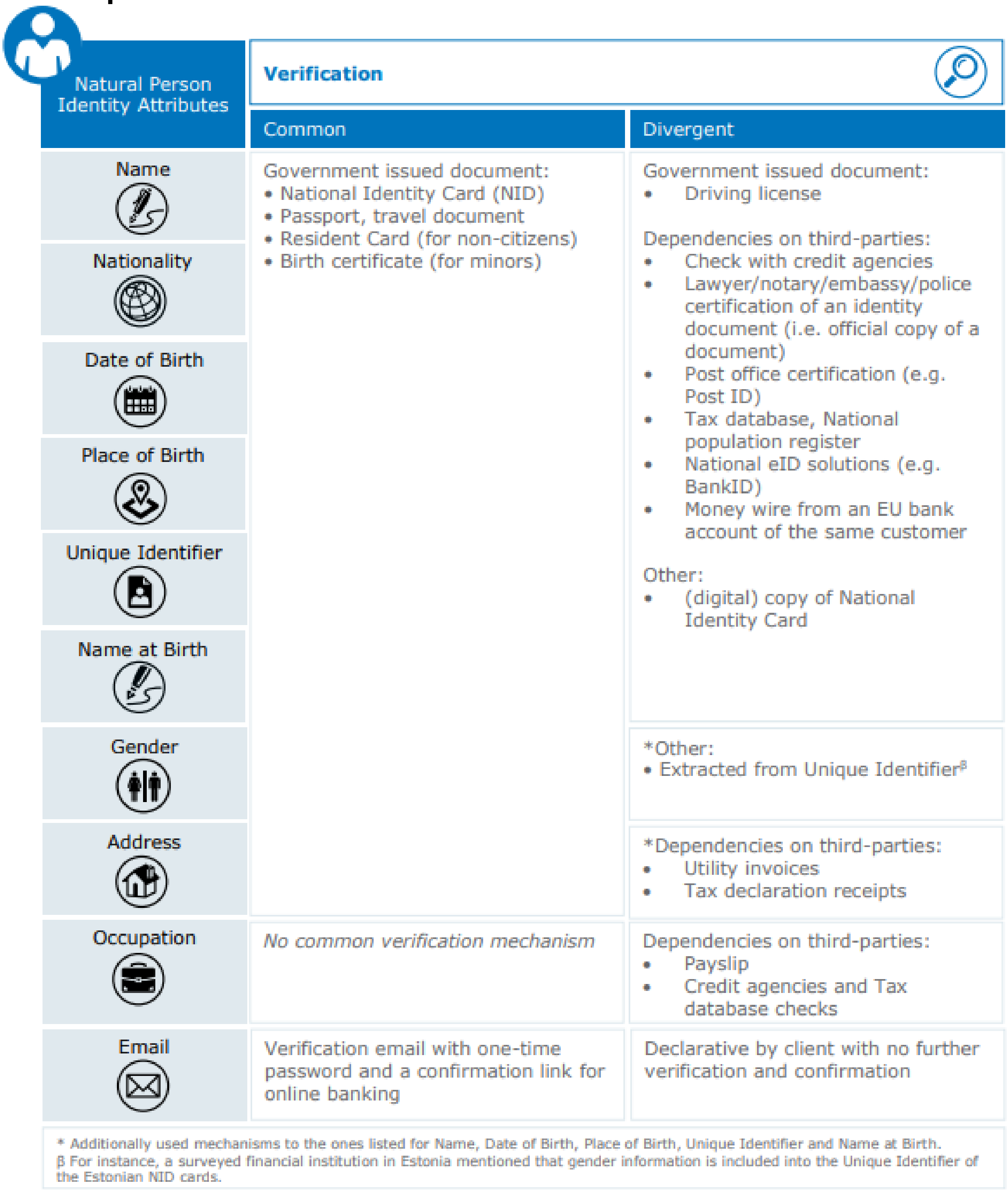
In 2016, the Commission proposed a set of additional amendments to 4AMLD to enhance the measures to combat money-laundering and financial terrorism. The European Compromise text issued on October 28, 2016 (denoted as '5AMLD') introduces amendments related to the use of electronic identification and trust services (as per the eIDAS Regulation) for KYC on-boarding, accessing funds and/or tracing electronic transactions. This suggests an amendment to 4AMLD in line with the legal framework on mutual recognition of notified eID schemes and means.

The 5th Anti-Money Laundering Directive (5AMLD) focuses on higher transparency in registrations of companies, trusts and similar legal arrangements that expect Member States to recognize and notify trusts or similar entities which are under their legal responsibility.

The objective of the latest directive (6AMLD) is to harmonize the European framework and to administer in all Member States effective, proportionate, and dissuasive money laundering-related sanctions that cannot be sufficiently enforced by Member States alone.

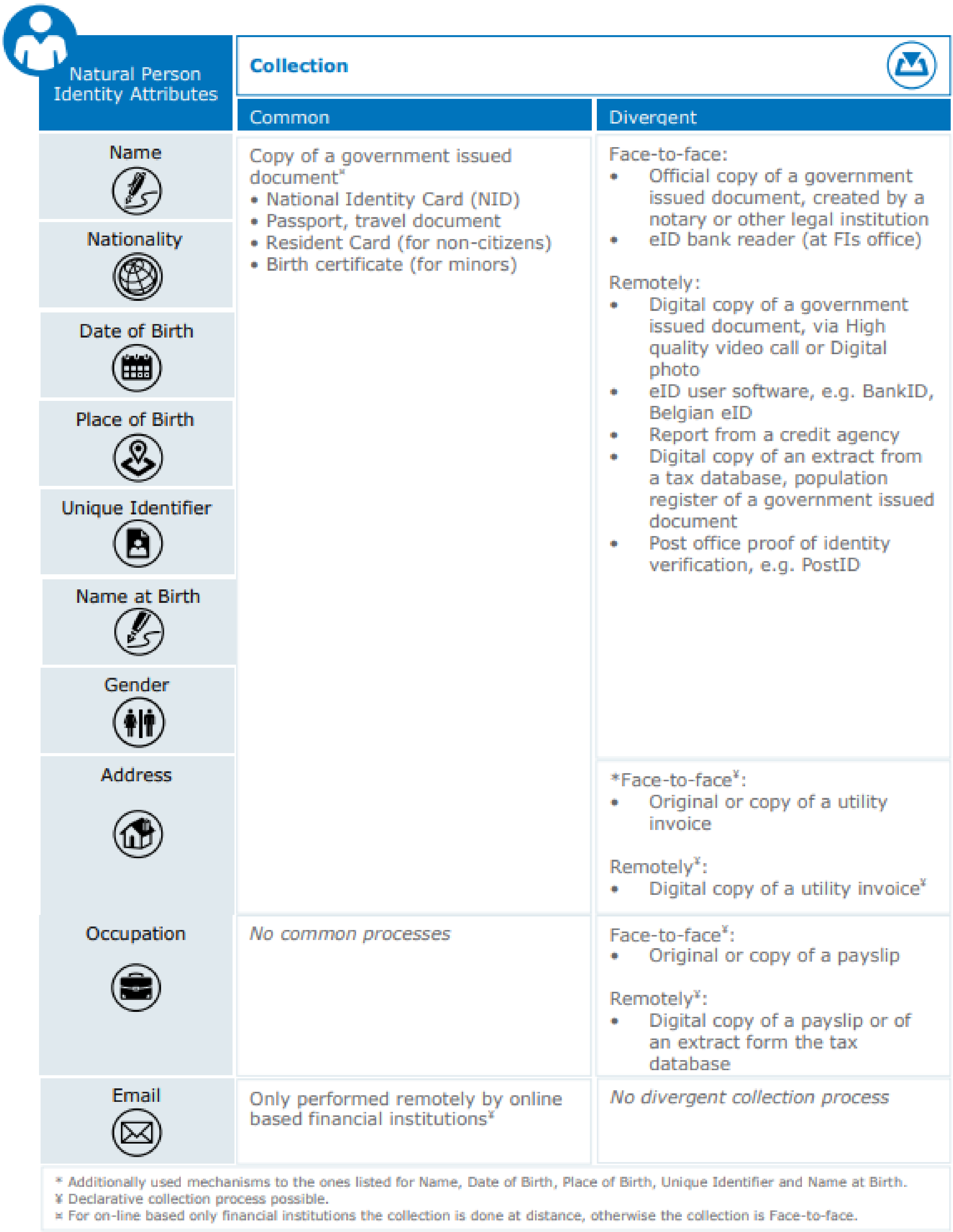
# APPENDIX 2 – Identity Attributes / Common and divergent verification mechanisms

## Natural person



| Natural Person Identity Attributes | Verification | |
|---|---|---|
| | Common | Divergent |
| Name | Government issued document:<br>• National Identity Card (NID)<br>• Passport, travel document<br>• Resident Card (for non-citizens)<br>• Birth certificate (for minors) | Government issued document:<br>• Driving license<br>Dependencies on third-parties:<br>• Check with credit agencies<br>• Lawyer/notary/embassy/police certification of an identity document (i.e. official copy of a document)<br>• Post office certification (e.g. Post ID)<br>• Tax database, National population register<br>• National eID solutions (e.g. BankID)<br>• Money wire from an EU bank account of the same customer<br>Other:<br>• (digital) copy of National Identity Card |
| Nationality | | |
| Date of Birth | | |
| Place of Birth | | |
| Unique Identifier | | |
| Name at Birth | | |
| Gender | | *Other:<br>• Extracted from Unique Identifier[β] |
| Address | | *Dependencies on third-parties:<br>• Utility invoices<br>• Tax declaration receipts |
| Occupation | *No common verification mechanism* | Dependencies on third-parties:<br>• Payslip<br>• Credit agencies and Tax database checks |
| Email | Verification email with one-time password and a confirmation link for online banking | Declarative by client with no further verification and confirmation |

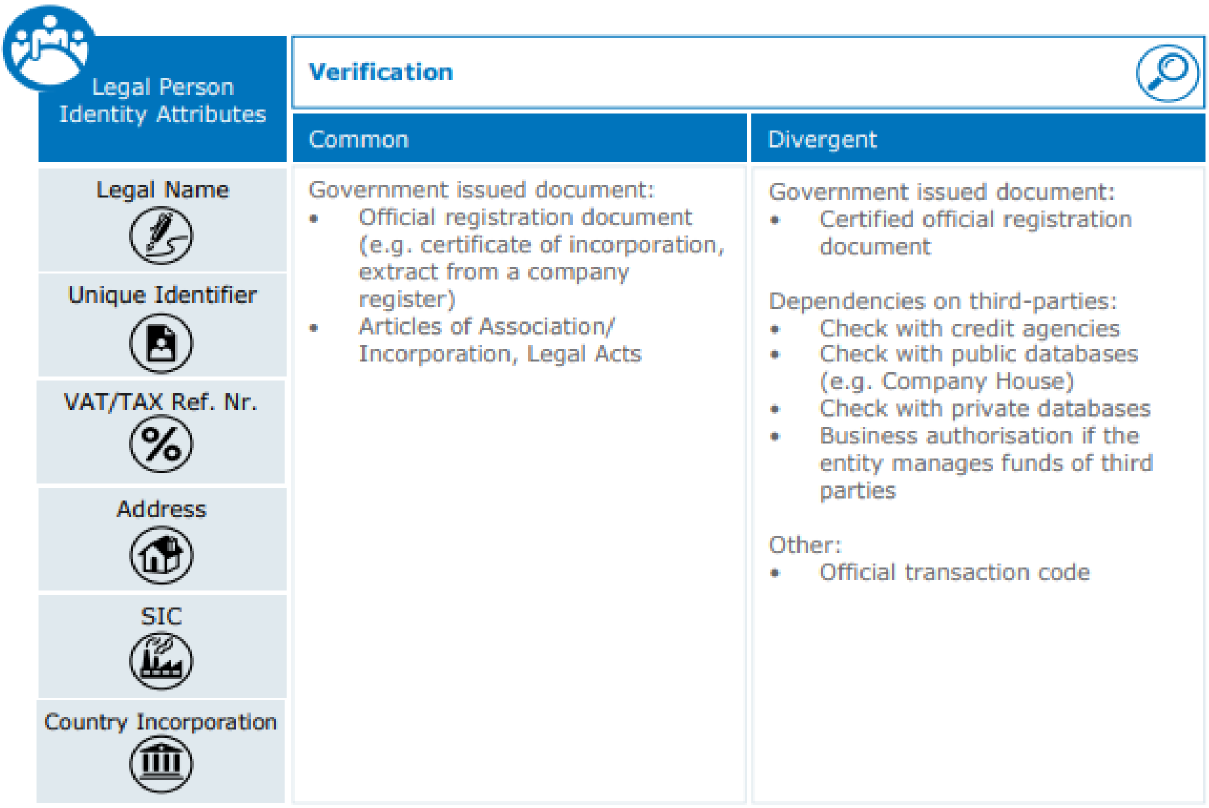
* Additionally used mechanisms to the ones listed for Name, Date of Birth, Place of Birth, Unique Identifier and Name at Birth.
β For instance, a surveyed financial institution in Estonia mentioned that gender information is included into the Unique Identifier of the Estonian NID cards.



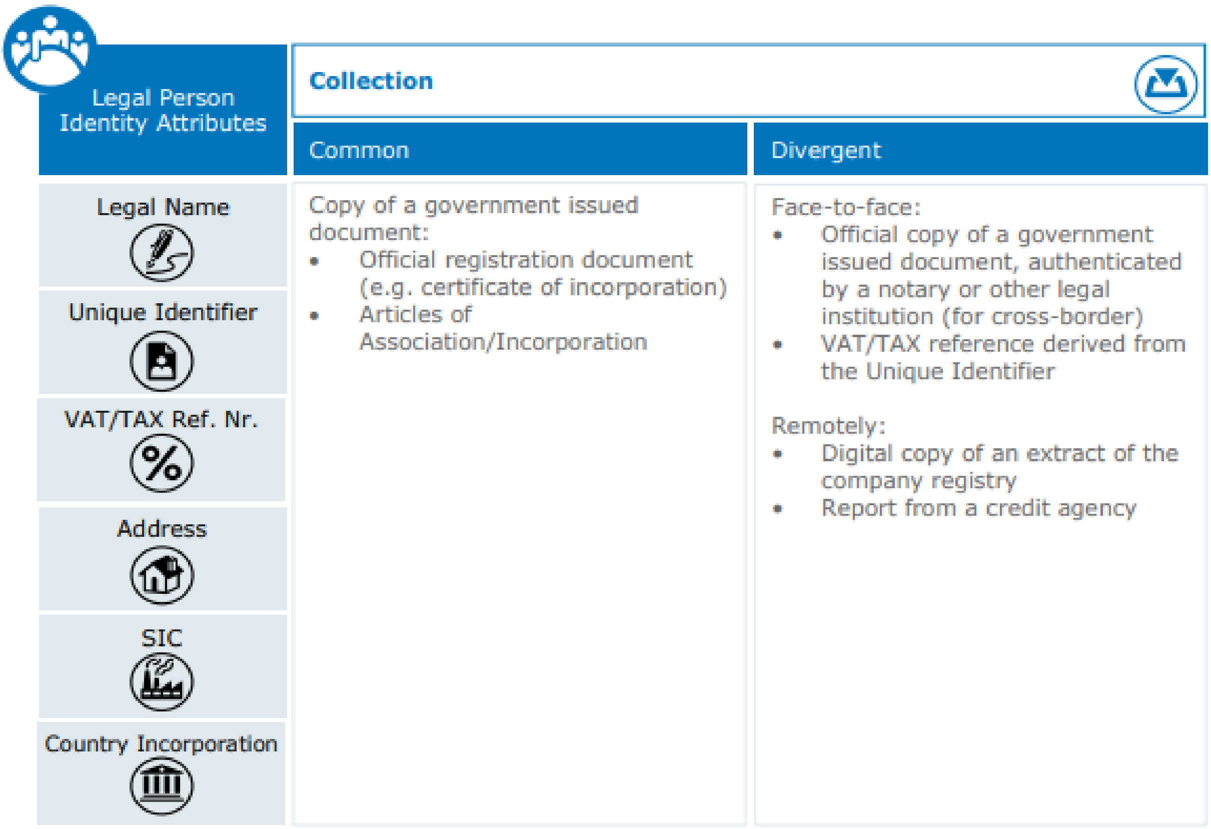
| Natural Person Identity Attributes | Collection | |
|---|---|---|
| | Common | Divergent |
| Name | Copy of a government issued document*<br>• National Identity Card (NID)<br>• Passport, travel document<br>• Resident Card (for non-citizens)<br>• Birth certificate (for minors) | Face-to-face:<br>• Official copy of a government issued document, created by a notary or other legal institution<br>• eID bank reader (at FIs office)<br>Remotely:<br>• Digital copy of a government issued document, via High quality video call or Digital photo<br>• eID user software, e.g. BankID, Belgian eID<br>• Report from a credit agency<br>• Digital copy of an extract from a tax database, population register of a government issued document<br>• Post office proof of identity verification, e.g. PostID |
| Nationality | | |
| Date of Birth | | |
| Place of Birth | | |
| Unique Identifier | | |
| Name at Birth | | |
| Gender | | |
| Address | | *Face-to-face¥:<br>• Original or copy of a utility invoice<br>Remotely¥:<br>• Digital copy of a utility invoice¥ |
| Occupation | *No common processes* | Face-to-face¥:<br>• Original or copy of a payslip<br>Remotely¥:<br>• Digital copy of a payslip or of an extract form the tax database |
| Email | Only performed remotely by online based financial institutions¥ | *No divergent collection process* |

* Additionally used mechanisms to the ones listed for Name, Date of Birth, Place of Birth, Unique Identifier and Name at Birth.
¥ Declarative collection process possible.
¤ For on-line based only financial institutions the collection is done at distance, otherwise the collection is Face-to-face.

## Legal person/entity



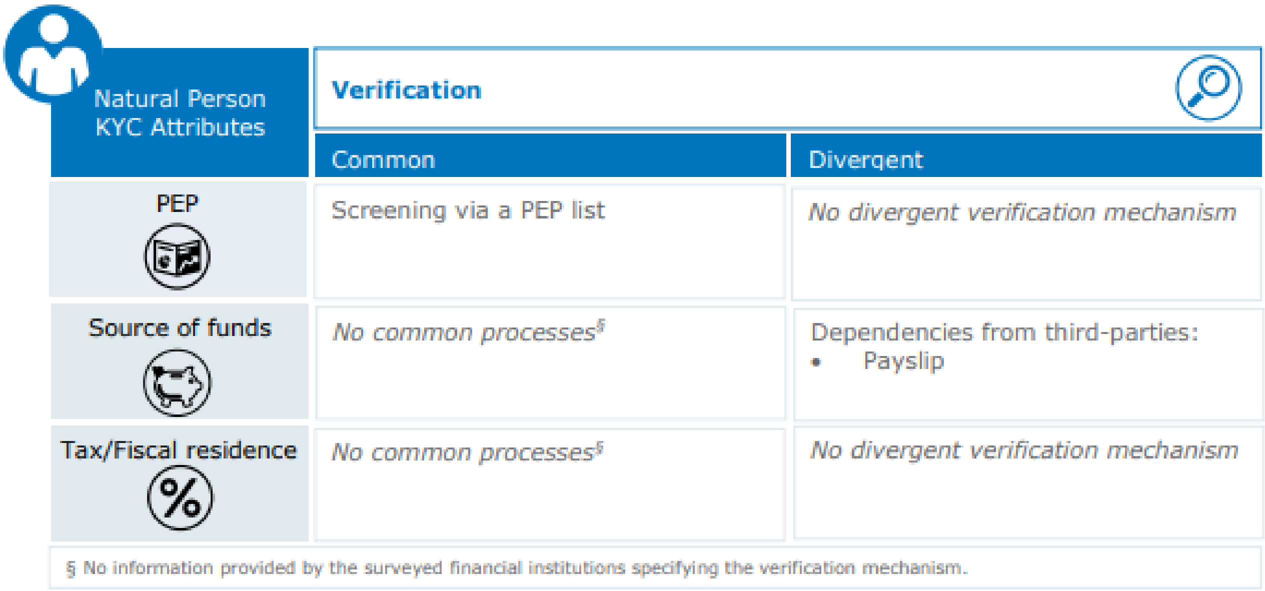
| Legal Person Identity Attributes | Verification | |
|---|---|---|
| | Common | Divergent |
| Legal Name<br>Unique Identifier<br>VAT/TAX Ref. Nr.<br>Address<br>SIC<br>Country Incorporation | Government issued document:<br>• Official registration document (e.g. certificate of incorporation, extract from a company register)<br>• Articles of Association/ Incorporation, Legal Acts | Government issued document:<br>• Certified official registration document<br><br>Dependencies on third-parties:<br>• Check with credit agencies<br>• Check with public databases (e.g. Company House)<br>• Check with private databases<br>• Business authorisation if the entity manages funds of third parties<br><br>Other:<br>• Official transaction code |



| Legal Person Identity Attributes | Collection | |
|---|---|---|
| | Common | Divergent |
| Legal Name<br>Unique Identifier<br>VAT/TAX Ref. Nr.<br>Address<br>SIC<br>Country Incorporation | Copy of a government issued document:<br>• Official registration document (e.g. certificate of incorporation)<br>• Articles of Association/Incorporation | Face-to-face:<br>• Official copy of a government issued document, authenticated by a notary or other legal institution (for cross-border)<br>• VAT/TAX reference derived from the Unique Identifier<br><br>Remotely:<br>• Digital copy of an extract of the company registry<br>• Report from a credit agency |

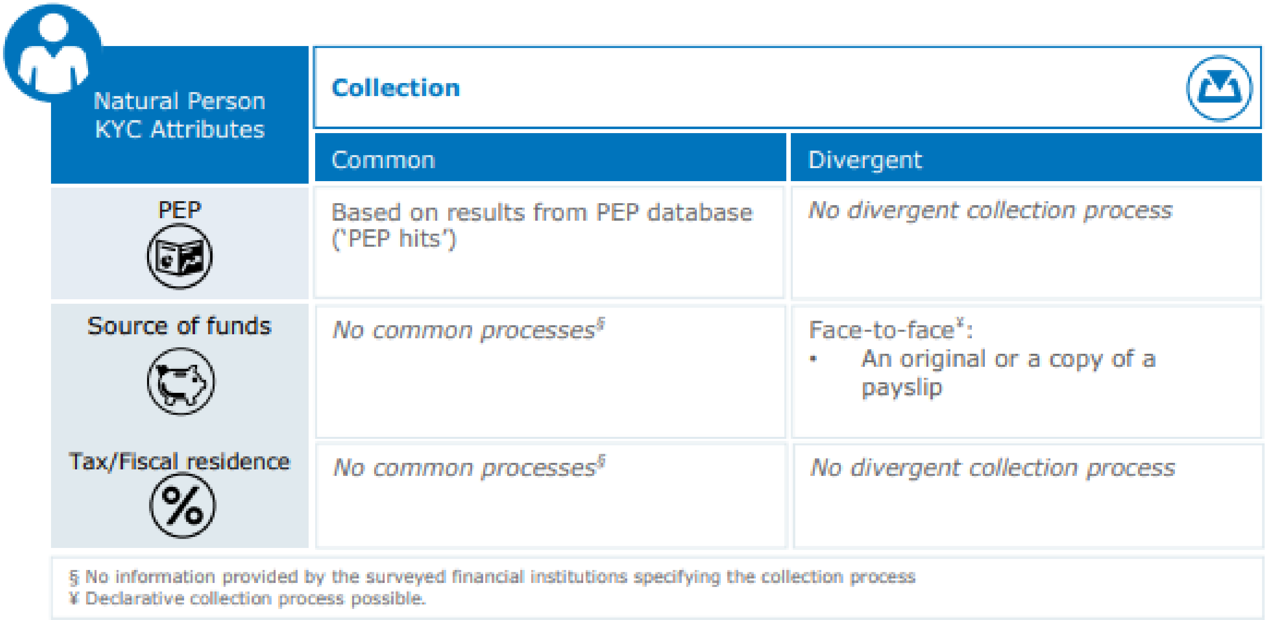
# APPENDIX 3 – KYC Attributes / Common and divergent verification mechanisms

## Natural person



| Natural Person KYC Attributes | Verification | |
|---|---|---|
| | Common | Divergent |
| PEP | Screening via a PEP list | *No divergent verification mechanism* |
| Source of funds | *No common processes*[§] | Dependencies from third-parties:<br>• Payslip |
| Tax/Fiscal residence | *No common processes*[§] | *No divergent verification mechanism* |

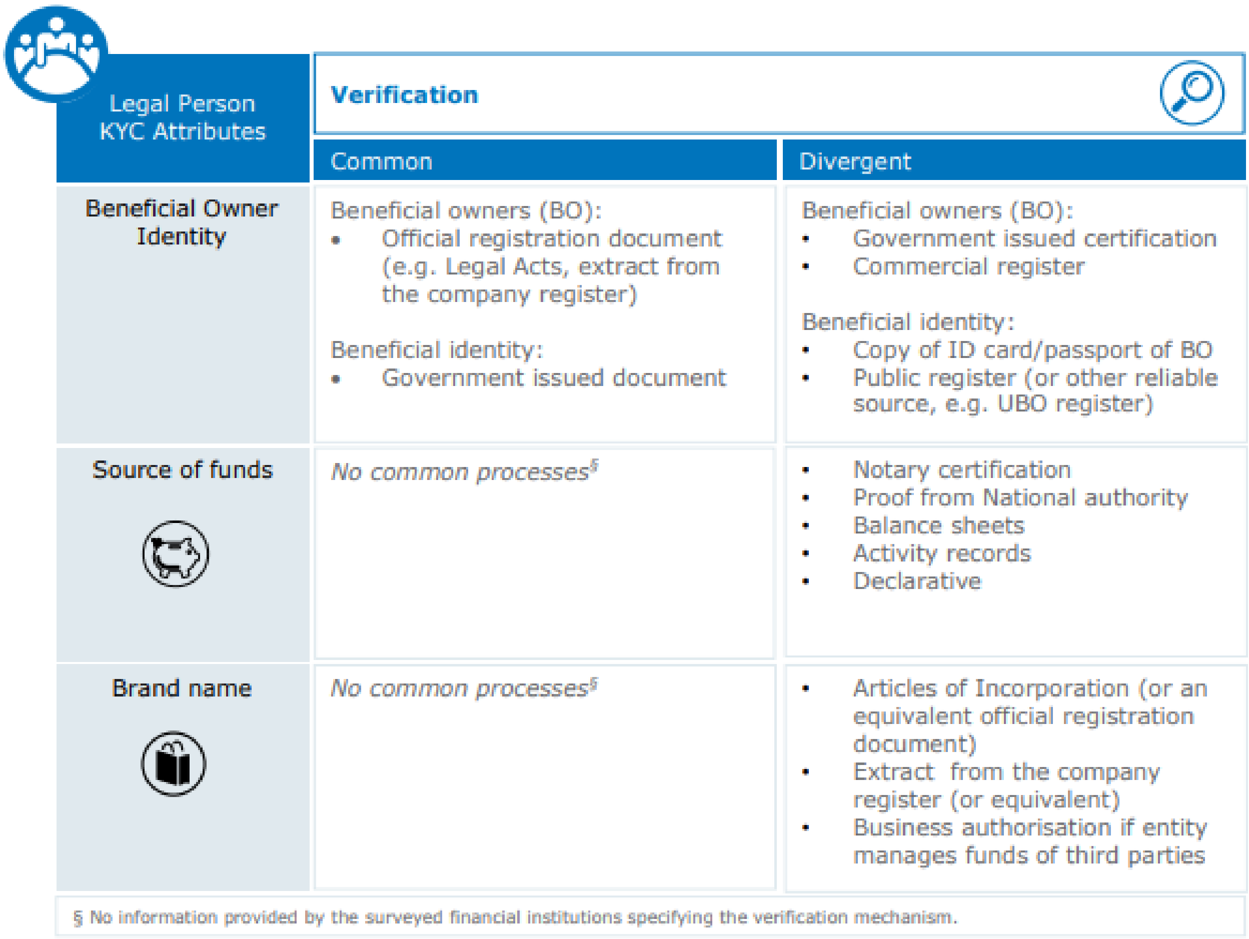
§ No information provided by the surveyed financial institutions specifying the verification mechanism.



| Natural Person KYC Attributes | Collection | |
|---|---|---|
| | Common | Divergent |
| PEP | Based on results from PEP database ('PEP hits') | *No divergent collection process* |
| Source of funds | *No common processes*[§] | Face-to-face[¥]:<br>• An original or a copy of a payslip |
| Tax/Fiscal residence | *No common processes*[§] | *No divergent collection process* |

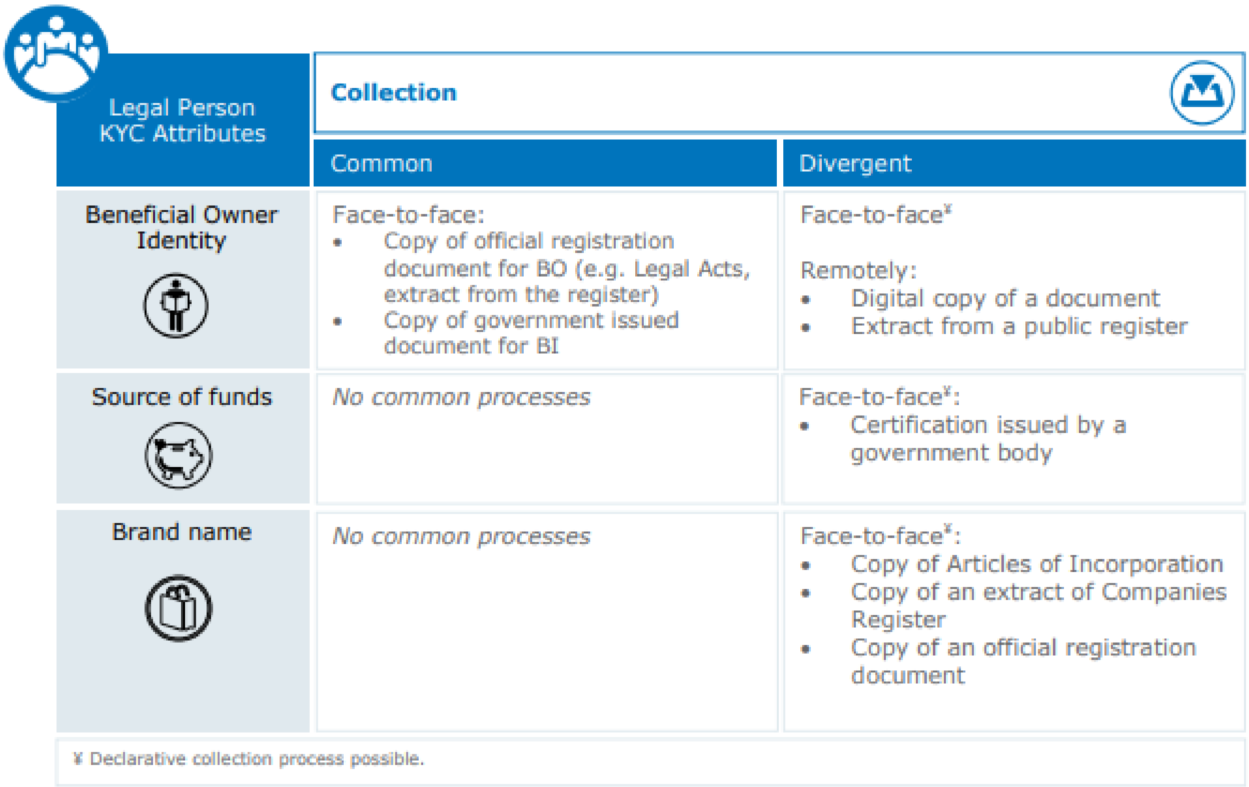
§ No information provided by the surveyed financial institutions specifying the collection process
¥ Declarative collection process possible.

## Legal person/entity



| Legal Person KYC Attributes | Verification | |
|---|---|---|
| | Common | Divergent |
| Beneficial Owner Identity | Beneficial owners (BO):<br>• Official registration document (e.g. Legal Acts, extract from the company register)<br>Beneficial identity:<br>• Government issued document | Beneficial owners (BO):<br>• Government issued certification<br>• Commercial register<br>Beneficial identity:<br>• Copy of ID card/passport of BO<br>• Public register (or other reliable source, e.g. UBO register) |
| Source of funds | *No common processes*[§] | • Notary certification<br>• Proof from National authority<br>• Balance sheets<br>• Activity records<br>• Declarative |
| Brand name | *No common processes*[§] | • Articles of Incorporation (or an equivalent official registration document)<br>• Extract from the company register (or equivalent)<br>• Business authorisation if entity manages funds of third parties |

§ No information provided by the surveyed financial institutions specifying the verification mechanism.



| Legal Person KYC Attributes | Collection | |
|---|---|---|
| | Common | Divergent |
| Beneficial Owner Identity | Face-to-face:<br>• Copy of official registration document for BO (e.g. Legal Acts, extract from the register)<br>• Copy of government issued document for BI | Face-to-face[¥]<br>Remotely:<br>• Digital copy of a document<br>• Extract from a public register |
| Source of funds | *No common processes* | Face-to-face[¥]:<br>• Certification issued by a government body |
| Brand name | *No common processes* | Face-to-face[¥]:<br>• Copy of Articles of Incorporation<br>• Copy of an extract of Companies Register<br>• Copy of an official registration document |

¥ Declarative collection process possible.

# APPENDIX 4 - Attributes used by Financial Institutions

## Natural Person

| Description | Data name | Data type |
|---|---|---|
| Family Name | | |
| First Name | | |
| Date of Birth | | |
| Unique Identifier | | |
| Current Address | | |
| Gender | | |
| Place of Birth | | |
| Country of Nationality | | |
| Family Name at Birth | | |
| First Name at Birth | | |
| Email | | |
| Country of Residence | | |
| Occupation | | |
| PEP | | |
| Source of Funds | | |
| Tax/Fiscal residence | | |

### A. Legal Person/Entity Attributes

| **Description** | Data name | Data type |
|---|---|---|
| Current Legal Name | | |
| Unique Identifier (Directive 2012/17/EU) | | |
| Current Address | | |
| VAT Registration Number | | |
| TAX Reference Number | | |
| Legal Entity Identifier (LEI) | | |
| EORI<br>Economic Operators Registration Identification | | |
| SEED<br>System of Exchange of Excise Data | | |

| | | |
|---|---|---|
| Country of Incorporation | | |
| Brand name | | |
| Email | | |
| Identification of Beneficial Owner | | |
| Source of funds | | |
| SIC | | |

**NOTES**:

1. All Cypriot companies or sole traders involved in cross border economic activities are required to register and apply for an **EORI number** with the Customs and Excise Department. Local companies must file a C1000 form with the Department.
2. **SEED** is the System for Exchange of Excise Data online verification. It provides a service to verify an Excise Number with a standard web browser. The SEED application is addressed to Economic Operators. It is necessary that all actors involved in the intra-Community movement of excise goods under suspension to be registered in the common EU registry **SEED (System of Exchange of Excise Data)**. Each entity should register in the Member State in which their main offices are situated. Based on this registry, an exchange of information is conducted verifying the legitimate nature of the movement and thus providing a useful tool in the fight against fraud and smuggling.
3. **SIC (Social Insurance Contributions).** In Cyprus each salaried person or self-employed person must have a Personal Tax Identification Code (T.I.C) and a Personal Social Insurance Number (S.I.C). Consequently, the registration of personnel is made though the Social Insurance Office and the Income Tax Office, unfortunately, on a paper application.

# APPENDIX 5 - Extracts from the Directive (EU) 2015/849 (‘4AMLD’) and amendments (5AMLD) in relation to eIDAS

## Customer Due Diligence

### Article 13.

1. Customer due diligence measures shall comprise:

(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;

> [5AMLD amendment: in Article 13(1), point (a) is replaced by the following: (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 and relevant trust services as set out in Regulation (EU) No 910/2014 or national law]

(b) identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer;

(c) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.

When performing the measures referred to in points (a) and (b) of the first subparagraph, obliged entities shall also verify that any person purporting to act on behalf of the customer is so authorised and identify and verify the identity of that person.

**2. Member States shall ensure that obliged entities apply each of the customer due diligence requirements laid down in paragraph 1. However, obliged entities may determine the extent of such measures on a risk-sensitive basis.**

### Article 14.

1. Member States shall require that verification of the identity of the customer and the beneficial owner take place before the establishment of a business relationship or the carrying out of the transaction.

## Performance by third parties

### Article 27.

1. Member States shall ensure that obliged entities obtain from the third party relied upon the necessary information concerning the customer due diligence requirements laid down in points (a), (b) and (c) of the first subparagraph of Article 13(1).

2. Member States shall ensure that obliged entities to which the customer is referred take adequate steps to ensure that the third party provides, immediately, upon request, relevant copies of identification and verification data and other relevant documentation on the identity of the customer or the beneficial owner.

> [5AMLD amendment: in Article 27, paragraph 2 is replaced by the following:

2. Member States shall ensure that obliged entities to which the customer is referred take adequate steps to ensure that the third party provides immediately, upon request, relevant copies of identification and verification data, including, where available, data obtained through electronic identification means and relevant trust services as set out in Regulation (EU) No 910/2014 or national law, and other

relevant documentation on the identity of the customer or the beneficial owner.]

***Beneficial ownership information***

## Article 30.

1. Member States shall ensure that corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership, including the details of the beneficial interests held. Member States shall ensure that those entities are required to provide, in addition to information about their legal owner, information on the beneficial owner to obliged entities when the obliged entities are taking customer due diligence measures in accordance with Chapter II. [..]

3. Member States shall ensure that the information referred to in paragraph 1 is held in a central register in each Member State, for example a commercial register, companies register as referred to in Article 3 of Directive 2009/101/EC of the European Parliament and of the Council (1), or a public register. Member States shall notify to the Commission the characteristics of those national mechanisms. The information on beneficial ownership contained in that database may be collected in

accordance with national systems. [..]

5. Member States shall ensure that the information on the beneficial ownership is accessible in all cases to:

(a) competent authorities and FIUs, without any restriction;

(b) obliged entities, within the framework of customer due diligence in accordance with Chapter II;

(c) any person or organisation that can demonstrate a legitimate interest.

The persons or organisations referred to in point (c) shall access at least the name, the month and year of birth, the nationality and the country of residence of the beneficial owner as well as the nature and extent of the beneficial interest held.

For the purposes of this paragraph, access to the information on beneficial ownership shall be in accordance with data protection rules and may be subject to online registration and to the payment of a fee. The fees charged for obtaining the information shall not exceed the administrative costs thereof.

## Record-keeping

## Article 40.

1. Member States shall require obliged entities to retain the following documents and information in accordance with national law for the purpose of preventing, detecting and investigating, by the FIU or by other competent authorities, possible money laundering or terrorist financing:

(a) in the case of customer due diligence, a copy of the documents and information which are necessary to comply with the customer due diligence requirements laid down in Chapter II, for a period of five years after the end of the business relationship with their customer or after the date of an occasional transaction;

(b) the supporting evidence and records of transactions, consisting of the original documents or copies admissible in judicial proceedings under the applicable national law, which are necessary to identify transactions, for a period of five years after the end of a business relationship with their customer or after the date of an occasional transaction.

Upon expiry of the retention periods referred to in the first subparagraph, Member States shall ensure that obliged entities delete personal data, unless otherwise provided for by national law, which shall determine under which circumstances obliged entities may or shall further retain data. Member States may allow or require further retention after they have carried out a thorough assessment of the necessity and proportionality of such further retention and consider it to be justified as necessary for the prevention, detection or investigation of money laundering or terrorist financing. That further retention period shall not exceed five additional years.

> [5AMLD amendment: in Article 40, paragraph 1 (a) points (a) and (b) are replaced by the following: [(a) in the case of customer due diligence, a copy of the documents and information which are necessary to comply with the customer due diligence requirements laid down in Chapter II, including, where available, information obtained through electronic identification means and relevant trust services as set out in Regulation (EU) No 910/2014 or national law, for a period of five years after the end of the business relationship with their customer or after the date of an occasional transaction.]

## Enhanced Due Diligence and high risk factors

## Annex III.

The following is a non-exhaustive list of factors and types of evidence of potentially higher risk referred to in Article 18(3):

(2) Product, service, transaction or delivery channel risk factors:

(a) private banking;

(b) products or transactions that might favour anonymity;

(c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;

> [5AMLD amendment: in point (2) of Annex III where a non-exhaustive list of factors and types of evidence of potentially higher risk referred to in Article 18(3) is stated, point (c) is replaced by the following:
>
> (c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic identification means or relevant trust services as defined in Regulation (EU) 910/2014.]

(d) payment received from unknown or unassociated third parties;

(e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;

[..]