Impulse

Identity Management in PUbLic SErvices

D3.2 Ethical and Legal Dictionary

Lead Author: Piercosma Bisconti Lucidi, Antonio Carnevale, Valerio Prosseda (CEL)

With contributions from: All

Reviewer: Domenico Racanelli (InfoCamere), Knut Blind (Fraunhofer ISI), Nicholas Martin (Fraunhofer ISI)

Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Delivery date:	30-11-2021
Version:	FINAL
Total number of pages:	41
Keywords:	Ethical and Legal Dictionary of the ID management technologies

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101004459

Executive summary

Disruptive technologies are too novel and, accordingly, their adoption in providing public services could encounter misunderstanding use and pay a non-proper terminology.

In this context, the aim of this deliverable is to construct a dictionary that collects all the usable ethical and legal terms to facilitate the understanding among researchers and a closer collaboration between the different interested stakeholders.

The dictionary represents a novelty of the scholarship within this topic, defining a minimal and preliminary language of ethical and legal terms, to find common understandings – inside and outside IMPULSE – in approaching the impacts of such technologies.

Document information

Grant agreement No.	**101004459**	**Acronym**	**IMPULSE**
Full title	**Identity Management in PUbLic SErvices**		
Call	DT-TRANSFORMATIONS-02-2020		
Project URL	https://www.impulse-h2020.eu/		
EU project officer	Giorgio CONSTANTINO		

Deliverable	**Number**	D3.2	**Title**	Ethical and Legal Dictionary
Work package	**Number**	WP3	**Title**	Multidisciplinary analysis of standards, legal and ethical implications
Task	**Number**	T3.2	**Title**	Definition of a shared and multidisciplinary dictionary of the identity management technologies

Date of delivery	**Contractual**	M04	**Actual**	M10
Status	version v07		☒Final version	
Nature	☒Report ☐Demonstrator ☐Other ☐ORDP (Open Research Data Pilot)			
Dissemination level	☒Public ☐Confidential			

Authors (partners)	CyberEthics Lab.			
Responsible author	**Name**	Piercosma Bisconti Lucidi, Valerio Prosseda		
	Partner	CyberEthics Lab.	**E-mail**	p.bisconti@cyberethicslab.com v.prosseda@cyberethicslab.com

Summary (for dissemination)	A dictionary collecting all the usable ethical and legal terms to facilitate the understanding among researchers and a closer collaboration between the different interested stakeholders.
Keywords	Ethical and Legal Dictionary of the ID management technologies

Version Log

Issue Date	Rev. No.	Author	Change
20/05/2021	v001	Antonio Carnevale, Piercosma Bisconti Lucidi (CEL)	Conceptual framework of the dictionary and TOC
15/06/2021	v01	Antonio Carnevale, Piercosma Bisconti Lucidi (CEL)	First list of terms
17/07/2021	v02	Piercosma Bisconti Lucidi (CEL)	Sharing the list of terms with Consortium
30/08/2021	v025	all	Consortium first round of contributions on new terms and meanings
29/09/2021	v03	Piercosma Bisconti Lucidi (CEL)	First refinement of the uniformity of all terms

26/10/2021		All	Consortium second round of contributions on new terms and meanings
29/10/2021	v04	Piercosma Bisconti Lucidi (CEL)	Second refinement of the uniformity of all terms
22/11/2021	v05	Domenico Racanelli (InfoCamere) Knut Blind (Fh ISI), Nicholas Martin (Fh ISI) Alicia Jiménez (GRAD)	Internal review
26/11/2021	v06	Antonio Carnevale, Piercosma Bisconti Lucidi (CEL)	Final version
10/10/2023	v07	Valerio Prosseda (CEL)	Reopening of the final version and completion of the living document

Table of contents

Abbreviations and acronyms

ICT: Information and Communication Technologies
IdM: Identity Management
B-Based IdM: Blockchain-based Identity Management
IdP: Identity Provider
RP: Relying Parties
SSO: Single Sign On
URI: Uniform Resource Identifier
FIdM: Federated Identity Management
B-Based IdM Systems: Blockchain Based Identity Management Systems
DL: Distributed Ledgers
BC: Blockchain
SSI: Self-Sovereign Identity
SSIdMS: Self-Sovereign Identity Management Systems
PoW: Proof of Work

1 Introduction

While the world population exceeds 7 billion, an increasingly larger part gains internet access, now widely recognized as a human fundamental right. Meanwhile, a large part of human activities is now carried out on the web: from social media to online purchasing to public administrations, many rely on the internet for providing services and information. A large part of these activities involves the identification of the user by the provider, in order to provide the service. The importance of reliability of identity on the web varies depending on the type of service the user is seeking. It is of small importance in the blogs login, increasingly important in social media login, fundamental for online banking and public administration services.

1.1 At the Intersection of Words, Technology and Socio-Cultural Systems

Disruptive technologies in identity management are novel and, accordingly, their adoption in providing public services could encounter misunderstanding due to a non-proper terminology. Identity management systems do not entail only a change in the procedure to verify identity on a technical level, but imply a change in the socio-technical systems, modifying the socio-political practices of democratic and participatory processes. The non-neutrality of technology towards the socio-political sphere has been a matter of discussion since disruptive technologies impacted our lives (Ropohl 1999). Identities and their management have always been a crucial element throughout history at the crossroad of technological development on their verifiability, and the democratic quality of nations (Leininger 2015). Of great importance is the way in which these technological changes are communicated and explained to the mass society (Castells 2013): while technology usually boosts participatory dynamics, it can also be a barrier for certain segments of the population, such as elders and other under-represented groups of people (Benjamin 2019).

User-experience issues were analysed in deliverable 3.1, and they might constitute an important barrier in the massive spread of identity management systems. In addition to this, the way technology is communicated is another fundamental issue to analyse in order to deliver effectively and transparently to the communication of both the public the benefits and the shortcomings of technological development.

In this context, the aim of this deliverable is to construct a dictionary of the Identity Management Technologies that defines the terms intertwining technological, ethical and legal definitions; this interdisciplinary understanding of the terminology is a way to facilitate the closest collaboration between the different stakeholders involved in the project and its demonstrations and pilots. Moreover, it aims to constitute a multidisciplinary ground to enhance the communication between researchers, institutions and the civil society, in order to enhance a common understanding of what identity management systems actually are.

1.2 Building a Multidisciplinary Dictionary

A common understanding of the terms defining a technology is a fundamental starting point for a transparent and fruitful discussion between experts, civil society and other relevant stakeholders. While the technological advances become more and more sophisticated, the segmentation of competences often prevents a complete understanding of the functioning and the societal impact of innovations. Multidisciplinary, in this context, is a key principle to manage this complexity. The aim of this dictionary is, therefore, to provide a common ground for practitioners, researchers and civil society in order to manage a multidisciplinary understanding of Identity Management systems based on blockchain.

Given the complexity of meanings to which the terms refer, we have decided to adopt a participatory methodology sharing all the research passages with experts and scholars of the Consortium:

- **Phase 1** (May 2021): The deliverable leaders (CEL) have extrapolated a first list of essential terms from (a) the scientific literature, (b) the deliverables already produced by the Consortium, in particular D3.1
- **Phase 2** (August 2021): This first list of high-level concepts was shared a first time with all partners who were asked to help provide explanation of terms according to three large semantic areas: (1) technological, (2) legal, (3) ethics and governance
- **Phase 3** (September 2021): This first filling of the semantic spaces has been processed by CEL and systematized
- **Phase 4** (October 2021): The systematized list of terms was re-shared with the partners who contributed to a greater refinement of the vocabulary
- **Phase 5** (November 2021): CEL has finalized the deliverable in the form of the vocabulary

1.3 The Structure of the Dictionary

As a result, the dictionary will be ordered as follows: the terms will appear in alphabetical order. Under every lemma there will be hyperlinks to related terms (e.g. the terms “Proof of Work”, “Proof of Stake”, “Proof of Authority”, “Byzantine Fault Tolerance” will link to their macro-category “Consensus Algorithm”). Every sub-concept (e.g. Authentication Protocol) will link only to its direct macro-concept (e.g. Authentication).

2 The Dictionary

Acceptance

The positive reception of a technology or a socio-technical system by members of society or test subjects. Acceptance can be double-sided, expressing a mere passive affirmative stance or a more positive and active dimension that involves support and interest from society. Additionally, acceptance is entailed in the psychological and social dimension of society and the interaction with newer and disruptive technologies. Rather than expressing a single process, acceptance must be intended as a multi-faced and dynamic process.

Access

The capacity of the user to access his/her own data and to easily retrieve all the claims and other data within his identity. There must be no hidden data and no gatekeepers. This implies that a user cannot modify all the claims associated with his identity and that every user can only access his/her own data.

Access control

A procedure used to determine if an entity should be granted access to resources, facilities, services, or information based on pre-established rules and specific rights or authority associated with the requesting party. The goal of access control is to minimize the risk of unauthorized access to physical and logical systems occurring, which would constitute a security breach.

Related term: Authentication

Accessibility

The extent to which products, systems, services, environments and facilities can be used by people from a population with the widest range of user (3.1) needs, characteristics and capabilities to achieve identified goals in identified *context*s of use (3.10). Context of use includes direct use or use supported by assistive technologies.

Accuracy

It is a quantitative measure of the magnitude of error, preferably expressed as a function of the relative error, a high value of this measure corresponding to a small error. Under the GDPR states that personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (article 5, paragraph, 1 letter d) GDPR).

Related term: Machine learning

Agreement

A reasonable opportunity to accept or deny participation. The agreement should be continuous, meaning that the participant should be allowed to leave the engagement at any point.

Amplification attack

A class of attack where the attacker attempts to exhaust a target system's CPU, storage, network, or other resources by providing small, valid inputs into the system that result in damaging effects that can be exponentially more costly to process than the inputs themselves.

Related Term: Cyberattack

Anonymization

A situation where an entity cannot be identified within a set of entities. Anonymity prevents the tracing of entities or their behaviour such as user location, frequency of a service usage, and so on. Anonymous information is information which does not relate to an identified or identifiable natural person, or personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. According to recital 26 GDPR, the principles of data protection should therefore not apply to anonymous information. Anonymisation techniques are an active research field, and various techniques exist. There is no agreed standard in EU legislation defining which technique is to be preferred, or what (if any) level of re-identification risk is allowed for the data still to be considered anonymised

Related term: Privacy

Application Programming Interface (API)

A connection between computers or between computer programs. It is a type of software interface, offering a service to other pieces of software. A program or a programmer that uses one of these parts is said to call that portion of the API. The calls that make up the API are also known as subroutines, methods, requests, or endpoints. An API specification defines these calls, meaning that it explains how to use or implement them.

Attribute

A set of data that describes the characteristics of a subject. The data includes the fundamental information for identifying a subject (e.g., full name, domicile, and date of birth), his/her preferences, and the information generated as a result of his/her activities. Some examples are given/family names, domiciles, ages, genders, roles, titles, affiliations, activity records, and reputations.

Related term: Identity

Authentication

Authentication is a process by which an entity can prove it has a specific attribute or controls a specific secret using one or more verification methods.
Authentication means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed.
Authentication can be single-factor or multi-factor. In the case of Identity Management Systems, authentication often proceeds by biometric factors.

Authentication factor

Piece of information and/or process used to authenticate or verify the identity of an entity
Authentication factors are divided into four categories:
— something an entity has (e.g., device signature, passport, hardware device containing a credential, private key);
— something an entity knows (e.g., password, PIN);
— something an entity is (e.g., biometric characteristic); or
— something an entity typically does (e.g., behaviour pattern).
[SOURCE: ISO/IEC 19790]

Related Term: Authentication

Authentication protocol

Defined sequence of information exchanges between an entity and a verifier that enables the verifier to perform authentication of an entity

Related term: Authentication

Authority

A trusted entity that is able to verify and authenticate identities. Classically, this was a centralized (or later, federated) entity. Now, this can also be an open and transparent algorithm run in a decentralized manner.

Autonomy

Autonomy is defined as a person's capacity to adhere to his/her proper reasons and ideas as not manipulated by other sources or constrictions. Agents have autonomy if their actions are in control of their own will, posing the condition of moral agency. The concept has a fundamental role in debates and applications over education policy, biomedical ethics, legal freedoms and rights such as the right to privacy, also converging in moral and political theory. The user must be central to the administration of identity.

Biometric data

Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Biometric recognition

Automated recognition of individuals based on observation of behavioural and biological characteristics. Examples of biometric traits include fingerprint, face, iris, palmprint, retina, hand geometry, voice, signature and gait. Represented in the b-ISO/IEC CD 2382-37

Related Term: Authentication factor

Black box

A system which can be described in terms of its inputs and outputs, although leaving unclear any knowledge of its internal workings. Its implementation is defined as "opaque" and thus “black”. Black box models are incomplete in virtue of leaving out details about underling mechanisms and that those models ultimately depend for their explanatory force on the promise that the functional models do, in fact, correspond to how the mechanism works. “Black box societies” are jurisdictions where the analysis and use of data is opaque, unverifiable, and unchallengeable.

Byzantine Fault Tolerance

The ability of a system to prevent or compensate for the negative effects of malicious behaviour of parties collaborating in a process. For a Blockchain system this means being able to preserve integrity of the system (and data) and prevent attacks based on some faulty nodes that have been hacked, or act intentionally to disrupt the network.

Related term: Consensus Algorithm

Blockchain

A Distributed Ledger Technology in which all network nodes keep a copy of the entire database. Transactions are sorted and divided into blocks, each one referencing the previous by hash, thus forming an ordered "chain of blocks". How blocks are created and accepted as part of the chain is stated by the Consensus Algorithm.

Related Term: Distributed Ledgers, Consensus Algorithm

Centralized Identity Management

A process where the data are stored and processed in a centralized way. From a governance perspective, this form of organization is overcome in functionality by distributed and federated

systems. Centralization in fact does not promote interoperability between dataset and causes replication of data. In IdM, systems are more and more replaced by federated or by SSO login.

Related Term: Identity

Certificate

A set of security-relevant data issued by a security authority or a trusted third party, that, together with security information, is used to provide the integrity and data origin authentication services for the data [ITU-T X.810].

Challenge-Response Protocol

An authentication protocol where the verifier sends the claimant a challenge (usually a random value or nonce) that the claimant combines with a secret (such as by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the verifier. The verifier can independently verify the response generated by the claimant (such as by re-computing the hash of the challenge and the shared secret and comparing to the response, or performing a public key operation on the response) and establish that the claimant possesses and controls the secret.

Related Term: Authentication Protocol

Classification model

A machine learning model whose expected output for a given input is one or more classes.

Related Term: Machine learning

Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)

An interactive feature added to web forms to distinguish whether a human or automated agent is using the form. Typically, it requires entering text corresponding to a distorted image or a sound stream.

Computational Resources

Computing resources include data storage, processing power, memory, networking.
Computational resources are one of the most important issues in DL based on proof-of-work (PoW). The vast amount of energy required by the PoW to validate transactions has been highlighted as an environmental issue both for the energy consumption and for the need of a high number of GPUs.

Related Term: Costs

Computer vision

It is the capability of a functional unit to acquire, process, and interpret visual data.

Confusion matrix

It is a matrix used to record the number of correct and incorrect classifications of tentative examples by a set of rules.

Related Term: Machine learning

Consensus Algorithm

Mechanism used by collaborating parties in a distributed system to reach agreement on the validity of the data. It is the process by which in blockchain transaction are validated. It is used in Blockchain systems to decide how a new block is created (ex. election/cooperative/competitive) and how a receiving node can decide whether its data or sequence is valid or not. It influences the way the system converges toward a "common shared version" of the data.
There are multiple ways to set up the consensus mechanism but, at the core of it, there is always the concept that most of the collaborating parties will accept the new transaction. The fact that consensus is based on algorithmic calculus and not on a trusted party is the reason why blockchain is said to be trustless.

Related term: Trust

Consent

Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. For consent to be informed and specific, the data subject must at least be notified about the controller's identity, what kind of data will be processed, how it will be used and the purpose of the processing operations as a safeguard against 'function creep'. The sharing of data must only occur with the consent of the user, it must still be deliberate and well-understood, and the withdrawal must be as easy as giving consent. The term incorporates voluntariness, comprehension, and agreement.

Control

Users must be in control of their identities. The user must be able to choose what to share or not, thus maintaining a certain degree of privacy for personal data. Indeed, this does not mean that users have full control of claims about their identity, even though they have the ultimate authority over it. This item expresses how much the user feels in control of the technology and how the sense of self-efficacy of the users affects technology acceptance.

Controller

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Costs related to a blockchain

It is the sum of all the resources needed to run a blockchain. It can be calculated as the sum of storage cost and execution costs multiplied by the nodes of the blockchain. It might or might not include the costs required to mitigate environmental impact.

Credential

A set of one or more claims made by an issuer. A verifiable credential is a tamper-evident credential that has authorship that can be cryptographically verified. Verifiable credentials can be used to build verifiable presentations, which can also be cryptographically verified. The claims in a credential can be about different subjects.

Credential Service Provider (CSP)

A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A CSP may be an independent third party or issue credentials for its own use.

Related Term: Credential

Cryptographic suite

A specification defining the usage of specific cryptographic primitives in order to achieve a particular security goal. These documents are often used to specify verification methods, digital signature types, their identifiers, and other related properties.

Cyber attack

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. [ISO 27100]

Data governace

Organizations and their personnel defining, applying and monitoring the patterns of rules and authorities for directing the proper functioning of, and ensuring the accountability for, the entire life-cycle of data and algorithms within and across organizations.

Data minimisation

The act of limiting the amount of shared data strictly to the minimum necessary to successfully accomplish a task or goal. GDPR requires that personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". This degree of privacy can be achieved with selective disclosure, range proofs and other zero-knowledge techniques, i.e. if only age is requested, then a precise date of birth has not to be disclosed.

Related term: Privacy

Data processing

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data protection by design

Is intended as the practices and measures implemented in the technology to assure data protection principles and safeguards toward the privacy and rights of the data subjects required by the law. Moreover, the controller and the processor must consider all the risks connected with data processing that could harm the rights and freedoms of the data subject. The controller and the processor must assess those risks before the data processing starts, and shape data processing to minimise potential implications and interferences with rights and freedoms.

Data protection by default

Implementation of appropriate measures by the controller in order to ensure the processing will be applied only to necessary data. Personal data collected, the extent of the processing, storage period and accessibility are subjected to those measures.

Data subject

An identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data subjectivation

A process in which the rights and powers of an individual's digital life are defined in virtue of being the owner of digital data, thus enabling the subject through the concept of data. Data subjectivation, then, is not so much the idea that subjectivity is increasingly digitally mediated, but that the subject is formed, defined, identified, and enabled in the possession and exercise of certain rights by digital forms based on both a conceptual and material structure specific to digital reality, namely the data.

Data tampering

Data tampering refers to the act of destroying, manipulating or editing data through unauthorized channels. Data tampering can be prevented by adopting data integrity measures, access control rules or strong authorization mechanisms.

Related Term: CyberAttack

Data transfer

Any activity that entails giving access, sharing, transferring or otherwise making available personal data collected/processed by a controller or a processer to another controller or processor.

Deontological ethics

The approach in which a certain ethical statement (either a prescription or a prohibition) has its *normative strength* in itself**.** No matter how certain beneficial consequences could stem from the violation of a prescription, in the deontological models of ethics we are compelled to follow norms just for their intrinsic value.

Digital divide

The term can be defined as a division or a social split between subjects that have or do not have access to or possibilities to use digital technologies (i.e. devices, connections, applications). The term comprises in itself the concepts of information inequality, knowledge gap and participation in the information society. Divide has not to be intended as a clear distinction between two separated categories but as a more complex and pervasive phenomenon of society that reflects economic, social, and cultural inequalities and a lack of innovation and development. Moreover, the digital divide inequality of capabilities or skills can be linked to the concept of "digital literacy" and the degree of literacy.

Design ethics

The systematic study of ethical concepts or principles in design. This approach underlines the ethical issues or conflicts that can occur during the design phase of a particular object, examining choices of designers and how those choices can modify, change or alter the moral and ethics values of a subject or more widely society.

Design thinking

Refers to the approach for designing products, innovations and services that entails philosophical and cognitive thinking. Creativity, as the production of new ideas, and innovation, as their successful implementation, are the principal attributes of the process as well as interdisciplinarity, user-centeredness, problem solving and experimentation.

Digital ID document verification

The process of verifying that all components of a digitalized image of an ID document (may be passport, national ID card, driving license, etc.) have not been tampered with in order to prevent fraud or identity theft.

Digital identity

From an individual-based definition, digital identity is the projection of some real attributes of an individual that are transferred over the web (Self-sovereign identity). This is aided also by a means of identification that is founded upon some natural properties of the individual. From a relational-based definition, the identity is shaped by social structure, and the uniqueness of this notion of identity is attributed to the fact that there is a relation towards another part, where the identity is given only because of this relation (Centralized identity; Federated identity model). What is more, individuals can have multiple identity of this sort, seeing an explosion of online different personas that someone can relate to.

Digital image

A digital image is an image composed of picture elements, also known as pixels, each with finite, discrete quantities of numeric representation for its intensity or grey level that is an output from its two-dimensional functions fed as input by its spatial coordinates denoted with x, y on the x-axis and y-axis, respectively.

Digital onboarding

It is an online process to register new users on an online platform belonging to a company or government service in order to access its products and services. During this process, users usually need to provide their ID, and if required, biometric information like a face scan or fingerprint.

Digital signature

A mathematical scheme for demonstrating the authenticity of a digital message or document. An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation, but not confidentiality protection.
Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

Related Term: Authentication

Dignity

From a philosophical standpoint dignity is considered a universal attribute of the self, responsible for self-legislation and control of own will, having a foundational role in human rights. Respecting the

dignity of every human is not only morally acceptable, but a precondition for auto-determination and freedom. In personal data processing, specific rules and measures must be taken to respect and safeguard human dignity and fundamental rights.

Disclosure

Delivering factual information regarding the rewards and risks associated with the action under consideration. The individual's accurate understanding of what is being presented is referred to as comprehension.

Discrimination

A disproportionately disadvantageous impact on the members of certain salient social groups and, in moral and political philosophy, the term is often confined to the unfavourable treatment of groups of individuals, on prejudiced and irrelevant grounds. Discrimination is prohibited by six of the core international human rights documents.

Distributed ledger (DLT)

A non-centralized system for recording events. These systems establish sufficient confidence for participants to rely upon the data recorded by others to make operational decisions. They typically use distributed databases where different nodes use a consensus protocol to confirm the ordering of cryptographically signed transactions. The linking of digitally signed transactions over time makes the history of the ledger effectively immutable.
A technology that enables transaction without a trusted third party, as the banking system for economic transaction. The absence of the trusted third party is supposed to represent a more democratic, peer-to-peer and horizontal system of transaction validation. The problem of trust is shifted from the third party to the consensus mechanism itself.

Encryption

In cryptography, encryption is the process of encoding information. The encryption process transforms plaintext to ciphertext by means of an encryption key.

Related term: Cryptographic suite

Enrolment

The process of inauguration of an entity into a context. Enrolment may include verification of the entity's identity and establishment of a contextual identity. Also, enrolment is a pre-requisite to registration. In many cases, the latter is used to describe both processes

Related Term: Identity

Entity

A thing with a distinct and independent existence, such as a person, organization, or device that performs one or more roles in the ecosystem.
A person or organization possessing separate and distinct legal rights, such as an individual, partnership, or corporation.

Related Term: Identity

Equality

The possibility to have the same freedom as anyone other for structuring one own's life and be treated in the same manner as others and a prerequisite for inclusion. Equality can be viewed from more standpoints such as legal, political, social and economic. All citizens must have equal general rights and duties, access and participation in political decisions, and possibilities of emancipation and auto-determination independently of their economic or social class.

Ethics by design

It is defined as an approach to integrate ethical values and principles in the design phase of a certain product or technology. Ethics by design focus is intended also for the development phases of products, in particular for shaping activities and verifying if the values proposed are successfully implemented. Technological design is concerned as a non-neutral force that embeds in itself values and consequences that can have effects for its users. Integrating and embedding moral values helps the development process to shape an ethical product or technology since the beginning, preventing effects that can only be discovered after their release on the market.

Existence

Users must have an independent existence. Behind digital identity is always present the body entity, the ineffable "I" as the core of identity. Self-sovereign identity allows to access only some limited aspects of the "I" that already exists and making them public and accessible. Existence cannot be entirely conceived in digital form as there could be the risk of a prescriptive and therefore normative use of the identity and the self from a technological standpoint.

Feature

A measurable property of an object or event with respect to a set of characteristics.

Related Term: Machine learning

Federated Identity Management

Federated Identity Management (FIdM) is a concept that allows cooperation on identity processes, policies and technologies across organization boundaries. It is considered a promising approach to facilitate secure resource sharing among collaborating partners in heterogeneous IT environments,

and it has emerged with the recognition that individuals frequently move between organization boundaries

Related Term: Identity

Feedback loop mechanism

The cause-effect process established in a system where outputs are taken as new inputs thus starting new cycles. In the development of a product, the users, customers and other stakeholders can provide their feedback to change certain characteristics or practices, or also leave them as they are.

Freedom

The capacity to give and withdraw the consent to take part in collective activities, as well as the capacity to give and withdraw the consent to data controlling and processing. It can be defined also a condition of liberation from social and cultural forces that are perceived as impeding full self-realization such as pre-existing social and technical bias.

Graph

A network of information composed of subjects and their relationship to other subjects or data.

Holder

A role an entity might perform by possessing one or more verifiable credentials and generating presentations from them. A holder is usually, but not always, a subject of the verifiable credentials they are holding. Holders store their credentials in credential repositories.

Human-centric design

The approach to systems design and development that aims to make interactive systems more usable by focusing on the use of the system and applying human factors/ergonomics and usability knowledge and techniques. The term “human-centred design” is used rather than “user-centred design” in order to emphasize that this document also addresses impacts on a number of stakeholders, not just those typically considered as users. However, in practice, these terms are often used synonymously. Usable systems can provide a number of benefits, including improved productivity, enhanced user well-being, avoidance of stress, increased accessibility and reduced risk of harm.

Human in the loop

The perception, from the user’s side, of being an active participant of the process of the technology, and not a mere spectator. In the development and testing stages of a certain technology, the presence and intervention of humans permits continuous feedback to better shape the result. Involving humans means making them an active part of the process and not left out of the technology itself, to develop a fruitful interaction between the parties.

Electronic Identification (eID)

The act of making an entity known, through a unique combination of attributes used for the authentication (i.e., assessing the identity) and authorization (i.e., granting permission) to electronic public or private services
The process of using personal identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person.

Related Term: Identity

Identifier

A series of digits, characters, and symbols or any other form of data used to identify a subject. Identifiers can be scoped by time and/ or space. Pseudonyms can be temporal and effective only for a specific service. Some examples are user account names, passport numbers, mobile phone numbers, employee numbers, pseudonyms, and Uniform Resource Identifier (URI).

Identity

A legal identity is defined as the basic characteristics of an individual's identity, e.g. name, sex, place and date of birth conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth. Digital identities enable tracking and customization of entity interactions across digital contexts, typically using identifiers and attributes. An identity consists of a set of attributes (along with their values) describing relevant aspects and properties of an entity. This information is dynamic: the set of attributes and their values can change over time. Different views on an entity's identity information can be created, disclosed, accessed and used by multiple parties. A view consists of an aggregation of one or more attributes. Each attribute can assume different values, depending on the view it belongs to and the context where it is used. Unintended distribution or use of identity information can compromise privacy. Collection and use of such information should follow the principle of data minimization.

Related Term: Entity

Identity document

A document issued by a state authority to an legal entity for providing evidence of the identity of that legal entity.

Identity provider

An identity provider, sometimes abbreviated as IdP, is a system for creating, maintaining, and managing identity information for holders, while providing authentication services to relying party

applications within a federation or distributed network. In this case, the holder is always the subject. Even if the verifiable credentials are bearer credentials, it is assumed the verifiable credentials remain with the subject, and if they do not, they were stolen by an attacker. This specification does not use this term unless comparing or mapping the concepts in this document to other specifications. This specification decouples the identity provider concept into two distinct concepts: the issuer and the holder.

Related Term: Identity

Immutability

Immutability is one of the key features of blockchain systems. It refers to the fact that data cannot be altered due to their organization. In blockchains, this feature is obtained by grouping transactions into blocks that are linked to the previous ones so that, in order to change a single data, the entire chain needs to be changed.
Immutability guarantees that past transactions cannot be altered. This is a property of DLT because each new block is linked with the previous one. It is a fundamental property since it ensures a high level of auditability. On the other hand, wrong transactions cannot be rectified and the "right to be forgotten", granted by GDPR, is applicable only with the conditions that there can be no personal data in the blockchain.

Related Term: Blockchain

Interoperability

The ability of a component (software or hardware) to be easily integrated with other components. An high level of interoperability can be achieved by making use of specific design patterns, standard protocols, common architecture designs. Identities should be as widely usable as possible. An identity that works only in limited protocols or architectures has less intrinsic value than an identity that is accepted and verifiable in more states. Persistence and autonomy help to assure the availability of identities over time and the control of the user over personal data.

Related Term: Distributed Ledgers

Issuer

A role an entity can perform by asserting claims about one or more subjects, creating a verifiable credential from these claims, and transmitting the verifiable credential to a holder.

Related Term: Identity

Knowledge-Based Verification

Identity verification method based on knowledge of private information associated with the claimed identity. This is often referred to as knowledge-based authentication (KBA) or knowledge-based proofing (KBP).

Related Term: Authentication

Levenshtein distance

Measure of the difference between two character sequences based on the minimum number of single character edits (insertion, deletion, or substitution) needed to convert one word to the other. ISO/IEC/IEEE 26531:2015(en), 4.24

Related Term: Optical Character Recognition (OCR)

Machine learning

It is the process by which a functional unit improves its performance by acquiring new knowledge or skills, or by reorganizing existing knowledge or skills.

Man-in-the-Middle Attack (MitM)

An attack in which an attacker is positioned between two communicating parties in order to intercept and/or alter data traveling between them. In the context of authentication, the attacker would be positioned between claimant and verifier, between registrant and CSP during enrolment, or between subscriber and CSP during authenticator binding.

Related Term: Cyberattack

Message Authentication Code (MAC)

A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. MACs provide authenticity and integrity protection, but not non-repudiation protection.

Minimal disclosure authentication

The authentication takes a verification path and signature of the user's identity attributes as inputs, and the verification method is distinguished according to whether the attribute in the path contains an int type. The output is whether the current user has passed the authentication. The user needs to disclose attributes for the verifier, the remaining non-essential attributes will be sent to the verifier in the form of ciphertext.

Mining

In the context of blockchain-based systems, mining is the process through which participants add transactions to the shared ledger. The process of mining includes creating a hash of a block of transactions with the aim of protecting data integrity.

Related term: Blockchain

Ownership

The right of possession over an object, an information or data, and the right to use it, manage it and grant it from the owner.

Optical Character Recognition (OCR)

It is the use of technology to distinguish printed or handwritten text characters inside digital images of physical documents, such as a scanned paper document. The basic process of OCR involves examining the text of a document and translating the characters into code that can be used for data processing. OCR is sometimes also referred to as text recognition.

Related Term: Computer Vision

Passphrase

A passphrase is a memorized secret consisting of a sequence of words or other text that a claimant uses to authenticate their identity. A passphrase is similar to a password in usage, but is generally longer for added security.

Related Term: Identity, authentication

Persistence

Identities must be long-lived. Identities should last forever, or as long as the user wishes. Even if private keys and data need to be changed, as a recreation of digital identity at different places, the identity remains. Although is arduous to accomplish this objective, identities should last until they've been outdated by newer identity systems and not contradict the "right to be forgotten". Users have the right to dispose of an identity and claims should be modified or removed as appropriate over time. This requires a firm separation between an identity and its claims: they can't be tied forever.

Personal Data

Any information relating to an identified or identifiable natural person. In particular an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal identity

A sense of ownership and attachment to certain properties of the self which define the person and which distinguish him/her from others. In this sense, personal identity is contingent and temporary and can change over time.

Phishing

Phishing is an illegal practice to steal personal information as credit card numbers, passwords etc. It is often used to steal digital identities and commit illegal acts online. It is one of the most important issues in identity management because users often fall into phishing.

Portability

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. In exercising the right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. This implies that data cannot be held by a singular third-party entity, therefore the premise of portability would fail its purposes. Transportable identities make sure that the user can maintain control of his identity over time, consequently improving the identity's persistence.

Privacy

European law defined the right to privacy as the right to the protection of personal data. Article 8 of the EU Charter of Fundamental Rights establishes that "Everyone has the right to the protection of personal data concerning him or her" and "such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law".

Privacy by Design

Privacy by design means that privacy must become integral to organizational priorities, project objectives, design processes, and planning operations. Privacy must be embedded into every standard, protocol and process that touches our lives in a preventative and non-remedial way. Thus the term can be described as a set of practices intended to protect the privacy of the user. For example, pseudonymisation, anonymisation, transparency and data minimisation are designed to implement data-protection principles, so as to be compliant with GDPR and effectively protect the rights of data subjects.

Related Term: Privacy

Processor

Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Profiling

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Proof of stake

It is a consensus algorithm proposed as an alternative to PoW. In this scenario, the creator of a new block is chosen in a deterministic way, depending on its stake. In other words, a participant can mine or validate a block depending on how many assets they own.

Related Term: Consensus Algorithm

Proof of work

It is a consensus algorithm firstly proposed by Satoshi Nakamoto. In this scenario, parties (miners) are involved in the consensus and they must solve a cryptographic puzzle to "mine" a block and add it to the blockchain.

Related Term: Consensus Algorithm

Protection

Is intended as the protection of the user's rights. The identity network must move over in order to protect the rights and the freedom of the individual whereby a conflict between the two needs to be solved. Algorithms for authentication have to be independent and decentralized, so as to be censorship-resistant and force-resilient. Moreover, protection of personal data of the subject the prevents informational inequality, informational injustice and discrimination of harm, encroachment on moral autonomy and human dignity, as to guarantee prevention of harm.

Pseudonymization

According to article 4 (5) GPDR, pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Related Term: Privacy

Representation

As defined for HTTP by [RFC7231]: "information that is intended to reflect a past, current, or desired state of a given resource, in a format that can be readily communicated via the protocol, and that consists of a set of representation metadata and a potentially unbounded stream of representation data."

Right of access

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Right to be forgotten

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data. This can be applied if: personal data are no longer necessary in relation to the purposes for which they were collected; the data subject withdraws consent; the data subject objects to the processing; the personal data have been unlawfully processed; the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject. In addition, data must naturally be erased if the processing itself was against the law in the first place.

Right to object

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing,

the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to restriction of processing

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

Security

The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (pseudonymization, encryption, confidentiality). In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Self-determination

It means the process of recognition and acceptance of certain normative tenets and acting from that recognition. Self-determination starts from the moment of acceptance of tenets on authority, on trust, or by own's decision, and not merely from the knowledge about them.

Self-sovereign identity

Self-sovereign identity is owned and controlled by a user without the need to rely on any external administrative authority and without the possibility that this identity can be taken away. This new type of approach shifts IdM systems from a Provider-centric model, where identity was bound with the service provider, to a user-centric model. The identity is freed from any provider because it is stored, accessed and authenticated through the chain.

Related Term: Identity

Sensitive Data

Sensitive Data are Personal Data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Shareability

The user must be able to decide to share an identity from one service to another.

Single Sign On

Single Sign-On (SSO) is an authentication process that allows a user to log into multiple applications with a single set of login credentials. SSO is a common practice in enterprises, where a client accesses multiple resources connected to a local area network (LAN). With Single Sign-On, the user logs in once and gains access to different applications without the need to re-enter the login credentials in each application.
The most widely used protocol for SSO is OAuth 2.0, supported by all the major Identity Service providers. The functioning of SSO requires three main actors: the Identity Service Provider, the Relying Party, the user. The first is the one who authenticates the digital identity, the Relying Party is the environment where the user is logging in.

Related Term: Authentication

Smart Contract

SCs are computer programs that reside inside blockchain systems. The execution of a SC can be autonomously done and it typically involves two parties (blockchain participants).

In Europe, only Italy and Malta have recognized the legal status of a smart contract.
According to Italian law, a "smart contract" is defined as a computer program that operates on technologies based on distributed registers. Its execution automatically binds two or more parties based on effects predefined by them

Social inclusion

The efforts made through policies and actions to promote and ensure the participation of the social corpus in the decision-making process, as well equal access to services and resources for auto-determination. This applies especially to the most marginalized such as women, persons with disabilities, sexual and gender minorities, the elderly, and ethnic and racial minorities.

Software Usability

Qualitative assessment of the extent to which a novice user interacts with software, to accomplish specific goals in a given use context with relative effectiveness, efficiency, satisfaction, and overall ease-of-use as the standard of measurement (Agarwal and Venkatesh, 2002; Baker, 2009; Karkin and Janssen, 2014)

Transparency

According to the HLEG group the data sets and the processes that yield the AI system’s decision, including those of data gathering and data labelling as well as the algorithms used, should be documented to the best possible standard to allow for traceability. Moreover, the ability to explain

both the technical processes of an AI system and the related human decisions is required for transparent AI systems. According to the GDPR the principle of transparency requires that any information and communication relating to the processing of personal data be easily accessible and easy to understand for the citizens (article 5, paragraph 1, letter a)). For that, implemented systems and algorithms should be free, open-source, well-known, and as independent as possible of any particular architecture.

Transport Layer Security (TLS)

An authentication and security protocol widely implemented in browsers and web servers. TLS is defined by RFC 5246. TLS is similar to the older SSL protocol, and TLS 1.0 is effectively SSL version 3.1. NIST SP 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations [SP 800-52], specifies how TLS is to be used in government applications.

Related Term: Authentication

Trust

The willingness of one entity (A) to be vulnerable to the actions of another entity (B), based on the expectations that the other entity (B) will perform an important action and refrain from opportunistic behaviour in a situation of risk or uncertainty, regardless of the first entity's (A's) ability to control or monitor that other entity's (B's) behaviour. At least three kinds of trust can be identified in the scope of software systems: Security or protection of personal data, being able to trust on other people's actions, and being able to trust what other people say.

In federated IdM systems the trustworthiness of the network is fundamental in order to run the federated system. Trustworthiness is reached if all the participants in the federated network can guarantee the same, high level of security standards and if some management best practices are shared in the network. In blockchain-based IdM systems the problem of trust seems to be resolved: the algorithm managing the consensus mechanism is said to be trustless, namely not requiring to be trusted. This is because the algorithm is fully deterministic and forecastable in its behaviour.

Trusted Third Party

Reputed, responsible and established fiduciary body all parties accept from an agreement, transaction or deal.
The trusted third party (TTP) is a warrantor that a transaction between two parties is valid. The warrantor must be trusted by both the parties. In an SSO login the TTP is the provider and the two parties are the relying party and the user. In the case of blockchain-based IdM systems there is no TTP.

Related Term: Trust

Universally Unique Identifier (UUID)

A type of globally unique identifier defined by [RFC4122]. UUIDs are similar to DIDs in that they do not require a centralized registration authority. UUIDs differ from DIDs in that they are not resolvable or cryptographically-verifiable.

Unsupervised learning

A learning strategy that consists in observing and analysing different entities and determining that some of their subsets can be grouped into certain classes, without any correctness test being performed on acquired knowledge through feedback from external knowledge sources.

Related Term: Machine learning

Usability

The extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. The "specified" users, goals and context of use refer to the particular combination of users, goals and context of use for which usability is being considered. The word "usability" is also used as a qualifier to refer to the design knowledge, competencies, activities and design attributes that contribute to usability, such as usability expertise, usability professional, usability engineering, usability method, usability evaluation, usability heuristic. Moreover, the term encompasses in itself the notions of user friendliness, ease of use and user satisfaction, and is also closely related to interaction and user experience (UX).

User Awareness

There is a delicate balance between the multiplication of authentication methods (password, captcha, one-time password, notification, messages, QR codes) and the user's awareness and digital literacy about the functioning of IdM, its risks and implications. The strongest system can be easily compromised if the user is not aware of how it works. Therefore, every technical solution must take into account the fundamental importance of the user experience in order to avoid design errors and shortcomings.

Related Term: User

User-centric design

User centric design is an approach that puts at the center of the design process the needs and wills of users. Great attention is given to users' expectation regarding the technology and its usability. It is defined as an ethical approach to design under the wider context of human-centered design.

Related Term: User

User-experience

User's perceptions and responses that result from the use and/or anticipated use of a system, product, or service. The notion implies the user's emotions, beliefs, preferences, perceptions, comfort, behaviours, and accomplishments that occur before, during and after use. User experience is a consequence of brand image, presentation, functionality, system performance, interactive behaviour, and assistive capabilities of a system, product or service. It also results from the user's internal and physical state resulting from prior experiences, attitudes, skills, abilities and personality; and from the context of use.

Validation

The assurance that a verifiable credential or a verifiable presentation meets the needs of a verifier and other dependent stakeholders. This specification is constrained to verifying verifiable credentials and verifiable presentations regardless of their usage. Validating verifiable credentials or verifiable presentations is outside the scope of this specification.

Related Term: Credential

Value

To recognize the influence of some features of a certain thing and consider it a principle or a standard of guidance for its importance in life or in a system. Some values can be treated as "universals" for their importance and applicability in many cases and uses. Value Sensitive Design approach treats values in a contingent way, analysing their importance for every particular context.

Value Sensitive design

A family of theoretical and empirical approaches born to study the development of new technology from a *value-based* perspective. With value-based design we aim to capture what are the fundamental values that are embedded in the process of designing technologies. In this approach, a multi-level method is presented, assessing the design process from a conceptual, empirical, and technical standpoint. Value-sensitive design claims that some fundamental assumptions are constitutionally present in the design phase, and it aims to uncover them using a multifaceted methodology. This approach has been applied, giving valuable insights, on the problem of cookies and informed consent.

Verifiable credential

A standard data model and representation format for cryptographically-verifiable digital credentials as defined by the W3C Verifiable Credentials specification [VC-DATA-MODEL].

Related Term: Credential

Verifiable data registry

A system that facilitates the creation, verification, updating, and/or deactivation of decentralized identifiers and DID documents. A verifiable data registry might also be used for other cryptographically-verifiable data structures such as verifiable credentials. For more information, see the W3C Verifiable Credentials specification [VC-DATA-MODEL].
A role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential schemas, revocation registries, issuer public keys, and so on, which might be required to use verifiable credentials. Some configurations might require correlatable identifiers for subjects. Some registries, such as ones for UUIDs and public keys, might just act as namespaces for identifiers.

Related Term: Credential

Verifiable Presentation

Data derived from one or more verifiable credentials, issued by one or more issuers, that is shared with a specific verifier. A verifiable presentation is a tamper-evident presentation encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification. Certain types of verifiable presentations might contain data that is synthesized from, but does not contain, the original verifiable credentials (for example, zero-knowledge proofs).

Verifiable timestamp

A verifiable timestamp enables a third-party to verify that a data object existed at a specific moment in time and that it has not been modified or corrupted since. If the data integrity could reasonably have been modified or corrupted since that moment in time, the timestamp is not verifiable

Related Term: Tampering

Verification method

A set of parameters that can be used together with a process to independently verify a proof. For example, a cryptographic public key can be used as a verification method with respect to a digital signature; in such usage, it verifies that the signer possessed the associated cryptographic private key. "Verification" and "proof" in this definition are intended to apply broadly. For example, a cryptographic public key might be used during Diffie-Hellman key exchange to negotiate a shared symmetric key for encryption. This guarantees the integrity of the key agreement process. It is thus another type of verification method, even though descriptions of the process might not use the words "verification" or "proof."
The evaluation of whether a verifiable credential or verifiable presentation is an authentic and timely statement of the issuer or presenter, respectively. This includes checking that the credential (or presentation) conforms to the specification, the proof method is satisfied, and, if present, the status check succeeds.

Related Term: Cryptographic suite

Verifier

A role an entity performs by receiving one or more verifiable credentials, optionally inside a verifiable presentation for processing. Other specifications might refer to this concept as a relying party.

Related term: Credential

Violation

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, thus violating the identity of a subject.

Voluntarism

Refers to the absence of control or coercion in the action.

Wholeness

The users are not separated by their data.

3 Conclusion

The last part of this vocabulary aims to underline the political and communicative valency of the words and the concepts implemented in the techical and non-technical discussion about Identity Management systems based on Blockchain. While this discussion might be extended to nearly all the discussions on technologies impacting the social systems, we believe that in this case it is particularly urgent to point out the importance of such a reflection.

In fact, Blockchain technologies grew up on the one hand in international relevance also thanks to the impressive hype that the narrative (decentralized, without controlling third-parties, trustless) generated in the public opinion. On the other hand, identity management systems impact the core aspects of the functioning of a society, namely how identities are regulated, verified and produced inside the society. The concept of socio-technical systems (Ropohl, 1999) well describes the co-implications between society, technological objects and the narratives and social discourses upon them. The description of the functioning of a technical object, for example to define it “trustless” or “self-sovereign”, is a linguistic operation that modifies societies, and impacts the way individuals relate with institutions and the public sphere as a whole. For example, the fact that Blockchains are without a trusted third-party moved a part of the population toward the adoption of cryptocurrencies for their business or investments. While this is true, the concept of “trustlessness” might be misunderstood as if Blockchains are fraud-free. The concept of self-sovereignity might trigger the presumption of a complete control of one’s identity, while this is true only technically and to a certain extent.

This reflection links with the broader theme of how to communicate technologies in the delicate balance between the need to involve people in the technological processes and the importance of providing a transparent communication, that conveys coherent contents on how the given technology works, what are its risks and benefits. This is important not only in terms of ethicality of communication, but also in terms of user-experience and regarding the broader impact on society: users will engage and relate with the technological object in light of how it is communicated. This means that correct and safe use are dependant on how the content of communication is conveyed.

This last section, that might be seen as a *caveat* toward an improper (namely misunderstandable) use in public society of technical terms, connects with the choice to disambiguate the different meanings of the terms in the vocabulary: every term can be understood differently depending on which is the discoursive dimension – technological, legal, ethical and governmental – involved.

The path to trustworthy technologies passes through trustworthy socio-technical systems, and this duty implies the use of terms and a style of communication that ensures that there is a coherent relationship between how technology is perceived in society and what it actually is.

4 References

Allen, C. The Path to Self-Sovereign Identity. 2016.
Available online: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new jim code*. Polity Press
Blackburn, S. *The Oxford dictionary of Philosophy*, 2008, Oxford University Press
Castells, M. (2013). *Communication power* (Second ed.). Oxford University Press
Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights, (2019). *Handbook on European data protection law : 2018 edition*, Publications Office of the European Union. https://data.europa.eu/doi/10.2811/343461
Leininger, A. (2015). Direct Democracy in Europe: Potentials and Pitfalls. *Global Policy*, 6(S1), 17-27. doi:10.1111/1758-5899.12224
Marijn Janssen, Paul Brous, Elsa Estevez, Luis S. Barbosa, Tomasz Janowski, *Data governance: Organizing data for trustworthy Artificial Intelligence*, Government Information Quarterly, Volume 37, Issue 3, 2020, 101493, ISSN 0740-624X, https://doi.org/10.1016/j.giq.2020.101493
Micheli, P., Wilner, S.J.S., Bhatti, S.H., Mura, M. and Beverland, M.B. (2019), Doing Design Thinking: Conceptual Review, Synthesis, and Research Agenda. J Prod Innov Manag, 36: 124-148. https://doi.org/10.1111/jpim.12466
Paul Upham, Christian Oltra, Àlex Boso, *Towards a cross-paradigmatic framework of the social acceptance of energy systems*, Energy Research & Social Science, Volume 8, 2015, Pages 100-112, ISSN 2214-6296, https://doi.org/10.1016/j.erss.2015.05.003.
Ropohl, G. (1999). Philosophy of socio-technical systems. *Techne: Research in Philosophy and Technology*, *4*(3), 186-194. https://doi.org/10.5840/techne19994311
Skorupski, J. (2010). MORAL OBLIGATION, BLAME, AND SELF-GOVERNANCE. Social Philosophy and Policy, 27(2), 158-180. doi:10.1017/S0265052509990197
Van Dijk, J. (2020) *The digital divide*, Polity Press

Some of the terms of this dictionary are derived from
https://gdpr-info.eu/art-4-gdpr/
https://gdpr-info.eu/art-15-gdpr/
https://gdpr-info.eu/art-16-gdpr/
https://gdpr-info.eu/art-17-gdpr/
https://gdpr-info.eu/art-18-gdpr/
https://gdpr-info.eu/art-20-gdpr/
https://gdpr-info.eu/art-21-gdpr/
https://gdpr-info.eu/art-25-gdpr/
https://gdpr-info.eu/art-32-gdpr/
https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en
https://www.iso.org/obp/ui/#iso:std:iso-iec:23053:dis:ed-1:v1:en
https://www.iso.org/obp/ui/#iso:std:iso:9241:-112:ed-1:v1:en
https://www.iso.org/obp/ui/#iso:std:iso:9241:-210:ed-2:v1:en
https://www.iso.org/obp/ui#home
https://plato.stanford.edu/index.html

5 Annex of new and expanded terms

Acceptance
Access
Accessibility
Agreement
Authority
Autonomy
Biometric data
Black box
Consent
Control
Controller
Data governance
Data minimisation
Data processing
Data protection by design
Data protection by default
Data subject
Data subjectivation
Data transfer
Deontological ethics
Digital divide
Design ethics
Design thinking
Digital identity
Dignity
Disclosure
Discrimination
Equality
Ethics by design
Existence
Feedback loop mechanism
Freedom
Human-centric design
Human in the loop
Interoperability
Minimal disclosure authentication
Ownership
Persistence
Personal data
Personal identity
Portability

Privacy by design
Processor
Profiling
Protection
Right of access
Right to be forgotten
Right to object
Right to rectification
Right to restriction of processing
Security
Self-determination
Sensitive data
Shareability
Social inclusion
Transparency
Usability
User-experience
Value
Value Sensitive design
Violation
Voluntarism
Wholeness