UNIVERSITÀ DEGLI STUDI DI SALERNO

DIPARTIMENTO DI INGEGNERIA INDUSTRIALE

Dottorato di ricerca in Ingegneria Industriale
Curriculum in Ingegneria Elettronica - XXXIV Ciclo

"Tesi di dottorato in : Blockchain, the distributed paradigm for secure metrology digitalization"

Laura De Santis

a.a. 2021/2022

ISBN 88-7897-129-4

UNIVERSITY OF SALERNO

DEPARTMENT OF INDUSTRIAL ENGINEERING

Ph.D. Course in Industrial Engineering
Curriculum in Electronic Engineering - XXXIV Cycle

BLOCKCHAIN: THE DISTRIBUTED PARADIGM FOR SECURE METROLOGY DIGITALIZATION

Supervisors
Prof. Domenico Capriglione

Prof. Vincenzo Paciello

Scientific Referees
Prof. Aimé Lay-Ekuakille
Prof. Miele Gianfranco

Ph.D. Course Coordinator
Prof. Francesco Donsì

Ph.D. student
Laura De Santis

Laura De Santis

Acknowledgments

I want to dedicate the conclusion of this journey to my brother Gianmarco, who passed away a few years ago. I miss you every day. I hope if you are observing me somewhere, you are proud of me. First, I would like to thank my parents, to whom I owe everything. It is not easy to follow a person with my personality. Still luckily, I had the opportunity to have two persevering people beside me who never gave up and allowed me to study, which I am most grateful for. In this regard, I want to thank my Supervisors, Professor Vincenzo Paciello and Professor Domenico Capriglione. A special note is for Vincenzo, who spurred me every time to overcome my limits, allowed me to get to know external research realities by broadening my horizons, and above all, I thank him for not giving up. A special note goes to Professor Consolatina Liguori and Professor Antonio Pietrosanto. Not only have you welcomed me with great sensitivity in your research laboratory, but you have been a great example of life on how to reconcile the institutional and managerial role with the human aspect. I won’t forget the precious lesson learned by both, and infinite gratitude. Thanks to Moise Ugwiri. You have been my companion on this journey. We shared moments of joy and weakness. Without you, this journey would not have had the same smell of discovery. Thanks, Moise, you are exceptional. I thank the legendary trio Daniele Buonocore, Giuseppe Ciavolino, and Salvatore Dello Iacono, who made the days in the laboratory familiar, like when you are among brothers. To Daniele in particular, I want to leave a message: you and Professor Liguori are the heart of that laboratory; don't ever change. I thank the engineer, Giuseppe Di Leo. Giuseppe has always been a model of a decent person and a loyal worker. I hope to take some ideas from him for my future career path. I thank Professor Francesco Donsì for patiently listening to my requests during the courses. I thank the engineers Marco Carratù and Teresa Foglia for being the bridge that allowed me to undertake this path. I wish you to crown your dream of love as soon as possible. Thank the University of Salerno for permitting me and many others to achieve the Ph.D. title.Thank you all for these three years. Our paths will never be diverging lines but curves with infinite tangents, even when we part ways.

Publications

A. Lisi, P. Mukherjee, L. De Santis, L. Wu, D. Lagutin and Y. Kortesniemi, "Automated Responsible Disclosure of Security Vulnerabilities," in IEEE Access, vol. 10, pp. 10472-10489, 2022, DOI: 10.1109/ACCESS.2021.3126401.

L. D. Santis, V. Paciello and A. Pietrosanto, "Blockchain-Based Infrastructure to enable Trust in IoT environment," 2020 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), 2020, pp. 1-6, DOI: 10.1109/I2MTC43012.2020.9128817.

V. Paciello, L. De Santis, D. Hutzschenreuter and I. Smith, "A universal metadata model for metrological complex quantities," 2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT, 2020, pp. 490-494, DOI: 10.1109/MetroInd4.0IoT48571.2020.9138287.

Y. Nie, L. De Santis, M. Carratù, M. O'Nils, P. Sommella, and J. Lundgren, "Deep Melanoma classification with K-Fold Cross-Validation for Process optimization," 2020 IEEE International Symposium on Medical Measurements and Applications (MeMeA), 2020, pp. 1-6,DOI: 10.1109/MeMeA49120.2020.9137222.

Index of contents

Table of Figures

Table of Tables

Abstract

Digital transformation is causing products, production, and economic processes to change rapidly and dramatically. This new demand presents new challenges to the existing system of quality infrastructure.

Industry 4.0 is a concept that describes the process of providing innovative products by using smart methods and procedures. This enables seamless asset lifecycle information, from plant concept to decommissioning, and digitally integrates value chains. It introduces many ideas that are relevant to taking advantage of these opportunities. These include machine-to-machine communication (M2M), cyber-physical system (CPSs), and the Internet of Things (IoT) [1]. M2M communication is the ability of industrial components to communicate. CPSs can monitor physical processes and create virtual copies of the world. They can also make decentralized decisions. Surrogate models, metamodels, and parameterized models could create virtual documents. These models are approximations of experimental or simulation data that can answer questions when direct measurement of the outcome of interest is not possible. With the further development of telecommunication, such a system has been embedded in the IoT field, which has become a concrete reality of everyday life. IoT is a lightweight network of "objects" such as devices, sensors, and actuators that can be connected to the Internet and communicate wirelessly. This structure aggregates and manages the data produced by the sensor devices on a head node that acts as the central administrator, e.g., a server [2]. In such a network, physical and virtual entities share attributes and communicate. Due to their versatility, IoT systems have been used in many applications such as car accident remote monitoring [3], control of crops for smart farms, supervision of smart cities, home automation, and optimization in the energy market through smart metering [4]. Different trust concerns limit the widespread adoption of the IoT systems, related both to the specific capabilities of the devices and to the high grade of connectivity supported by the system [5]. In the particular case of manufacturing and Industry 4.0, under the term Distributed Sensor Services, the authors [6] describe such systems in terms of any physical measure that digitize real-world quantities as a sensor operation, also including complex instruments that combine multiple measurements, along with the (network-) interfaces to historical and current data, and the computational resources required for data processing. The interoperability of heterogeneous distributed systems is essential for automation purposes [7]. Functional modeling of sensors and processing modules that provide a concise added value separate from

proprietary implementations is required. Moreover, to ensure the system's proper function, the devices and produced data must be considered reliable from the legislative and regulatory points of view.

The widespread adoption in a unified European Market of such technologies is sharply limited by Trust concerns for IoT devices regarding reliability, traceability, integrity, the privacy of the data, and cybersecurity of software and hardware components. In a hyperconnected society, the need for improved quality and security of interconnected devices is crucial, especially if there is a strong interdependence with human activity. Interdependence so affects the different levels of machine and system development. It is utopian to think that a final product results from a single effort in a modern market. Often, complex products result from the cooperation of different suppliers (e.g., raw materials, hardware development, software development, development, and support of the ITC infrastructure). Each development phase is subject to review by the authorities in charge of market surveillance (e.g., National Accreditation Body, National Cybersecurity Authority, etc.). Although this procedure is necessary, manufacturers often perceive it as a strong brake on the competitiveness of their products by significantly increasing the time to market [8]. The National Institute of Standard Technologies (NIST) identifies 17 technical trust-related- concerns for IoT adoption both in people's lives and in the enterprise's environments [9]. Trust in IoT includes four main specifications related to cybersecurity issues and data trust: Control and ownership, IoT certification criteria, Data integrity, and Security [10], [11]. All quality assurance processes such as certification, accreditation, and market surveillance must be digitalized to meet these challenges. All parties involved must be digitally connected and interoperable, and the network data flow needs to be traceable. One hindrance, in this case, is due to the fragmentation of legislation in the legal field. A procedure for the assessment of products and services is still being developed, the components of which are produced in different regions of the European community (e.g., a measuring device whose hardware is designed and certified in Italy, the firmware is developed and verified in Germany, the linked application is produced in Finland).

While there is a strong need for a legislative effort at the community level to standardize and standardize the legislation relating to the safety and quality certifications of the products transiting the European market, on the other hand, a key aspect to consider is the means and technological infrastructures necessary to streamline and optimize the traceability and verifiability procedures of systems and products [12] [13]. In such a system, it should be considered that the stakeholders involved do not necessarily trust each other. The national authorities constitute a trusted third party for the individual states, but this assumption cannot hold in a community system. Therefore, the development of an infrastructure based on a consortium of parties is required in which each information flow is available in a decentralized manner, i.e., not under the control of a single entity but of a community of well-known and trusted parties (e.g., Authorities and Governments) and accessible to the various market stakeholders [8]. Product information must be tracked securely. A traditional database has some limitations in this sense suffering from a single point of failure, subject to date tempering. The approach based on distributed ledger technology (aka blockchain) solves a good part of these fundamental problems while presenting other significant challenges from a technical point of view [14].

This thesis considers this technology's capabilities and challenges to achieve both data trust and traceability with digital certification as the point of trust.

Chapter 1

Introduction

1.1 Background and Regulations in Digital Transformation

Considering the enormous economic opportunity offered by a single digital market, the European Commission has issued a Digital Single Market Strategy for Europe to promote the essential aspects such as Cloud Computing, Big Data, and Platforms [15], [16], [17]. The European Commission's New Approach to Digitalization could help overcome existing barriers to innovation in the legal metrology sector. A Quality Infrastructure proposed by the commission [18] can be defined as the entire institutional framework required to establish and enforce standardization, metrology, and accreditation. It also includes the conformity assessment services needed to prove that products and services comply with specified requirements. Measurement instrument sensors can be fully developed within the required accuracy limits based on individual customer needs, addressing new business and service models. These are determined using field data and user data. Therefore, there will be an increasing demand for data-based services and business models, such as those based on big-data processing systems. The European manufacturers' associations feel that inefficient processes within the quality infrastructure prevent the development of new products and the exploitation of technological potential to streamline processes [19]. Manufacturers' associations contemplate marketing concepts based on the technological transition from a locally concentrated instrument to a distributed device with cloud-located storage, data-based services, and virtualized processing software. This led to the increasing demand for legal architectures for these technologies.

Legal metrology is the discipline that supervises the correctness of measurements and the protection of users of measuring instruments and their customers. The main actors in legal metrology are users and manufacturers of the measurement instruments, the National Metrology Institute (NMI), and the market surveillance and verification/inspection national authorities. The European Directive [18] regulates the stakeholders’ responsibilities and rights, providing a quality structure that oversees new product integration, design, production, placement in the marketplace, and usage. The Notified Bodies evaluate the conformity of the design to the essential requirements. Market surveillance and user surveillance oversee the placement on the market and the correct use of instruments. The instrument's re-verification or inspection is the responsibility of the verification and inspection authorities. This establishes a trust chain that runs from the development phase through production and ends with the instrument in use. The European regulations cover more than three hundred million units annually sold on the European market [20]. Notified Bodies oversee conformity assessments of measuring instruments and issuing type-approval certificates. In the EU, there are 120 of these notified bodies, 900 companies in measuring instruments production for over 5 million estimated verifications per year only in central Europe, and 850 million measuring devices on the EU market, which are responsible for a share of 4 % to 6 % of the European Gross domestic product [21]. Many processes can be defined within the legal framework and established using a traditional communication medium. These processes include exchanging information among partners, such as documentation of the instrument design provided to the manufacturer by market surveillance when the instrument is used. These interactions are not currently based on state-of-the-art communication pathways or coordinated via platforms. A requirement to collect data specifically for each role within this context has been established. For example, the notified body records all instruments used during conformity assessments. This information is extremely sensitive. Another example is performance data for a measuring device. The manufacturers shall conduct sample testing on all available measuring instruments, register complaints about non-conforming devices, recalls, and recalls, and inform distributors of any such monitoring. The market surveillance authorities will collect the necessary data to identify non-compliant measurement instruments, their origin, the risk involved, and the duration and nature of any national measures. They also need to know the economic operators who made the argument. On request, data is extracted from metrology databases using traditional methods based on intermediator queries made by the database's keeper and then transferred to the requestor. Direct queries from authorized partners to the data provided by the members are not possible. Many processes involve many partners. Their agreement must be based on the different actions that need to be completed before any final process can begin. One example is modifying, repairing, or updating legally relevant software. If the process is digitalized via a platform, there are excellent prospects for streamlining it. Manufacturers' associations see marketing strategies that take advantage of innovations driven by the growing market. These are facilitated by technology that has advanced significantly. Manufacturers object that current regulations implemented by analog quality infrastructures hinder the development of market-driven technologies. The analog quality infrastructure could be restructured to allow for digitalization. This would remove any barriers that prevent innovation. To remove any barriers to innovation in legal metrology, it is being planned to make processes digitally using state-of-the-art digital technology. This will allow for streamlining, harmonizing, and coordinating [19].

The “European Metrology Cloud” [21], promoted by joint enforcement of the PTB and NIST, is the main project that has been proposed to address those mentioned above problem. The main point that was identified in the project are:

- The digital transformation of metrological services.
- The use of Metrology for analysis of large quantities of data.
- Secure Metrology communication systems in digitalization.
- Appling Metrology Science for simulations and virtual measuring instruments.

To address this task, the implementation strategy is focused on:

- Developing a secure, interoperable digital standard for measurement data exchange that can be used in metrology, calibration, and accreditation, upgrading the entire calibration hierarchy digitally.
- Extends and combines existing databases and data infrastructures in a trusted core platform for a digital quality network, Metrology Cloud, and provides partners with personalized access to such digitally updated infrastructure.
- Building a virtual and mathematics-aided Metrology competence group to support the paradigm shift in simulations as critical components of measurement procedures.

1.2 Digital Metrology in the chain of quality

Notably, the first point highlighted in [21] involves the quality infrastructure (metrology, standardization, and accreditation) through the basic concept of metrological traceability. According to the International vocabulary of metrology (VIM) [22], metrological traceability is:

> *"The property of a measurement result that can be linked to a reference via a documented, unbroken chain of calibrators, each is contributing to the measurement uncertainties."*

The International Laboratory Accreditation Cooperation (ILAC) considers the elements for confirming metrological traceability to be:

> "*An unbroken metrological traceability chain to an international measurement standard or a national measurement standard, a*

> *documented measurement uncertainty, a documented measurement procedure, accredited technical competence, metrological traceability to the SI, and calibration intervals"* [23].

The metrological traceability chain definition in [22] states:

> *"Sequence of measurement standards and calibrations used to relate a measurement result to a reference".*

The calibration hierarchy determines the metrological traceability chain used to establish the metrological traceability of a measurement result to a measurement unit. The reference is the international definition of a measurement unit through the international standard. To maintain metrological traceability and quality control, it is essential to create a chain of traceability where each measurement step and the correlated uncertainty must be documented. This is in line with the ISO 17025:2017 standard [24] [4], which specifies the requirements for the quality infrastructure stakeholder to satisfy the traceability principle in right and trustable conditions. New risks are associated with the digitalization process, leading to information integrity breaches. This process is error-proof because it relies on a well-established hierarchy with accredited calibration laboratories. To address the risk of data integrity breaches and eliminate the risk of compromising calibration certificates, the PTB introduced the concept of a Digital Calibration Certificate (DCC) [11], which serves for the electronic storage, the authentication, encryption, and signed transmission, and the uniform interpretation of calibration results. Information integrity is determined by the official national electronic signatures, following the eIDAS [25] regulation and time stamps.

The main problems that DCC is intended to address are:

- **Harmonization**: the DCC provides a unified international format for measurement data and certification, machine and human-readable.
- **Security**: the DCC document is bounded with an electronic signature linked to a public key associated with a trusted entity (e.g., an authorized person, corporation, or device). The identity infrastructure is based on the concept of Public Key Infrastructure.
- **M2M communication**: The document format is based on Mark-Up Language (XML), simplifying the M2M communication protocols and data processing. This is particularly relevant in IoT-related environments where automation is a critical feature that is highly desirable.

1.3 Digital Metrology in Legal Metrology

The scope of Legal is regulation and control of measurement instruments to ensure the accuracy of measurements and regulate consumer relations [26] [27]. The field covered by legal metrology regulations, established by government agencies and international committees, is legal control over measurement instrument (MI) and type approval, including documentation and code inspection, validation, and verification as described before. Legal metrology requires more complicated procedures, specialized security requirements, and best practices from well-known technical standards [28]. The OIML directive D-31 [29] and WELMEC Software Guide 7 [30] are the most widely used standards for software-controlled measurement instrument design and deployment. One security problem example happens when vendors and consumers have competing interests, the foremost trying to maximize profits, while the other trying to minimize prices by counterfeit measurements. For instance, this is typical in developing countries, e.g., on fuel meters and fuel. The most challenging aspect of cybersecurity is the so defined Legally relevant Software. In the field of Legal metrology, this is related to the part of the code directly involved in the measurement data processing. [31] It can be argued that, as the digital calibration certificate use a digital signature to grant consistency and trust in the produced data, the same concept can be applied to the measurement software. The use of asymmetric cryptography in a Public Key Infrastructure should enforce the authenticity that data are produced from a corrected, calibrated, and regulated device and the data themself are correct. This is not limited to the measurement data but to the communication software itself. On the opposite to legacy systems, modern measurement instrument infrastructure, especially with the advent of the Industry 4.0, IoT, and Industrial IoT (IIoT), most of the data processing is executed in the cloud, in a centralized or distributed fashion, leaving the electronic measurement device only in charge of extracting and communicate the physical quantity in the form of electronic measure. This enforces standard calibration certificate format and electronic signature for data communication.

However, such digitalization and the wide use of wireless networks directly or indirectly connected to the internet are vulnerable to cyber-attack, especially in the context of distributed applications such as IoT and IIoT. The Public Key Infrastructure (PKI) relies on a centralized trusted third party (TTP), i.e., the certificate authority (CA), making the involved sensor susceptible to cyber-attack. Traditionally CA PKI is sensitive to some specific form of “Man in the middle Attach” (MIM) known as Split-World Attacks [32]. Moreover, CA PKI can introduce a relevant computational overhead to manage many devices as in most IoT contexts. Other drawbacks are needed to trust manufacturer generated certificates in Embedded IoT context, high certificate signing cost, slow certificate signing process, and difficulties in maintaining root certificate lists [33].

There are different kinds of approaches to solve this issue. Still, distributed ledger technology (DLT) seems the most promising due to the high resiliency and independency from a trusted third party (TTP). DLT enables high transparency level but, on the other hand, could be in contrast to General Data Protection Regulation (GDPR) and the ISO-IEC 17025 [24] [8] [34]. Particularly relevant in this case are the “Right to be forgotten” and the “Privacy by design” principles, which impose the anonymization and the effaceable of some sensitive data correlated manly with user identity and behavior and the “Confidentiality Principle” i.e., the calibration laboratories shall have policies and procedures to ensure the protection of its customers' confidential information and proprietary rights, including strategies for protecting the electronic storage and transmission of results. On the opposite platform based on a high level of transparency and data persistency, as a public blockchain strongly contrasts with such principles. This limits the amount and kind of data stored on a public ledger, specifically user-sensitive data. Nevertheless, the entities involved are not just simple users but, for the most part, institutional entities, which on the opposite are interested in being easily recognizable and traceable. So, privacy, in this case should not be a problem. Moreover, different identity management strategies could be implemented with DLT that are often use-case related. Two Outstanding approaches are distributed PKI [35] [36] and the Self Souverain Identity (SSI) approach based on DLT [37].

1.4 Digital Metrology in Predictive Maintenance

The standard inspection and calibration process as described in ISO/IEC 17025 [24] requires time-based calibration of measurement instruments to ensure the validity and correctness of the quality standard. The process is very inefficient when applied to the industrial and manufactories sector, especially from the point of view of the Smart Industry. Smart factories use digitalization, data-driven production, agent-based systems, and digital twins to maintain their equipment. These factories employ edge, fog, and deep learning methods to control manufacturing processes. The ratio between predictive maintenance and legacy time-based calibration maintenance is the same as the digital calibration documents and infrastructure and their legacy version based on paper. Due to the increasing use of robots, digitalization, and artificial intelligence in production lines, predictive maintenance is becoming more critical. The four main trends are Industry 4.0 for predictive maintenance, smart manufacturing for condition-based maintenance, fault diagnosis for maintenance and prognostics, and remaining functional life analysis [38]. All this approach highly relies on extensive data collection to be effective. In the context of IoT, the amount of data itself is not a problem, but on the opposite, for reliable solutions the data quality is crucial indeed. Another embracing aspect is the accessibility of data. Despite the large volume, organized e structured collections of information are of much greater interest than unstructured ones. Stakeholders in the European Market can offer such added value if coordinated under a common platform from authority institutions, whose presence can enforce trust between not trusted parties. Quality infrastructure entities and legal metrologies' institutes could be engaged in the scenario of a decentralized digital platform in which regulated and standardized measurement data flow under the appropriate policies.

1.5 Analysis of unaddressed issue and research question explored

From what has been described in the previous ones, in order to establish to guarantee an effective digitalization of the metrological infrastructure, three research areas to be explored are identified:

- Digital standardization and formalization of metrological context: digital calibration certificates in an effort to solve the problem of harmonization of formats, introduce a broader issue that is the formalization and standardization of all documentation related to the metrological infrastructure, which includes the area of accreditation in addition to the digital conversion of a metrological taxonomy, i.e., the hierarchy of areas, sectors and metrological categories related to the calibration and calibration processes.

- Digital identification and signature security: as highlighted from the point of view of legal metrology, the authenticity of metrological data must be strengthened when entering the digital and automation realm through some form of digital signature that acts as a guarantee to its legacy counterpart. The digital signature systems are currently based on centralized systems that present a series of limitations when entering the scope of distributed systems, as is supposed to be the case of cloud infrastructure at the European level. This opens an exciting field of exploration linked to decentralized digital identification systems and in particular what advantages these systems introduce to their predecessors.

- Distributed approach applicability: from a purely technological point of view, given the nature of the problem, the limitations in terms of performance and effectiveness in the transition to digital systems based on a distributed approach become of particular interest. This includes how DLT technology can act as a trusted anchor point in the field of digital metrology to solve some of the main concerns regarding interoperability and trustworthiness and what capability it can offer.

- Digital metrology integration in IoT ecosystem: as highlighted in the very beginning, Industry 4.0 and IIoT are the main drivers of the digital transformation required in, and not only, metrological field. It is of particular interest for the research to take into consideration the specific aspects of interconnected devices, e.g., computing capacity, connectivity, energy consumption requirement, network configuration, to determine their ease of use in the digital infrastructure.

1.6 Structure of the thesis

To answer the research questions, the thesis is organized as follows:

- In Chapter 2, at first a review of the previous work of metrology traceability digital platform and infrastructure is carried out. Then an extensive state of the art on the DLT is provided. This also includes the integration between IoT and DLT technology analysis. By comparing the different nuances of DLT, i.e., the blockchain, and their applications, selection criteria are elaborated to evaluate the most suitable solution for the development of use cases of interest for the research questions asked in the previous paragraph.
- Chapter 3 focuses on the Digital Metrological Traceability Infrastructure. After an introduction to the concept of digital chain of traceability, compressive of the specific requirement and constraint, a proof of concept for a distributed metrology infrastructure is proposed with different approaches. Then a comparison between these approaches is carried out.
- In, Chapter 4 qualitative and quantitative analyses are performed to show the primary limitations of the proposed system in term of applicability to metrological field.
- Chapter 5 summarizes the conclusions of the thesis and suggests areas for future work.

Chapter 2

State of art and previous work

This chapter start reviewing existing research on field of digital metrology and set the base knowledge necessary to understand the context problems.

The second part of this chapter discuss digital identification problem, comparing existent solution with new distributed approach the exploit DLT.

The DLT technology's components, features, architecture, and scopes are presented in the first part of this chapter. This section also discusses the IoT and Blockchain integration solutions are discussed.

2.1 Digital Metrology Overview

2.1.1 The Measurement Information Infrastructure

The idea of a digital metrology infrastructure begins to emerge well before Industry 4.0. the concept of automation in calibration and test systems has been well established for decades. At the same time, for decades, the results of the operations related to the calibration testing process, the definitions of instrument specifications, and the scope of accreditation have been in paper format or through their equivalent in pdf or similar formats. As already highlighted since 2013 in [39] the automated system records the measurement results in a temporary file or database, but the data elements are unlikely to strictly relate to any standardized schemas universally recognized by end customer. Information is transferred to a paper or electronic document. Someone manually extracts and feeds the information into the subsequent processes. Incorporating humans into the process can lead to mistakes and costs and the possibility of transcription errors at either one or both ends. The same author then introduces the idea of a Measurement Information Infrastructure (MII) [40], underlining how the digitization process is very advantageous in reducing this risk. The definition of a semantic for metrological context significantly enhances the representation of metrological processes through the machine-readable aid data increasing precision. The paper outlines the basic structure of the Metrology information economy by identifying four fundamental actors, i.e., the manufacturer, the accreditation bodies(AB), the calibration laboratories (CL), and the end-user, and three fundamental objects of the metrological sphere, i.e., instrument specifications, scopes of accreditation (SoA), and the calibration certificates(Fig. 1).

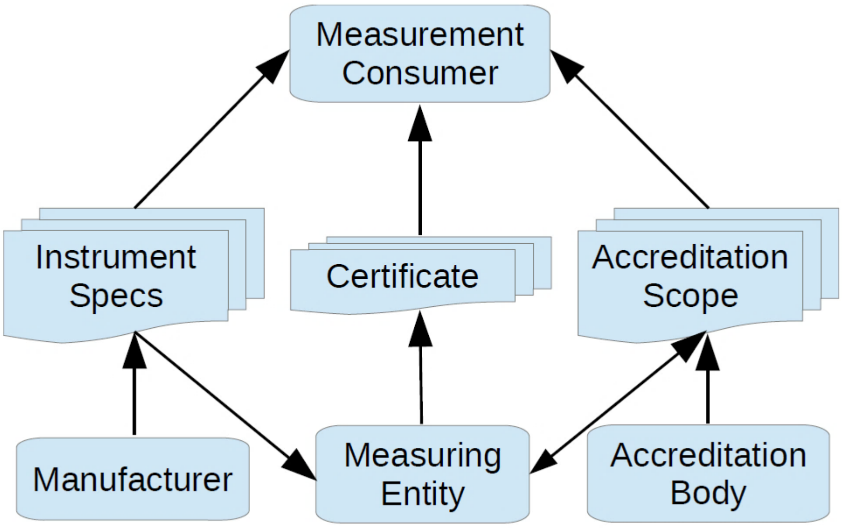


Figure 1 *Metrology Information Framework*

All documents can be described and then validated by a shared underlying semantics, making them interoperable from a digital representation point of view. An automated information economy is described as the process of applying computer science to metrology to enable all measurement-related software to produce, exchange and consume standardized semantic measurement information directly, and to generate human-readable summaries for monitoring and auditing.

This implies:

- Create a globally standardized infrastructure for creating, locating, communicating, and processing measurement information.
- Replace manually processed documents with unambiguous machine-readable data.
- Automated data validation in MII documents, e.g., administrative content, dates, traceability, accreditation status and scope, range and uncertainty, security signatures

- Lower the information barriers between testing & calibration labs, instrument manufacturers, vendors, Accreditation Bodies, and measurement consumers.
- Record traceability data back to the SI, itemize each intermediate calibration process uncertainty contributor, account for upstream correlations.

On the opposite the manual information economy due to its intrinsic human error propension implies:

- Weakly standardized taxonomies with high risk of misinterpretation.
- Labour-intensive processing that could be unfeasible in some case especially when we consider the high volume of production of IoTs devices
- Economically compromised data.

2.1.1.1 SoA data model

The first concrete outcome of this research is the definition of an XML schema for XML Schema for Accreditation Scopes [41] [42]. In Taxonomy for Meteorology [43] the author from the MII group define a standard for expressing the calibration laboratory capabilities, ISO/IEC 17025 Scope of Accreditation (SoA) in an XML formatted dataset. This XML schemas in combination with a set of released open software tools [44] allow the generation a traditional SoA document and automated verification of final uncertainties on a calibration test report to comply with a SoA.

In describing the model, the authors use a holistic approach to the problem. As already mentioned, all the elements in the metrological plan share a common semantics. The common denominator is identified in the taxonomy. The taxonomy hierarchy for identifying the metrological quantity that the generic document finds itself describing is as follows:

1. Measure/Source (required)
2. Measured quantity(required)
3. Subcategory

Subcategory

Subcategory

…

Two pieces of information are required to describe a metrological quantity: the value and its unit of measurement. The authors discuss the problem of the representation of units of measurement and the ambiguity that may arise from the superimposition of names, e.g., fpm can mean flash per second in optical measurements or feet per minute in speed measurements. The problem is solved by defining a dataset where the quantities are bounded to unit symbols and each symbol's full name. When a record is ambiguous for the end-user, the latter can consult the dataset available on the platform. At the same time, M2M communication, this ambiguity is not an issue precisely because in processing the data, the tools solve and validate the schema directly by referring to the dataset. It should be noted that this problem would not exist when the units are represented with reference only to the official SI-units. The complete scheme of the taxonomic representation can be described through the BNR[11] grammar:

Taxon ::= ProcessType . (Quantity | Ratio | Coefficient) [. Model]

ProcessType ::= Measure | Source

Quantity ::= RQK (. Descriptor)*

RQK ::= <any name in the quantity kind registry>

Descriptor ::= <any measurand-qualifying term>

Ratio ::= Ratio . Quantity

Coefficient ::= Coefficient.RQKn.RQKd (. Descriptorn)* (. Descriptord)*

Model ::= Model . ModelName

ModelName ::=

The following table shows some examples:

Table 1 *Example of Taxonomy*

MII Taxon	**Alias**
Measure.MassDensity.Solid	Density of solid
Measure.Pressure.Pneumatic.Absolute.Static	Absolute pressure, Gas medium
Source.Current.AC.Sinewave.3Phase	AC Current, Meters

[1] Backus-Naur form: “|” separates alternatives, “*” means zero or more consecutive instances, angle brackets enclose descriptive text, parentheses group tokens

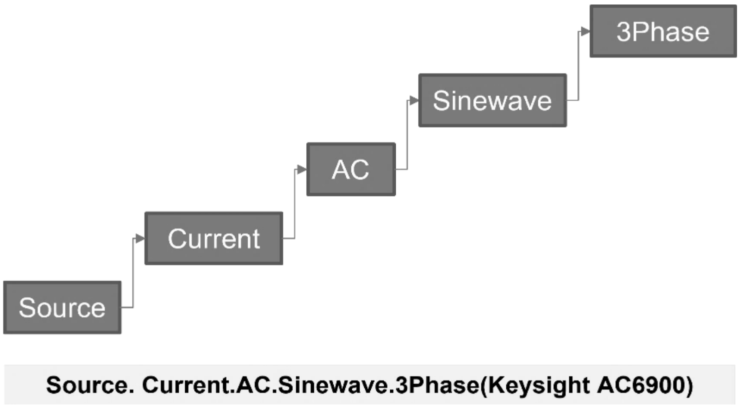


Figure 2 *Graphical representation of hierarchical record*

The scheme of the SoA document is structured in three basic elements, which are shown in the following image. Fig. 3 shows some examples:

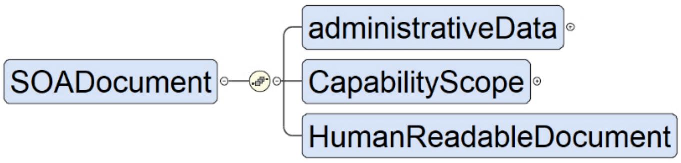


Figure 3 *SoA core elements*

The administrative data collects the information necessary to identify the accrediting body and that relating to the validity of the accreditation (Fig. 4).

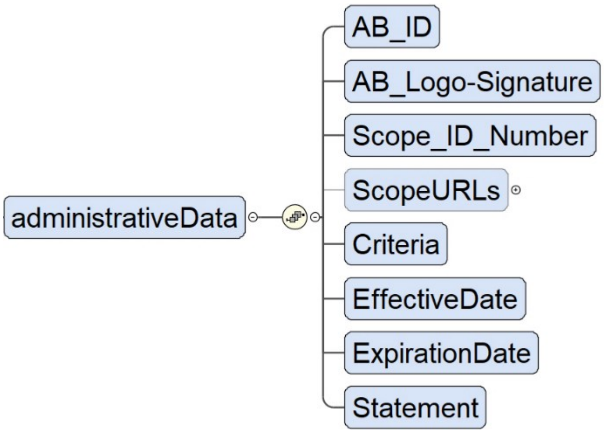


Figure 4 *Administrative data definition*

The capability scope characterizes the accreditation object, e.g., the calibration laboratory. The Calibration and Measurement Capabilitiy (CMC) field, in particular, describes all the accreditation scope for which the laboratory is authorized to issue calibration certificates. The CMCs are the container that structures the table reported in the paper certificates of the SOAs. The CMC structure is shown in Fig. 5.

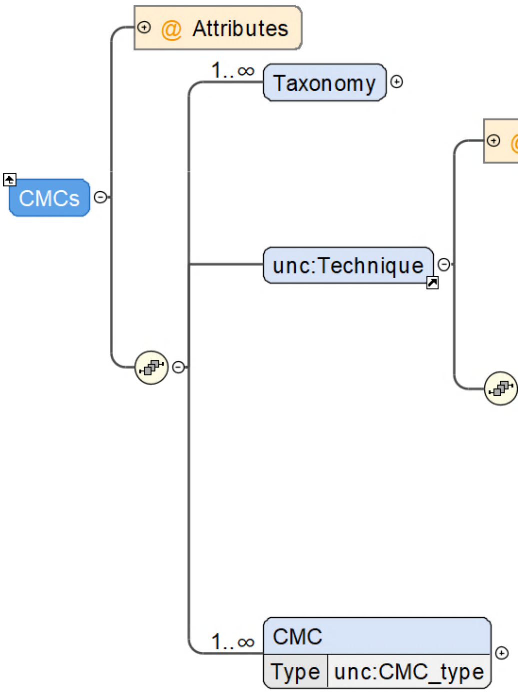


Figure 5 *CMCs definition*

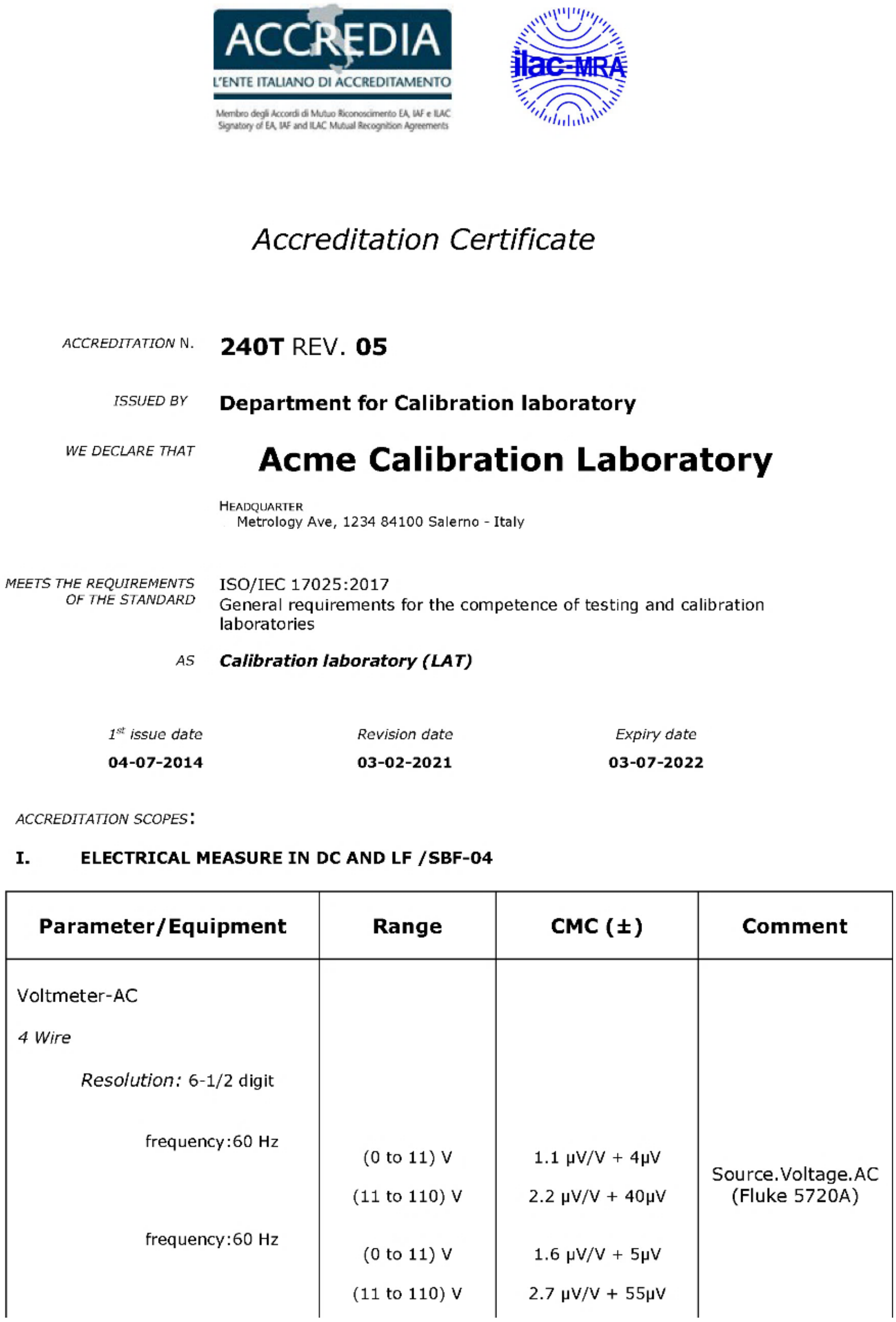
In particular:

- Taxonomy describes the type of measure to be represented, e.g., Measure.Voltage.AC.

- The technique specializes measurement by providing the metadata necessary to describe the records of the specific measurement, including the nominal specifier, e.g., Measure.Voltage.AC.LowVoltage, the maximum range of application, the specific parameters for the measurement, the representation of uncertainty.

- The CMC represents the actual records in which each element represents a set of data that respect the structure of the metadata provided in the technique.

Let us assume we have the following certificate (Fig. 6):



ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO
Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
Signatory of EA, IAF and ILAC Mutual Recognition Agreements

ilac-MRA

Accreditation Certificate

ACCREDITATION N. **240T** REV. **05**

ISSUED BY **Department for Calibration laboratory**

WE DECLARE THAT **Acme Calibration Laboratory**

HEADQUARTER
Metrology Ave, 1234 84100 Salerno - Italy

MEETS THE REQUIREMENTS OF THE STANDARD ISO/IEC 17025:2017
General requirements for the competence of testing and calibration laboratories

AS ***Calibration laboratory (LAT)***

1st issue date	*Revision date*	*Expiry date*
04-07-2014	**03-02-2021**	**03-07-2022**

ACCREDITATION SCOPES:

I. ELECTRICAL MEASURE IN DC AND LF /SBF-04

Parameter/Equipment	**Range**	**CMC (±)**	**Comment**
Voltmeter-AC *4 Wire* *Resolution:* 6-1/2 digit			
frequency:60 Hz	(0 to 11) V (11 to 110) V	1.1 µV/V + 4µV 2.2 µV/V + 40µV	Source.Voltage.AC (Fluke 5720A)
frequency:60 Hz	(0 to 11) V (11 to 110) V	1.6 µV/V + 5µV 2.7 µV/V + 55µV	

Figure 6 *Scope of Accreditation Certificate example.*

An extract of the equivalent XML model is shown:

<soa:SOADocument>

```
  The administrative part
<soa:administrativeData>
<soa:AB_ID> ACCREDIA_IT</soa:AB_ID>
<soa:AB_Logo-Signature/>
<soa:Scope_ID_Number> SBF-04</soa:Scope_ID_Number>
<soa:Criteria>ISO/IEC 17025:2017</soa:Criteria>
<soa:EffectiveDate>3/02/2021</soa:EffectiveDate>
<soa:ExpirationDate>3/07/2022</soa:ExpirationDate>
<soa:Statement/>
</soa:administrativeData>
<soa:CapabilityScope>
<soa:MeasuringEntity>Acme Calibration Laboratory
</soa:MeasuringEntity>
<soa:Location>
<soa:OrganizationAddress>
<soa:Street>1234 Metrology Ave</soa:Street>
<soa:City>Salerno</soa:City>
<soa:State>Italy</soa:State>
<soa:Zip>84100</soa:Zip>
</soa:OrganizationAddress>
</soa:Location>
  The scope of accreditation
<soa:Activities>
<soa:Activity>
<unc:CMCs>
<mtc:Taxon name="Measure.Voltage.AC">
<mtc:Result>
<uom:Quantity name="voltage"/>
</mtc:Result>
<mtc:Parameter name="frequency">
<uom:Quantity name="frequency"/>
</mtc:Parameter>
</mtc:Taxon>
<unc:Technique
name="Measure.Voltage.AC.LowVoltage">
</unc:Technique>
<unc:Switch>
<unc:Case>
<unc:Assertion>
<unc:Name>Resolution</unc:Name>
<unc:Value>6-1/2 digit</unc:Value>
</unc:Assertion>
```

```
<unc:Assertion>
<unc:Name>Connection</unc:Name>
<unc:Value>4 Wire</unc:Value>
</unc:Assertion>
<unc:Ranges variable_name="frequency"><unc:Range>
<unc:Start test="at">60</unc:Start>
<unc:End test="at">60</unc:End>
<unc:Ranges
variable_name="nominal"variable_type="parameter">
<unc:Range>
<!-- row 1 -->
<unc:Start test="at">0</unc:Start>
<unc:End test="at">11</unc:End>
<unc:ConstantValue const_parameter_name="k_nominal>
0.0000011</unc:ConstantValue>
<unc:ConstantValue const_parameter_name="k_range"
>0.000004</unc:ConstantValue>
</unc:Range>
<unc:Range>
<!-- row 2 -->
<unc:Start test="after">11</unc:Start>
<unc:End test="at">110</unc:End>
<unc:ConstantValue const_parameter_name="k_nominal"
>0.0000022</unc:ConstantValue>
<unc:ConstantValue const_parameter_name="k_range"
>0.000045</unc:ConstantValue>
</unc:Range></unc:Ranges></unc:Range></unc:Ranges>

   …
```

2.1.1.2 The Internet of Measurement things , the architectural framework

The efforts of the MII group are mainly related in defining the data models for the digital representation of the semantics and the taxonomy of the metrology word while Nikoo et all [45] concretely discuss the architectural framework of Digital Metrology Infrastructure for calibration industries. The discussion considered the emergent requirements driven from Industry 4.0 and IIoT for a high degree automation process in the field of calibration that could reduce the time to market without compromising the product quality. In the analysis the authors consider a well-known existing service, Metrology.Net. The Metrology.NET automated calibration system is a distributed platform for the testing and calibration process. Based on modular approach for data management and metrology automation, it is designed to be a system of systems to bridge the gap between various types of metrology software applications currently used at calibration labs. The system is a client-server platform that uses a central hub and a series of agents distributed in the various laboratories configured locally to perform calibration tasks which are then processed centrally. Fully automated calibration increases the calibration labs' capabilities in productivity, and accuracy thanks to the standardization of the platform. A calibration task can be seen as the collection results of a specific set of test points. Once test results are collected for all test points, the calibration job can be considered complete, and the system can review the collected data and certify the instrument. By integrating the standardized data model proposed by the MII group, with a reference layered architecture for IIoT proposed by Industrial Internet Consortium (IIC) [46], the authors define a three-tiered architecture (see Fig.7) framework containing,

- Physical Layer: performing the data collection.
- MII Cloud Services Layer : performing data analysis and organization.
- Application Layer: responsible of processing information and provide the services.

The authors focus on automation services related to calibration and the issue of the accreditation certificate. However, no indications are given on the concrete implementation or proof of concept of the system. However, it is pointed out that the proposed system has the great advantage of making metrological knowledge available in a distributed form against the current silos-based system.

2.1.2 The European Initiatives

At the European level, the most crucial initiative in the metrology field is the European Metrology Cloud, intending to support conformity assessment and market surveillance services. It allows the development of new technology-driven services and reference architectures for an infrastructure that enhances the development of a single digital market, an objective strongly supported by the European Commission [8].

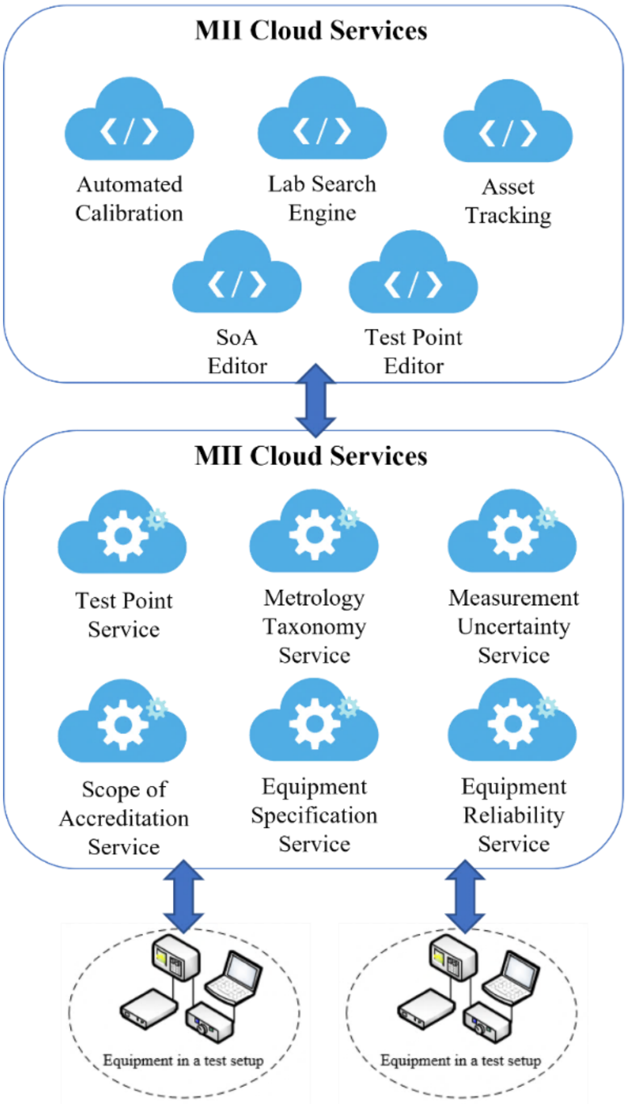

MII Cloud Services
Automated Calibration
Lab Search Engine
Asset Tracking
SoA Editor
Test Point Editor
MII Cloud Services
Test Point Service
Metrology Taxonomy Service
Measurement Uncertainty Service
Scope of Accreditation Service
Equipment Specification Service
Equipment Reliability Service
Equipment in a test setup
Equipment in a test setup

Figure 7 *MII Cloud Architecture*

The primary point of the proposal is establishing a data infrastructure for European metrology using a trustworthy "core" -platform in the member states. Commonly to the project of the MII, two fundamental points are identified to allow the birth of such an infrastructure:

- Common data model: necessary to allow the silent recognition of information traveling in the infrastructure and to allow the exchange of services.

- An architectural framework that allows establishing communication protocols, storage systems, and information flow control policies.

To this end, the PTB has set up a series of research projects to investigate and develop solutions for digitalization in the metrology field. For the first objective, the most important project is SmartCom which develops a universal model of representation of metrological quantities known as the Digital International System of Unit (D-SI) [11]. The model developed refers to the international system of SI measurement, to VIM [22], to GUM [47] and to CODATA [48], the international standards and principles for the representation of metrological quantities. The second important result of the same research group is the digital calibration certificate (DCC). The DCC provides a model compliant with the ISO-IEC 17025 standard [24], i.e., the reference standard in the context of accreditation and certification. The DCC provides a metadata schema in the form of an XML schema that enables the following properties to the certificates:

- **Validity**: the certificate can be validated to a commonly recognized scheme. From a formal point of view, every error is identified in an automated way and no longer through a human operator, significantly reducing the risk of transcription errors.

- **Verifiability**: one of the properties required to transmit a document in digital form is authenticity and the ability to trace its origin. The DCC, therefore, requires the use of a digital signature by the issuing authorities.

- **Interoperability**: through the XML format, the certificate is machine-readable, so once produced, it can be processed directly by electronic and computer systems without the human operator being forced to carry out the transcription operation.

Compared to the approach used by MII, the SmartCom approach is more restrictive about the representation of units of measurement. The D-SI exclusively use the seven fundamental units, while for the derived units, it defines a formal algorithm that can be verified through the TraCIM system [49] [50]. Contrary to the MII digital system for the representation of quantities, the D-SI resolves the problem of the ambiguity of the a priori measurement by excluding measures that are not universally recognized. The advantage is the reduction of the resulting ambiguities and the number of metadata to be stored in the digital metrological vocabulary.

2.1.2.1 D-SI and DCC data model

The XML schema of the D-SI builds the necessary foundation for a unique representation of the metrological quantities in digital form. To do this, the D-SI establishes the set of possible representable quantities shown in the diagram in Fig. 8.

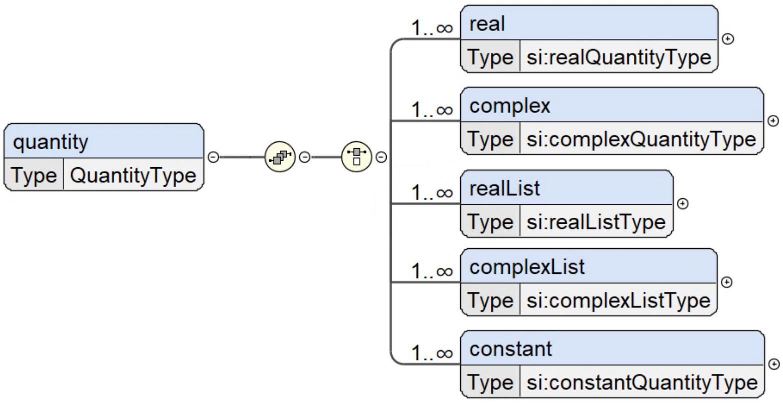


Figure 8 *D-SI quantities*

In addition to the real and complex quantities, the scheme also provides the representation of vector and matrix in the form of lists necessary in the case of aggregate data, which is very common in activities related to metrology where repeated measurement is essential to ensure a reasonable degree of approximation. Going into more detail, we focus on the case of real quantity (Fig. 9).

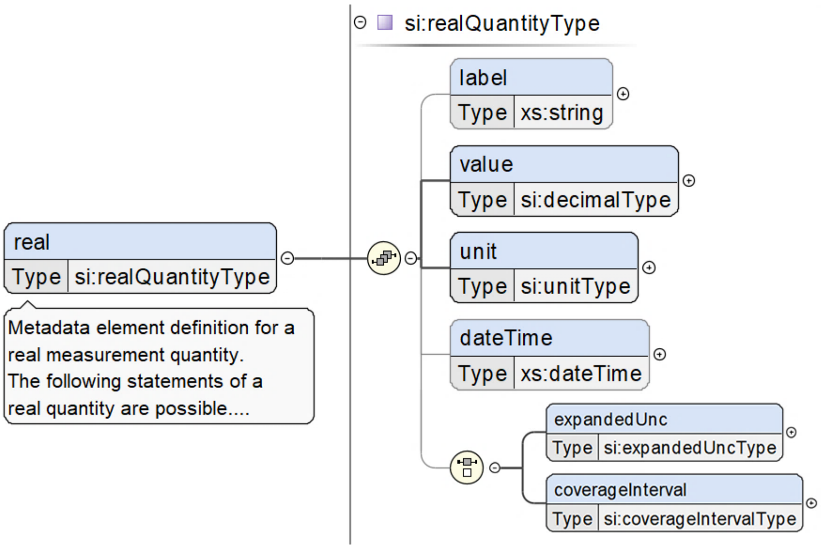


Figure 9 *D-SI real quantity XML definition*

As can be seen from the diagram, a real quantity (or more generally a metrological quantity) requires two necessary elements, i.e., The value and the unit, and a series of optional elements, including measurement uncertainty. To be fully characterized, the record of a metrological quantity must have all the fields described above. The definition of the SI unit refers to the most recent BIMP Brochure [51].

Once the D-SI scheme has been defined, we can move on to the description of the DCC. According to what is defined in the official brochure [11] the DCC is structured in four layers and is presented in Fig. 10.

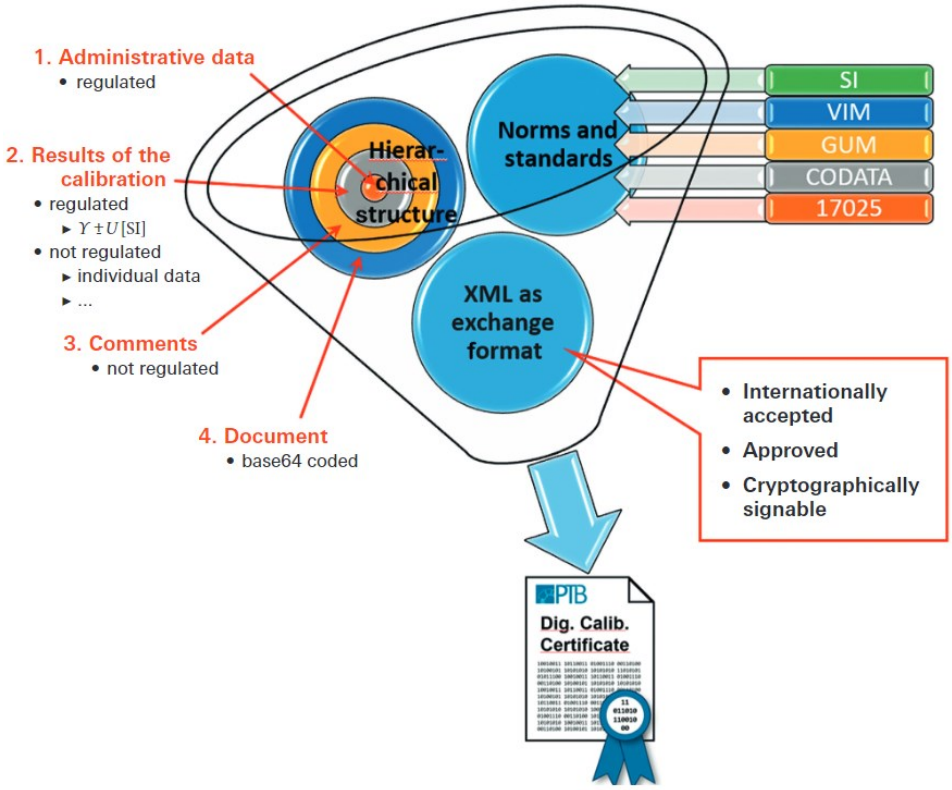


Figure 10 *DCC conceptual scheme [11].*

These layers include both mandatory and optional unregulated additional information that is not necessarily machine-readable, e.g., the calibration certificate digital URL.

Summarizing the layers functionality:

- Administrative shell: This layer is regulated data. It includes mandatory information to make the DCC identifiable, including the unique DCC ID and identification of the calibration laboratory, customer, and items.
- Calibration results: Calibration results: This layer is regulated and contains measurement results following the D-SI format rules [52] [50] [53] . It also contains Individual calibration information considering influence conditions, calibration methods, and individual results.
- Individual information It includes general, optional, and additional comments and calculation tables and graphics for any data format, which the recipient typically requests.
- Optional attachment: A human-readable file can be stored here (e.g., PDF format). This layer will not allow for machine-reading.

The xml structure is shown in Fig 11.

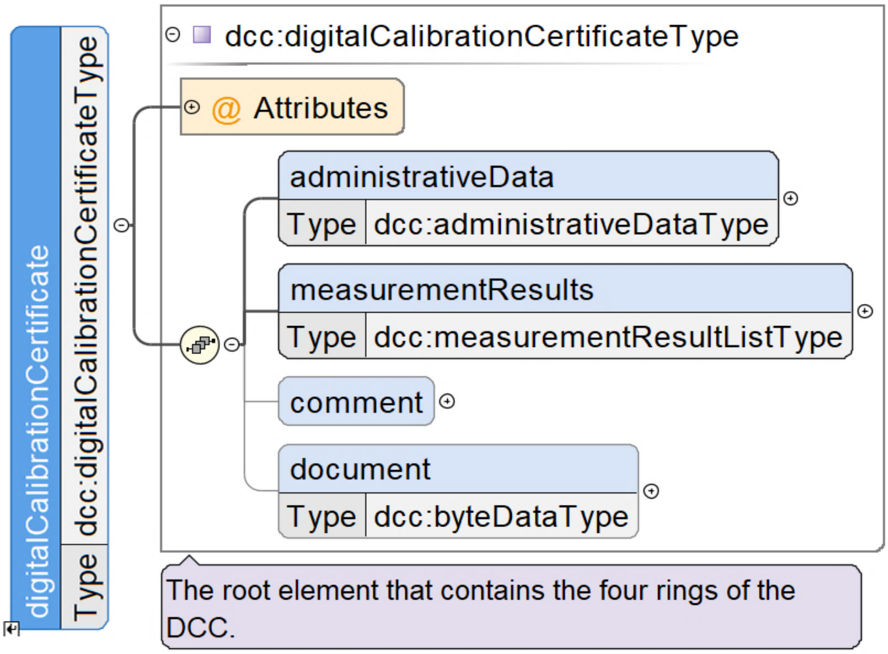

digitalCalibrationCertificate
Type dcc:digitalCalibrationCertificateType
dcc:digitalCalibrationCertificateType
@ Attributes
administrativeData
Type dcc:administrativeDataType
measurementResults
Type dcc:measurementResultListType
comment
document
Type dcc:byteDataType
The root element that contains the four rings of the DCC.

Figure 11 *DCC xml schema basic structure.*

The organization of the second layer is of essential importance. Fig11 shows the diagram's structure relating to the single measurement result. Each result must be described by a series of identifiers, e.g., name, description, methods used, instrumentation used, conditions of influence, and metadata relating to the measures themselves. Then the actual numerical results of the measurements are reported through the container results, where the metrological quantities are reported following the D-SI scheme.

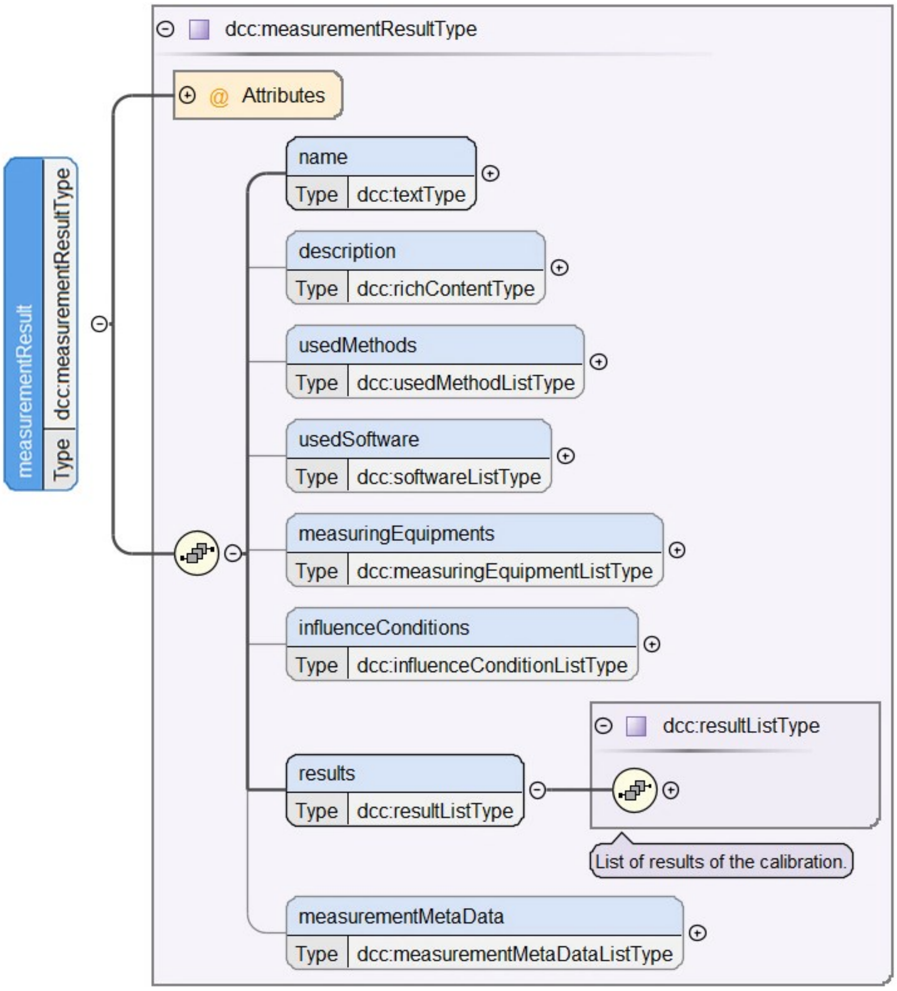

dcc:measurementResultType
Attributes
measurementResult
Type dcc:measurementResultType
name
Type dcc:textType
description
Type dcc:richContentType
usedMethods
Type dcc:usedMethodListType
usedSoftware
Type dcc:softwareListType
measuringEquipments
Type dcc:measuringEquipmentListType
influenceConditions
Type dcc:influenceConditionListType
results
Type dcc:resultListType
dcc:resultListType
List of results of the calibration.
measurementMetaData
Type dcc:measurementMetaDataListType

Figure 12 *DCC measurement results XLM schema definition*

Following is an example in XML format of the calibration certificate of a temperature sensor.

```
Layer 1

<dcc:administrativeData>
<dcc:coreData>
<dcc:countryCodeISO3166_1>DE</dcc:countryCodeISO3166_1
>
```

```
<dcc:usedLangCodeISO639_1>en</dcc:usedLangCodeISO639_1
>
<dcc:uniqueIdentifier>GP_DCC_temperature
</dcc:uniqueIdentifier>
<dcc:issuer>calibrationLaboratory</dcc:issuer>
<dcc:receiptDate>1957-08-13</dcc:receiptDate>
<dcc:beginPerformanceDate>1957-08-
13</dcc:beginPerformanceDate>
<dcc:endPerformanceDate>1957-08-
13</dcc:endPerformanceDate>
<dcc:performanceLocation>laboratory</dcc:performanceLo
cation>
</dcc:coreData>

  The subject of calibration
<dcc:item>
<dcc:content lang="en">Temperature
sensor</dcc:content>
</dcc:item>
<dcc:manufacturer>
<dcc:name>
<dcc:content>NationalInstrument</dcc:content>
</dcc:name>
</dcc:manufacturer>
<dcc:model>EWR3547</dcc:model>
<dcc:issuer>customer</dcc:issuer>
<dcc:value> customer-item</dcc:value>
<dcc:name>
<dcc:content lang="en">Measurement equipment no
567.</dcc:content>
</dcc:name
<dcc:issuer>calibrationLaboratory</dcc:issuer>
<dcc:value> calibrationLaboratory-item</dcc:value>
<dcc:name><dcc:content lang="en">Equipment no
867.</dcc:content></dcc:name>
<dcc:item>

  The issuer of calibration
<dcc:calibrationLaboratory>
<dcc:contact>
<dcc:name><dcc:content>Kalibrierfirma
GmbH</dcc:content></dcc:name>
<dcc:eMail>info@kalibrierfirma.xx</dcc:eMail>
<dcc:phone>+49 123 4567-89</dcc:phone>
<dcc:location>
<dcc:city>Musterstadt</dcc:city>
<dcc:countryCode>DE</dcc:countryCode>
<dcc:postCode>00900</dcc:postCode>
<dcc:street>Musterstraße</dcc:street>
<dcc:streetNo>1</dcc:streetNo>
```

```
</dcc:location>
</dcc:contact>
</dcc:calibrationLaboratory>

  The customer of calibration
<dcc:customer>
<dcc:content>KundeGmbH</dcc:content>
<dcc:eMail>info@kunde.xx</dcc:eMail>
<dcc:location>
<dcc:city>Musterstadt</dcc:city>
<dcc:countryCode>DE</dcc:countryCode>
<dcc:postCode>00900</dcc:postCode>
</dcc:location>
</dcc:customer>
</dcc:administrativeData>

  Layer 2

<dcc:measurementResult>

  Here methods describe hoe the conformity is
evaluated
<dcc:usedMethods>
<dcc:usedMethod refType="basic_uncertainty"/>
<dcc:usedMethod refType="gp_temperatureSensor">
<dcc:norm>DKD-R 5-1:2018</dcc:norm>
</dcc:usedMethod>
</dcc:usedMethods>

  Reference instrument
<dcc:measuringEquipments>
<dcc:measuringEquipment refType="basic_normalUsed">
<dcc:content lang="en">Pt 100
thermometer</dcc:content>
</dcc:measuringEquipment>
</dcc:measuringEquipments>
<dcc:results>

  Representation of the calibration data table
<dcc:result refType="gp_measuringResult1">
<dcc:data>
<dcc:list refType="gp_table1">
<dcc:quantity refType="basic_referenceValue">
<dcc:content lang="en">Reference value</dcc:content>
<si:realListXMLList>
<si:valueXMLList>306.248 373.121 448.253 523.319
593.154</si:valueXMLList>
<si:unitXMLList>\\kelvin</si:unitXMLList>
</si:realListXMLList>
<dcc:measurementMetaData>
<dcc:metaData refType="basic_calibrationValue">
```

```
<dcc:declaration>
<dcc:content lang="en">Calibration value</dcc:content>
</dcc:declaration>
<dcc:data><dcc:quantity><si:realListXMLList>
<si:valueXMLList>306 373 448 523 593</si:valueXMLList>
<si:unitXMLList>\\kelvin</si:unitXMLList>
</si:realListXMLList></dcc:quantity></dcc:data>
</dcc:metaData>
</dcc:measurementMetaData>
</dcc:quantity>
<dcc:quantity refType="basic_measuredValue">
<dcc:content lang="en">Indicated measured value
probe</dcc:content>
<si:realListXMLList>
<si:valueXMLList>306.32 373.21 448.36 523.31
593.07</si:valueXMLList>
<si:unitXMLList>\\kelvin</si:unitXMLList>
</si:realListXMLList>
</dcc:quantity>

<dcc:quantity refType="basic_measurementError">
<dcc:content lang="en">Measurement error</dcc:content>
<si:realListXMLList>
<si:valueXMLList>0.072 0.089 0.107 -0.009 -
0.084</si:valueXMLList>
<si:unitXMLList>\\kelvin</si:unitXMLList>
<si:expandedUncXMLList>
<si:uncertaintyXMLList>0.061</si:uncertaintyXMLList>
<si:coverageFactorXMLList>2</si:coverageFactorXMLList>
<si:coverageProbabilityXMLList>0.95</si:coverageProbab
ilityXMLList>
<si:distributionXMLList>normal</si:distributionXMLList
>
</si:expandedUncXMLList>
</si:realListXMLList>

Conformity statement
<dcc:metaData refType="basic_conformity">
<dcc:conformityXMLList>PASS</dcc:conformityXMLList>
</dcc:metaData>
</dcc:measurementMetaData>
</dcc:quantity></dcc:list></dcc:data></dcc:result>/dcc
:results>
</dcc:measurementResult>
```

2.1.2.2 Metrological Service Ecosystem Platform

Similarly to the work done in [45] Opperman et all. [54] also introduce a platform model based on a distributed architecture for consolidating metrological services at the European Project level. The authors' proposal aims to provide a detailed model of the infrastructural architecture that guarantees the properties of flexibility, safety, and interoperability. They consider two fundamental aspects of the metrological context: the extreme variety of pre-existing infrastructures and the need to guarantee a high degree of security in accessing services and data management. Most of the data and information processed are subject to strict legal regulations. For instance, calibration certificates have a high legal value as they help define the validity of the minimum requirements for production equipment, e.g., industrial plants. This indirectly determines the validity of the Declaration of Conformity documents issued with a product by manufacturers, according to the "New Legislative Framework" of the European Union [55]. The infrastructure proposed by Opperman et al., I.e., AnGeWaNt is designed and implemented according to the Service-oriented architecture, a software architecture model which classifies software components as services. These services are distinct units, stateless, loosely coupled, and can be combined flexibly. The units communicate via REST (REpresentational State Transfer). REST requires HTTP- or HTTPS-based communication without adding additional protocols.

The proposed platform exhibits three independent modules:

- **AnGeWaNt platform** is made of a web-based user interface and services. A separate application container is used for each service allowing independent deployment, maintenance, and operation according to the software separation requirement (S1) of WELMEC 7.2 Software Guide [30].The list of services and their functionality are reported in table x. Among the provided services the platform exposes:

    a. Declaration of conformity request service

    b. Software update request service

    c. Device Specification request service

    d. Digital Calibration request service

- **User management module** is made of the user manager and token manager services. All user-related data is decoupled from any specific application and stored in a separate database. This ensures the protective software interface requirement (Software Separation Requirement S3) outlined in the WELMEC 7.2 Software Guide

[30].Because the highly distributed nature of the architecture it is session free, and token based. Tokens are assigned to either a user or a device which authenticate themselves, or a service to prove its authenticity. All authentication and authorization are encoded in a standard JWT (JSON Web Token), and it is generated after successful login. It provides single sign on (SSO) for all authorized applications and services within the AnGeWaNt platform.

- **Cross functional module** is made of two service in charge of services intercommunication, i.e., the document storage service and the common principal data service. The former hosts all documents related to a specific measuring instrument. It acts as a revision-safe archive store that will meet the legal archive obligations for measuring instruments throughout their life span and enable traceability. It also allows data owners to specify access role policy to establish privacy and security. The common principal data service handles information from manufacturers, notified bodies, authorities, users, measuring instruments, and device types are used across different types of processes and documents. It is accessible through the front-end to fill in e.g., a calibration update request. This service is the essential component to facilitate the user experience.
- **External infrastructure module** is a restful interface that ties third-party systems, e.g., the manufacturers' systems, to AnGeWaNt to provide interoperability.

The solution proposed by Opperman et all. is more complete compared to MII case. They also discuss the security aspect by identifying three attack vectors: WEBXSS (Cross-site scripting attack), AWEBDOS (Denial-of-Service attack), and AWEBSOCKET (introducing malicious code via web socket). The authors state that the platform is resilient to WEBXSS and AWEBSOCKET while resistance to AWEBDOS depends on the infrastructure implementation.

2.1.3 Benefits of network effects and interoperability for metrological services

Both projects highlight the great advantage of digital metrological transformation when carried out with a new distributed paradigm. On the opposite, in the existing system, data are collected in isolated silos, and the relationships between stakeholders (e.g., instrument owners, manufacturers, or service providers) have been mainly bilateral. Point-to-point solutions allow full control but are more resource intensive in development and maintenance. On the opposite shared platform will enable system integration efficiencies. When digital platforms became the central point for organizing the interaction and operations between consumers, providers and developers of goods or services we call this phenomenon Platform economy [56]. This new business model is based on the creation of data starting from the interactions between stakeholders.

Platform's economy can be classified based on the way they create value. Three main types can be distinguished:

- **Increasing options:** for goods and services exchanging, e.g., Amazon and eBay that provide a broad selection of products.
- **Complementarity:** based on innovation, operating systems and cocreation, e.g., in Google Android where majority of the value is created by the complements provided by the third-party application developers.
- **Quantity:** In these platforms the value increases as new users join to the network, e.g., Facebook and PayPal, or by the total amount of content in the platform like in Wikipedia, Scopus, Elsevier.

Providing network effects to the players in the ecosystem will enable system integration efficiencies considering that:

- only one integration to the shared platform is needed decreasing required development efforts and costs,
- data and system compatibility are established for all partners in the ecosystem. Shared platform requires a shared vision of the solution and interest from the parties to use common tool,
- the traceability of the certificate will improve as all the certificates are stored in a shared platform,
- a wider use of calibration data is established. Sharing non-critical and anonymized data within the ecosystem improves the data quality for any individual user as, e.g., uncertainty information can be compared against a larger peer group.

The previously proposed metrology platform architectures, i.e., MIII and AnGeWaNt, implement at least the first and third value creation increasing competitiveness in the modern digital market.

However, to be effective, the platform-based approach needs to expose the following key features:

- **Long-Term Storing**: digital metrology certificates is the medium to store and transfer metrology certificate data from issuer to instrument owner and usually is mandatory for both. For instance, Calibration certificates are crucial in quality assessment, and therefore they need long term archaization.

- **Document Management** : To enable full data integrity for the document data management, process needs to be digitalized as a closed loop process. Platform act as communication hub for both certification requests and issuance. The whole process can be done without any manual entries that endanger the data integrity.
- **User management** : It is needed to manage stakeholder relationships, access rights, visibility rules and signature rights. It could be successfully achieved by integrating to the existing user management systems in organization's system architecture or establishing a new distributed one.
- **Integration API** : The platform should be interoperable to the existing systems like calibration management and production, quality, and maintenance systems with APIs. The degree of integration should be flexible based on the number of services required
- **Version management** : The global digital documents standard will potentially have different versions in the future - that is normal for any digital file format as the needs evolve. Backward and forward compatibility should be granted. This is especially important to manufacturer who need to support several versions in their products.
- **Harmonized digital documents** : issuers need platform features to create a standardized format XML file from the metrological data and to sign the XML file to authorize the results. The creation of the XML file can be done automatically from the data.
- **Signing digital documents** : Digital certificates should be secured with cryptographical digital signatures. For instance, for calibration laboratory or accredited body it is essential to have the ability to trace the signature back to the issuer which creates the trust in the calibration certificates.
- **Verification** : The verification feature is required to verify the origin of the data and the data integrity. The origin of the data is ensured with, e.g., PKI infrastructure used to sign the data. The data integrity is ensured by validating the digital signature and the data schema.

2.2 Digital Identities Paradigms

The proposed initiatives emphasize the importance of a standard data model and focus on a cloud paradigm that allows easy integration of the platform's services from an architectural point of view. The distributed approach is compelling, given the dimensionality of the problem. We report an estimate of the cardinality of the stakeholders in the metrological domain. [45]:

- **Accreditation Body** : 10E1.
- **Measurement Entity** : 10E3.
- **SoA document** : 10E3.
- **Manufacturer** : 10E4.
- **Instrument Specification Document** : 10E7.
- **Calibration Certificate** : 10E10.
- **Measurement consumer** : 10E5.

This estimate is downward and not updated, but it is already sufficient to demonstrate how the monolithic approach is less suitable to meet the demand in the metrology market.

Both solutions also hint at the need to establish security protocols for communication, identification, and role management considering the various entities that cooperate on the network, the types of information, legal and non-legal, private, and public. To guarantee the authenticity of the data and allow its secure transmission, the use of a certified digital signature, e.g., Qualified electronic signature (QeS) or European EiDAS seal [57], as well as exploiting the underlying TLS security protocol. These systems are based on the concept of Trusted Authority or Trusted Third Party, i.e., they are centralized or hierarchical systems. Every time a user needs to access a service or connect over a secure layer it needs to contact a central authority who certifies the user identity.

The newly decentralized concept of Self Sovereign Identity proposes a new digital identities paradigm where user control directly control their identities, and any other "attribute" that a person may possess. The theme has a disruptive significance in the digital ecosystem , if only one thinks that what the current Internet lacks, is precisely a layer of verification of identity of the subjects interacting on the network.

When the Internet was created in the DARPA laboratories, the main problem was to create a "network of networks". The TCP / IP protocol has served this purpose very well, but this protocol only identifies the address of the computer that is connected to the network, but says nothing about the person, organization or thing that uses that computer and that interacts online through it. To solve this problem, models have therefore been introduced to identify online actors. The first is a centralized model in which to create an identity it is necessary to register an account with the person who provides the online services. This causes various problems: the multiplication of identities, the fact that that account exists only on the servers of that subject, thereby making it impossible to access the services if the account is canceled, the total absence of control over the data by of the person holding the account, the widening of the attack surface for possible identity theft.

The next model, which has developed to deal with these problems, is that of federated identity. In this case, a third party (Identity Provider - IdP) is inserted between the service provider and the person who intends to use them. The latter will have an identity (account) registered with the IdP and will be able to use the services provided by third-party sites without having to re-register on their sites, but by accessing through said identity. The federated identity model is the one we use through the so called "Social login", i.e., by accessing a platform or site using the identity we have registered on one of the most popular social networks or platforms. It should be noted that this model is the one used in Italy (and in Europe in general) through the SPID (Public System of Digital Identity), where some subjects they perform the role of Identity Provider and based on requests from the various service providers, provide the identification data of the person using SPID by "passing" said data for the purpose of identifying the same. However, the federated model also presents some problems. One of the most obvious is what occurred with Public Digital Identity System (SPID): given that the user is free to decide the IdP with which to activate a digital identity, the service provider must necessarily interface with as many IdPs as possible, since otherwise would be able to identify the user . For non "institutional" identity services such as SPID, however, the opposite problem occurs not all online services accept the same Identity Providers IdPs, and it is therefore the user who is forced to create multiple digital identities with different suppliers. Furthermore, it must be considered that the most important IdPs are one of the biggest targets for attacks by hackers and, therefore, one of the biggest causes of online identity theft. Third , federated digital identities are no more "portable" than centralized ones. If the account on Google or Facebook is canceled (as well as an account with a SPID IdP) it will no longer be possible to access the services nor, on the other hand, transfer one's identity to another IdP (but it will be necessary to activate one new). Finally, Identity Providers such as Google or Facebook, for reasons of security and protection of personal data, are not able to help users securely share the most "sensitive" information, such as identity documents, health data, financial data.

The Self Sovereign Identity (SSI) is a third model, decentralized and made possible thanks to distributed ledger technologies, the DLT. The major novelty of this model is that it is no longer “account-based”, but that it operates in the same way as real identity. It is based, in fact, on a direct relationship with the party that needs to verify an attributor (identity or other) of the SSI holder, but unlike the previous models none of the parties involved must register an account. Rather, the SSI model is about sharing a connection that persists if the parties intend to maintain it; when the need for identification ceases, the connection fails, and the "data" are no longer available to the person who authenticated. Additional key concepts in SSI are Verifiable Credentials (VC) [58] with which certain attributes of a subject or other types of information relating to him are "certified" (for instance, possession of a driving license, possession of a school, a pilot's license, a birth certificate, etc.). In this case we have a trilateral relationship, in which on the one hand there is the one who issues the credentials (the public but also private body that "certifies" a certain status), the "owner" of the credentials, to which they are issued and that he can keep in his wallet, and, finally, the one to whom the credentials are presented. To allow the authenticity of credentials to be checked, the SSI model provides for the use of "decentralized identifiers" (DIDs) [59], i.e. identifiers of the subjects who issue verifiable credentials that have the characteristic of being permanent , cryptographically verifiable, decentralized and "solvable" that is, able to identify not only the public key of the issuer but also the address connected to it.

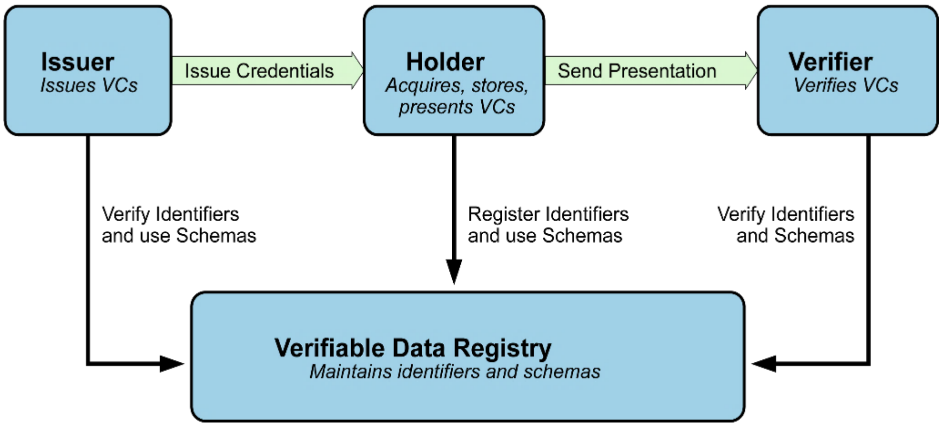

Issuer
Issues VCs
Issue Credentials
Holder
Acquires, stores, presents VCs
Send Presentation
Verifier
Verifies VCs
Verify Identifiers and use Schemas
Register Identifiers and use Schemas
Verify Identifiers and Schemas
Verifiable Data Registry
Maintains identifiers and schemas

Figure 13 *SSI ecosystem*

It is important to underline that the DIDs have already been implemented in the W3C context and therefore, already constitute a "standard".

SSI were expressly taken into consideration in the European Parliament Report on distributed ledger technologies of 2018 [60], which expressly underlined :

" DLT supports the creation of new models in order to change the current concept and today's digital identity architecture;"

and it was noted

" Digital identity extends to people, to organizations and objects and further simplifies identity processes such as "Know your customer", while allowing personal control over data".

2.2.1 Decentralized identifier (DID)

At a high level, a decentralized identifier (DID) is simply a new type of globally unique identifier with special features designed for blockchains. But at a deeper level, DIDs are the tip of the iceberg of an entirely new layer of decentralized digital identity and public key infrastructure (PKI) for the Internet. This decentralized public key infrastructure (DPKI) could have as much impact on global cybersecurity and cyberprivacy as the development of the SSL/TLS protocol for encrypted Web traffic (now the largest PKI in the world).

In the history of the Internet, every identifier that is both globally unique and globally resolvable -- meaning you can look it up and obtain metadata about the resource it identifies -- has required some type of centralized administration. For example, both IP (Internet Protocol) addresses and DNS (Domain Name System) names -- the foundations for the Internet and the Web -- require centralized registries and registrars.

Although these centralized systems are very efficient, this architecture has long been recognized as both a single point of control (and thus potential censorship) and a single point of failure. So, in the last few years, several groups began independently investigating decentralized alternatives. UUIDs (Universally Unique Identifiers) developed in the 1980s, was the first kind of not centralized authority-based identifier (IETF RFC 4122 [61]). The need for is also not new. This class of identifiers was standardized as Then URNs (Uniform Resource Names) was the first kind of persistent identifiers for entity (RFC 8141 [62]). However, UUIDs are not globally resolvable and URNs, if resolvable, require a centralized registration authority. Also, neither UUIDs nor URNs can inherently cryptographically verify ownership of the identifier. For DLT identity, and SSI, which can be defined as a lifetime portable digital identity that does not depend on any centralized authority and can never be erased a new class of identifier is required. After the W3C Verifiable Claims Working Group was approved in March 2017, in July 2017 the DID specification [59] was contributed to the W3C Credentials Community Group.

2.2.1.1 The Format of a DID

DIDs can be adapted to work with multiple DLT by following the same basic pattern as the URN specification.

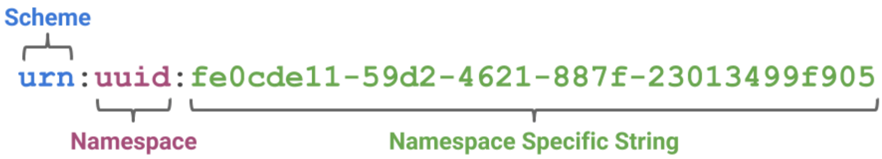

Scheme
urn:uuid:fe0cde11-59d2-4621-887f-23013499f905
Namespace
Namespace Specific String

Figure 14 *URN example [59].*

However, the difference is that with DIDs the namespace component identifies a DID method, i.e., the format of the method-specific identifier. DID methods define how DIDs work with a specific blockchain. Note that the method specific identifier string must be unique in the namespace of that DID method.

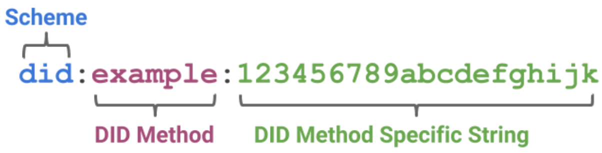


Figure 15 *DID example [59].*

2.2.1.2 DID Documents

DID infrastructure can be thought of as a global key-value vocabulary stored in a database where the database is all DID-compatible DLT, or decentralized networks. The key is a DID, and the value is a DID document. The DID document describes the public keys and service endpoints necessary to realize cryptographically verifiable interactions with the identified entity. A DID document is a valid JSON Linked Data (JSON-LD) object that uses the DID defined in the DID specification. This includes six core components:

- The DID itself, so the DID document is fully self-describing.
- A set of public keys or other proofs that can be used for authentication or interaction with the identified entity.
- A set of service endpoints that describe where and how to interact with the identified entity.

- A set of authorized capabilities for the identified entity, or other delegated, to make changes to the DID document.
- Timestamps for auditing.
- An optional JSON-LD signature if needed for verifying the integrity of the document.

2.2.1.3 DID Methods

A specific goal of DID architecture is to enable DIDs and DID documents to be adapted to any modern blockchain, distributed ledger, or other decentralized network capable of resolving a unique key into a unique value. It does not matter whether the blockchain is public, private, permissionless, or permissioned. What does matter is how a DID and DID document are created, resolved, and managed on a specific blockchain. Defining this is the role of a DID method specification. DID method specifications are to the generic DID specification as URN namespace specifications (UUID, ISBN, OID, LSID, etc.) are to the generic IETF URN specification (RFC 8141) [62].

A DID method specification must define the following:

- The DID method name.
- The ABNF[1] structure of the method-specific identifier.
- How the method-specific identifier is generated or derived.
- How the CRUD operations are performed on a DID and DID document

How CRUD operations are performed vary the most across different DID methods implementation. For instance:

- **Create**: some DID methods may generate a DID directly from a cryptographic key pair. Others may use the address of a transaction or a smart contract on a DLT.
- **Read**: some DID methods uses DLT that can store DID documents directly on it. Others uses DID resolvers to construct them dynamically based on attributes of a DLT record. Still others may store a pointer on the blockchain to a DID document stored in other decentralized storage networks such as Interplanetary File system (IPFS) [63].

[1] Augmented Backus–Naur form is a metalanguage based on Backus–Naur form (BNF), but consisting of its own syntax and derivation rules.

- **Update**: the most security-critical operation because control of a DID document represents control of the public keys or proofs necessary to authenticate an entity (and stole the identity). DID document update permissions can only be enforced by the target DLT. The DID method specification must define precisely how authentication and authorization are performed for any update operation.

- **Delete**: on a blockchain DID entries are immutable, so they can never be “deleted” but they can be revoked. A DID method specification must define how this termination is performed, e.g., by writing a null DID document.

2.2.1.4 DID Auth

All blockchain identity systems allow the cryptographic authentication of an identity owner. The protocols use some type of cryptographic challenge/response like the Secure, Quick, Reliable Login(SQRL) [64] and the Web Authentication protocol [65] currently being standardized by W3C. These protocols use a one-time challenge issued by the relying party, signed by the identity owner's private key, and then verified by the relying party using the identity owner’s public key. Compared to SQRL and Web DIDs will enable verification of the public key against the blockchain identified by the DID method. The DID Auth specification will standardize this cryptographic challenge/response authentication protocol so it can be used with any DID that supports it.

2.2.1.5 DIDs and Privacy by Design

Privacy is a MUST requisite in any identity management solution especially in system that uses immutable public DLT. DID architecture can incorporate Privacy by Design at the very lowest levels of infrastructure and thus become a powerful, new, privacy-preserving technology when it exhibits the following features:

- **Pairwise-unique DIDs** : While DIDs can be used as well-known public identifiers, they can also be used as private identifiers issued on a per-relationship basis. So rather than a person having a single DID, like a cell phone number or national ID number, she can have hundreds of pairwise-unique DIDs that cannot be correlated without consent yet can still be managed as easily as an address book.

- **Off-chain private data** : Storing any type of personal identifiable information on a public blockchain, even encrypted, or hashed, is dangerous for two reasons: 1) the encrypted or hashed data is a global correlation point when the data is shared with multiple parties, and 2) if the encryption is eventually broken, the data will be forever accessible on an immutable public ledger. The best practice is to store all private data off-chain and exchange it only over encrypted, private, peer-to-peer connections.

- **Selective disclosure** : The decentralized PKI (DPKI) based on allow individuals gaining greater control over their personal data in two ways:

    1. it enables to share data using encrypted digital credentials.
    2. credentials can use zero-knowledge proof cryptography [66] for data minimization, e.g., you can disclose that you are over a certain age without disclosing your exact birthdate.

2.2.2 Verifiable credential

DIDs act as the base layer of decentralized identity infrastructure. On top of them are verifiable claims. This is the technical term for a digitally signed electronic credential that conforms to the interoperability standards being developed by the W3C Verifiable Claims Working Group. Note that in all three cases, the parties interact with the DID layer to register DIDs as persistent identifiers for issuers or holders, and to resolve those DIDs to obtain the public keys needed to verify the signature of an issuer or holder. Since any issuer may provide claims to any holder who may present them to any verifier, this results in set of rich, interlocking trust relationships that do not need to conform to any pre-established hierarchy, a web of trust.

In Verifiable Credentials (VC) information about the subject must be shared with third parties, by proving to those third parties that the DID subject has ownership of certain attestations or attributes. This proof is based on the cryptographic link between the VC, the DID subject the VC is about, and the issuer of the VC, which can be the own DID subject (self-asserted claims), or a trusted entity. Trust on the issuer is established either by trusting the issuer's DID (e.g., out-of-band, bilateral relationship, trusted lists) or by any other means. The third party can then use the presented cryptographically protected proof to verify the ownership and trustworthiness of the claims about the subject. As the presentation of the claims is managed totally by the users, they can decide on which specific pieces of information about themselves they want to share with third parties; by means of this selective disclosure of attributes privacy and personal data protection is reinforced. The flow of information of the verifiable claims generation and use is depicted in the picture below, coming from the W3C working draft of the Verifiable Credentials Data Model [58]. In this Data Model, credentials are considered as a set of one or more claims made by an issuer. For implementing DID and VC, organizations working on SSI are relying on the use of Distributed Ledgers / Blockchains to support the registry of identifiers. In particular, the

Decentralized Identity Foundation (DIF) is proposing the architecture, based on the following components3:

- **User agent** : a Web client that mediates the communication between holders, issuers, and verifiers.
- **Universal Resolver** : a server featuring a pluggable system of DID Method drivers that enables resolution and discovery of DIDs across any decentralized system.
- **Universal Registrar**: a server that enables the registration of DIDs across any decentralized system that produces a compatible driver.
- **Identity Hubs** : secure personal datastores that coordinate storage of signed/encrypted data, and relay messages to identity-linked devices.

2.2.2.1 Structure of Verifiable credential

The W3C VC data model define the base properties required in the SSI environment. VC schemas in the W3C data model is based on JSON linked-data format but the data model can be implemented in every Metadata format, e.g., XML. The schema (JSON-LD format) is shown in in Fig. 16.

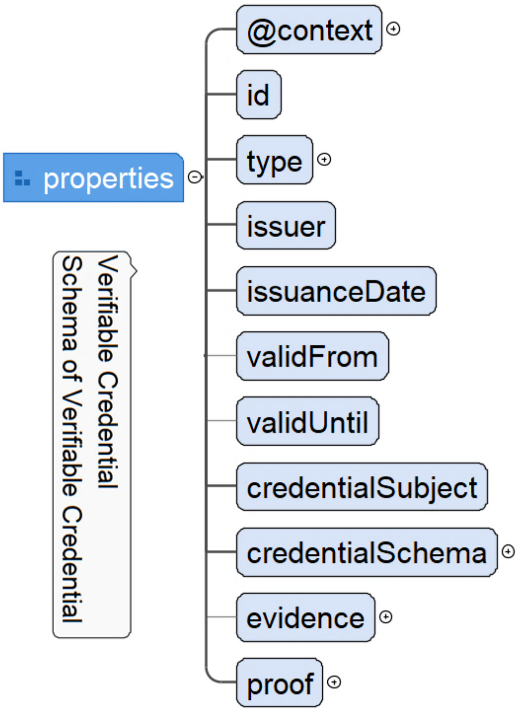


Figure 16 *Verifiable credential Schema*

Properties identifies:

- **Actors** : the issuer and the subject of the credentials, identified by their DID.
- **Credential** : the unique identifier of the credential, his type, his context
- **Timestamps** : the issuance and validity dates.
- **Additional evidence** : external link to related document or proofs.
- **Cryptographic proof** : the signature, the type of signature, his purpose , the verification method. It allows to verify that the credential is valid and verify the source.
- **Claims** : the properties that the credential describes about the subject.

From a data model point of view, the VCs can be seen as information graphics. Fig. 17 shows an example.

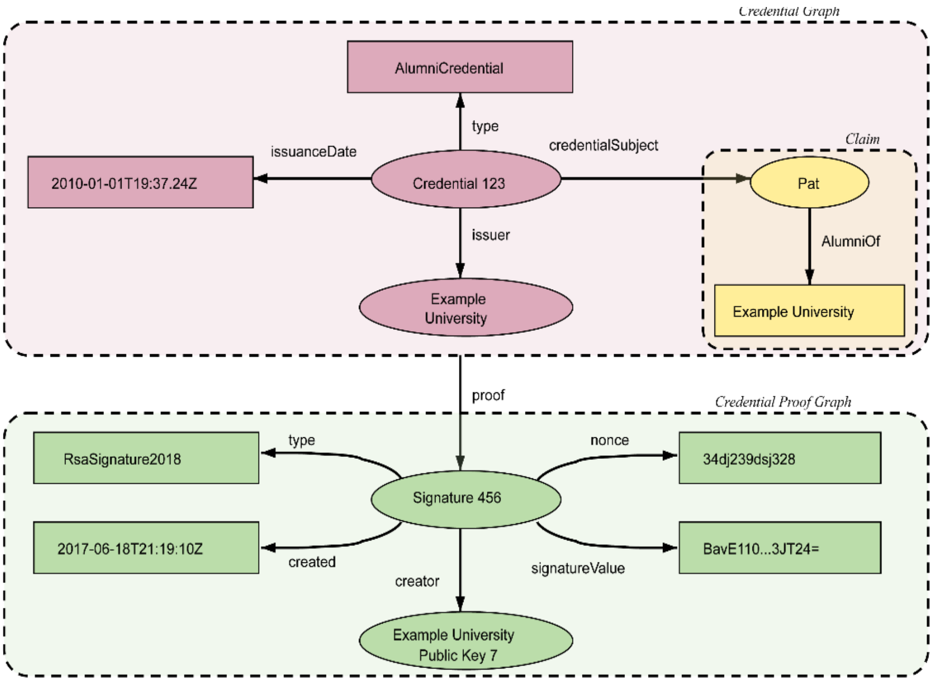


Figure 17 *VC graph.* 🟪 *Credential,* 🟨 *Claims,* 🟩 *Proof [58].*

The credential subject describes the specific properties of the subject that he/she want to be certified. To allow the validation of the structure of the Claims properties, the VC leverage on a decentralized schema registry, Trusted Schema Registry (TR), where the schemas structure is permanently stored. When someone need the validate a VC, the validator look-up the schema registry record of that refers to the specific schema. Then it uses to validate the structure of the specific credential against the schema. The credentialSchema property describe the credential specific type and allow to identify his location (Fig. 18).

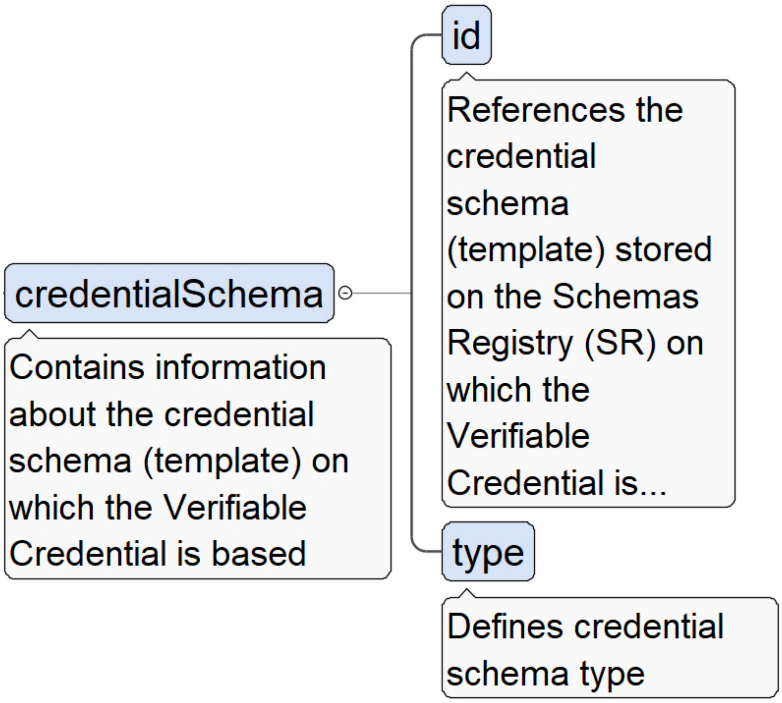

credentialSchema
Contains information about the credential schema (template) on which the Verifiable Credential is based
id
References the credential schema (template) stored on the Schemas Registry (SR) on which the Verifiable Credential is...
type
Defines credential schema type

Figure 18 *CredentialSchema schema.*

When a subject receives a VC, he/she stores it in his wallet. When a verifier asks for a specific credential, for instance to authorize the subject to access a specific service, the subject present him a Verifiable Presentation(VP). A presentation is a container of VCs from a specific subject and a specific verifier as recipient that allow subject to share selectively his credential. VP allow to verify that who is presenting the credential is really the subject of the VCs and not a malicious actor that is impersonating the subject. As the VC the VP can be described as linked information graph. An example is shown in Fig. 19.

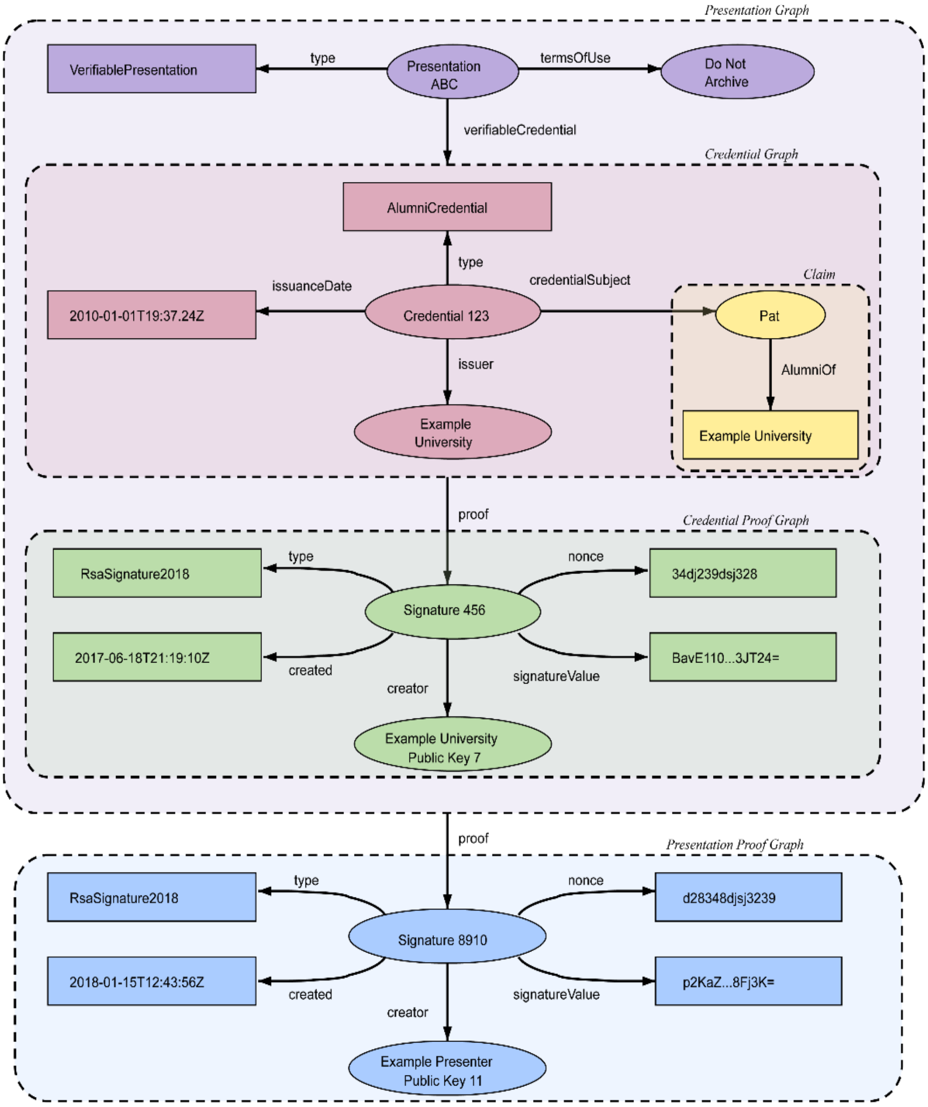


Figure 19 *Verifiable presentation graph example [58].*

2.2.3 Trust framework and verification approaches

SSI scheme based on DIDs, VCs, digital wallets, and decentralized registries is not an alternative to a PKI infrastructure, but a new generation PKI based on decentralized protocols, standards, and technologies. In traditional PKI, identity credentials, e.g., electronic certificates as X.509, are issued by certificate authorities (CAs). CA could be designated by government or could be well known authorities (e.g., banks, universities etc.). CAs maintain lists of certificates that have been revoked, called certificate revocation lists (CRL). When a certificate is presented to a verifier by the subject, the verifier can verify its status against the CRL. Alternatively, to check revoked certificates the verifier could use online certificate status protocol (OCSP), in which he requests directly to the CA's the status of a particular certificate. It passes the certificate's serial number to the CA's, and receive a digitally signed response containing the certificate status, i.e. "good", "revoked", or "unknown". Sometimes a root CA generates a first certificate, and then a chain of linked certificates is built from that first certificate, e.g., corporation and subdomain scenarios. To verify the final certificates of the chain, the verifier, generally a browser agent, resolves the entire root of trust and verifies it up to the root CA. Let's consider the IP protocol and the Domain Name System (DNS). The Internet Assigned Numbers Authority (IANA) and five regional Internet registries (RIRs) globally manage the IP address space. The DNS instead is maintained and can be resolved against root servers operated by 12 trusted entities. Like how DNS allows IPs to associate with known domain names, public key directories (PKDs) can associate public keys with entities, e.g., the European Commission maintains a PKD with public keys associated with all the Country Members. The infrastructure and the entity responsible for these PKDs are usually centralized, and when there is not a trusted central entity or infrastructure, it is not easy to create these PKDs. The verification of current digital certificates relies on centralized PKDs, CRLs, and OSCPs and do not allow universal verification. Additionally, there are not secure and portable personal repositories to manage personal credentials, and issuance and verification processes are generally not compatible nor interoperable between different entities or countries. Moreover, PKD usually allow one public key per identity, which does not allow rights, such as anonymity and the right to be forgotten, nor facilitates key rotation, recovery, or delegation,

In the SSI scheme, CAs are known as issuers and digital certificates follow the VC standard, not the X.509. PKD is replaced with DIDs. In the SSI scheme, each identity can have an unlimited number of unique identifiers, or DIDs, and each DID can have an unlimited amount of various public keys and authentication mechanisms that are associated. Centralized PKD and DNS can be linked to a DID with use of smart contract registry when retro compatibility is necessary. This allows central Authority to issue credential with the new paradigm of VC still preserving their authority role in the conventional system. Converting PDK and DNS centralized registry in decentralized registry allow a complete decentralized approach. Having the possibility to register the proofs of a VC in smart contract allows for on-chain PKDs and CRLs and enables anyone to verify the digital credential against any node connected to the network.

Verification of VC could be summarized as three step process:

- Verification of signatures on credential
- Verification of Credential status on decentralized CRL
- Verification of the issuer of credential.

When issuer verification consists in verifying if an issuer is authorized from a trusted authority to issue certain type of credential. This chain of trust is kwon as trust framework [67]. For instance, in the case of digital calibration certificates, entities that designate the authorized calibration laboratory are Accreditation Body. The Accreditation Body designate these laboratories by maintaining trusted lists (TLs). If a verifier receives a verifiable presentation of a digital calibration certificate, they will attempt to verify whether the issuer is indeed an entity that has been authorized by a recognized Accreditation Body.

Trust frameworks lead to the proliferation of roots of trust that can resolve the chain from the issuer to trusted authority for the certificate to be trusted by a verifier. This could be implemented both off-chain or on-chain using smart contracts. The possible combination of PKD , certificate standards, credential verification process, identifier , trusted list, root of trust and trusted framework rule is reported in the following table.

Table 2 *Trust models combinations*

PKD	Certificate Standard	Credential verification	Identifier	TLs, Root of Trust, and Trust Framework
off-chain /on-chain	X.509	off-chain CLR (http)	public key	off-chain
off-chain /on-chain	X.509	on-chain CLR (smart-contact)	public key	off-chain /on-chain
off-chain /on-chain	VC	on-chain CLR (smart-contact)	DID	off-chain /on-chain

In SSI scheme, there are two options for resolving a root of trust and verify the issuer's authorization:

- **Smart-contract-based (Trusted registry)** : if the DIDs of the trusted authorities authorized for the issuance of a particular VC are registered in smart contract-based PKDs and TL, it is possible to resolve against that smart the entire root of trust (Fig 19).
- **Chain of VCs** : An alternative to using smart contracts is requiring each entity in the root of trust to send a VC that contains claims to proof its own identity and role to the entity below in the root of trust. Therefore, if the final issuer has 4 entities above to reach the root-CA or top trusted issuer, this final issuer will send to the subject 4 credentials (one for each issuer in the root of trust) plus the VC that that contains whatever attributes the final issuer is certifying to the subject. The process is similar for presentation. Verifiers do not go against a smart contract to resolve and verify the root of trust, but it does it off-chain using all the linked VCs similarly to X.509 chain of trust (Fig 20).

2.3 DLT overview

Two tools, digital wallets and Blockchain networks are perfectly compatible with the DID/VC standard. Instead of having to carry a physical chip card, remember a password, then connect to a computer with a device to authenticate with electronic services, it is safer, more natural, and user-friendly to allow individuals to access their digital certificates and identifiers via an application that is available on any device connected to the internet. This system is known as a "digital wallet" in the context of SSI. Regarding blockchain, despite VCs can be verified against centralized registries and that DIDs can be resolved against centralized databases, the potential to use decentralized, public, and reliable ledgers to store the proofs of VCs and resolve DIDs opens a broader range of possibilities.

DLT is a connection protocol that identifies a distributed database logic technology (data stored on multiple connected machines, called nodes). The records are organized in a distributed ledger linked with some non-invertible cryptographic function (e.g., hashing). The network's transparency and security are ensured by each node copying the register. A consensus mechanism verifies each transaction in the network. This ensures that at most 51% of participants agree to it.

The Blockchain chief ingredients are:

- **Block** : blocks store valid transactions. The structure is made of a header and body. In the current header hash, hash of previous block, timestamp, nonce value and Merkle root is stored to bind the blocks together. The body is the container o valid transactions. Figure 1 reports the scheme of the generic block.

- **Ledger** : The linked blocks form a chain (i.e., Blockchain), with each additional block reinforcing the previous ones. The blockchain uses a consensus mechanism to establish the fitness of recorded pieces of information to guarantee agreement in the network. When a transaction is generated, it is brought to the Network to be verified by blockchain participants; it becomes the permanent, immutable, and unmodifiable reference of that specific transaction [4], [68].

- **Smart Contract** : a piece of code that allows information transactions and decision-making stored in the blockchain to be public to the network and reliable. Smart contracts are used to manage digital assets. Smart contracts grant security provisions for operation in form of transactions. They can be used for simple transactions such as exchanging money between entities or more complex transactions such as property registration or assignment of rights [69].

DLT main relevant features [70] are listed below:

- **Distributed** : as a Pear-to-Pear (P2P) network DLT avoids centralized system issues, e.g., single point of failure or lack of trust, higher costs, etc.

- **Pseudo-anonymity** : This means that the identity of the users is not broadcast to others except for the one who takes part in the transaction. Identities are represented with a public key and not personal data (this is not entirely correct in a private network where a different form of identification is required)

- **Time-constrained** : transactions are timestamped with a starting time and duration.

- **Security and Trust** : smart contract technology enforce mutually beneficial agreements between entities. They provide versatility being programmable and offer security and trust to their users.

- **Immutability** : blockchain data are unchangeable and cannot be altered

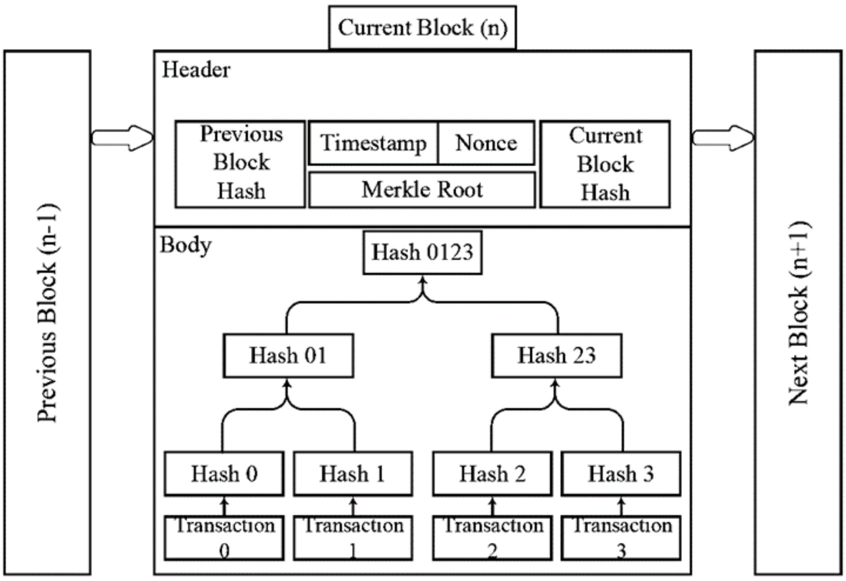


Figure 20 *DLT block structure.*

2.3.1 Types of DLT

Despite the potential of using DLT/blockchain is known, in this relatively young technology, many challenges are currently unsolved. Multiple trade-offs between decentralization, security, and scalability of a blockchain-based system exist. This is known as a **blockchain trilemma** [71] (Fig. 21).

The key proprieties are explained in detail:

- **Security** : the ability to maintain the integrity of the registry distributed against attacks through an internal control mechanism.
- **Scalability** : non-functional features related to system load capacity, throughput, and transaction processing latency.
- **Decentralization** : accessibility, availability, and transparency of data for all participants, consistency of the status of the Ledger among all nodes, resistance to censorship.

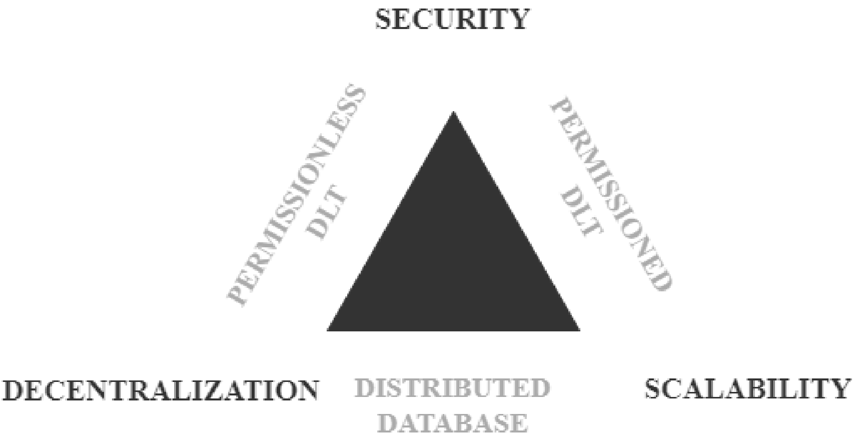


Figure 21 *Blockchain trilemma*

Only two features out three can be optimized concurrently, which defines three different types of distributed ledger databases [72]:

- **Public** : anyone can access the ledger thanks to the robust security granted by a complex consensus mechanism at the cost of reduced scalability. Examples are Bitcoin [73] and Ethereum [74]
- **Private /Consortium** : the users' identities are known in advance in a private blockchain, and the control is limited to a predetermined set of authorized subjects. This system gives up decentralization in favor of scalability and privacy. An example is Hyperledger Fabric [75].
- **Distributed Databases** : these systems withdraw security in support of scalability and decentralization, not to be considered as a standard distributed ledger. It constitutes an excellent off-chain storage system to be combined with the blockchain system. Interplanetary File System (IPFS) [63]and Swarm represent two typical examples.

A comparison in terms of transaction cost, throughput, latency, trust decentralization, and openness between permissioned and permissionless DLT is provided in the following table [76].

Table 3 *DLT Comparison*

Features	Permissionless	Permissioned
Transaction cost	High	Medium/low
Throughput	Low	Medium/Low
Latency	High	Medium/Low
Trust	High	Medium
Decentralization	High	Medium
Openness	High	Medium

2.3.2 DLT generalized architecture

Although the different types of blockchain being implemented with different architecture, a generalized structure can be represented by the following layers [77]:

- **Data layer** includes data blocks, timestamps, encryption techniques, and hash functions.
- **Network layer** specifies the type of network, communication mechanism, and verification mechanisms.
- **Consensus layer** specifies how the nodes achieve the agreement on the blocks that should be added to the ledger. There are many consensus mechanisms for that. All network nodes with enough computational power can participate in bloc mining and consensus.
- **Incentive layer** encourages the nodes' participation in mining process. There are different kinds of incentives that will be described in the following sections.
- **Contract layer** provides the programming capability of the DLT network. The rules defined at this level set how entities communicate and how services are provided to network nodes.
- **Application layer** is the users' interface to the DLT, very application specific.

The structure is summarized in Fig. 22.

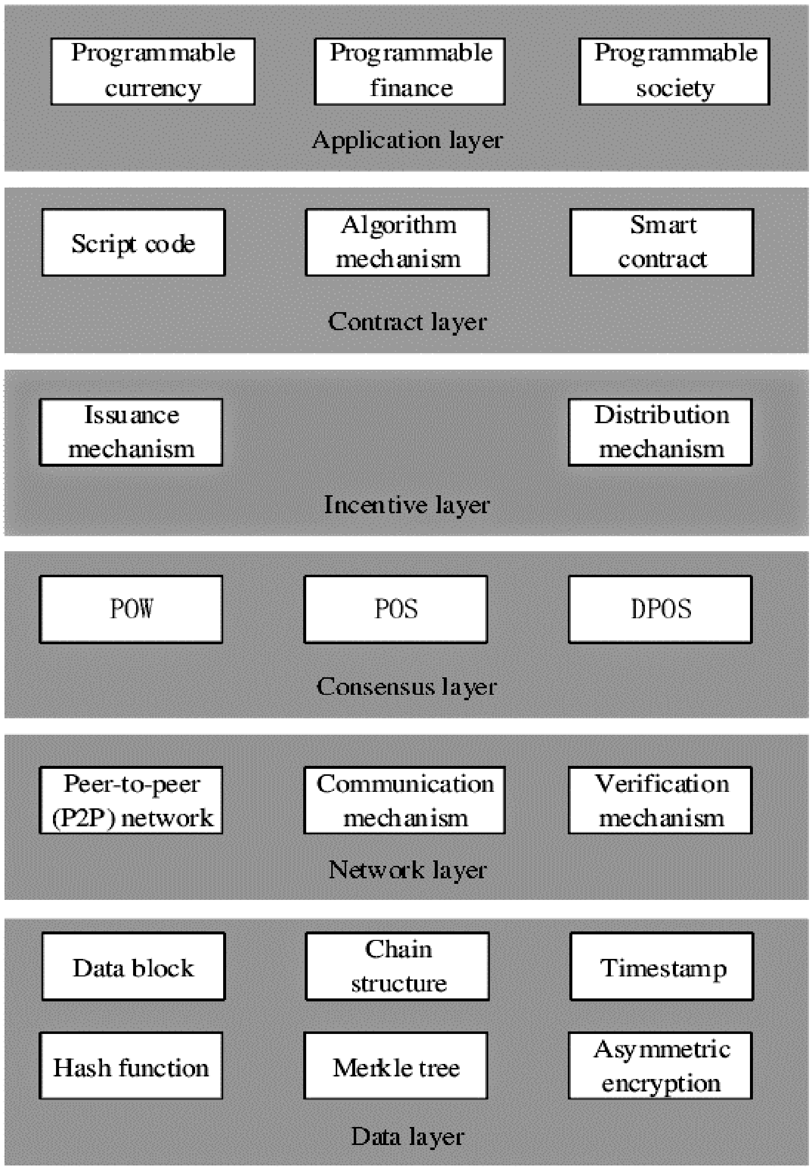


Figure 22 *DLT layers architecture*

Many algorithms can be used in blockchain technology to reach consensus among the network nodes. Some of the most popular include PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated Proof of Stake), PBFT (Practical Byzantine Fault Tolerance), and PoA (Proof of Authority) [78], [76]. A consensus mechanism is the base of trust among the nodes.

A detailed explanation of the mentioned protocol is provided:

- **PoW**: PoW is the native consensus of bitcoin. It consists of a cryptographic puzzle. The winner is the miner who solves the given problem the first time. He or she is then awarded a prize (the mined coin). PoW is well secured but at the cost of high-power consumption.
- **PoS and DPoS**: In PoS, block mining is allowed only to the node with the most significant stake. This implies low computational. Miners are incentivized to be honest because they risk losing all their stake. The main problem is the "nothing at stake" [79], a cyber-attack that led to the "double spending" [80] issue, i.e., a form of fake malicious transaction that allows the attacker to be counterfeit the spending of his coin without reducing his wallet amount. DPoS [81] is a variant of PoS in which real-time voting in conjunction with a reputation system is combined with the stake paradigm. In practice, all nodes vote a set of delegates. The higher is the node stake, the higher is the influence of the vote. The selected delegates mine the new block. The chosen delegates are constantly updated based on their efficiency and trustiness.
- **PBFT**: First used in Hyperledger, PBFT [82]is a deterministic protocol based on state machine replication (SMR), allowing high fault-tolerant service mechanism. The protocol is made of five steps:

    1. Request phase: the server receives a message from the user marking it with a timestamp.
    2. Pre prepare phase: message is assigned an order number while broadcasted in the network.
    3. Prepare phase: nodes broadcast the values in the network waiting for the other nodes responses.
    4. Commit phase: agreement on the selected messages from the step 2 is reached on more than 66% of the nodes.
    5. Reply phase: the sender receives back a response from the network.

- **PoA**: The PoA is based on the concept of an Authority node who is the responsible to choose the miner. To every miner is given a finite amount of time, in which he tries to solve the puzzle. If time elapse a new miner is selected [82].

In [83] the authors performed a detail comparison of the various consensus algorithm in term of throughput, tolerance and efficiency that is summarized in table 4:

Table 4 *Comparison of consensus protocol*

	Consensus	Throughput	Tolerance	Efficiency
PoW	Probabilistic	Low	≤25%	Less
PoS	Probabilistic	High	Varies	Intermediate
DPoS	Deterministic	High	Varies	> PoS
PBFT	Deterministic	High	≤33%	High
PoA	Deterministic	High	Varies	High

2.3.3 Incentives in DLT

The incentives, that could be of monetary, entertainment or service-oriented nature [84] can be classified into two major groups: User centric, Platform Centric. In the first case the strategies are based on user participation motivated by rewards in competition. The most common mechanism in such case is the use of auction with a prize in form of money, resource, reputation etc.

In the Platform Centric on the opposite the user gets incentives only if their platform allows the proper operation of the system. In such cases user depend on the data of the platform itself. To get a proper service, there are incentivized to join the consensus protocol. Typical examples are platforms in which the data correctness or identity anonymity are granted (e.g., e-Healthcare) [85].

2.3.4 Real world DLT platforms

2.3.4.1 Bitcoin

The first DLT has been implemented in the Bitcoin protocol by Satoshi Nakamoto [73], called Blockchain, that stores a list of blocks securely linked together with cryptography. Here we will discuss the characteristic of the protocol because, as bitcoin has been the first working blockchain, most of the subsequent DLT share with it many aspects of the cryptographic protocol.

As introduces before a ledger of a cryptocurrency such as Bitcoin can be thought of as a state transition system, where there is a "state" consisting of the ownership status of all existing bitcoins and a "state transition function" that takes a state and a transaction and outputs a new state which is the result. The "state" in Bitcoin is the "unspent transaction outputs" or UTXO, the collection of all coins that have been mined and not yet spent, with each UTXO having a denomination and an owner. A transaction contains one or more inputs, with each input containing a reference to an existing UTXO and a cryptographic signature produced by the private key associated with the owner's address, and one or more outputs, with each output containing a new UTXO to be added to the state. Essentially, each transaction in the block must provide a valid state transition from what was the canonical state before the transaction was executed to some new state. Note that the state is not encoded in the block in any way; it is purely an abstraction to be remembered by the validating node and can only be (securely) computed for any block by starting from the genesis state and sequentially applying every transaction in every block. Additionally, note that the order in which the miner includes transactions into the block matters. The validity condition in the above list that is specific of the system is the requirement for "proof of work”. An important scalability feature of Bitcoin is that the block is stored in a multi-level data structure. The "hash" of a block is only the hash of the block header, a roughly 200-byte piece of data that contains the timestamp, nonce, previous block hash and the root hash of a data structure called the Merkle tree storing all transactions in the block. A Merkle tree is a type of binary tree, composed of a set of nodes with many leaf nodes at the bottom of the tree containing the underlying data, a set of intermediate nodes where each node is the hash of its two children, and finally a single root node, also formed from the hash of its two children, representing the "top" of the tree. The purpose of the Merkle tree is to allow the data in a block to be delivered piecemeal: a node can download only the header of a block from one source, the small part of the tree relevant to them from another source, and still be assured that all the data is correct. The reason why this works is that hashes propagate upward: if a malicious user attempts to swap in a fake transaction into the bottom of a Merkle tree, this change will cause a change in the node above, and then a change in the node above that, finally changing the root of the tree and therefore the hash of the block, causing the protocol to register it as a completely different block (almost certainly with an invalid proof of work). The Merkle tree protocol is arguably essential to long-term sustainability. A "full node" in the Bitcoin network, one that stores and processes the entirety of every block, takes up about 374 GB of disk space in the Bitcoin network as of December 2021, and is growing by over a gigabyte per month. Currently, this is hardly viable for user desktop computers and phones, and mainly specialists and hobbyists will be able to participate. A protocol known as "simplified payment verification" (SPV) allows for another class of nodes to exist, called "light nodes", which download the block headers, verify the proof of work on the block headers, and then download only the "branches" associated with transactions that are relevant to them. This allows light nodes to determine with a strong guarantee of security what the status of any Bitcoin transaction, and their current balance, is while downloading only a very small portion of the entire blockchain. Despite its notoriety Bitcoin Blockchain is only well suited for monetary application because natively does not support the smart contracts.

2.3.4.2 Ethereum

The intent of Ethereum is to create an alternative protocol for building decentralized applications, providing a different set of trade-offs that we believe will be very useful for a large class of decentralized applications, with particular emphasis on use cases where rapid development time, security for small and rarely used applications, and efficient interoperability are important. Ethereum does this by building what is essentially the ultimate abstract foundational layer: a DLT with a built-in TURING-COMPLETE PROGRAMMING LANGUAGE, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions. Ethereum [74] focuses more on the development of decentralized applications (DApps) with smart contracts, i.e., a software that is executed in the Ethereum Virtual Machine (EVM) by all the nodes of the Ethereum network. A user with an Ethereum account can invoke a smart contract function with a transaction that executes a piece of code, and eventually stores a state in the Ethereum blockchain. In Ethereum, the state is made up of objects called "accounts", with each account having a 20-byte address and state transitions being direct transfers of value and information between accounts. An Ethereum account contains two field beyond the standard above mentioned: the account's contract code if present and the account's storage (empty by default).

"Ether" is the main internal crypto fuel of Ethereum and is used to pay transaction fees. In general, there are two types of accounts: externally owned accounts (EOA), controlled by private keys, and contract accounts, controlled by their contract code. An externally owned account has no code, and one can send messages from an externally owned account by creating and signing a transaction; in a contract account, every time the contract account receives a message its code activates, allowing it to read and write to internal storage and send other messages or create contracts in turn.
The term "transaction" is used in Ethereum to refer to the signed data package that stores a message to be sent from an externally owned account.

Two field are especially important:

- **STARTGAS** value, representing the maximum number of computational steps the transaction execution can take.
- **GASPRICE** value, representing the fee the sender pays per computational step.

This fields regard network functionality. To prevent denial of service attacks each EVM operation is associated a cost in gas: if the summation overcomes agas limit set by the user or the block gas limit, whichever the lowest, the execution halts. Finally, the user pays a fee proportional to the gas spent multiplied by the gas price, i.e., an amount in Ether (ETH) assigned to each unit of gas by the user. Contracts have also the ability to send "messages" to other contracts. Essentially, a message is like a transaction, except it is produced by a contract and not an external actor. Thus, contracts can have relationships with other contracts in the same way that external actors can. This could be thought as an equivalent of a subroutine in standard programming language.

2.3.4.3 Hyperledger Fabric

The classical example of a private and permissioned ledger is Hyperledger Fabric [75]. Hyperledger's design philosophy is based on modularity to respond to the variety of Use Cases for different market sectors. In the following list various levels of abstractions are explained that represent the essential components of developing a Blockchain for commercial applications:

- **Asset** : It defines the resources that are subject to exchange operations on the blockchain. They can represent tangible assets (real estate and hardware), intangible assets (contracts and intellectual property). The state of assets can be altered by smart contracts. They are represented in Hyperledger Fabric as a collection of key-value pairs, with state changes recorded as transactions on the ledger.
- **Consensus** : It allows an agreement on the order of transactions, confirms its correctness, requires confirmation of the Smart Contract Layer for the validation of transactions
- **Smart Contract (chiancode)** : An IfThisThanThatlogic follows for validating transactions by implementing the specific business logic required by the use case.
- **Identity & Privacy Services** : They guarantee the creation of instances, identification, registration, authentication, revocation of components, actors, and authorizations on the network. Furthermore, they enable privacy on specific data.

- **APIs** : They allow interfacing to the application network and clients
- **Interoperability** : It allows the interfacing of multiple blockchains

Essential for the definition of the suitable solution for a specific Use Case are the Assets and smart contracts that allow the management, updating and privacy of data on the blockchain as well as the implementation of business logic. To better understand the key concepts of architecture, let us consider the simple example of two organizations (to maintain ourselves in the general case of a consortium). As mentioned, both want to participate in the system to develop a common business. To do this, they create an exclusive communication bridge called a channel. Only those who participate have access to the stored data. In this way, if, for instance, several organizations want to share data with certain partners rather than others, they can use separate channels.

The four main elements of the system (Fig. 23) are:

- **Peer** : node with archiving and approval function for transactions (endorsement policy) fundamental for the consensus mechanism. The peers host the Smart Contracts (called chaincode) with which the business logic is implemented. This code supports various programming languages, such as Java, Go and Nodejs.
- **Orderer** : is one of the most important components used in the consensus mechanism as it is responsible for ordering transactions, creating, and distributing new blocks to all peers.
- **Certificate Authority (CA)** : at least one per organization is responsible for managing user certificates such as registration, authentication, and revocation. Because Hyperledger is a permissioned network, only authorized users can query or invoke (create) a transaction on a channel.
- **Client** : any application that interacts with the blockchain network whether it is for an end user, or an admin. Customer may interact with the Fabric network based on the permissions, roles and attributes specified in the certificate derived from the CA server.

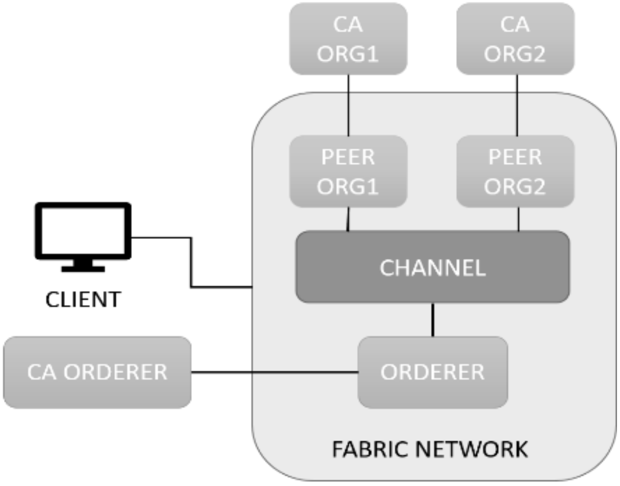


Figure 23 *Hyperledger based architecture*

In the Hyperledger Fabric blockchain, all participants have known identities. To do this, it uses a Public Key Infrastructure (PKI) to generate cryptographic certificates linked to organizations, network components and end users or client applications. As a result, data access control can be performed both at the overall network level and on individual channel channels. This system is implemented with a Membership Service Provider (MSP) service (Fig. 24).

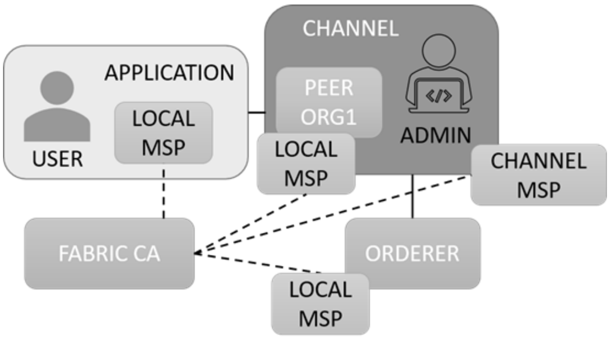


Figure 24 *Hyperledger Fabric Certificate Authority*

The service provides an identity for:

- **Peers and Orderers**
- **Client Application**
- **Administrators and users**

Identities are provided by the CA. A network contains multiple MSP instances, typically one per organization. This service also guarantees the possibility of encrypted communications by including TLS resources. Each client application (user) has a local MSP service where user identities are stored. These include a private one to sign transactions and the X.509 digital certificate containing the user's information and public key. The same applies to administrators' local MSPs. The speech is slightly complicated in the case of peers / orderers for which the local MSPs contain a list of Administrator Certificates, a list of CA certificates, and a list of authorization revocation certificates. These extra certificates are intended to verify the validity of the identities and permissions of the elements requesting access to the node resources. Channels are also associated with MSPs to determine which nodes can join the channel and which client applications can read or write to the channel.

2.3.5 Choosing a blockchain

After the widespread adoption of DLTs, new architectures have been proposed to satisfy the requirements of different use cases. Bitcoin and Ethereum are so-called public and permission less networks because any peer can join freely to the consensus and read/write transactions and have problems about privacy and performances; private and/or permissioned networks exist as well introducing restrictions into the participation process improving therefore privacy and performances. In [72] a clear comparison among these networks and standard centralized network is carried out.

The analysis is based on:

- Public Verifiability of the system state.
- Transparency of the data.
- Privacy of actor involved.
- Integrity of information.
- Redundancy of data.
- Trust Anchor i.e., the highest system authority.

The authors developed an easy to apply flow chart diagram that is based on the requirement and precondition of the possible use case specifies the kind of system that better satisfies the problem. The diagram is reported in Fig. 25.

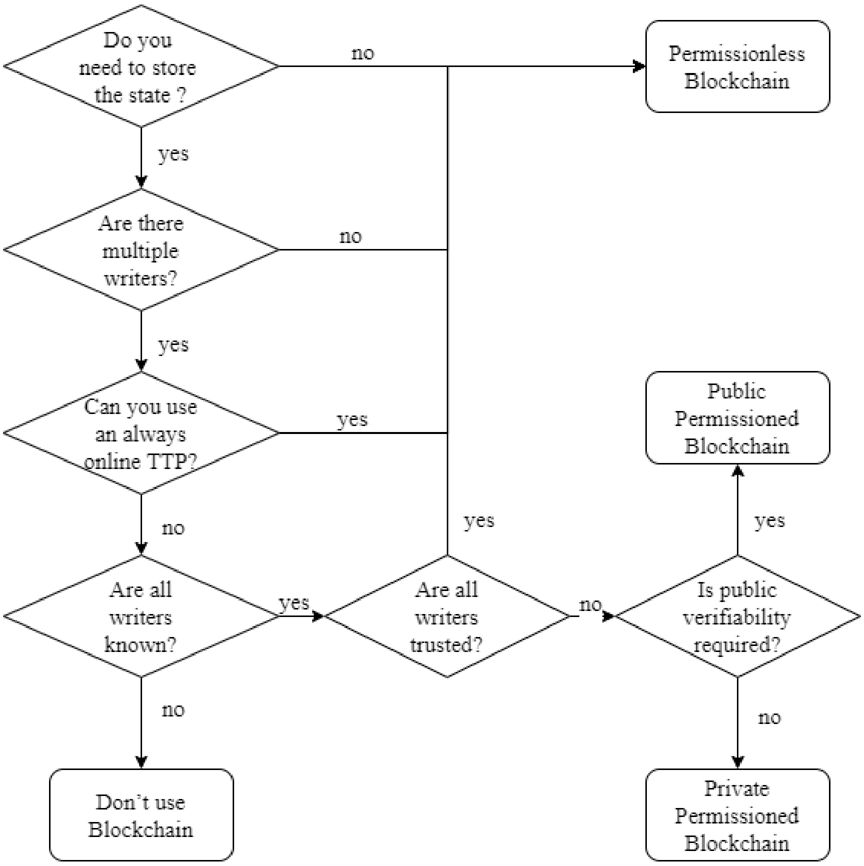

Do you need to store the state ?
no
Permissionless Blockchain
yes
Are there multiple writers?
no
yes
Can you use an always online TTP?
yes
Public Permissioned Blockchain
no
yes
yes
Are all writers known?
yes
Are all writers trusted?
no
Is public verifiability required?
no
no
Don't use Blockchain
Private Permissioned Blockchain

Figure 25 *Blockchain selection criteria*

2.4 Blockchain and IoT integration

Blockchain applied to the IoT (BIoT) represents a critical element to provide reliability and privacy for Smart Home, Smart Industries, Smart Grid [86], and widespread applications for "smart city". It establishes the opportunities to automate and integrate manual processes within the digital era, which allows a more in-depth interaction between humans and machines to maximize process efficiency [4] [87] [88] [70]. In [68], the authors describe three possible alternatives: IoT-IoT, IoT-Blockchain, Hybrid approach, as shown in Fig. 26.

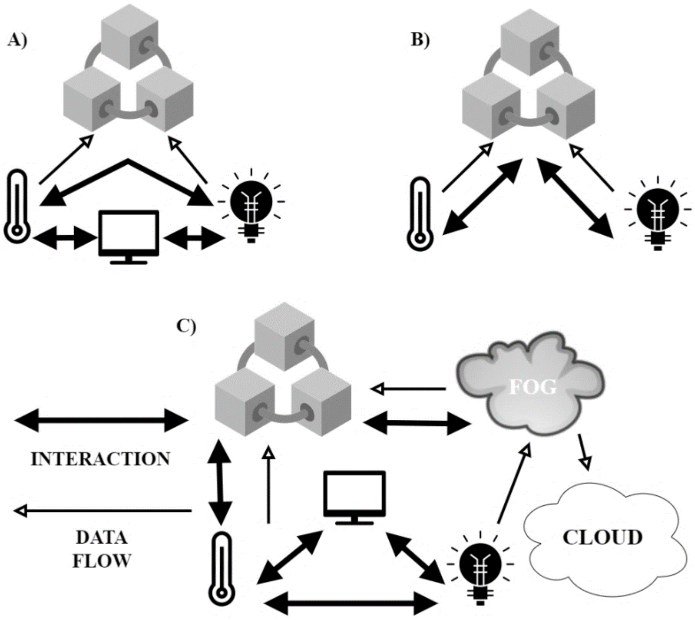


Figure 26 *1 BIoT: A) IoT-IoT, B) IoT-Blockchain, C) Hybrid.*

Table 5 *Comparison of IoT-blockchain architecture*

Architecture	Features	Pros
IoT-IoT	Device inter-communication and sporadic interaction with BC, partial storage in BC.	Low latency
IoT-Blockchain	All interactions recorded on the blockchain.	Immutable interactions record
Hybrid	Fog and cloud computing as an intermediary between IoT devices and BC.	Computational burden sharing, excellent reliability.

In the integration of the two technologies, generally the devices used as end nodes have limited resources. The transmission of data to the end-user is rarely done directly (device-server), but rather a multi-level architecture is preferred in which a Gateway collects information from multiple sensors, and then it is forwarded to the server [89], [90], [4], [88]. Fig. 27 describes the concept.

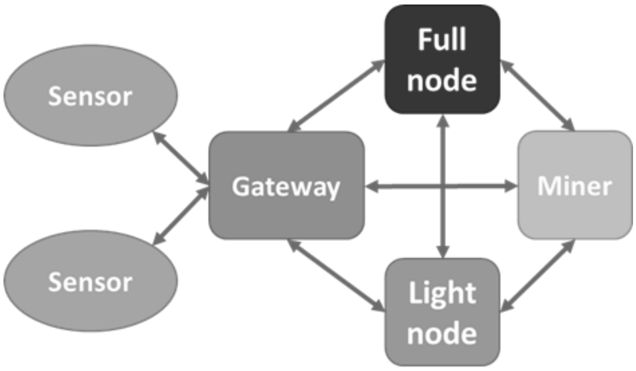


Figure 27 *Gateway centric architecture*

As said some protocol could be very resource consuming, and in general not all device in IoT network con support a full-client software capable to store the whole chain or validate transaction. To solve this issue a light client node protocol is preferred. In such protocol the node act as non-validator with free/partial storage, able only to propose transaction. This led to a more versatile logical configuration of the network. This gateway-centric approach inherently brings the opportunity of executing software solutions on IoT gateways. For this reason, applications with hybrid architecture are easier to integrate, even at the cost of partial use of the blockchain, therefore an application-oriented optimization approach is required.

Chapter 3

Proposed System Architecture

In this section based on what has been analyzed in the previous characters a system architecture to address the different problematics is proposed. Two different use cases are analyzed in detail to show the potential of the proposed system.

3.1 Main challenge

As stated before, because of the unavoidable digitalization process, the DCC interoperable standard has been proposed to address the harmonization of the calibration system. However, it can't be of practical use without an underling digital infrastructure. The suggested platform should grant:

- **Traceability and Auditability** : The certification process should be well documented, traceable, and auditable in case of legal controversy. Device, technicians, legal entities and produced document should be uniquely identifiable and retrievable to piece together the chain of trust and chain of traceability.
- **Integrity** : The produced data and attestation must not be corruptible, otherwise every form of credibility and potential use case will be compromised.
- **Security and Trust** : The platform should be resilient to cyber-attack, failure, and manumissions from both internal and external entities. Involving multiple actor both in public and private sector it should grant a form of trust for all participant, preferably in distributed fashion and not relying on single authority.
- **Privacy** : The platform should be compliant to regulation in term of sensitive data. When not needed personal data should be anonymized and only symbolic reference should be of public domain for management and governance.
- **Interoperability and Scalability** : As stated in the first chapter the platform should be supposed to provide services to many user and

devices requiring scalability. Because the preexistence of stakeholders personal database the system should provide a uniform interface. To enhance the extensibility all services should be loosely coupled.

3.2 Identifying use case scenarios

The analyzed ecosystem is made of institutional entities i.e., governments, accreditation bodies, public entities i.e., calibration laboratory and manufacturers, and final user, i.e., civilian. To be able to issue calibration certificates, laboratories must be certified from the accreditation bodies that who themselves need to be accredited by NMIs or governments. Industries and manufacture produced devices that in turn are used both for calibration purpose and for as final product, e.g., in the manufacturing process itself or for personal or public usage from citizens. Devices are such important that should be considered themselves as an active element of the discussed environment. To simplify the analysis, we will make the following assumptions:

1. Devices and instruments should be uniquely identifiable.
2. Institutional entities, public entities and end user should have a unique identifier.
3. Government can accredit institution to issue digital scope of accreditation certificates.
4. NMI and accredited laboratories can issue digital calibration certificates
5. Notified Body can approve LR software update for instrument.
6. Market Surveillance can issue digital declaration of conformity certificates
7. Manufacturer produce device and issue ownership certification to buyers.
8. Technician and physical person that act on behalf of institution is it is assimilated to the institution itself.
9. Device can sign the measure with their own keys

Although these assumptions are very simplifying, they allow us to describe the problem in a more concise and uniform way.

Hence, we can than identify the following scenario:

- Issuance of Digital Scope of Accreditation Certificate (DSoA)
- Issuance of Digital Calibration Certificate (DCC)
- Issuance of Digital Declaration of Conformity Certificate (DDoC)
- Device Chain Traceability recovery and measurement certification
- Trustable Measurement recording

3.2.1 Scenario 1: Issuance of Digital Scope of Accreditation

Description	A laboratory aims to obtain accreditation to provide calibration services and expand its business. The laboratory submits a request to the accreditation body. After a careful verification procedure, the delegate of the institution confirms the suitability of the laboratory and compliance with the regulations. It then issues a digital certificate to the laboratory and records proof of accreditation on the quality platform.
Objective	The laboratory needs to own an appropriate attestation that can be unequivocally recognized from any third-party auditor to be trustable and obtaining engagements.
Precondition	The laboratory, among other things, must provide the proof to be in possession of the appropriate equipment in to issue calibration services.
Steps	1. The laboratory submits on the quality platform the request for accreditation. 2. The laboratory performs a series of automated test to provide digital evidence of the submitted scope of accreditation. 3. The accreditation body verifies the reported capabilities, the digital documents and in case a delegate perform a physical inspection for the laboratory. The verification process is successful, and the inspector notifies the accreditation body.

	4. The accreditation body issues a digital certificate to the laboratory and records proof of accreditation on the quality platform.
Outcome	A digital accreditation for the laboratory is registered on the platform.
Remark	Despite the digital record is trustable and persistent the accreditation body should retain control on the authorization of the accredited entities. It should be possible to revoke the accreditation.

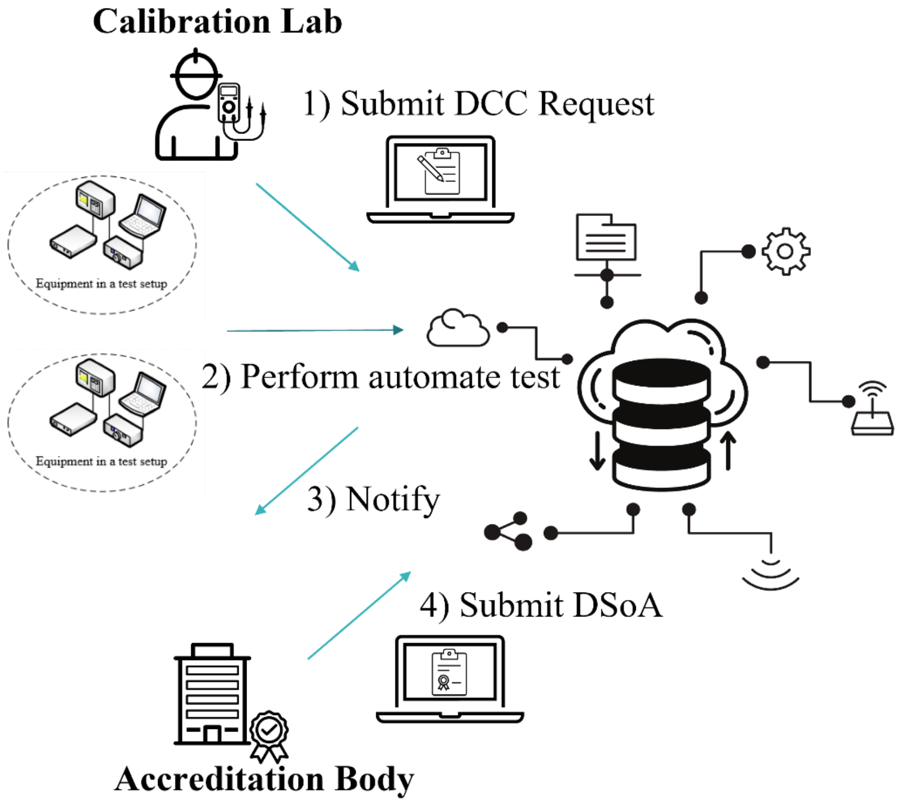


Figure 28 *Flow diagram: scenario 1.*

3.2.2 Scenario 2: Issuance of Digital Calibration Certificate

Description	A manufacturer was commissioned to produce a batch of devices for a humidity sensor plant for a university campus. Given the large number of devices, he decides to use only a limited number of samples as a reference to be calibrated with a good degree of accuracy to provide an estimate of the entire lot. To do this, the manufacturer hire an accredited laboratory which carries out the calibration procedure by recording the certifications in digital format.
Objective	The produced certificate should be auditable from any possible third party. The laboratory should release a digital proof the documents are authentical and not tempered to the manufacturer that indeed he could exhibit to the buyer to assess the quality of his products.
Precondition	The laboratory must be accredited from an accreditation body. A proof of the accreditation should be embedded in the produced document. The laboratory must also own the appropriate equipment that has been already certified with a correlated proof to perform a proper calibration procedure. The laboratory must also embed this proof in the certification in order to make them valid.
Steps	1. The manufacturer hires the laboratory to perform the calibration. He submits a DCC request on the platform 2. The laboratory receives the devices. 3. The laboratory performs the automated calibration procedure registering the digital proofs on the platform.

	4. The laboratory produced the Digital Calibration Certificate and register it on the platform.
Outcome	1. The devices have been properly calibrated. 2. A digital non-repudiable, trustable, and permanent proof of the entire process has been registered on the public quality platform 3. The Digital Calibration Certificate have been stored on the platform.
Remark	As can be seen from the previous step the measurement equipment needs to be transparently and uniquely identifiable to assess that the has been used in the process without the possibility of repudiation. Their IDs must exist on the platform.

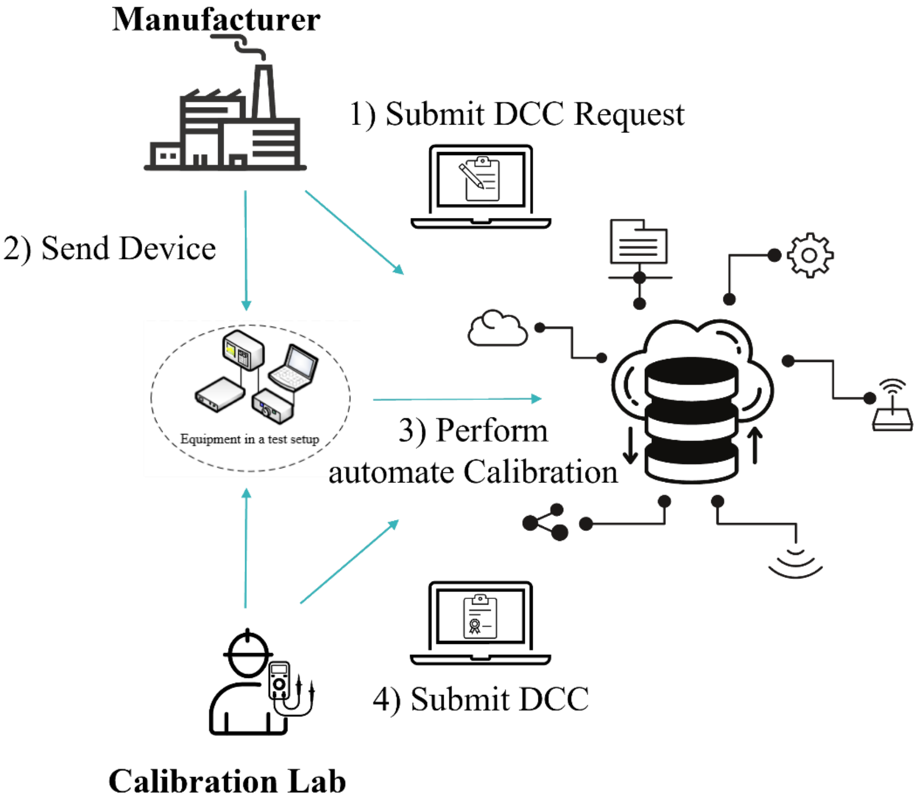


Figure 29 *Flow diagram: scenario 2*

3.2.3 Scenario 3: Issuance of Digital Declaration of Conformity

Description	A manufacturer releases a software update for his top-of-the-line IoT device. To complete the process the update must be approved from the Notified Body and Market surveillance. The former test and approve the software, the latter performs a batch test on a lot of devices.
Objective	The platform should support automatization of intercommunication in the approval process. Digital proof related to the software should be auditable from the involved parties (Notified Body, Market Surveillance, Manufacturer).
Precondition	There are no preconditions for this use case.
Steps	1. The manufacturer submits the software update request filling the appropriate form on the platform. 2. The Notified Body receive a pull notification of the request . 3. The Notified Body receive the software and test it. 4. Once test is complete the notified body approve the software update on the platform. 5. Market Surveillance is notified of a new approved software update. 6. Market Surveillance perform a batch test. 7. If test is positive Market Surveillance renew the Digital Declaration of Conformity for devices.
Outcome	1. The software has been properly audited and a proof of integrity is registered on the platform. 2. A digital non-repudiable, trustable, and permanent proof of the entire process has been registered on the public quality platform

Remark	The digital proof of software integrity will be further used to for verification purpose.

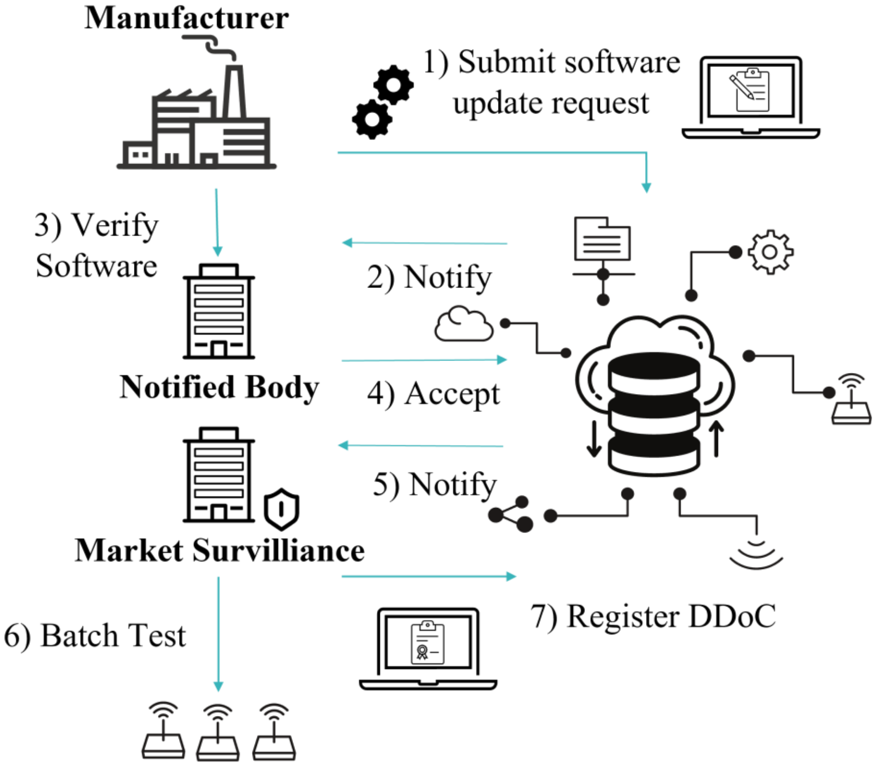


Figure 30 *Flow diagram: scenario 3*

3.2.4 Scenario 4: Device chain of traceability

Description	A customer wants to buy some fruit on the local market. When weighing the goods, he has a doubt that the balance is not properly calibrated. However, his wife is an accredited measurer, so he is aware of the traceability chain. He decides to check online. By scanning a QR code present on the instrument, it retrieves the entire history of traceability associated with it, up to the primary standards. Ironically, at the second link in the chain he recognizes the laboratory where his wife works. Interpret the event as a sign that it is better to finish shopping and go home.
Objective	Provide customer or third-party verifier with the entire traceability history of measurement instrument.
Precondition	The device should be registered on the platform.
Steps	1. To retrieve the traceability history of the device the customer provides to the platform its unique identifier (for instance scanning a QR-code). 2. Throw the platform exposed APIs the entire chain of traceability is recursively restored and displayed to the customer.
Outcome	The customer is enabled to unequivocally verify the entire traceability history of the device.
Remark	The open accessibility of all released document not necessarily fit well in all possible scenario. Some cases may require a higher level of privacy. Only necessary information should be disclosed. The appropriate level of access control can also protect sensitive information depending on the case.

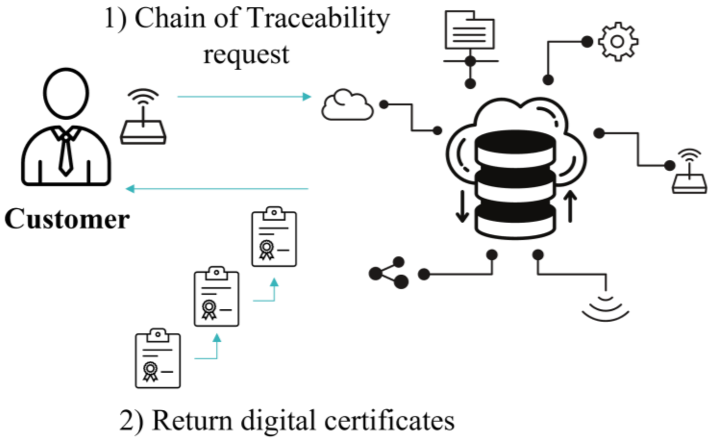

1) Chain of Traceability request
Customer
2) Return digital certificates

Figure 31 *Flow diagram: scenario 4.*

3.2.5 Scenario 5: Measurement signature

Description	A well-known electrical infrastructure manager has the ambitious goal of granularly optimizing facility overloads. To do this, it decides as a first experiment to install an infrastructure of distributed sensors based on smart meters in a critical areas of the country's most populous metropolis. Due to the high number of devices in the plant, to reduce costs, he decides to buy a very large lot but at a low price. Not trusting the quality of the measurements produced, he decides to calibrate a limited number of meters to be used as ground truth for subsequent comparative analyses. To keep track of the specific ground truth data, the manager decides to use the DCC standard which, although not officially approved, perform well in the digital data flow tracking as it is immediately processable and verifiable and associated with the uncertainty information. Once the data collection is complete, it cross-analyses the measurements between the group of non-calibrated devices and those collected by the calibrated sensors. The uncertainty associated with the two groups is quite

	compatible. Nevertheless, a relevant group of measurements coming from uncalibrated sensors diverges substantially from the others in terms of accuracy. In the same way, he realizes that one of the ground truth devices show a similar behavior. Since the device is registered on the quality infrastructure, it can easily identify it and from a second check it discovers a fault in that part of the network.
Objective	Link the measurement data with uncertainty expressed through the calibration certificate. The device data exchanged through the DCC representation should be univocally linked to the data and traceable.
Precondition	The calibrated instrument must be registered on the platform. A proper private key must be used to sign data.
Steps	1. The manager calibrates the specific ground truth device and register them on the platform 2. The manager stores the private keys in the device. 3. Collected measures are signed and a cryptographic proof of their integrity is stored on the platform. 4. The stored data are than analyzed gradually thanks to the unique correlation with their device.
Outcome	1. The enhanced data traceability allows a better and more reliable. 2. Measure and their uncertainty can be considered trustable, and integrity is preserved.
Remark	On the opposite of the previous point only a proof on integrity is stored publicly on the platform preserving privacy.

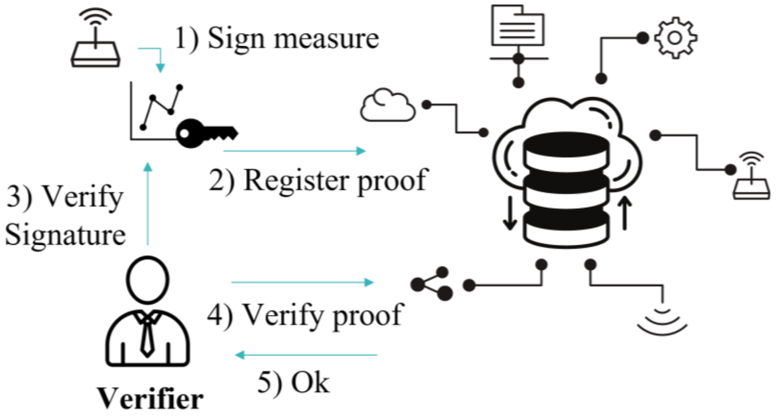


Figure 32 *Flow diagram: scenario 5*

3.3 Functional requirement

Three categories of interdependent functional requirements are identifying: identity and access management (IAM), information verifiability, data retrievability.

3.3.1 Identity and Access Management (IAM)

To grant security and integrity the entities acting on the system should be identifiable in order policy violation, misbehavior, and integrity corruption. This will simplify all types of digital interactions between different parties, both public and private sector, and on the end will disentangle final users, i.e., citizens, public administrations, private parties from the mutual recognition burden. Identities are not meant to be exclusively reserved for physical person or Institution. They are a key future to easily identify physical object that are accountable for the quality of produced information, e.g., smart sensor. Identification and authentication allow authorization and control of the system enforcing role-based control paradigm other than enforce privacy for every stakeholder and their specific business. It should be noted that intrinsically the ecosystem does not provide for equal role for all. We should distinguish for instance between authorities and user. Beside the fact that authorities should act as guarantors of trust they should be capable to issue other entities of authority, attest credential, authorize permission i.e., entities credential. On the other and user that don't join the system actively, but only as passive consultant of public information doesn't necessarily need to disclose his/her personal information if the platform must be a privacy complaint.

In summary the platform should:

- enable authoritative status of predefined users
- allow generic user identification and authentication
- allow authorities to define for other user specific certification privileges
- allow privacy preserving identification
- allow unique registration of artifacts e.g., certificate or device

3.3.2 Information Verifiability

Integrity of data could not be attested without some form of proof especially in a sheared environment in which all participant doesn't fully trust each other. The trust in authorities itself is not sufficient to grant the authenticity of data if such information is vulnerable to fraudulent manumission during their life cycle. Furthermore, while assuming the existence of such temper-proof record what can grant that it won't be lost or destroyed? To avoid accidental data lost actual service providers rely on redundancy to enforce their storage platform. This however does not prevent the risk of manipulation from the provers their self. When approaching a cross border environment as in the European Community. Finally, information, such as produced data and certification can highly simplify redundant manual practice and highly enhance data greedy optimization algorithm if shared across stakeholder under the appropriate shared governance rather than stuck in isolated silos.

However not all information is equal. some data could be more sensitive than other e.g., administrative data could not of the same importance as a for instance the temperature measure in a civil house. Data are related to context and different entities should have different degree of according to their role (Role Based Access Control RBAC), and attribute (Attribute Based Access Control ABAC).

The system should:

- allow information traceability with some form of certification
- allow information spreading in distributed fashion
- enable temper resistant information verification
- enable consensus and transparency in case of information updates
- allow selective operability on data based on role and or attribute

Such properties are well-matched with the paradigm of blockchain technology. Specifically, also for this category of requirement its highly suggestable the use of a public but permissioned platform to enforce the RBAC/ABAC policy. It should be noted that a prerequisite for the applicability of this condition is the existence of an IAM policy, so this requirement is strictly depending on the first category.

3.3.3 Data storage and retrievability

DLT/Blockchain technology is well suited to store data in a distributed, secure, and redundant fashion. Nevertheless, one of the main problems is related to storage. Large quantitative of data represent an excessive overhead for this kind of platform both in term of storage and of computational cost when processed in distributed fashion. This could represent a not negligible hindrance in term of scalability and latency that could limit the platform adoption. So, the data storage on-chain should be minimized as possible to grant the minimum level of performance required in the different possible use cases. To deal with such large data off-chain storage should be provide. Off-chain storage allow an easier management and indexing of data enhancing retrievability. There are two possible choices: standard centralize storage or decentralize storage system. In order to be consistent with the distributed nature of the platform and avoid the well-known problem related to centralized platform, e.g., single point of failure, opacity, etc., the system should opt for decentralized distributed storage. This will enhance the redundancy of the system and in principle the reliability. Also, ABAC should be valid on both on and off chain data.

The system should:

- minimize on-chain data storing, mainly proof of data authenticity
- provide off chain storage preferably in distributed fashion
- enable efficient indexing and retrieval of data

To accomplish the requirements a distributed database or file system will be embedded in the platform. An IPFS based system as Orbit DB could grant the required access control.

3.4 Proposed solution

Due to the basic requirements of our system a public permissioned network fit most of our needs. All provided service are developed based on the [54] approach, so they are loosely coupled, the REST approach is used for microservice communication. The platform architecture (Fig. 33) is layered as follow:

- **Node/network layer** : on this level the basic block-chain operation as the peer-to-peer protocol, transaction gossip, consensus is managed. Part of the access policy and control policy in managed and enforced on this layer.

- **Smart contracts layer** : The routine and protocol execution are power by the smart contracts that make the operation on the platform trustable and non-repudiable.

- **API/Service layer** : part of the Governance policy is executed on top of the blockchain. Everything is synchronized by means of a proper standard back-end solution powered by Node.js framework. This layer contains access points for all platform provided service.

- **Front-End layer** : user interface developed in react-native for an app-based interaction flow with the underling distributed backend.

3.4.1 Network architecture

As stated, the metrological infrastructure is based on a public permissioned network. Specifically, to implement such architecture Hyperledger Besu has been selected as DLT. The administration and governance of the system is managed by a subset of high-grade well recognized authority. For obvious reason it is supposed that the NMIs of every country joining the network will perform this role. As stated in the previous character the running nodes of the network are supposed to be well known. The communication protocol and the security of the network is accomplished with two concurrent solutions:

- **off-chain permission** : nodes that join the network are supposed to be allowed do it. This is implemented locally with an appropriate configuration file. This represents a whitelist both for node and accounts.

- **on-chain permission** : this is accomplished with smart contract that store and manage the account, node, and admin allow-lists. On-chain permission allows all nodes to access the allow-lists via a single source: the blockchain. To enforce the access control two contracts, deployed immediately after the instantiation of the genesis block, manage permission for node, account and a third smart contract store the list of admins node and account.

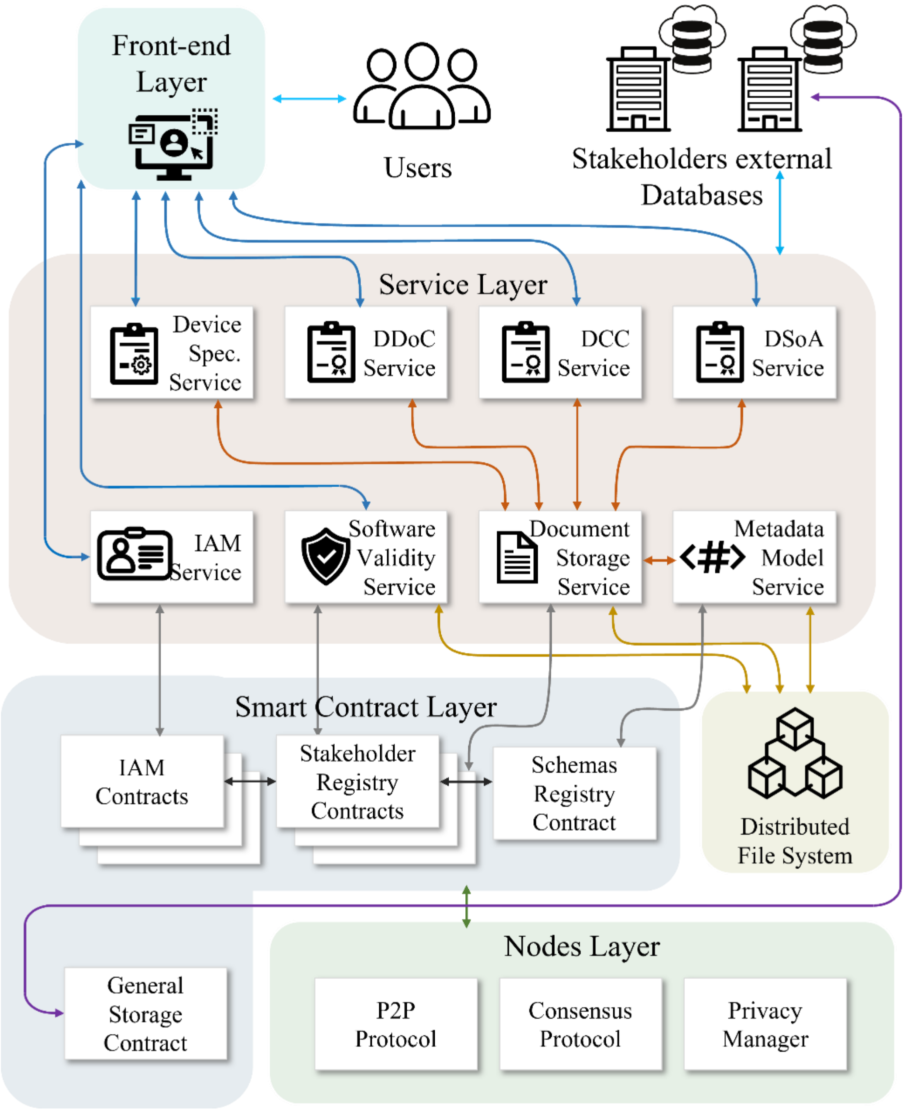


Figure 33 *Metrology Quality Infrastructure*

Because some tasks require a certain degree of privacy, e.g., software registration, validation and approval, the system leverages also on the private transaction manager functionality provided by the Tessera component joint to Hyperledger Besu. Each instance of a node is joint with an IPFS node that run inside a private network too. The OrbitDB are responsible to manage the off-chain storage. A management Agent is coupled with the nodes system. The agent exposes different RESTful API endpoints to the front-end for admins and for users. Everything is executed in Docker containers hosted on cloud infrastructure, e.g., the Amazon Web Service (AWS) cloud (Fig. 34).

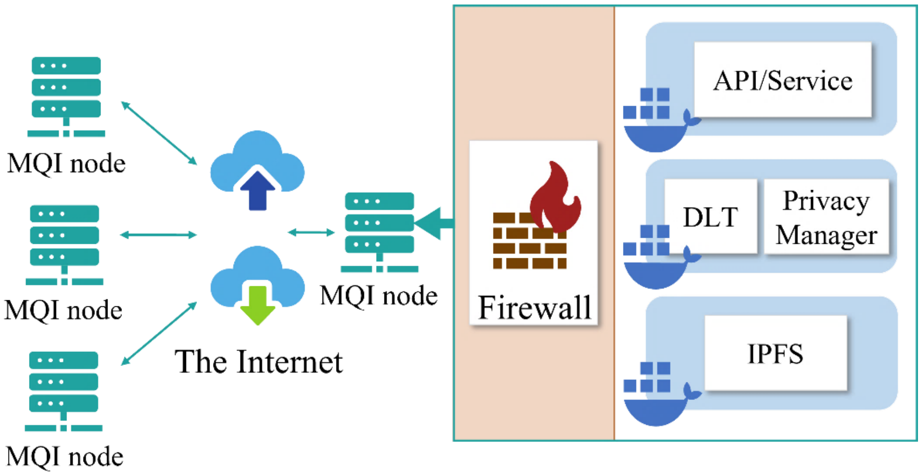


Figure 34 *The underling network infrastructure*

3.4.2 Service and API layer

The system relay on different Services/APIs:

- **Digital Scope of Accreditation Service** : It provides an automate service for DSoA issuance. It interacts with the Document Storage Service to retrieve the appropriate digital document that describe the testing procedure necessary to obtain the required accreditation. The access to the service is mediated through the IAM service. Once the test and verification process are completed the produced DSoA is validate against the schema through the Metadata Model Service. Then the document is stored on the distributed file system and a proof is registered on the DLT by means of the Document Storage Service.

- **Digital Calibration Certificate Service** : It provides an automate service for DCC issuance. It interacts with the Document Storage Service to retrieve the appropriate digital document that describe the testing procedure necessary to obtain the required certification. The access to the service is mediated through the IAM service. Once the test and verification process are completed the produced DCC is validate against the schema through the Metadata Model Service. Then the document is stored on the distributed file system and a proof is registered on the DLT by means of the Document Storage Service.

- **Software Validity Service** : It provides a software registration and verification service. The service exploits the privacy features of the infrastructure securing the software identifier (usually a hash supporting versioning) only among the interested party (i.e., the

Manufacturer, the Notified Body, and the Market Surveillance). The manufacturer registers the software hash and external URL through the service. The Notified Body retrieve the software , perform test, and approve it. The service could be later used for software verification from Market Surveillance.

- **Digital Declaration of Conformity Service** : It provides an automate service for DDoC issuance. It interacts with the Document Storage Service to retrieve the appropriate digital document necessary to issue the required approval and to verify if the software that will be tested on device batches has been already approved by means of the Software Validity Service. The access to the service is mediated through the IAM service. Once the test and verification process are completed the produced DDoC is validate against the schema through the Metadata Model Service. Then the document is stored on the distributed file system and a proof is registered on the DLT by means of the Document Storage Service.

- **Device Specification Service** : It provides a distributed storage service for manufacturer and user for Dev Specification Documents. It interacts with the Document Storage Service to store the documents. The service is public accessible. Only manufacturer has write-access right. The access to the service is mediated through the IAM service. The documents are stored on the distributed file system and a proof is registered on the DLT by means of the Document Storage Service.

- **Identity and Access Management Service** : It provides an interface for the blockchain core services and the smart contract that manage identity and authentication. It provides access token to access specific services based on the user role stored in the IAM smart contracts and Stakeholder Registry. Based on the identity model the identity and role verification could be different. For instance, in an SSI model, it queries the blockchain to resolve a DID and verify a token signature (that could represent a VC) through the DID document. However, regardless the identity model, once identity and role are verified it issue an access token for the desired service. This approach allows to reduce the amount of personal data to be stored on the cloud platform in compliance with GDPR.

- **Document Storage Service** : It provides a common storage system. Every document (Certificate , Template , Specification) is stored on the distributed file system through this service. It strictly interacts with the Metadata Model Service to validate the schemas of the stored document. On the DLT side it interacts with the stakeholder registry to store documents proof and with IPFS to store the whole documents.

- **Metadata Model Service** : It allows to retrieve the appropriate template (JSON/XML) necessary to process and validate a digital document (DSoA, DCC, DDoC, etc.). It interacts with the schema registry contract(s) to store the proof of the schema and with IPFS to store the whole schema. This core service is necessary to assure interoperability.

- **General Proof Storage Service** : This functionality lives on the blockchain and is directly accessible from the stakeholder databases. Whenever a stakeholder wants to store a signed data, it can access this smart contact. If the device, has its own private and public key it can directly sign the data. Otherwise, the device owner should sign the data embedding the device ID.

- **Front-End** : It is a special kind of service publicly available through a mobile/web interface. It exposes a user interface to all other services. It also includes a wallet API to manage the user public and private key and/or his/her decentralized identity and credential (in case of SSI) on the client side. The wallet allows to sign transaction off-chain or VC to interact with the identity system.

3.5 Approaches

We propose two different implementations of the system based on DLT technology. The first approach is a pure blockchain approach. All data and proof are stored on-chain and linked to IPFS. Users only store their keys. The second approach is based on SSI identity model. Users store both keys and Verifiable Credentials. The proposed solution allows also credential verification on chain.

3.5.1 Pure blockchain infrastructure

The first solution is based on a pure blockchain approach, i.e., no additional standards are involved in the protocol. The system is made of:

- **Organizations** : Organizations are considered public entities. They include Government Authority, Public Administration, Accreditation Body, Market Surveillance, Notified Body, Calibration Laboratories, Manufacturers. Organizations do not directly issue digital documents but delegate a technician for this purpose. Each organization is uniquely identified by an address on the network, name, type, identity, certifying identity, a reference to the accreditation or certification document, certification permission identifies.

- **Technician** : associated with an identity, the membership organization, and an address on the network.
- **Devices**: associated with a unique id.
- **Software meta store**: a collection of registered software metadata and status.
- **Measurement meta store**: a collection of registered measures with their metadata.

In traditional environment based on X.509 certificate to establish a secure certification chain for organizations, each new organization record is digitally signed by the certifying party, the same happens for the technicians. In a decentralized approach smart contacts provide the same capabilities. Ethereum has a built in PKI system that natively inherit the digital signature capabilities. Each transaction in Ethereum is signed by means of the private key of the account performing it. To enable automation the smart contract only needs to implement a Role Based Access Control (RBAC) policy in which the involved party goes under restriction on their write/read operation based on their role. A substantial difference exists among an entity and an object recorded on the blockchain. Entities are linked with an account (address) on the blockchain, while the objects are not. This characteristic enhances protection. Institutions and technicians can interact with the infrastructure, enlarge it, alter it, and are the real actors of the network. The security of the system is based on their authority, and they must have a unique identity. Conversely, the certificates are nothing more than elements of the database that any user of the network with appropriate authorizations can check. A second problem is data storage. As mentioned, the certificates are associated with external references, e.g., URLs, that store the complete reports and certificates. This reduces the load on-chain, which on the opposite can be extremely costly to maintain. To this end, IPFS represents a perfect match with blockchain technology for off-chain storage. Data uploaded to IPFS can be retrieved by a unique associated identifier hash. The access control is granted through OrbitDB software layer which allow to specify access policy (public, restricted, private).

3.5.1.1 Registries and smart contract

The smart contracts retain all the structures and identities of our system. The base contract is the Authority Contract, managed by national governments. The authority contract deploys a proxy contract for each institution based on its role. Each organization has its own contract in which it stores all relevant administrative and use case related information. The authority contract shares control of the proxies' contracts with their owner and can revoke them. It provides the following method for any kind of stakeholder:

- **Register stakeholder** : It deploys a proxy contract for the specific stakeholder sharing control with the stakeholder EOA. It also stores the address of the EOA and the deployed contract address with its status in a key value store. It grants the specific stakeholder to the proxy contract.
- **Unregister Stakeholder** : This function allows the authority to revoke the active status of a stakeholder. It also revokes the stakeholder role from the related proxy contract.
- **Get Stakeholder** : This function is a getter for the stakeholder contract.

The allowed proxy contract templates are:

- **The Manufacturer Contract** : This contract retains all administrative information of a Manufacturer. It also contains the list of all manufacturer products identified by a unique id and the related metadata, i.e., the device name, the serial number, the validity and expiration date, the revocation status, the device specification document external reference, the list of DCC certificate, the software ID if present, the list of Calibration certificate ID, the list of Declaration of Conformity certificate ID. This type of contract can register or unregister device and software.
- **The Accreditation Body Contract** : This contract retains all administrative information of an Accreditation Body. It also contains the list of all DSoA issued identified by a unique id and the related metadata, i.e., the external URL to the DSoA, the contract address of the accredited laboratory, the validity and expiration date, the revocation status, the delegate address. This type of contract can register or unregister DSoA.
- **The Calibration Laboratory Contract** : This contract retains all administrative information of a Calibration Laboratory. It also contains the list of all laboratory equipment identified by the device unique id and the related metadata, i.e., the device owner, the rental status, the validity and expiration date, the active status. It also stores the list of all DCC issued identified by a unique id and the related metadata, i.e., the external URL to the DCC, the calibrated device ID, the validity and expiration date, the revocation status, the delegate address. This type of contract can register or unregister DCC.
- **The Notified Body Contract** : This contract retains all administrative information of a Notified Body. It also stores the list of all approved software identified by a unique id and the related metadata, i.e., the

external URL to the software, the validity and expiration date, the revocation status, the software manufacturer related address. This kind of contract can approve software.

- **The Market Surveillance Contract** : This contract retains all administrative information of a Market Surveillance organization. It also stores the list of all DDoC issued identified by a unique id and the related metadata, i.e., the external URL to the DDoC, the device ID, the validity and expiration date, the revocation status, the delegate address. This kind of contract can register or unregister DDoC.

All contract stores a list of delegates identified by an Ethereum EOA and the related metadata, i.e., the organization contract address, the delegate's name, mail, and title. Each contract is coordinated by the authority contract (Fig. 35). When a contract needs to register a document/device it performs a delegate call to the authority inter-contract methods. For instance, when a calibration laboratory issues a DCC it calls the internal certify method that store the certificate metadata and then it calls the external certify method in the authority contract. The external method stores a reference of the certificate and the issuing laboratory. Then the authority contract pushes the DCC ID in the device metadata stored in the manufacturer contract of the calibrated device (fig). The inter-contact methods are: Add DSoA, Add DCC, Add DDoC, Register Device. All contracts expose the appropriate getters for stored data. The verification processes can be performed partly on-chain (expiration and revocation) and partly off-chain (e.g., proper chain of calibration).

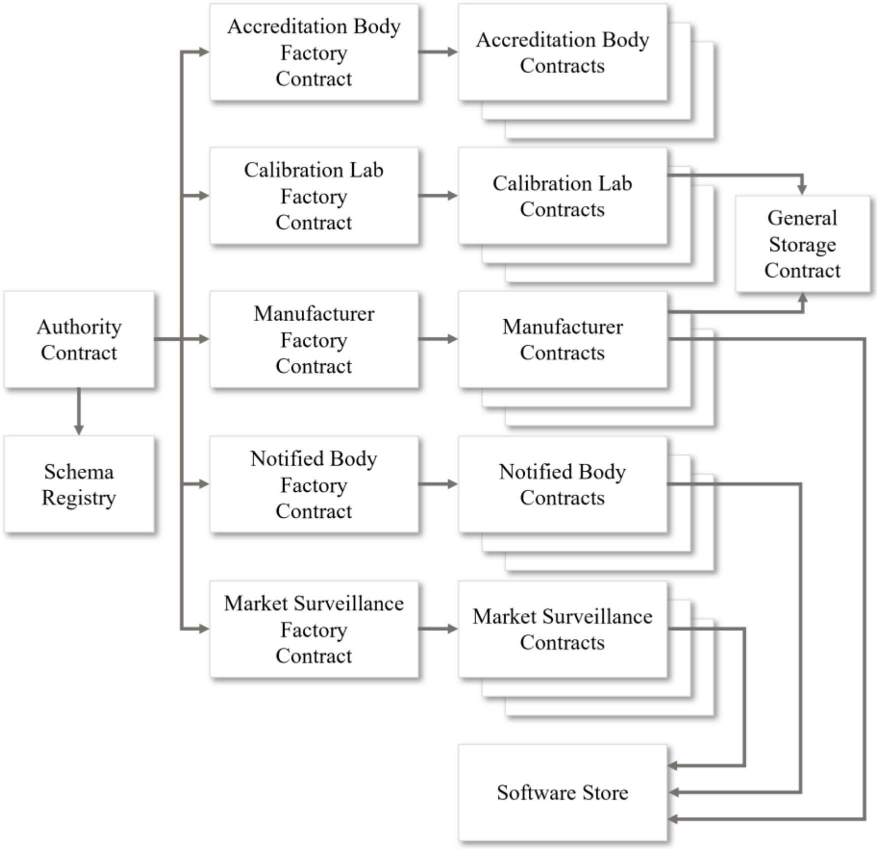

Accreditation Body Factory Contract
Accreditation Body Contracts
Calibration Lab Factory Contract
Calibration Lab Contracts
General Storage Contract
Authority Contract
Manufacturer Factory Contract
Manufacturer Contracts
Schema Registry
Notified Body Factory Contract
Notified Body Contracts
Market Surveillance Factory Contract
Market Surveillance Contracts
Software Store

Figure 35 *Pure blockchain smart contracts structure*

3.5.2 SSI approach

The system is wholly based on decentralized identities and on the ability to issue verifiable credentials to all the actors involved. Therefore, the relationships between the actors also determine the SSI data model. All components are identified by a DID, and the respective DID document. Authorities manage the governance of access to system resources. Authorities can partially delegate this governance to accreditors and certificate issuers. Access management must occur by registering a DID, necessary for identification and authentication to access the system services. Access to services must be subject to an access control policy. Not all entities have equal access to all resources. These policies are managed through smart contracts. Once access to the platform has been established, the entity may or may not identify itself in one of the following categories:

- **Admin** : the network-administrators. They issue smart-contract and manage their policy.
- **Authorities** : they have the task of carrying out the on-boarding of other entities in the system, they can issue credentials for:
  1. Identity Issuer (i.e., issuer of verifiable identity comparable to a national identity document or a passport). Government public administration is an example of Identity Issuer
  2. Device Identity Issuer (i.e., issuer of verifiable identity comparable to serial number or DUI, i.e., device unique identifier). Manufacturers are an example of Device Identity Issuer
  3. DSoA issuer. Accreditation bodies are an example of DSoA Issuer.
  4. DDoC issuer. Market Surveillance are an example of DDoC Issuer.
  5. Software Approver. Notified body are an example of software approver.
- **Accreditation bodies** : they can carry out the onboarding of Calibration Laboratory and issue DSoA credentials that turn the Calibration Laboratory in a DCC issuer.
- **Calibration Laboratories** : they can issue DCC credentials. These certificates are nothing more than a special form of credential issued to devices.
- **Manufacturing companies** : they produce the devices they sell to third parties. If they have certified devices, they are the holders of the latter's credentials.
- **Market Surveillance** : they approve software update and issue DDoC for devices.
- **Notified Bodies** : they test and approve new software. It’s not necessary for them to issue credential.
- **Device** : these are the subjects of the certifications. They can be the holders of their certificates themselves.

Verifiable credentials can be specialized of the following types:

- ID

- DevID
- Accreditation
- DSoA certification
- DCC certification
- DDoC certification

The credentials must conform to models accepted by the parties involved and, therefore, be validable. It means that outside the possibility of verifying they must be formally correct. They therefore require the registration of schemas. Based on the role or level it is necessary to verify which credentials an issuer can issue. To ensure integrity, a unique and non-repudiable proof of their existence must be recorded for each credential. Furthermore, the certification's status must be registered to allow its revocation.

3.5.2.1 Data Model

This part defines the data model for DID and the verifiable credential (VC) that is necessary for the underlying implementation of the role and function of the system.

A. DID schema and method specification

As already reported, a DID is composed of the two significant parts of method and identifier. Since the key argument of the thesis concerns the DCC, this acronym (dcc) will identify the method. The specific identifier can be created in two ways:

- Creation timestamp hash in combination with an internal index.
- Blockchain based address.

The first implementation is more general but involves greater implementation complexity, while in the second case, the intrinsic capacity of the underlying blockchain is exploited to generate unique identifiers. The blockchain address could be a EOA address or a smart contract address. It should be noted that the use of a smart contract as DID allows the association of the DID with generic functions that reinforce both its governance and functional autonomy. The smart contract approach relies on the proxy pattern in which a smart contract representing an entity performs operation using delegated call to another smart contract. This model refers to the one proposed by AlastriaID [91] or the legacy uPort DID protocol [92].

Here is an example:

$$did\colon mqi\colon eeacf848efb9924a383eabc52146083c$$

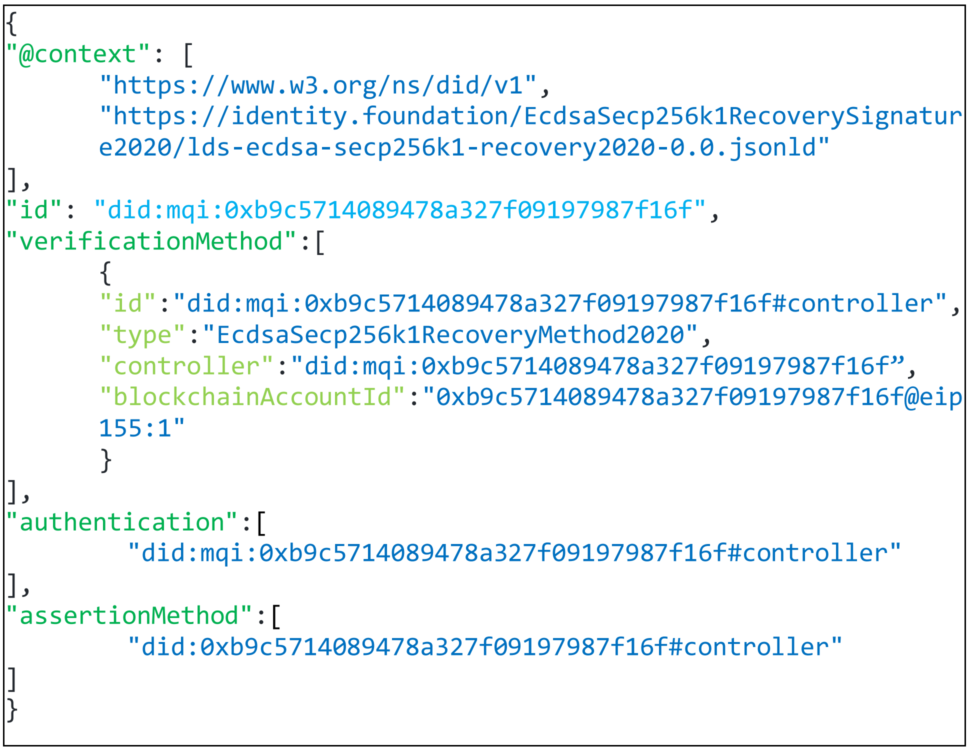
The DID document, the counterpart of the did that allows its use as an identifier for verifiability, is not physically stored in the registry. However, the specification of how to reconstruct it (virtual resolution) is given in [59] starting from the schema and a few basic information. In the Ethereum community, a pattern known as EIP-1056 [93]. utilizes a smart contract for a lightweight identifier management system intended explicitly for off-chain usage. The described DID method allows any Ethereum smart contract or key pair account, or any secp256k1 public key to become a valid identifier. Such an identifier needs no registration. In case that key management or additional attributes such as "service endpoints" are required, they are resolved using EIP-1056 smart contracts. EIP-1056 proposes a way of a smart contract or regular key pair delegating signing for various purposes to externally managed key pairs. This allows a smart contract to be represented, both on-chain and off-chain or in payment channels through temporary or permanent delegates. The main advantages of this method are:

- Free and private identifier creation
- Supports multi-sig (or proxy) wallet for account controller
- Supports secp256k1 public keys as identifiers
- Supports decoupling Ethereum interaction from the underlying identifier
- Flexibility to use key management

The DID document's outline follows the minimal specification of the W3C, i.e., context, DID, and public key, and a context extension to support non Ethereum public key standard. An example of a did document is reported in Fig. 36:

B. Credential

As already specified, the VC can be very generic and generally consist of an issuer, a series of claims referring to a subject, and a subject to whom they are issued. The issuer's signature is embedded to establish their integrity and verifiability. Specializations can be expressed either through the context property described by the W3C specification or the schema property. Given the recursiveness of the system (a VC can refer to the property of issuing another VC, e.g., a certain accreditation certifies the possibility of issuing certain certificates), the use of the schema property becomes fundamental to



```
{
"@context": [
      "https://www.w3.org/ns/did/v1",
      "https://identity.foundation/EcdsaSecp256k1RecoverySignatur
      e2020/lds-ecdsa-secp256k1-recovery2020-0.0.jsonld"
],
"id": "did:mqi:0xb9c5714089478a327f09197987f16f",
"verificationMethod":[
      {
      "id":"did:mqi:0xb9c5714089478a327f09197987f16f#controller",
      "type":"EcdsaSecp256k1RecoveryMethod2020",
      "controller":"did:mqi:0xb9c5714089478a327f09197987f16f”,
      "blockchainAccountId":"0xb9c5714089478a327f09197987f16f@eip
      155:1"
      }
],
"authentication":[
        "did:mqi:0xb9c5714089478a327f09197987f16f#controller"
],
"assertionMethod":[
        "did:0xb9c5714089478a327f09197987f16f#controller"
]
}
```

Figure 36 *DID Document Example.*

avoid the creation of too many context types that should instead provide only a metamodel of verifiable credentials, not specialized models. What specialize a VC is the credential schema associated with the credential subject. For instance, the DCC VC such credentials express all information necessary to link the calibration event with the DCC digital certificate (Fig. 37).

Although the DCC model was developed based on XML, there are some reasons why the JSON format has also several advantage. JSON is object-based and is much smoother than XML. Although this may slightly reduce security, having a smaller and less complex amount of data to describe the same information makes it advantageous, especially in the ambit of large quantities of data and constrained devices. Furthermore, W3C DID, and VC data model implementation natively support JSON and JSON-LD model. However, this research project provide support both for XML format and for JSON-LD format.

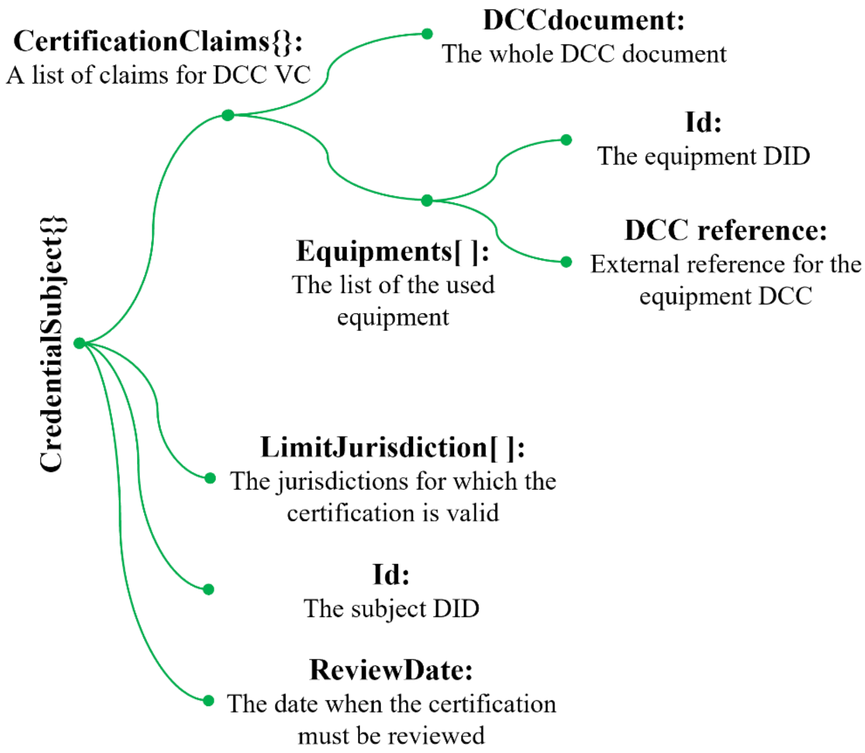

CredentialSubject{}
CertificationClaims{}:
A list of claims for DCC VC
DCCdocument:
The whole DCC document
Id:
The equipment DID
DCC reference:
External reference for the equipment DCC
Equipments[ ]:
The list of the used equipment
LimitJurisdiction[ ]:
The jurisdictions for which the certification is valid
Id:
The subject DID
ReviewDate:
The date when the certification must be reviewed

Figure 37 *DCC Credential Subject.*

3.5.2.2 Registries and smart contract

The registries are reliable data sources (single source of truth) established between different parties within the system based on different governance structures and on the scope. They enable the utilization of Decentralized Identifiers and VC acting as Trust services. The category of registry depends on what kind of information they should represent.

We distinguish five main contracts:

1. **Identity registry** : light weighted DID registry (EIP-1056 [93]).
2. **Infrastructure contract** : the infrastructure contract allows the implementation of the metrological infrastructure Role Based Access Control. It implements an Issuer Store in which each issuer is registered and linked to is Role. Whenever a new verifiable credential is going to be registered, the contract policy checks the issuer authorization. The contract is linked to the Credential Registry where the credential Id and metadata are stored. This

contract allows to verify the VC on-chain. It also supports delegation. The infrastructure contract is based on EIP-1812 [94] proposal. This proposal is based on EIP-712 [95] standard , i.e., a standard for hashing and signing of typed structured data as opposed to just byte strings. The proposal allows to define a blockchain (Ethereum based) data structure for a generic on-chain verifiable credential. This way credential signature is verifiable both on-chain and off-chain. The Credential Data Struct consist of the following field: issuer(DID), subject(DID), validFrom/To, data, typeHash and version. The data field is the SHA2 value of the credential subject in the original verifiable credential. This is due to limit the amount of data processed on chain to reduce speed up computation and avoid public disclosure of the credential subject on-chain (although credential subject is not explicit stored in a registry it appears as an input parameter in the registration function, which is still stored on-chain after computation). The typeHash value represent the credentialSchema ID. Credential schema also support versioning that is described by the version value.

3. **Credential registry** : the credential registry stores the credentials and their metadata in a key-value store. The credential is identified by their hash. The hash value is evaluated following the EIP-1812 [94] proposal. The credential Metadata struct is made of the IpfsHash , the from/to fields, and the status field. The IpfsHash allow to retrieve the VC off-chain on IPFS. The from/to field allow expiration verification. The status allows to revoke credential if necessary. An extra field embedded in the key value store is the credential issuer. This is a necessary field to enforce authorization policy in revocation process. This minimal set of information is selected to avoid disclosure of unnecessary information.

4. **Schema registry** : the schema registry stores the trusted CredentialSchema in a key value store. Only domains admins are allowed to register new schemas. A schema is identified by the first version hash of the schema. The schema's metadata are the values related to the schema key. The metadata contains the Ipfs Hash URL of the schema, the domain contract(i.e., the contract that is authorized to use the schema, the infrastructure contract in our case) and the version. The registry stores all versions of the schemas to support compatibility.

5. **Software Store** : this contract allows storage of software proof in form of hash and related metadata for approval process. The

records in the store are private to the manufacturer , the Notified Body, and the Market Surveillance. This policy is complaint with (Software Separation Requirement S1 and S3) outlined in the WELMEC 7.2 Software Guide [30].

6. **General data Store** : this contract allows to register prof related to generic data structure, for instance signed measured data. In this approach device own they personal DID they can sign transaction off-chain and just store the hash value of the measurement collection. Alternatively, it can embed the signature in the data collection and store it in a conventional database off-chain. In any case the produced data are verifiable through the signature .

The smart contracts schema is shown in Fig.38.

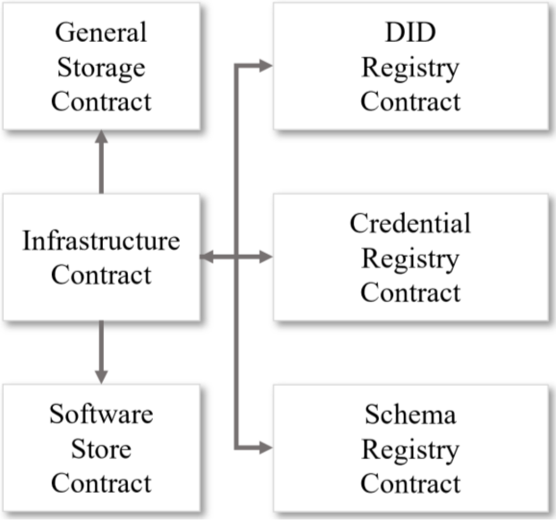


Figure 38 *SSI smart contract schema.*

3.6 The general system interaction flows

At a high level, the flow of interactions can be divided into three scopes:

- **Authentication and Identification**: it defines the sub-flows necessary to obtain registration on the platform of a DID and the release of VC identities for generic entities.
- **Issuer registration**: describes the sub-flows necessary for register an Issuer (Manufacturer, Accreditation Body, Market Surveillance etc.). A special case regards the Calibration Laboratory. To become an

Issuer a Calibration Laboratory, also need an accreditation indeed. So also, the certification sub-flow is included in this case.

- **Certification issuance**: describes the process for issuing a digital certification(DSoA, DCC, DDoC).

3.6.1 Authentication and Identification

The sequence diagram shows the sub-flow necessary for the registration of an entity. The procedure is general for each entity and does not characterize its role. The interaction with smart contract is slightly different in the two approaches.

In the first phase, the subject generates the keys and stores them in the wallets. Then it sends a request to the registration authority, starting the challenge-response procedure to verify that the entity owns the private key it claims to own. Optionally, the registration authority can request a legacy registration to associate the EOA with legacy credentials (email and password). The diagram omits this step. Once the procedure is completed, the server adds the entity EOA in the allowed-account list calling the IAM smart contract:

Table 6 IAM interaction flow part 1.

Sender → Receiver	**Interaction**
Entity →Entity Wallet	Request new keys
Entity Wallet →Entity Wallet	Generate and store keys
Entity →Registration Authority	Request for DID registration
Registration Authority → Entity	Send challenge
Entity →Entity Wallet	Ask challenge signature
Entity Wallet →Entity	Return signature
Entity →Registration Authority	Send challenge + signature
Registration Authority → Authority Wallet	Ask for signature check
Authority Wallet → Registration Authority	Signature verified
Registration Authority →IAM contact	Send EOA public key

IAM contact → IAM contract	Verify Access Control Policy
IAM contracts → IAM contract	Insert EOA public key

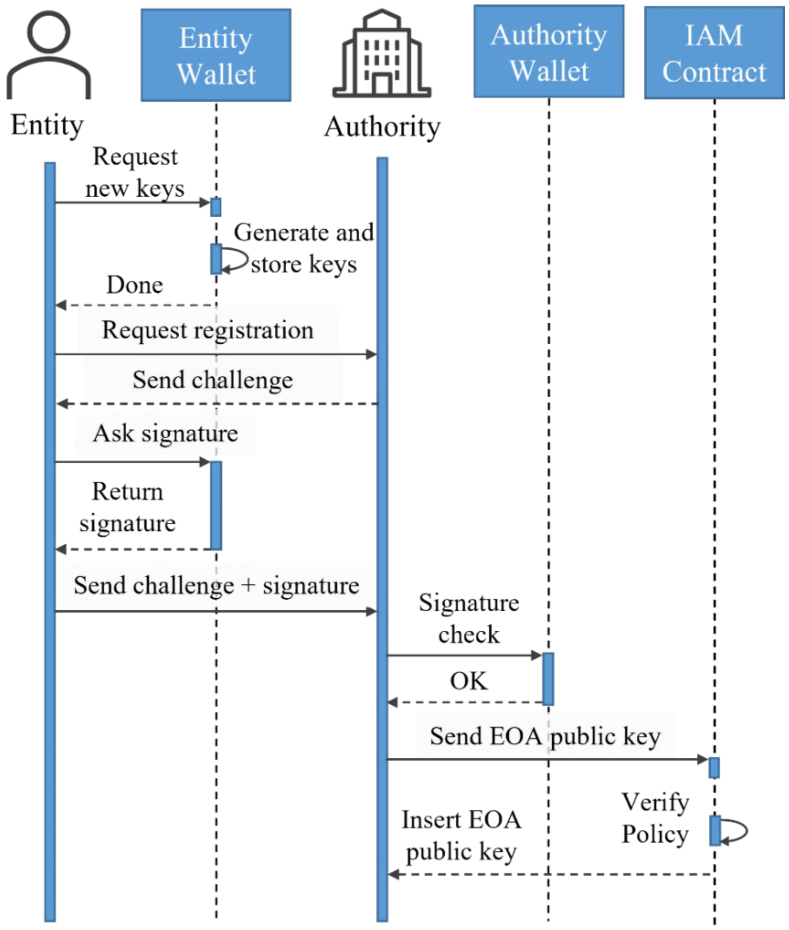


Figure 39 *IAM interaction flow part 1.*

3.6.1.1 Entity registration with pure blockchain approach

In the second phase the Authority register the entity based on his role. The authority calls the register stakeholder providing all necessary inputs for the specific stakeholder. The authority contract calls the stakeholder factory contract that instantiate the new stakeholder contract. After deployment the authority contract link in its internal store the stakeholder EOA to the new contract address. The authority sends the newly deployed contract address to the Entity. In summary:

***Table** 7 IAM interaction flow part 2, pure blockchain approach.*

Sender → Receiver	**Interaction**
Registration Authority → Authority Contract	Send stakeholder EOA and registration data
Authority Contract → Stakeholder Factory	Call registration function
Stakeholder Factory ^{new} → Stakeholder Contract	Deployment
Stakeholder Factory → Authority Contract	Return contract address
Authority Contract → Registration Authority	
Registration Authority → Entity	

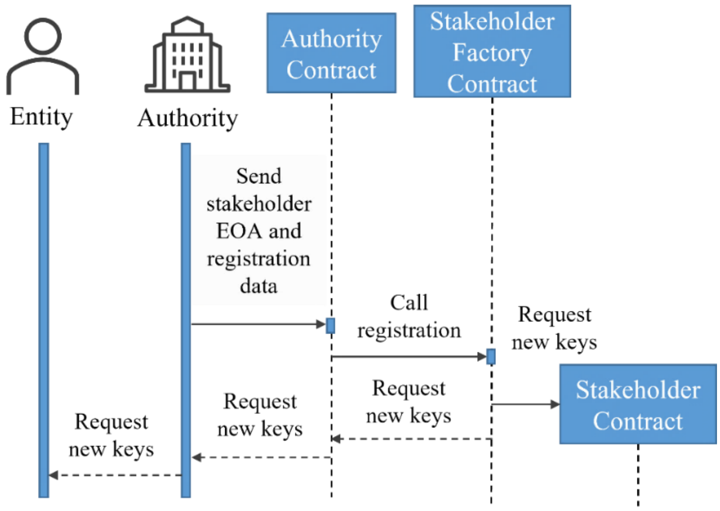


Figure 40 *IAM interaction flow part 2, pure blockchain approach.*

3.6.1.2 Entity registration with SSI approach

The authority sends a request to the IAM Service in the second phase, including the VC necessary for registration (Identity VC). The IAM service check the access policy verifying the authority address in the Quality Infrastructure store than it stores the verifiable credential through the credential contract. After the verification and the approval process the authority sends the VC to the Entity. In summary:

Table 8 *IAM interaction flow part 2, SSI approach.*

Sender → Receiver	Interaction
Authority → Authority Wallet	Generate VC
Authority Wallet → Authority	Return VC
Authority →IPFS	Store Acc. DOC
IPFS → Authority	Return IPFS URL
Authority →IAM service	Send VC
IAM service →Quality Contract	Verify Policy
Quality Contract →Credential Contract	Store VC
Authority → Entity	Send VC
Entity →Entity Wallet	Store VC

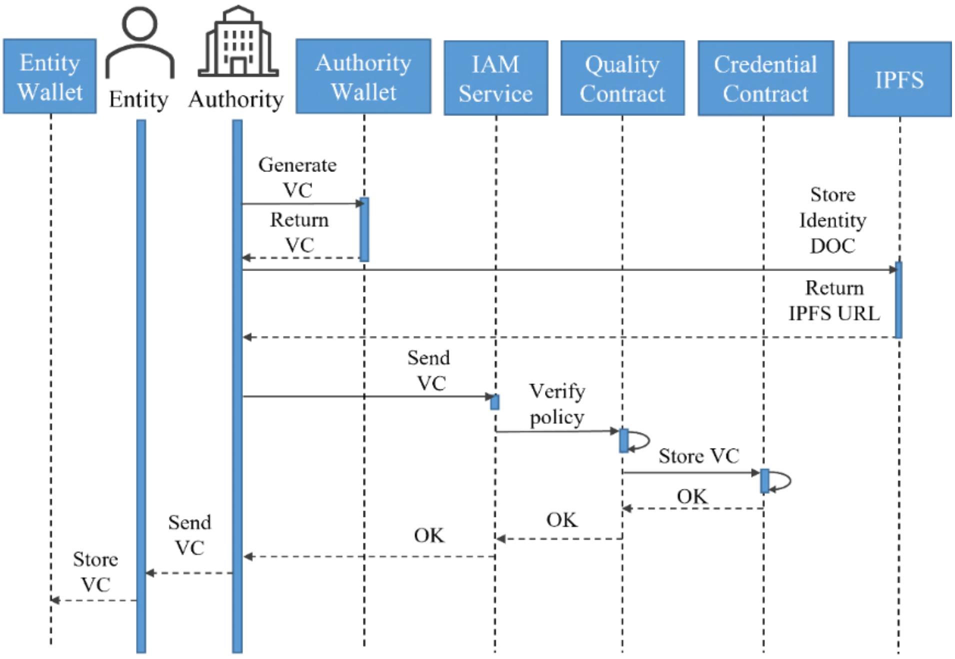


Figure 41 *IAM interaction flow part 2, SSI approach.*

3.6.1.3 Device registration

In pure blockchain approach the manufacturer to register a device need to call an internal function in his contract. In the SSI approach device are considered special kind of entity so the registration is identical to the previous case.

3.6.2 Accreditation

The accreditation of a certifier or another accreditor in the pure blockchain approach is realized through an internal function call in the Authority to the add accreditation function. In the SSI approach the accreditation of a stakeholder need the issuance of a verifiable credential. The interaction flow is almost identical to the previous case. The substantial difference is in the policy verification. In that case the quality infrastructure contract verify that the stakeholder role is aligned with the credential type provided in the verifiable credential. The general rule is that Authority can accredit every stakeholder except the Calibration laboratory while Accreditation body is in charge to accredit Calibration Laboratory. Once accredited the stakeholder is registered in the Issuers register.

Table 9 *Accreditation interaction flow, pure blockchain approach.*

Sender → Receiver	Interaction
Issuer → Accreditor	Ask Accreditation
Accreditor →IPFS	Store Acc. DOC
IPFS → Accreditor	Return IPFS URL
Accreditor →Accreditor Contract	Call Accreditation Function
Accreditor Contract → Accreditor Contract	Store Accreditation
Accreditor Contract → Authority Contract	Store Accreditation Proof
Authority Contract → Accreditor Contract → Accreditor→ Issuer	Return Proof ID

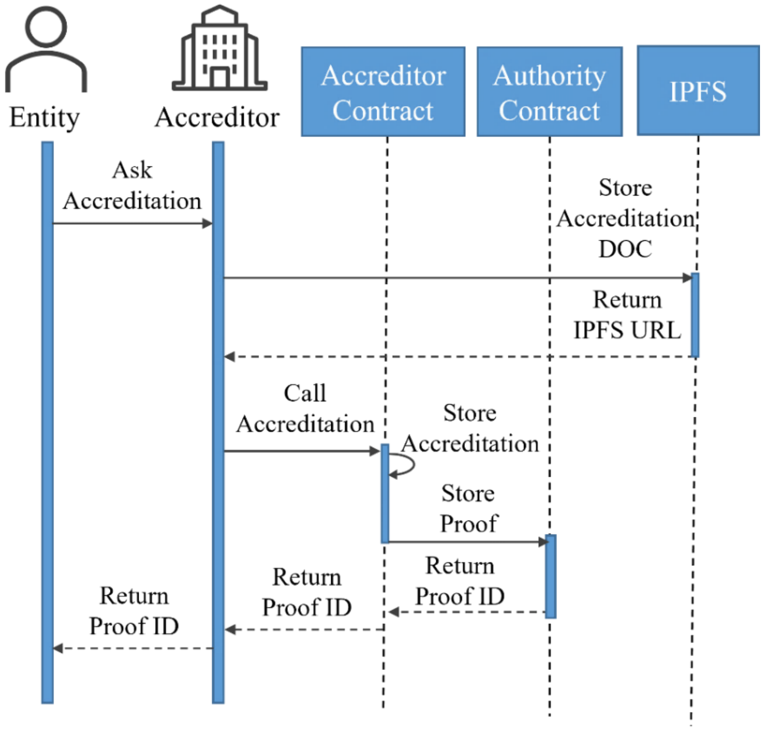


Figure 42 *Accreditation interaction flow, pure blockchain approach.*

Table 10 *Accreditation interaction flow, SSI approach.*

Sender → Receiver	**Interaction**
Issuer → Accreditor	Ask Accreditation
Accreditor → Accreditor Wallet	Generate VC
Accreditor Wallet → Accreditor	Return VC
Accreditor →IPFS	Store Acc. DOC
IPFS → Accreditor	Return IPFS URL
Accreditor →Quality Contract	Send VC
Quality Contract →Quality Contract	Verify Policy
Quality Contract →Credential Contract	Store VC
Accreditor → Issuer	Send VC
Issuer → Issuer Wallet	Store VC

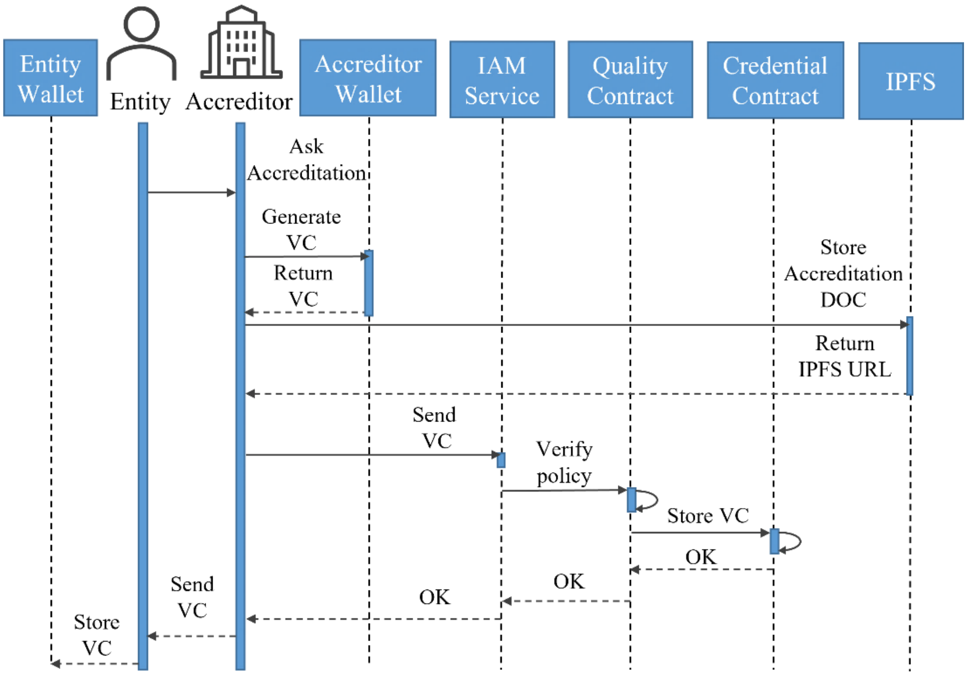


Figure 43 *Accreditation interaction flow, SSI approach.*

3.6.3 Certification

The certification requires the registration of the issuance of Digital document. In both approach this require the formal verification of the document structure and access policy. First the Issuer collect all data to fill the document form using the front-end service. The front end calls the metadata model service that receive the XML/JSON document. The metadata model service calls the schema registry retrieving the external URL of the document schema. The metadata model service retrieve from IPFS the schema and proceed with validation. After this procedure it store the document through the document storage service. The document storage service uploads the document on IPFS than it stores the hash proof. In case of pure blockchain approach the hash, proof is a structured record stored in one of the stakeholder contracts depending on the kind of document (e.g., the DCC is stored in the Calibration laboratory contract store). In case of SSI the VC related to the document is stored in the credential registry. In the end the contracts return the IPFS link and the hash proof of the document. The flow is summarized in the following table for the case of DCC Issuance:

Table 11 *Certification interaction flow, part 1.*

Sender → Receiver	**Interaction**
Entity → Front-End	Ask for DCC
Front-End → Calibration Service	Require form
Calibration Service → Front-End	Return form
Front-End → Issuer	Require form filling
Issuer → Front-End	Provide inputs
Front-End → Schema Service → Schema Registry	Ask for DCC schema
Schema Registry → Schema Service	Return schema URL
Schema Service → IPFS	Ask schema
IPFS → Schema Service	Return schema
Schema Service → Schema Service	Validate schema
Schema Service → Front-End	Validation OK

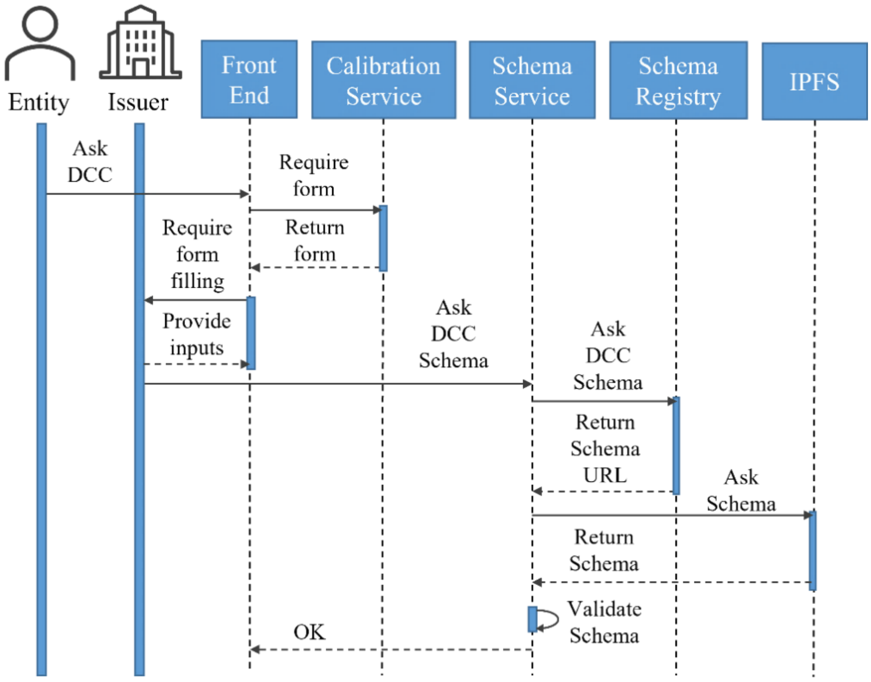


Figure 44 *Certification interaction flow, part 1.*

Table 12 *Certification interaction flow, part 2.*

Sender → Receiver	Interaction
Front-End → Doc Storage Service	Send Doc
Doc Storage Service → Doc Storage Service (SSI)	Convert doc in VC
Doc Storage Service (SSI) → Issuer Wallet	Require signed VC
Issuer Wallet → Document Storage Service (SSI)	Get signed VC
Doc Storage Service → IPFS	Upload Doc
IPFS → Doc Storage Service	Get IPFS URL
Doc Storage Service → Stakeholder Contract (PB) Doc Storage Service → Credential Registry (SSI)	Store proof record
Stakeholder Contract → Doc Storage Service (PB) Credential Registry → Doc Storage Service (SSI)	Get hash proof
Doc Storage Service →Front-End → Entity	Get hash proof and IPFS URL Get VC (SSI)
Entity → Entity Wallet (SSI)	Store VC

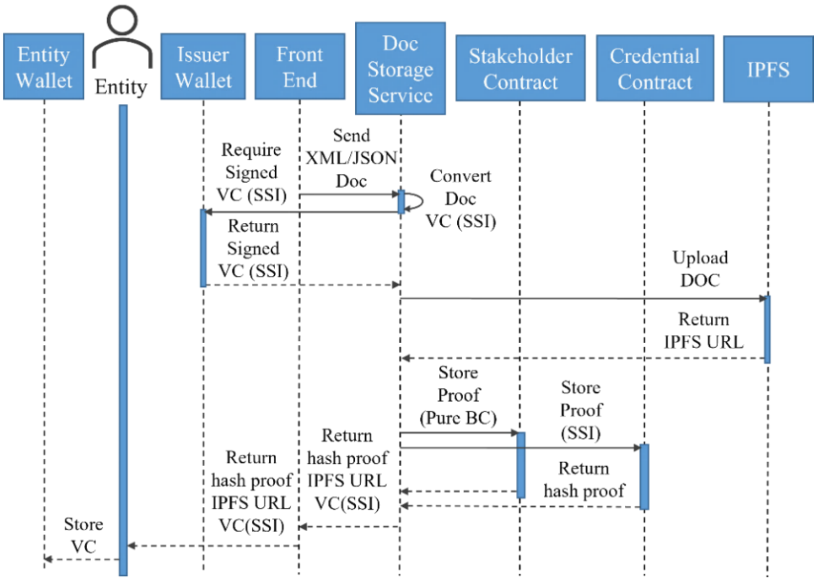


Figure 45 *Certification interaction flow, part 2.*

3.6.4 The chain of traceability

The chain of traceability use case is the simplest scenario to implement. As a precondition, we suppose that certificates are all public along the traceability chain. We suppose that a person has access to a device and would like to retrieve the entire traceability chain. We suppose that the device has his ID/DID on the platform. The user accesses the Frontend of the quality infrastructure. With his/her smartphone, he selects the Document Storage Service. The web page asks him/her to use web NFC to identify the device. With the NFC, the device authenticates with the server using his wallet. Then the Document Storage Service queries the Stakeholders Contracts/ Credential Contract to retrieve the IPFS URL of the certificates related to the device. It retrieves the documents from IPFS. From the document, it extracts the IDs/DIDs of the calibration equipment and repeats the procedure mentioned above for each IDs/DIDs. The process is reiterated until the last certificate that should not contain any reference to equipment. The service builds a graph of certificates. The front-end then presents the result. In summary:

Table 13 *The chain of traceability interaction flow.*

Sender → Receiver	**Interaction**
User → Front-End	Ask for device chain of traceability
Front-End → User	Ask for dev ID/DID
User → Front-End	Provide dev ID/DID
Front-End → Doc Storage Service	Require certificates
Doc Storage Service → Stakeholder Contract (Pure Blockchain)	Ask IPFS URL
Doc Storage Service → Credential Registry (SSI)	
Stakeholder Contract → Doc Storage Service (Pure Blockchain)	Return IPFS URL
Credential Registry → Doc Storage Service (SSI)	
Doc Storage Service → IPFS	Get Doc
IPFS → Doc Storage Service	Return Doc
Doc Storage Service → Doc Storage Service	Get Equip. IDs/DIDs
Repeat until equipment’s certificates has no reference	

Doc Storage Service → Front-End	Provide cert. graph
Front-End → User	Display results

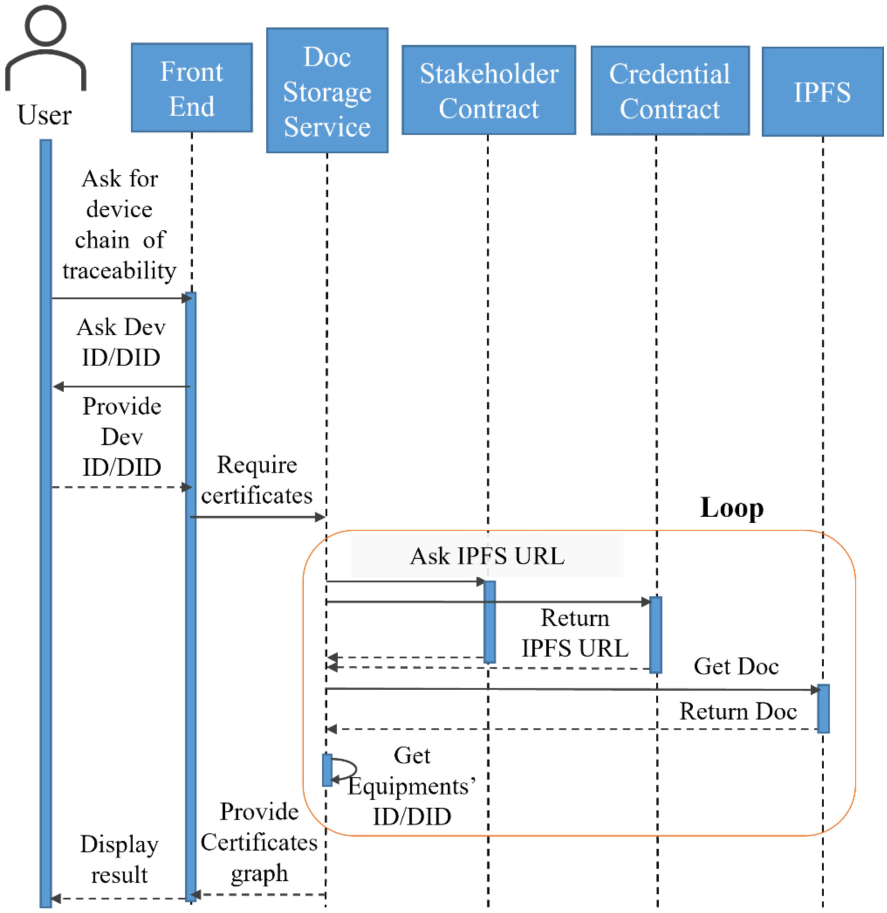


Figure 46 *The chain of traceability interaction flow.*

3.6.5 Trusting measure with respect to the traceability chain

A classic use of the blockchain is to register a hash proof for any data set. Even in the case of measurements produced by a device, the mechanism applied is always the same: a hash function is applied to the data (for example, sha256) after which the hash and the sender are registered on the blockchain in the general storage register. Subsequently, to verify the data, it is possible to calculate the hash again and query the blockchain to ascertain its existence. In the case of measurements produced by a device, in addition to the DID, a timestamp is also associated with the hash. The flow interaction is as follows. Once the record is ready the device sends it to the general storage contract. The storage contract stores the record the hash produced from the concatenation of the sender ID/DID, the timestamp, and the produced measures. When necessary, it is possible to verify both the authenticity of the data and the author.

Table 14 *Trustable measurement interaction flow.*

Sender → Receiver	**Interaction**
Stakeholder Device → Device Manager (Who own a valid private key)	Send new measure
Device Manager → Device Manager	Generate hash proof from measure, ID/DID, and timestamp
Device Manager → General Storage Contract	Send new hash proof and timestamp
General Storage Contract → Device Manager	Registration completed

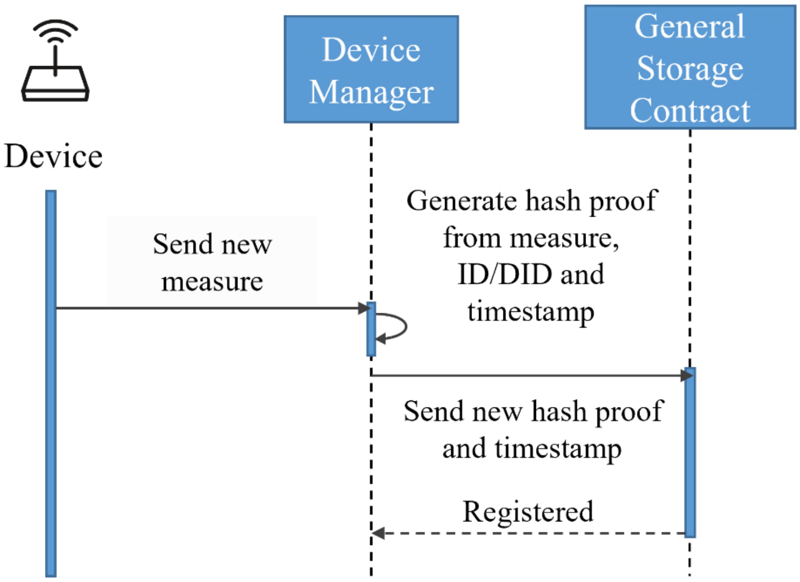

Device
Device Manager
General Storage Contract
Send new measure
Generate hash proof from measure, ID/DID and timestamp
Send new hash proof and timestamp
Registered

Figure 47 *Trustable measurement interaction flow.*

Chapter 4

Qualitative and quantitative analysis

The following chapter compares the two proposed approaches in qualitative and quantitative terms.

First, the qualitative analysis highlights the advantages and disadvantages of the two approaches from a high-level view. Secondly, performance measures are carried out based on a concrete implementation of the proposed system. The metrics are defined, and the results are shown and compared.

4.1 Qualitative analysis

The two proposed approaches differ mainly in representing the entities registered on the blockchain. The pure approach defines the stakeholders statically and a priori. The entire identity system is specified on the blockchain using proxy contracts that are specific to each stakeholder. In the case of SSI, the constraint of statically defining the identity system does not exist. It only requires the definition of a storage contract for the Issuers and another for the credentials. The roles are dynamically updatable by changing the records in the Issuer contract. Also, from the point of view of the representation of the devices, the two approaches differ substantially. In the pure approach, the devices are represented by a record on the blockchain. Vice versa, in the SSI case, each device has its own DID (and its EOA). A first consequence is related to the case of the use of the recording of measures. In the pure approach to digitally signing a measure, the devices depend on their owner's EOA. The stakeholder must sign in place of the device. This step introduces another trust requirement in the verification process.

On the contrary, with the SSI approach, each device owns a private key and can digitally sign the measures it produces. The device does not need to submit the transaction on the blockchain directly, but the signature of the transactions can take place off-chain. A proxy (e.g., IoT gateway) receives the signed verification transaction and submits it to the blockchain. Another advantage of the SSI-based system is the ease with which it can perform key rotation for the devices (which is particularly critical in the case of IoT devices). The keys associated with the EOAs are used for identification and secure communication through the TLS protocol. In general, thanks to the DID registry, besides the intrinsic keys of an EOA, it is possible to associate other keys for different purposes.

Furthermore, through the DID registry, it is possible to remap DID to a different EOA without modifying it, enhancing system flexibility. Finally, unlike the pure approach, the SSI approach only requires the DID and credential registries to be safe. The VCs can be easily verified only through the information relating to the DIDs and the revocation status of the VC. The off-chain verification is one more step that allows the automation of the confirmation of the Issuer's role by eliminating the need to build a chain of VCs to establish the Trust Anchor of the System (see section 2.2.3).

The table below shows the qualitative comparison of the two systems:

Table 15 *Qualitative comparison of the used approaches*

Approach	**Pure blockchain**	**SSI**
Identity System Flexibility	Static (LOW)	Dynamic (HIGH)
Device Identifier	Static ID	DID
Device Key Rotation	None	Extremely flexible
Off-chain Verification	No	Yes

4.2 Quantitative analysis

This analysis investigates how both approaches perform in practice. First an overview of the various performance metrics that will be measured during the benchmarks are discussed. The benchmarks methodology and the system set-up are then described, as well as the smart contract used. The results are then compared. The DLT technology used is based on a Public Permissioned Blockchain, i.e., Hyperledger Besu [96] .

4.2.1 Performance Metrics

We are interested in the throughput to test the network in the two configurations as the type of transaction under test varies. The throughput is calculated globally over the entire test interval. Generally, the throughput can undergo slight variations over time, but we are interested in the average performance.

The following equations define throughput:

$$N = Total\ number\ of\ transactions$$

$$t_{start,i} = Creation\ time\ transaction\ i$$

$$t_{stop,i} = Commit\ time\ transaction\ i$$

$$Throughput = \frac{N}{\max\left(t_{stop,i}\right) - \min\left(t_{start,i}\right)}$$

The second metric to consider is transaction latency. The latter is defined as the time difference between creating and committing a transaction. We opt for a measure of average latency.

$$Latency_i = t_{stop,i} - t_{start,i}$$

$$AvgLatency = \frac{\sum_{i=1}^{N} Latency_i}{N}$$

The last factor to consider is the success rate of the transactions, i.e., the Success Rate.

$$Success\ Rate = \frac{SuccessTxs}{FailedTxs + SuccessTxs} * 100$$

4.2.2 Experimental Set-Up

The test environment used in the benchmark is Hyperledger Caliper, a generalized test tool for various blockchain implementations. The use of calipers makes it possible to ensure that the tests carried out are conducted through multiple frameworks using the same type of flow and guarantees comparability. The test environment was instantiated via docker container on System Debian Linux on an AWS t3.large instance.

Caliper currently collects the following performance metrics [97]:

- Error rate
- Transaction/Read(or queries) throughput.
- Transaction/Read (or queries) latency(minimum, maximum, average)

The network topology is shown in the Fig. 48. The consensus protocol selected is IBTF2.0, a more robust variant of Proof of Authority. The number of validators that the BFT can guarantee is four. Two regular nodes were then added to more likely simulate the propagation delay.

Each node was instanced via docker container on Debian Linux System on AWS t3.xlarge instances for validators and on AWS t3.large instances for regular nodes.

The table summarizes the hardware characteristics for each node.

Table 16 *Nodes hardware and software configuration*

Node	Processing Units	Virtualization Software	RAM	Storage
Caliper Test Environment	2 vCPU	Docker 20.10. 2	8 GB	St1 shared EBS instance Storage: 125GB Throughput: 7,500 MB/s
Validator Node	4 vCPU		16 GB	
Validator Node	2 vCPU		8 GB	

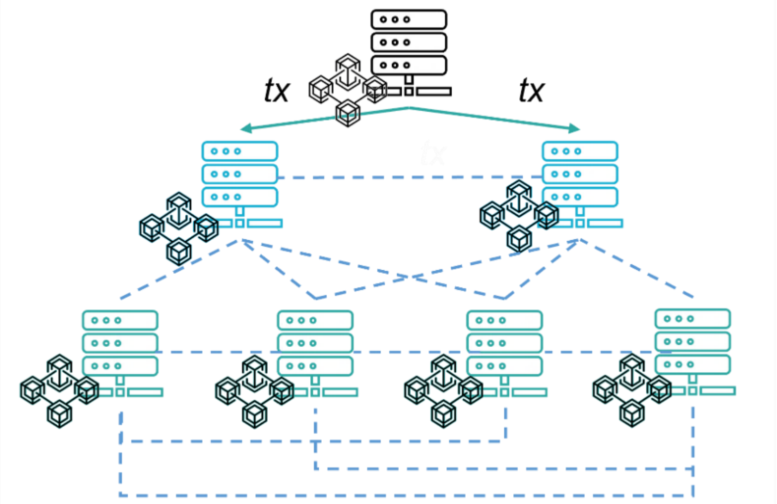


Figure 48 *Test environment configuration*

4.2.3 Gas: classifying transaction based on computational cost

The gas measures how much computation power (per node) is required to execute a transaction in an Ethereum network. The transaction cost (in gas) can increase according to the type of operations carried out. Write operations are the most critical as they require access to the permanent memory of the Ethereum Virtual Machine (EVM). The second type of highly gas-consuming operation is cycles. The use of temporary memory, on the other hand, consumes a relatively small amount of gas. One category of zero-cost transactions (in terms of gas) is query operations. In general, all the operations that do not require consensus can be performed locally by accessing their copy of the blockchain.

The primary operations involving smart contracts analyzed in the interaction flow can be classified based on the gas cost. The gas measurement per transaction was carried out using the Truffle software combined with custom test scripts written in Node.js. Truffle is a test environment that simulates a local blockchain Ethereum with a set of pre-configured test accounts.

The tests include several phases.

- Registration of a stakeholder
- Accreditation of an Issuer
- Issuance of a Certificate
- Registration of a generic hash proof

The table shows the estimated costs for both approaches

Table 17 *Gas consumption per case and approach*

Operation	Pure Blockchain	SSI
Registration	*Average on stakeholder*	
	2.4 10E6	9.7 10E4
	Device	
	1.6 10E5	9.7 10E4
Accreditation	*Average on stakeholder*	
	2.2 10E5	1.7 10E5
Certification	*Average on stakeholder*	
	2.5 10E5	9.7 10E4
Hash-proof storage	7.3 10E4	

By a visual inspection, we realize that the System based on the SSI approach outperforms the System based on the pure blockchain approach. The significant differences are evident in the case of registration and in that certification.

4.2.4 Baseline performance

To establish the most suitable configuration for the network, we refer to the benchmark carried out by Mark Soelman [96]. In the analysis provided, the author provides a comparison of the performance of a network based on Hyperledger Besu as the following parameters vary:

- **Block time** : time between the production of a new block and the previous one
- **BlockGasLimit** : Maximum amount of Gas allowed per block. It affects the number of executable transactions per block. Costly transactions require a high limit for the same throughput
- **Number of Validators** : the author demonstrates that as the number of validators increases, the system's latency increases very slowly.

> However, vice versa tends to decrease the error rate for high TPS. It is because the error rate is strictly related to the buffering capacity of the transactions. Each validator has a transaction pool at its disposal to buffer excess transactions when the BlockGasLimit is exceeded. As the number of validators increases, virtually every pool will contain a certain percentage of different transactions. This fact effectively increases the size of the global transaction pool. Statistically, fewer transactions are discarded, reducing the error rate.

The analysis is based on a classic smart contact or a Non-Fungible Token (NFT) contract. An NFT is an asset represented on a blockchain associated with an owner who is unique and not interchangeable. An NFT contract is very similar to a General Proof Storage Contract. In [98] the author tests the system's capabilities with a specific type of Single Read-Single Write transaction., i.e., an asset transfer. The cost of this transaction is approximately 60,000 gas units. The type of transaction closest to this value in the case of Metrology infrastructure is the registration of a hash-proof (about 70000 gas units).The original baseline benchmark configuration is reported in the following table:

Table 18 *Baseline benchmark configuration.*

Contract Visibility	Public
Number of Peers	3
BlockTime	2 sec (default)
Block Gas Limit	1.25 10E7 gas unit (default)
Transaction Pool Limit	4096 transactions (default)
Consensus Protocol	IBFT 2.0

With this configuration the NFT transactions on the network can reach around 80 TPS with an average Latency of 1.08 sec and Error rate null. The author proofs that increasing the BlockLimt of 3 time (around 50000000 gas unit) the throughput moves to 320 TPS with 1.3 sec latency and Error Rate null. Starting from the original code available on GitHub [99], we replace the NFT contract with the General Storage contract. We also change the Caliper configuration file to test only the record registration operation. The variations to the original configuration are the number of Peers (6) and the Block Gas Limit (50,000,000 gas unit).

The test on our system shows a throughput of 320 TPS with an average latency of 1.5 sec and an Error rate null. This configuration will be used to test write and read- write operation for all type of transaction of our interest. Regarding query transactions (Request per second or RPS), to determine a test limit, we refer to the official report by Hyperledger Besu [100] relating to the performance enhancement of version 1.5. The report states an RPS maximum rate of around 8600. The RPS test limit has been settled to 8000. The same report underlines for the case of TPS a maximum TPS rate of 350, which complies with the results reported in [98].

Once the network configuration was established, stress tests were carried out, lasting one minute for each type of transaction.

4.3 Test results

The following tables show the results of the tests carried out organized by configurations (first approach and second approach).

Table 19 *Pure blockchain approach test result.*

Pure Blockchain Approach				
Name	**Sent**	**Success Rate**	**Latency (sec)**	**Throughput (TPS)**
Registration	19200	56.18 %	7.12	179.7
Accreditation	19200	87.86 %	3.93	281.1
Certification	19200	84.7 %	1.66	270.9
Store hash	19200	100%	1.5	320.0
Query DCC	480000	100%	0.32	8000.0

Table 20 *SSI approach test result.*

SSI Approach				
Name	**Sent**	**Success Rate**	**Latency (sec)**	**Throughput (TPS)**
Registration	19200	100%	1.65	320.0
Accreditation	19200	99.6%	1.97	318.7
Certification	19200	100%	1.66	320.0
Store hash	19200	100%	1.5	320.0
Query DCC	480000	100%	0.32	8000.0

4.3.1 Result discussion

As can be seen from the results shown, the softer transactions (gas cost equal to less than 100,000 units) are compatible with the maximum throughput of the network. Despite this, one more consideration must be made for the case of recording a hash associated with a measurement. Measurements are collected continuously from millions of devices in IoT systems. The throughput of a network thus constructed is therefore limiting for this use case. In the case of HARD transactions (gas cost greater than 100,000 units), on the contrary, we note how the maximum throughput of the network is reduced the more the gas units required increase. It is especially evident in the pure approach as we expected. The case of recording is the most emblematic. As already mentioned, registration is a crucial process for the infrastructure. Low throughput is extremely limiting regardless of possible use cases. The causes of the high gas cost for the pure approach are to be found in the registration protocol of an entity:

As previously described, registration is divided into three phases:

- Generation of the public and private key pair associated with an EOA.
- Initialization and deployment of a proxy contract by the authority contract.

- Registration of the address pair of the proxy contract and EOA of the entity in the authority register.

Despite the advantages introduced by this implementation, which aims to optimize the access mechanism to the system functions (i.e., IAM) by minimizing the implementation complexity from the programmer's point of view, unfortunately, it has the disadvantage of a high cost of gas. It is due to the factory method design pattern [101]. The authority contract manages the factory contracts for proxy contracts. It implies that at the creation of an Entity, the gas cost includes the deployment of a new proxy contract, which significantly increases the cost of registration.

As for the accreditation in the case of SSI, TPS slight decrease because the on-chain accreditation also implies the issuer's registration in the Issuer registry. It does not represent a substantial limitation, given that the accreditation operation is a one-off operation (less than once a year). In the SSI approach, the certification (or, in general, the issuance of a DDoC) is not limited. Also, this operation is considered a not-so-frequent operation, so the TPS obtained is compatible with the domain of the problem.

Finally, the reading operations have a high RPS in both approaches and are more than compatible with the problem domain.

4.4 Requirement fulfillment

4.4.1 IAM

The requirements relating to Identity and Access Management are fully satisfied by both approaches. In particular :

- Both Pure Blockchain and SSI approach enable authoritative status of predefined users (e.g., Admin and Authorities) in a decentralized fashion

- Both approaches allow generic user identification and authentication through on-chain(Pure Blockchain Approach) or off-chain/VC (SSI Approach).

- Both approaches allow authorities to define for other user specific certification privileges, i.e., Issuer role, by mean of decentralized registry.

- From the privacy point of view, it should be noted that SSI is more privacy preserving compared to the Pure Blockchain Approach. SSI only store.

- Minimum amount of information related to VC identifier. The other approach explicit require personal information storage on chain to enforce privileges policy.

- Both approaches allow unique registration of artifacts e.g., certificate or device. As stated, the SSI approach result in a more flexible management of Device Identity outperforming the first approach

4.4.2 Information Verifiability

The requirements relating to verifiability are met by both approaches due to the nature of blockchain technology regardless of the method:

- Information traceability is grant by means of immutable identifiers, hash-proofs, and timestamp.

- Information spreading is carried out in distributed fashion thanks to P2P protocol

- Consensus protocol grants temper resistant information verification and transparency in case of information updates

- Permissioning and smart contract-based Access Control grant selective operability on data based on role and or attribute

4.4.3 Data storage and retrievability

The requirements relating to storage and retrievability are completely satisfied only by the SSI approach:

- SSI minimize on-chain data storing on contrary on Pure Blockchain approach.

- IPFS provide off chain storage in distributed fashion

- The IPFS middleware OrbitDB enables efficient indexing and retrieval of data

Chapter 5

Conclusion and shortcomings

5.1 Summary

The study presented focuses on the need to digitalize the metrology sector. From the preliminary analysis presented in the first chapter, four primary areas of investigation have been identified, namely:

1. Metrological context standardization
2. Digital identity framework
3. Distributed approach applicability and advantages
4. Metrology integration with IoT

The first area has been extensively investigated in the state of art. The literature search reveals that the digital standardization process of the metrology sector has been an issue that has been recurring for more than a decade. This trend is prolonged, making it difficult to replace the legacy system based on papers and pdf documents. It was clear from the analysis that one of the main limitations is the problem of establishing a shared standard. The emergence of the IoT ecosystem in recent years has given a renewed boost to this research sector. The main outcomes are the definition of metadata schemas for metrological quantities and metrological documents (e.g., DCC, DSoA, DDoC). Another important trend focuses on the definition of a shared digital metrological infrastructure. The main initiatives in this regard are the European Metrology Cloud in the EU and the corresponding international Measurement Information Infrastructure. Standardization and infrastructure definition are strongly linked as a digital platform cannot function without a common standard recognized by the participants, and conversely, the standards are less effective in communication and transmission without a protocol and an infrastructure that supports them. More studies also show how platform-based systems are virtuous in accelerating the growth and updating of the system of interest while simultaneously increasing competitiveness and cooperativity.

The second area is strongly linked to the security challenges of the digitization process. In the beginning, the internet was based on centralized client-server paradigms. The limited number of devices connected to the network allows this solution to be effective in security. Secure communication was based almost exclusively on a few certified authorities that acted as trust anchors in guaranteeing the digital identity of the connected devices, both server and client. With the evolution of the network, new paradigms have upset the defined traditional system, e.g., the Cloud, the IoT ecosystem, and the ever-increasing number of distributed paradigms. Research shows that as the entities connected growth, this led to higher system complexity, expanding the attack surface and, therefore, the risks related to security. Many devices also introduce greater management complexity. In response, new, more streamlined, and versatile identity paradigms have been proposed as part of the research. Among these emerges the paradigm based on Self-Sovereign Identity. The analysis reported in state of the art shows how the main goals of this paradigm are essentially the possibility of defining a universally verifiable, non-falsifiable, privacy-preserving, and highly flexible identity system in contrast to the main limitations of legacy systems. The SSI framework is agnostic to the implementation infrastructure. However, decentralized systems based on Distributed Ledger Technology will embrace the decentralization principle supported by the framework.

The third research area investigated the possibility of using a decentralized system, i.e., a blockchain system, as an underlying infrastructure to the distributed cloud for the metrology sector. State of the art analyzes some of the leading DLT solutions highlighting the characteristics and advantages of each. The third chapter of this thesis proposes a cloud infrastructure that exploits blockchain technology to guarantee the properties of verifiability, security, and decentralization that are highly advantageous in the metrological cloud system. It is especially true when the shared data and measures are legally relevant. Therefore, a purely blockchain-based metrological system was designed to investigate the potential and applicability of this technology in the analyzed domain. At the same time, the SSI approach was also integrated to overcome the intrinsic limitations related to privacy and scalability that blockchain technology intrinsically brings with it.

All project design choices consider the IoT. The fourth chapter highlights how the SSI framework improves the security of the communication of metrological data without sacrificing flexibility, privacy, and verifiability.

The safety, traceability, and authenticity of the metrological quantities are the three key points of the analysis. The proposed system demonstrates that combining the new identity protocols with DLT can satisfy the requirements.

5.2 Main limitations

The two most critical points of the proposed system are mainly related to privacy and scalability on a large scale.

Privacy and verifiability are two properties that tend to conflict easily. Blockchain technology is particularly valid in guaranteeing the verifiability of the recorded data at the expense of privacy. The use of a permissioned variety partially limits the dissemination of information to unauthorized entities. However, the use of such systems alone is not sufficient to fully guarantee a Privacy System compatible with international directives on the security of personal data, e.g., GDPR in European countries. Some blockchains allow further strengthened access control using on-chain enrollment. Hyper ledger Besu and Fabric are two examples that provide this functionality through private transactions and private data collections. However, this comes at the cost of reducing verifiability for outside observers. Another commonly used method is to register only hash proofs on the network that allow you to check the integrity of the data without making it public on the decentralized system. This method is effective when the amount of evidence to be recorded is contained within certain limits. This approach is therefore strongly linked to the use case. For instance, chapter four showed that a blockchain-based system is readily applicable to certification systems of public bodies or entities where the request rate is limited (low minimum throughput), and privacy issues are less stringent. Conversely, it has been seen that the same system is of limited applicability in the case of recording referable measures, especially in the case of very high throughput required, e.g., IoT ecosystem.

Both problems present an immediate and more obvious solution: off-chain execution of operations requiring heavy computation or a high degree of privacy.

5.2.1 Moving off-chain

Taking advantage of the SSI system and verifiable credentials does not imply that VCs' verification must be entirely on-chain. The verifiability of the revocation is the only operation necessary to keep on-chain. The integrity and authenticity can be safely verified off-chain thanks to the fact that the SSI takes advantage of blockchain technology to ensure universal verifiability but does not depend on the latter. Even in the case of certified measures, using the digital signature based on DID is sufficient to guarantee the integrity and accountability of the recorded data without necessarily having to refer to a system distributed as proof storage. All that is needed is a valid DID and an appropriate role and credentials to guarantee the properties described above (e.g., DCC in the case of devices that must produce certified measurements). For this purpose, the decentralized secretary becomes only a trust anchor for public keys and, at most, a store of issuer roles. Let's consider the use case of measurements recording again . In this case we can embed the certified registered measure in a JWS Token in which the payload is the measurement expressed following the XSD schema of the DCC. A JWS token contain all necessary information to certify the provenience of the payload and its validity (thanks to the digital signature). Once the record is ready the device sends it to the storage system . When necessary, it is possible to verify both the authenticity of the data and the sender through the proof in the JWS.

Updates to the registration procedure are as follows:

- Measures are placed in a JWT and signed with the private key generating a JWS token
- No hash proof is recorded on the blockchain

The new protocol is entirely off-chain. The only interactions with the blockchain are associated with verifying the signature in the JWS. They are query operations, i.e., the query of the public key associated with the device, the query of its DCC VC, optionally query of all DCC VCs necessary to reconstruct the Chain of Traceability.

5.3 Shortcomings

Several options that favor the use of the proposed system have not been analyzed in the context of this thesis and represent the future field of analysis to favor its adoption. To name the two main ones:

- Different blockchain technologies that natively have a higher nominal throughput, one of all Hyperledger Fabric.
- Data anonymization systems such as Zero Knowledge proof protocols [66] .

The solutions analyzed in the thesis represent a starting point and not a point of arrival for research in digitization in the metrological field and beyond, in digital identity system.

Bibliography

[1] S. Yin, J. Bao, Y. Zhang and X. Huang, "M2M Security Technology of CPS Based on Blockchains," *Symmetry,* vol. 9, 2017.

[2] S. Cho and S. Lee, "Survey on the Application of BlockChain to IoT," 2019.

[3] P. Fraga-Lamas and T. Fernández-Caramés, "A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry," *IEEE Access,* vol. 7, pp. 17578-17598, January 2019.

[4] A. Panarello, N. Tapas, G. Merlino, F. Longo and A. Puliafito, "Blockchain and IoT Integration: A Systematic Survey," *Sensors,* vol. 18, 2018.

[5] A. Imani, A. Keshavarz-Haddad, M. Eslami and J. Haghighat, "Security Challenges and Attacks in M2M Communications," *2018 9th International Symposium on Telecommunications (IST),* pp. 264-269, 2018.

[6] R. H. Schmitt and C. Voigtmann, "Sensor information as a service – component of networked production," *Journal of Sensors and Sensor Systems,* vol. 7, p. 389–402, 2018.

[7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys Tutorials,* vol. 17, pp. 2347-2376, 2015.

[8] F. Thiel and J. Wetzlich, "The European Metrology Cloud: Impact of European Regulations on Data Protection and the Free Flow of Non-Personal Data," in *19th International Congress of Metrology*, 2019.

[9] J. Voas, D. Kuhn, P. Laplante and S. Applebaum, *Internet of Things (IoT) Trust Concerns,* 2018.

[10] R. Shah, M. McIntee, S. Nagaraja, S. Bhandary, P. Arote and J. Kuri, "Secure Calibration for High-Assurance IoT: Traceability for Safety Resilience," *ArXiv,* vol. abs/1908.00740, 2019.

[11] S. G. Hackel, F. Härtig, J. Hornig and T. Wiedenhöfer, "The DigitalCalibration Certificate (2017)," 2017. [Online]. Available: https://oar.ptb.de/files/download/5a9803864c91840b9b2a3ce5.

[12] NIS, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," 2016.

[13] ENISA, "The "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")," 2017.

[14] P. Boucher, S. Nascimento and a. M. Kritikos, "How blockchain technology could change our lives," in *EPRS European Parliamentary Research Service*, 2017.

[15] "Register of Commission Documents - COM(2014)442," 02 07 2014. [Online]. Available: https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2014)442&lang=en. [Accessed 12 12 2021].

[16] "Register of Commission Documents -COM(2015)192," 06 05 2015. [Online]. Available: https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2015)192&lang=en. [Accessed 12 12 2021].

[17] "Register of Commission Documents - COM(2016)288," 31 03 2016. [Online]. Available: https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2016)288&lang=en. [Accessed 12 12 2021].

[18] "Register of Commission Documents - COM(2016)272," 11 04 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:52016DC0199. [Accessed 12 12 2021].

[19] I. Turner, "Recent Software Developments – The view of the weighing industry,," *PTB-Mitteilungen,* p. 3–6, 2017.

[20] "Interim Evaluation of the Measuring Instruments Directive - Final report - July 2010 - CSES," 2010.

[21] F. Thiel, M. Esche, F. Grasso Toro, D. Peters, A. Oppermann, J. Wetzlich and M. Dohlus, "A digital quality infrastructure for Europe: The European metrology cloud," *PTB - Mitteilungen Forschen und Prufen,* vol. 127, pp. 83-97, December 2017.

[22] "JCGM 200:2012 International vocabulary of metrology – Basic and general concepts and associated terms (VIM)," BIPM, 2012.

[23] "ILAC P10:07/2020 : Policy on Metrological Traceability of Measurement Results. International Laboratory," ILAC, 2020.

[24] "ISO/IEC 17025:2017 General requirements for the competence of testing and calibration laboratories," 2017.

[25] "EU 910/2014 electronic IDentification Authentication and Signature," 2014.

[26] B. A. R. Filho and R. F. Gonçalves, "Legal metrology, the economy and society: A systematic literature review," *Measurement,* vol. 69, pp. 155-163, 2015.

[27] A. Oppermann, F. Grasso Toro, F. Thiel and J.-P. Seifert, "Secure Cloud Computing: Reference Architecture for Measuring Instrument under Legal Control," *Security and Privacy,* vol. 1, May 2018.

[28] M. Esche and F. Thiel, "Software risk assessment for measuring instruments in legal metrology," in *2015 Federated Conference on Computer Science and Information Systems (FedCSIS)*, 2015.

[29] OILM, "General requirements for software-controlled measuring instruments - Consolidated edition with Amendment 1 (2020)," 2019. [Online]. Available: https://www.oiml.org/en/publications/documents/en/files/pdf_d/d031-consolidated-e19.pdf.

[30] W. W. G. 7, "WELMEC Software Guides," 2020. [Online]. Available: https://www.welmec.org/welmec/documents/guides/7.2/2020/WELMEC_Guide_7.2_v2020.pdf.

[31] D. Peters, M. Peter, J.-P. Seifert and F. Thiel, "A Secure System Architecture for Measuring Instruments in Legal Metrology," *Computers,* vol. 4, pp. 61-86, March 2015.

[32] "A Security Issue with Google Certificate Transparency and Prevention Through CertLedger," 2019. [Online]. Available: https://medium.com/@certledger/a-security-issue-with-chromes-certificate-transparency-and-prevention-through-certledger-f511cd02fe2b#:~:text=Although%20the%20log%20maintains%20more,%E2%80%9CSplit%2DWorld%20Attack%E2%80%9D.. [Accessed 03 11 2021].

[33] A. Singla and E. Bertino, "Blockchain-Based PKI Solutions for IoT," in *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, 2018.

[34] "EU 2016/679 General Data Protection Regulation," 2017.

[35] J. Lou, Q. Zhang, Z. Qi and K. Lei, "A Blockchain-based key Management Scheme for Named Data Networking," in *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, 2018.

[36] T. Jiang, H. Fang and H. Wang, "Blockchain-Based Internet of Vehicles: Distributed Network Architecture and Performance

Analysis," *IEEE Internet of Things Journal,* vol. 6, pp. 4640-4649, 2019.

[37] A. Mühle, A. Grüner, T. Gayvoronskaya and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review,* vol. 30, pp. 80-86, November 2018.

[38] M. Pech, J. Vrchota and J. Bednář, "Predictive Maintenance and Intelligent Sensors in Smart Factory: Review," *Sensors,* vol. 21, 2021.

[39] M. Kuster, "Metrology: Standardize and Automate!," *Cal Lab: The Int. J. of Metrology,* vol. 20, no. 2, pp. 26-34, 2013.

[40] M. Kuster, "Toward a Measurement Information," in *MSA*, 2015.

[41] D. Zajac, "XML Schema for Accreditation Scopes," 2016.

[42] D. Zajac, "Updated XML Schema for Accreditation Scopes,," 2017.

[43] M. Schwartz, "Creating a Taxonomy for Metrology," *Cal Lab,* vol. 25, no. 1, pp. 31-37, 2018.

[44] "CalLabSolutions Digital SoA," [Online]. Available: https://github.com/CalLabSolutions/Metrology.NET_Public.

[45] M. Saeedi Nikoo, M. Ç. Kaya, M. Schwartz and H. Oğuztüzün, "Internet of Measurement Things: Toward an Architectural Framework for the Calibration Industry," 2019, pp. 81-102.

[46] S. W. Lin, B. Miller, J. Durand, G. Bleakley, A. Chigani, R. Martin, B. Murphy and M. Crawford, "The industrial internet of things volume G1: reference architecture," *Industrial Internet Consortium,* p. 10–46, 2017.

[47] ISO-IEC, "ISO IEC Guide 98 1 2009(E) Uncertainty of measurement -- Introduction to the expression of uncertainty in measurement," 2009.

[48] E. Tiesinga, P. J. Mohr, D. B. Newell and B. N. Taylor, "CODATA recommended values of the fundamental physical constants: 2018," *Rev. Mod. Phys.,* vol. 93, no. 2, p. 025010, June 2021.

[49] "TraCIM service operated at PTB," PTB, 2019. [Online]. Available: https://tracim.ptb.de. [Accessed 29 November 2021].

[50] B. Müller, D. Hutzschenreuter, J. H. Loewe and R. Klobučar, "Validation of SI-based Digital Data of Measurement using the TraCIM System," *Journal of Sensors and Sensor Systems (JSSS),* 2021.

[51] BIMP, "SI Brochure: The International System of Units (SI)," 2019. [Online]. Available: https://www.bipm.org/en/publications/si-brochure. [Accessed 2021].

[52] B. Ačko, H. Weber, D. Hutzschenreuter and I. Smith, "Communication and validation of metrological smart data in IoT-networks," *Advances in Production Engineering & Management,* vol. 15, p. pp 107&ndash;117, 2020.

[53] D. Hutzschenreuter, R. Klobučar, P. Nikander, T. Elo, T. Mustapää, P. Kuosmanen, O. Maennel, K. Hovhannisyan, B. Müller, L. Heindorf, B. Ačko, J. Sýkora, F. Härtig, W. Heeren, T. Wiedenhöfer, A. Forbes, C. Brown, I. Smith, S. Rhodes, I. Linkeová, J. Sýkora and V. Paciello, "SmartCom Digital System of Units (D-SI) Guide for the use of the metadata-format used in metrology for the easy-to-use, safe, harmonised and unambiguous digital transfer of metrological data," 2019.

[54] A. Oppermann, S. Eickelberg and J. Exner, "Digital Transformation in Legal Metrology: An Approach to a Distributed Architecture for Consolidating Metrological Services and Data," in *Information Technology for Management: Towards Business Excellence*, Cham, 2021.

[55] "New legislative framework, 2008. Internal Market, Industry, Entrepreneurship and SMEs," [Online]. Available: https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en.

[56] J. Nummiluikki, T. Mustapää, K. Hietala and R. Viitala, "Benefits of network effects and interoperability for the digital calibration certificate management," 2021.

[57] "eIDAS, L 910/2014," *EU:Official Journal,* 2014.

[58] "Verifiable Credentials Data Model v1.1," 09 11 2021. [Online]. Available: https://www.w3.org/TR/vc-data-model/. [Accessed 03 12 2021].

[59] W3C, "Decentralized Identifiers (DIDs) v1.0," 03 08 2021. [Online]. Available: https://www.w3.org/TR/did-core/. [Accessed 01 01 2022].

[60] "European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation," 2018. [Online]. Available: https://www.europarl.europa.eu/doceo/document/TA-8-2018-0373_EN.html. [Accessed 10 10 2021].

[61] IETF Internet Engineering Task Force, "A Universally Unique IDentifier (UUID) URN Namespace," 07 2005. [Online]. Available: https://www.ietf.org/rfc/rfc4122.txt. [Accessed 01 12 2021].

[62] IETF Internet Engineering Task Force , "Uniform Resource Names (URNs)," 04 2017. [Online]. Available: https://www.ietf.org/rfc/rfc8141.txt. [Accessed 01 12 2021].

[63] "IPFS is the distributed web," 2017. [Online]. Available: https://ipfs.io/. [Accessed 3 6 2019].

[64] "SQRL - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/SQRL. [Accessed 1 11 2021].

[65] "Web Authentication: An API for accessing Public Key Credentials - Level 2," 01 04 2021. [Online]. [Accessed 01 11 2021].

[66] "Zero-knowledge proof - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Zero-knowledge_proof. [Accessed 14 03 2021].

[67] N. I. o. S. a. T. (NIST), "NIST Interagency or Internal Report (NISTIR) 8149, Developing Trust Frameworks to Support Identity Federations".

[68] A. Reyna, C. Martín, J. Chen, E. Soler and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems,* vol. 88, pp. 178-190, 2017.

[69] L. Ante, "Smart contracts on the blockchain – A bibliometric analysis and review," *Telematics and Informatics,* vol. 57, p. 101519, 2021.

[70] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos and C. Yang, "The Blockchain as a Decentralized Security Framework [Future Directions]," *IEEE Consumer Electronics Magazine,* vol. 7, pp. 18-21, 2018.

[71] Q. Zhou, H. Huang, Z. Zheng and J. Bian, "Solutions to Scalability of Blockchain: A Survey," *IEEE Access,* vol. 8, pp. 16440-16455, 2020.

[72] K. Wüst and A. Gervais, "Do you Need a Blockchain?," in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 2018.

[73] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system,* 2009.

[74] V. Buterin, "Ethereum white paper," 2013. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper. [Accessed 3 6 2019].

[75] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman and Y. a. o. Manevich, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *13 EuroSys conference*, 2018.

[76] W. Viriyasitavat and D. Hoonsopon, "Blockchain characteristics and consensus in modern business processes," *Journal of Industrial Information Integration,* vol. 13, pp. 32-39, 2019.

[77] "The Layered Structure Of The Blockchain Architecture," 2022. [Online]. Available: https://www.cryptologi.st/news/blockchain-layers-the-layered-structure-of-the-blockchain-architecture. [Accessed 2022].

[78] C. Cachin and M. Vukolic, "Blockchain Consensus Protocols in the Wild (Keynote Talk)," in *31st International Symposium on Distributed Computing (DISC 2017)*, Dagstuhl, 2017.

[79] W. Li, S. Andreina, J.-M. Bohli and G. Karame, "Securing Proof-of-Stake Blockchain Protocols," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, Cham, 2017.

[80] G. Karame, "On the Security and Scalability of Bitcoin's Blockchain," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA, 2016.

[81] S. Zhang and J.-H. Lee, "Analysis of the main consensus protocols of blockchain," *ICT Express,* vol. 6, pp. 93-97, 2020.

[82] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems," *IEEE Transactions on Knowledge and Data Engineering,* vol. 30, pp. 1366-1385, 2018.

[83] A. Baliga, "Understanding Blockchain Consensus Models," 2017.

[84] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen and D. I. Kim, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access,* vol. 7, pp. 22328-22370, 2019.

[85] W. J. Gordon and C. Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability," *Computational and Structural Biotechnology Journal,* vol. 16, pp. 224-230, 2018.

[86] F. Lombardi, L. Aniello, S. De Angelis, A. Margheri and V. Sassone, "A Blockchain-based Infrastructure for Reliable and Cost-effective IoT-aided Smart Grids," in *Living in the Internet of Things: Cybersecurity of the IoT*, 2018.

[87] M. Díaz, C. Martín and B. Rubio, "State-of-the-art, challenges and open issues in the integration of internet of things and cloud computing," *J. Netw. Comput.,* no. Appl. 67 (2016), p. 99–117, 2016.

[88] A. Y. Kazim Rifat Ozyilmaz, "Designing a Blockchain-Based IoT With Ethereum, Swarm, and LoRa," *IEEE Consumer Electronics Magazine ,* vol. 8, no. 2, pp. 28 - 34, 2019.

[89] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," *IEEE Internet of Things Journal ,* vol. 5, no. 2, pp. 1184-1190, 2018.

[90] L. Vangelista, A. Zanella and M. Zorzi, "Long-range IoT technologies: the dawn of LoRa," in *Future Access Enablers of Ubiquitous and Intelligent Infrastructures*, 2015.

[91] Alastria, "Alastria Idenity," [Online]. Available: https://github.com/alastria/alastria-identity/wiki.

[92] "uport-project/uport-identity: uPort Contracts for managing identity DEPRECATED," [Online]. Available: https://github.com/uport-project/uport-identity. [Accessed 13 11 2021].

[93] "Eip-1056 Ethereum Lightweight Identity," 03 05 2018. [Online]. Available: https://eips.ethereum.org/EIPS/eip-1056. [Accessed 05 01 2022].

[94] "EIP-1812: Ethereum Verifiable Claims," 03 03 2019. [Online]. Available: https://eips.ethereum.org/EIPS/eip-1812. [Accessed 12 12 2021].

[95] "EIP-712: Ethereum typed structured data hashing and signing," 12 10 2017. [Online]. Available: https://eips.ethereum.org/EIPS/eip-712. [Accessed 27 11 2021].

[96] "Hyperledger Besu Ethereum client - Hyperledger Besu," Hyperledger Fountadtion, 04 03 2022. [Online]. Available: https://besu.hyperledger.org/en/stable/. [Accessed 13 12 2021].

[97] "Hyperledger Caliper Explained and Installation Guide (Ubuntu)," [Online]. Available: https://nima-afraz.medium.com/hyperledger-caliper-explained-and-installation-guide-ubuntu-c38dc16d3dcf. [Accessed 30 12 2021].

[98] M. Soelman, "Permissioned Blockchains: A Comparative Study," 2021. [Online]. Available: https://fse.studenttheses.ub.rug.nl/25270/1/Final%20Submission.pdf. [Accessed 2021].

[99] M. Soelman, "FabricBesuBenchmark," [Online]. Available: https://github.com/Viserius/FabricBesuBenchmark. [Accessed 2021].

[100] H. Foundation, "Hyperledger Besu 1.5 Performance Enhancements," 6 8 2020. [Online]. Available: https://www.hyperledger.org/blog/2020/08/06/hyperledger-besu-1-5-performance-enhancements. [Accessed 13 1 2022].

[101] "Contracts Architecture - OpenZeppelin Docs," [Online]. Available: https://docs.openzeppelin.com/cli/2.6/contracts-architecture. [Accessed 2021].

List of Symbol

A

AB *Accreditation Bodies*

ABAC *Attribute Based Access Control*

B

BIoT *Blockchain IoT*

C

CA *Certificate Authority*

CL *Calibration Laboratories*

CMC *Calibration and Measurement Capability*

CODATA *Committee On Data for Science & Technology*

CPS *Cyber-Physical System*

CRL *Certificate Revocation Lists*

CRUD *Create Read Update Delete*

D

DApps *Decentralized Application*

DCC *Digital Calibration Certificate*

DDoC *Digital Declaration of Conformity Certificate*

DID *Decentralized Identifiers*

DLT *Distributed Ledger Technology*

DNS *Domain Name System*

DPKI *Decentrilized Public Key Infrastructure*

DPoS *Delegated Proof of Stake*

DSoA *Digital Scope of Accreditation Certificate*

D-SI *Digital International System of Unit*

E

eIDAS *electronic IDentification Authentication and Signature*

EMC *European Metrology Cloud*

EOA *Externally Owned Account*

ETH *Ether*

EVM *Ethereum Virtual Machine*

G

GDPR *General Data Protection Regulation*

GUM *Guide to the Expression of Uncertainty in Measurement*

I

IETF *Internet Engineering Task Force*

IIC *Industrial Internet Consortium*

IIoT *Industrial Internet of Things*

ILAC *International Laboratory Accreditation Cooperation*

IoT *Internet of Things*

IP *Internet Protocol*

ISO *International Organization for Standardization*

J

JSON-LD *JSON Linked Data*

JWT *JSON Web Token*

M

MI *Measurment Instrument*

MII *Measurement Information Infrastructure*

MIM *Man in the middle Attach*

M2M *Machine to Machine*

N

NIST *National Institute of Standard Technologies*

NMI *National Metrology Institute*

O

OCSP *Online Certificate Status Protocol*

OIML *International Organization of Legal Metrology*

P

PBFT *Practical Byzantine Fault Tolerance*

PKDs *Public Key Directories*

PKI *Public Key Infrastructure*

PoA *Proof of Authority*

PoS *Proof of Stake*

PoW *Proof of Work*

PTB *Physikalisch-Technische Bundesanstalt*

P2P *Pear-to-Pear*

R

RBAC *Role Based Access Control*

REST *REpresentational State Transfer*

RPS *Request per second*

S

SoA *Scope of Accreditation*

SPID *Public Digital Identity System*

SSI *Self Souverain Identity*

T

TPS *Transaction per second*

TTP *Trusted Third Party*

U

URN *Uniform Resource Names*

UTXO *Unspent Transaction Output*

UUID *Universally Unique Identifiers*

V

VC *Verifiable Credentials*

VIM *International vocabulary of metrology*

Pubblicazione edita a cura del
Dipartimento di Ingegneria Industriale