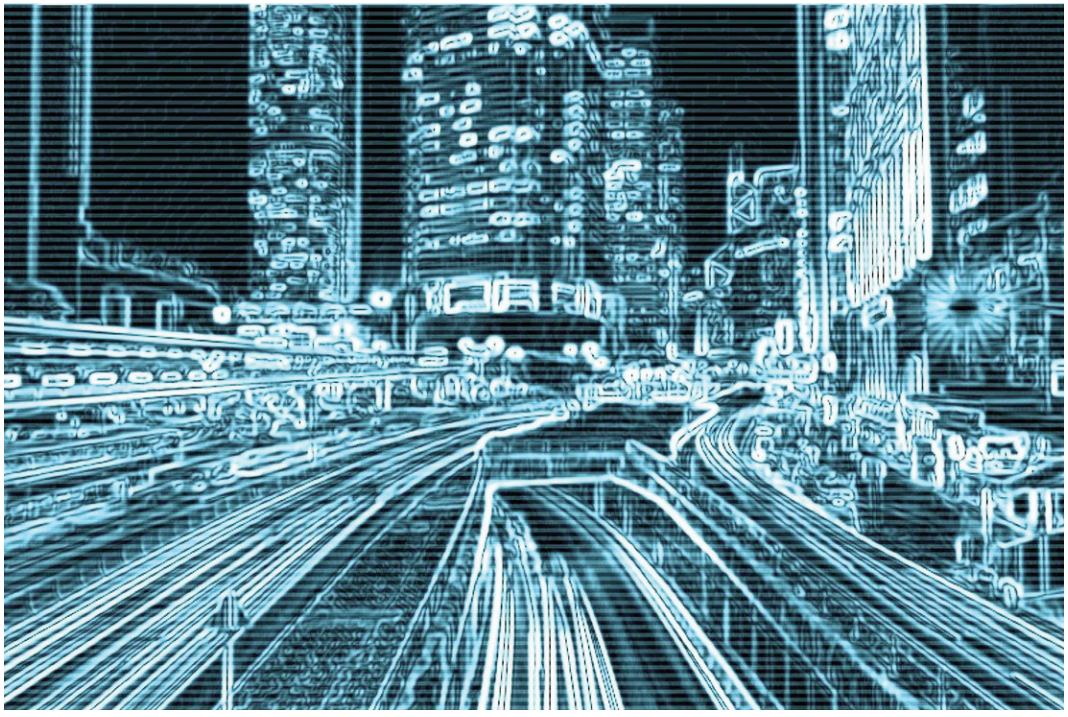
OIML BULLETIN

VOLUME LXII • NUMBER 3
JULY 2021

Quarterly Journal

Organisation Internationale de Métrologie Légale



Digital transformation in legal metrology

BULLETIN

VOLUME LXII • NUMBER 3

JULY 2021

THE OIML BULLETIN IS THE JOURNAL OF THE ORGANISATION INTERNATIONALE DE MÉTROLOGIE LÉGALE

The Organisation Internationale de Métrologie Légale (OIML), established 12 October 1955, is an intergovernmental organization whose principal aim is to harmonize the regulations and metrological controls applied by the national metrology services of its Members.

EDITOR-IN-CHIEF: Anthony Donnellan
EDITOR: Chris Pulham

THE ONLINE BULLETIN IS FREE OF CHARGE

PUBLISHED ONLINE BY THE BIML

OIML SECRETARIAT

BUREAU INTERNATIONAL DE MÉTROLOGIE LÉGALE (BIML)

11 RUE TURGOT – 75009 PARIS – FRANCE

TEL: 33 (0)1 4878 1282
FAX: 33 (0)1 4282 1727
INTERNET: www.oiml.org or www.oiml.int
www.metrologyinfo.org

BIML STAFF

DIRECTOR
Anthony Donnellan (anthony.donnellan@oiml.org)

ASSISTANT DIRECTORS
Paul Dixon (paul.dixon@oiml.org)
Ian Dunmill (ian.dunmill@oiml.org)

STAFF MEMBERS (IN ALPHABETICAL ORDER)
Jalil Adnani: Database Systems Management (jalil.adnani@oiml.org)

Jean-Christophe Esmiol: IT Systems Management (jean-christophe.esmiol@oiml.org)

Florence Martinie: Administrator, Finance (florence.martinie@oiml.org)

Luis Mussio: Engineer (luis.mussio@oiml.org)

Chris Pulham: Editor/Webmaster (chris.pulham@oiml.org)

Patricia Saint-Germain: Administrator, Members (patricia.saint-germain@oiml.org)

OIML MEMBER STATES

ALBANIA
ALGERIA
AUSTRALIA
AUSTRIA
BELARUS
BELGIUM
BRAZIL
BULGARIA
CAMBODIA
CANADA
P.R. CHINA
COLOMBIA
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DENMARK
EGYPT
FINLAND
FRANCE
GERMANY
GREECE
HUNGARY
INDIA
INDONESIA
ISLAMIC REPUBLIC OF IRAN
IRELAND
ISRAEL
ITALY
JAPAN
KAZAKHSTAN
KENYA
REP. OF KOREA
MONACO
MOROCCO
NETHERLANDS
NEW ZEALAND
NORTH MACEDONIA, REPUBLIC OF
NORWAY
PAKISTAN
POLAND
PORTUGAL
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SERBIA
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SWEDEN
SWITZERLAND
TANZANIA
THAILAND
TUNISIA
TURKEY
UKRAINE
UNITED KINGDOM
UNITED STATES OF AMERICA
VIETNAM
ZAMBIA

OIML CORRESPONDING MEMBERS

ANGOLA
ARGENTINA
AZERBAIJAN
BAHRAIN
BANGLADESH
BARBADOS
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
COSTA RICA
DOMINICAN REPUBLIC
ECUADOR
ESTONIA
FIJI
GABON
GEORGIA
GHANA
GUATEMALA
GUINEA
GUYANA
HONG KONG, CHINA
ICELAND
IRAQ
JORDAN
KIRIBATI
KUWAIT
KYRGYZSTAN
LATVIA
LITHUANIA
LUXEMBURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MAURITIUS
MEXICO
MOLDOVA
MONGOLIA
MONTENEGRO
MOZAMBIQUE
NAMIBIA
NEPAL
NIGERIA
OMAN
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
QATAR
RWANDA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SUDAN
CHINESE TAIPEI
TRINIDAD AND TOBAGO
UGANDA
UNITED ARAB EMIRATES
URUGUAY
UZBEKISTAN

Contents

OIML BULLETIN

VOLUME LXII • NUMBER 3
JULY 2021

technique

update

DIGITAL TRANSFORMATION IN LEGAL METROLOGY:

SEE EDITORIAL, AND FEATURE ARTICLES STARTING ON PAGE 5

FLORIAN THIEL

Physikalisch-Technische Bundesanstalt (PTB)

Digital transformation in legal metrology

Digital transformation is usually soberly defined as the process of using digital technologies to create new – or modify existing – processes, services, cultures, and customer experiences to meet changing business and market requirements.

Over more than a decade, the PTB's *Metrological Information Technology* Department – together with WELMEC Working Group 7 *Software* and OIML TC 5/SC 2 *Software in Measuring Systems* – have put much enthusiasm into supporting the process of digital transformation in legal metrology by, for example, updating existing guidelines and standards as well as organising a series of international workshops. During this period I found two quotes (unfortunately of unknown origins) to be very helpful when considering which route to follow:

- "Digital Transformation is not an end in itself! It is a facilitator to make metrological services even better"; and
- "Digital Transformation is a journey not a destination".

With this in mind, the benefits of the underlying digital technologies for the sake of legal metrology could be evaluated. These technologies have matured significantly over the past ten years – namely Embedded Systems, the Internet of Things, Cloud Computing, Blockchain, and Big-Data concepts. They have facilitated completely new technology fields and data-driven markets such as Industry 4.0, Machine Learning, and Artificial Intelligence-based Smart Services provided by digital platforms. These technologies can be exploited for legal metrology, namely to overcome barriers to innovation caused by regulations, better coordinate legal processes, reduce development costs, and minimise the time to market of innovative products and services.

Therefore, we considered it helpful for all stakeholders to come together on a regular basis to discuss the challenges and opportunities that digital transformation brings. These workshops were well received by stakeholders far beyond the European Region.

We were very honoured to be approached by the OIML to organise a Webinar to cover this topic. The Webinar aimed to explore contemporary challenges, opportunities and solutions regarding digital transformation in legal metrology and to provide a platform for the exchange of strategies, concepts and first steps towards realisations.

By compiling the programme we aimed to cover the strategic and regulatory point of view as well as applications and specific technologies. To this end, topics such as the holistic view of the impact of digital transformation on metrology as a whole, as described by the OIML/BIPM Joint Task Group, first realisations of established digital networks in the Russian Federation presented by the Rosstandart and in Europe described by the PTB, as well as the benefit of specific technologies, e.g. blockchains and smart contracts, described by INMETRO, were provided.

A video recording of the webinar is available via the OIML website and it is my pleasure to present this compilation of corresponding articles to our worldwide legal metrology partners in a special issue of the OIML Bulletin to provide in depth information about each topic.

Our mutual journey continues, and I sincerely hope that this special edition will enrich your trip! ■

Florian Thiel (florian.thiel@ptb.de) is Head of the PTB Department *Metrological Information Technology* and Convener of WELMEC WG 7 *Software*

DIGITAL TRANSFORMATION

Digital Transformation in (Legal) Metrology – The View of the BIPM-OIML Joint Task Group

Dr Roman Schwartz
CIML President

OIML-PTB WEBINAR

DIGITAL TRANSFORMATION IN LEGAL METROLOGY

5 MAY 2021

1 Introduction

As President of the CIML, it is my great pleasure to open this OIML-PTB Webinar with a presentation about Digital Transformation in Legal Metrology – or, as I would say, metrology in general and legal metrology in particular. I will also be presenting the view of the OIML/BIPM Joint Task Group.

Let me start by thanking all the speakers; I would also like to thank the BIML team in Paris and last but not least you, the participants. I am pleased to see that we have about 200 participants showing interest in this Webinar and the topic of Digital Transformation in Legal Metrology.

2 BIPM

I would like to start by looking at the new BIPM website; I find the new design very attractive and congratulate the BIPM. On their website the BIPM is introduced as the International Organization established by the Metre Convention through which member states act together on matters related to measurement science and measurement standards. It is the home of the International System of Units (the SI) and the International Reference Timescale UTC.

3 OIML

The OIML is the International Organization of Legal Metrology, whose mission is to enable economies to put in place effective legal metrology infrastructures that are mutually compatible and internationally recognized for all areas for which the government takes responsibility, such as those which facilitate trade, establish mutual confidence and harmonize the level of consumer protection worldwide.

4 Joint Task Group (JTG)

In October 2020 a new BIPM/OIML Joint Task Group (JTG) was established after approval by the respective International Committees, namely the CIPM and the CIML. The JTG is made up of six members including the CIPM and the CIML Presidents and the BIPM and BIML Directors. The major aims of the JTG are to foster and enhance cooperation between the BIPM and the OIML in order to facilitate both organizations in serving their member states, and to speak with one single voice for metrology. The major strategic objectives of the JTG are to develop and promote a common vision and a common holistic concept of metrology as a key element for the active promotion of the quality infrastructure (QI) concepts.

The action plan includes, but is not limited to, the joint promotion and support of digital transformation of metrology.

Metrological activities are always related to quality infrastructure activities, with the consequence that the digital transformation of metrology requires a holistic approach of all parties working in quality infrastructure of the country or the economy.

5 Major pillars of the quality infrastructure

The three major pillars of the quality infrastructure (see Figure 1) are metrology, standardization, and accreditation. Six international organizations have responsibility for international harmonization:

- the BIPM and the OIML for metrology;
- ISO and the IEC for standardization; and
- ILAC and the IAF for accreditation.

Below the metrology institutes, the standardization bodies, and the accreditation bodies, are the calibration laboratories, testing laboratories, certification bodies, and inspection bodies.

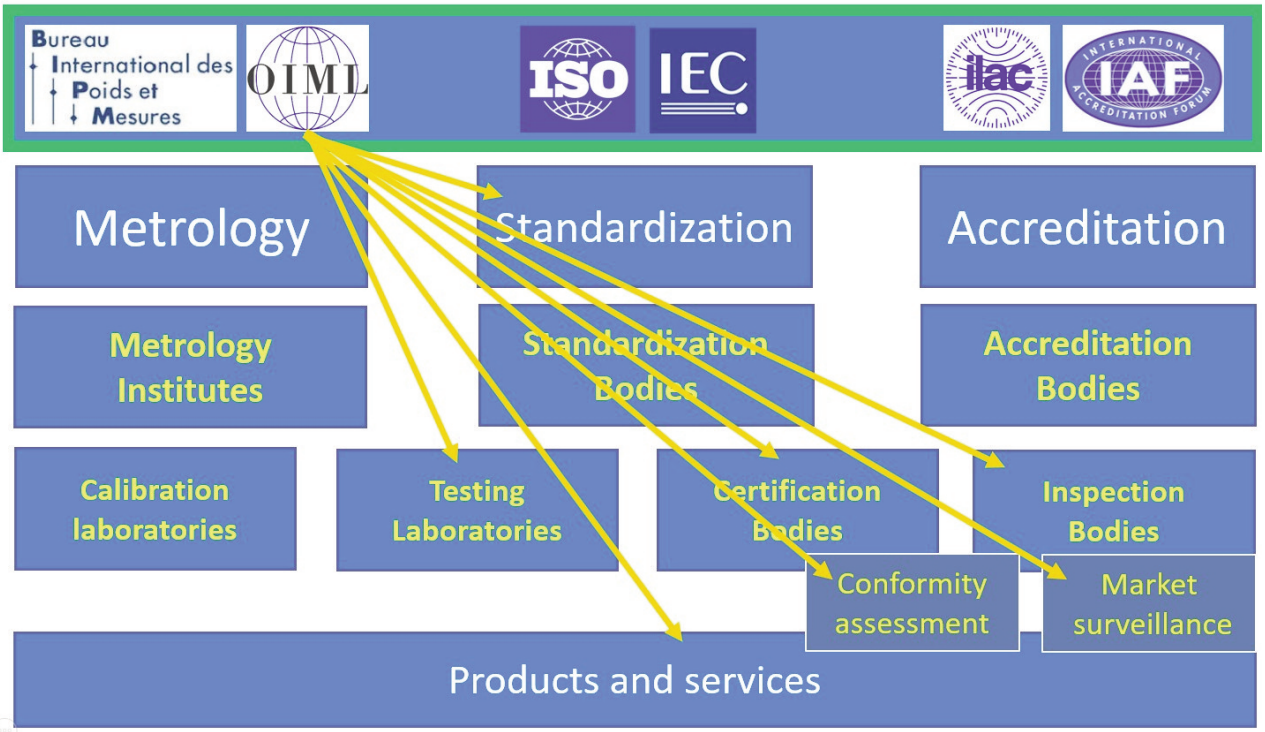


Figure 1 - The three major pillars of the quality infrastructure

6 Quality Infrastructure (QI) activities

In addition, according to the definition of INetQI, the *International Network on Quality Infrastructure*, QI activities also include conformity assessment and market surveillance. In Figure 1 the yellow arrows show the quality infrastructure activities in which the OIML is primarily involved. Concerning the digital transformation of metrology, it is the view of the BIPM/OIML JTG that the digital transformation of scientific, industrial and legal metrology activities requires a holistic approach which includes all the relevant aspects and activities from the beginning, i.e. calibration or re-calibration, testing or re-testing, certification or re-certification, verification or re-verification and inspection, market surveillance, accreditation, and standardization. This activity requires good cooperation on the part of all stakeholders – for example manufacturers or manufacturers' associations, national or regional regulatory and supervising bodies, and international organizations in the field of quality infrastructure such as the BIPM, OIML, ISO/IEC, and ILAC/IAF.

7 Product life cycle

A real challenge, especially for legal metrology, is the digital transformation of the various processes during the life cycle of a product. The life cycle of a product (i.e. the measuring instrument) begins with the manufacturer, who is responsible for the product design and the production line. There, a third party takes care of the conformity assessment steps, comprising type examination and the surveillance of the quality system for production. These two steps, accompanied by market surveillance activities, guarantee that the products which are placed on the market are in conformity with the approved type. These activities are often designated as pre market activities.

Once the customer has bought the product and put it into use, the customer becomes responsible for its correct installation and use. The customer must ensure that a qualified body performs the required verification, maintenance, repair, and software updates. These activities are often designated as post-market activities. In some countries, market surveillance is referred to as post market activity.

Looking at the various processes during the life cycle of a product, it becomes obvious that digital transformation of the various processes can only be successful and effective if it is based on the exchange of fair and traceable digital data. *Fair + T* data (see Figure 2) means findable, accessible, inter-operable, reusable, and data that is traceable to the SI.

Figure 3 presents a more detailed view of a what a fully digitalized life cycle of a networked instrument could look like in the future. This can also equally be

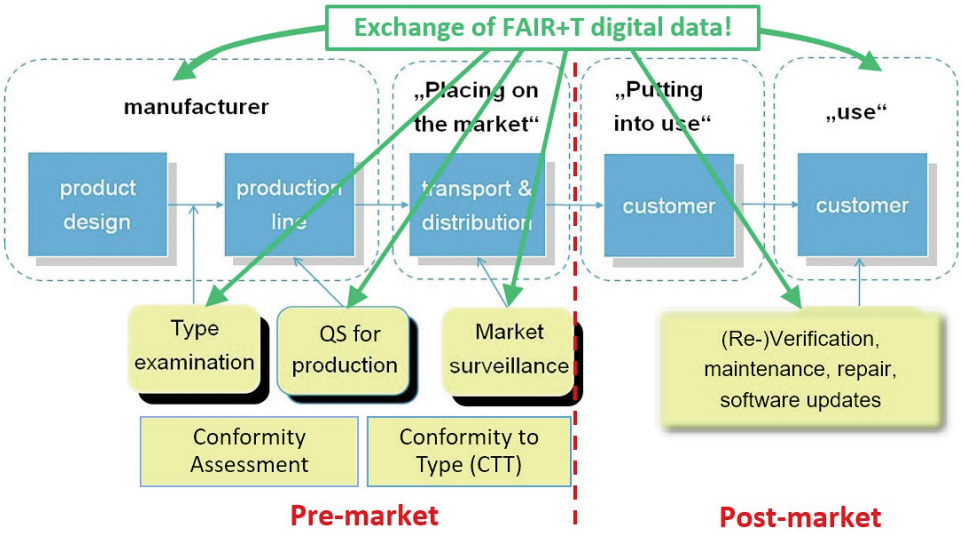


Figure 2 – Exchange of *FAIR + T* digital data during the life cycle of a product;
FAIR + T means: *F*indable, *A*ccessible, *I*nteroperable, *Re*-usable and *T*raceable to the SI

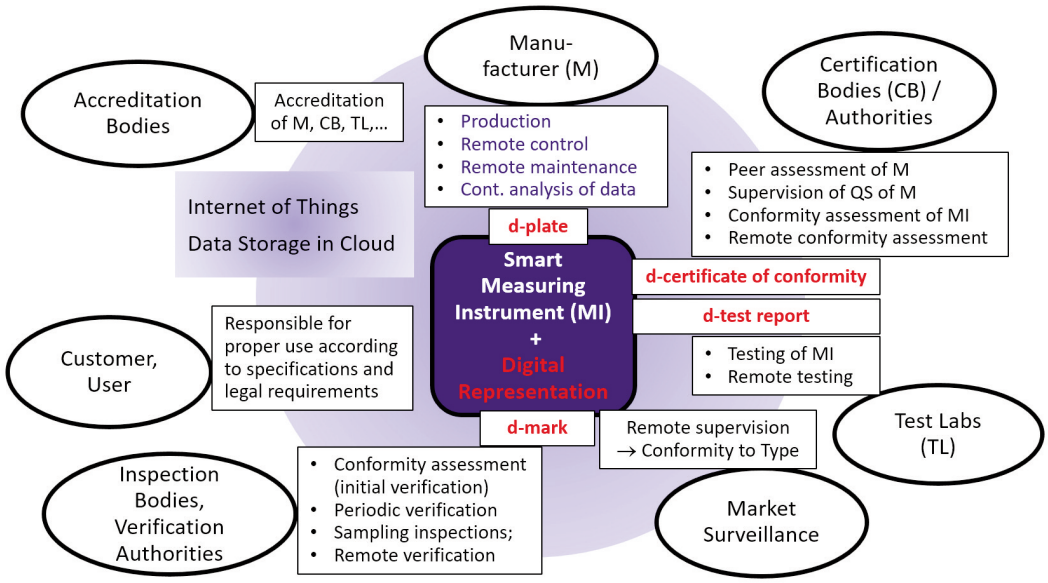


Figure 3 – Detailed view of a fully digitalized life cycle of a product (measuring instrument) with its digital representation

applied to other metrology activities such as calibration. The blue circle represents the internet of things and where data are stored in a secure cloud; the box in the center represents a physical smart measuring instrument and its digital representation.

The digital representation of the physical instrument contains not all, but the *relevant* data of the individual instrument throughout its lifetime.

The life cycle starts again with the manufacturer, who is responsible for the production of the measuring instrument, its remote control, its remote maintenance, as well as the continuous analysis of incoming data. The smart measuring instrument is marked electronically, for example with a digital plate, which forms part of the data stored as a digital representation. The certification body (or other responsible authority) takes care of either peer assessment or accreditation of the manufacturer, the supervision of the manufacturer's quality system for production, and also the conformity assessment of a new type of measuring instrument (which could be done remotely in the future). The certificate of conformity – and of course the test report – may be stored electronically, for example via a digital certificate of conformity, which is again stored as a digital representation,

provided that a test laboratory has successfully performed a test maybe by remote testing, and issued an electronic or digital test report to be used by the certification body.

The market surveillance authority will perform a remote supervision and will remotely ensure conformity to type. The initial verification and the periodic re-verifications, as well as sampling inspections and other activities of the inspection bodies and the verification authorities, will also be done remotely where an electronic or digital mark is stored in the digital representation of the instrument. We can expect in the future suddenly after a transition period that all the information stored as a digital representation completely replaces the traditional way of hardware marking on verified instruments. Of course, the customer is responsible for the correct use according to the specifications of the manufacturer, and the legal requirements.

Last but not least, the accreditation bodies are responsible for the accreditation of the manufacturers and of the other stakeholders, for example the certification body and the test laboratory. To be very clear, this is a vision and not yet reality, but many colleagues are working hard to make this vision become reality in the not so distant future, as we will hopefully demonstrate during today's webinar.

Again, I would like to repeat that from my point of view and from the BIPM/OIML Joint Task Group's point of view, the digital transformation of all metrology processes can only be successful and effective if it is based on the exchange of fair SI-based digital data where the emphasis is on the "I", in other words the interoperability of data and processes.

8 Further examples of the digital representation of metrology processes

For legal metrology purposes, digital representations contain all the relevant information that the responsible bodies need to perform: conformity assessment, verification, and market surveillance in a machine-readable way.

Digital representations also "know" the relevant standards and regulations, and provide machine-readable information about them. They also contain all the relevant information for customers so that they may gain trust and confidence in the products and quality measures. They provide machine-readable interfaces for users and manufacturers to enable smart quality assurance. They also combine machine-readable documents and certificates, hence enabling automation of the digital QI processes. Very importantly, they are secured and validated to provide access to information only two eligible parties (for example by the use of blockchain technology).

9 Digital certificate of conformity in metrology (D-CoCM)

Besides the European metrology cloud, the digital certificate of conformity in metrology (D-CoCM) is a good example of a digital transformation process that has already started. It is a PTB project which is being carried out in cooperation with the weighing industry. The idea is that the D-CoCM forms part of the digital representation of a measuring instrument under legal control, for example a weighing instrument, where it will contain type evaluation certificates, certificates of supervised manufacturers, quality systems for the production, and other relevant documents. It will provide the legally prescribed information as machine-readable data, for example a digital plate, a digital test report, a digital verification mark, etc., to enable stakeholders to perform all the legally prescribed actions. This requires a holistic approach to address the needs of all stakeholders involved during the lifecycle of an instrument. Again all this is intended to be realized using *FAIR* + *T* (i.e. traceable) digital data, based on the SI.

10 JTG joint statement of intent

Lastly, I would like to present the view of the Joint Task Group on a possible joint statement of intent regarding digital transformation of metrology as part of the international quality infrastructure.

The BIPM/CIPM-OIML/CIML Joint Task Group:

- **Recognizes** the importance of the **International System of Units (SI),** which underpins all measurements in industry, trade, legal metrology, and science;
- **Recognizes** the necessity for a **digital transformation of industrial, legal and scientific metrology** activities and processes in close cooperation with all stakeholders in the field of quality infrastructure (QI);
- **Supports** that **digital representations of physical devices** should rely on robust, unambiguous and machine-actionable data, using the **SI** and aiming at

meeting the **FAIR principles** (https://en.m.wikipedia.org/wiki/FAIR_data), to facilitate efficient processes in industry, economy, society, modern research and development globally;

- **Invites other organizations** to join this initiative towards a **digital QI framework**.

Concerning the timeline, it is planned to prepare a final draft document by mid-July 2021 so that it can be signed by the participating international organizations in the course of this year, where the CIPM and the CIML will hold their meetings in October 2021. ■

OIML-PTB Webinar:

Digital Transformation in Legal Metrology

The OIML and the PTB organised a Webinar on Digital Transformation in Legal Metrology on 5 May 2021. The event explored contemporary challenges, opportunities and solutions regarding digitalisation in legal metrology and especially provided a platform for the exchange of strategies, concepts and first steps towards realisations. The Webinar was chaired by Dr Florian Thiel (PTB Germany), Convener of WELMEC Working Group 7 Software.

Digital technologies have matured significantly over the past ten years - namely Embedded Systems, the Internet of Things (IoT), Cloud Computing, Blockchain and Big-Data concepts. These have facilitated completely new technology fields and data-driven markets such as the industrial internet, Industry 4.0, Machine Learning, and Artificial Intelligence-based Smart Services provided by digital platforms.

These technology and data-driven possibilities, together with concepts for digital platforms, can be exploited for the benefit of all stakeholders in legal metrology, e.g. to overcome barriers to innovation set up by regulations, better coordinate legal processes, reduce development costs, and reduce the time to market of new products.

The time is now right for all stakeholders in legal metrology to come together to discuss the challenges and opportunities that digitalisation brings. The Webinar brought together experts from different technical disciplines, as well as representatives from industry, science, testing authorities, notified bodies, and regulatory authorities to discuss and present their visions, solutions and practical digital realisations in the field of legal metrology.

The Editors of the OIML Bulletin express their thanks to the authors of the articles in this edition of the Bulletin for transforming their Webinar presentations into publishable articles.

DIGITAL TRANSFORMATION

Blockchains and legal metrology: applications and possibilities

Wilson S. Melo Jr.
Brazilian National Institute of Metrology, Quality, and Technology (INMETRO)

OIML-PTB WEBINAR

DIGITAL TRANSFORMATION IN LEGAL METROLOGY

5 MAY 2021

1 Abstract

Blockchains are an emerging technology with a huge potential to accelerate the digital transformation of different segments. In the context of legal metrology, blockchains can impact many applications and activities related to information management, workflow automation, and reliability of measuring instruments and systems. Further, blockchains depend on oracle devices, which feed the system with information from the external world. When one considers physical assets, smart meters will become these oracles and, consequently, blockchains will require specific legal metrology activities and regulations. In this paper we discuss this mutual interdependency, describing potential applications and research results already published. These topics are key to making scientists and metrologists aware of the implications of blockchain technology and how it will impact legal metrology over the coming years.

Introduction

The concept of digital transformation in metrology concerns a process of progressive adoption and integration of a large set of new technologies [1]–[8]. We call them "Technologies 4.0", in a glaring reference to the fourth industrial revolution and its novel ideas, processes, methods, and tools [9]. Indeed, Industry 4.0 is the digital transformation of 21st-century industry under the influence of nine technological "pillars": Big data, cloud computing, robot automation, horizontal and vertical integration, the Internet o Things (IoT), additive manufacturing, augmented reality, simulation, and cybersecurity. However, it is worth noting that these technologies are also transforming other areas besides industry. Smart grids, vehicular communication (i.e., V2V and V2I), e-health, and smart cities are examples of complex systems resulting from the digital transformation in energy production/distribution, transportation, healthcare, and management of urban spaces [9]. So we can deem that these technologies are creating a true "Society 4.0" since this digital transformation has profound implications in all human activities. Consequently, legal metrology is also a target of these technologies and will undergo significant changes over the coming years [7].

Information is the elementary fuel in digital transformation [7], [9]. Consequently, technologies that are able to manage information and integrate other technologies are emerging as effective and disruptive tools. Blockchain is one of these technologies. In the last decade, blockchain has drawn the attention of stakeholders in different areas, mainly due to its expressive success as a cryptocurrency platform [10]–[13]. However, blockchains can do more than manage bitcoin wallets. Indeed, one can describe blockchain as a true integrator among different digital technologies such as cloud computing, Big data, and IoT. The following topics summarize this concept:

- A blockchain implementation relies on a network of independent peers that work cooperatively, usually in a cloud computing-based environment.
- Blockchains work as reliable and immutable data storage systems, so they also can support and consolidate Big data applications.
- Blockchains use smart contracts to automate workflows, enabling horizontal and vertical integration among different systems.
- One of the main features of blockchains is to create trust among parties that do not trust each other, enhancing cybersecurity.

The possibilities of applying blockchains to digital transformation processes are countless [11], [13]. In a recent survey about blockchain-based applications, Dai et al. [11] cite ongoing projects in various sectors such as energy trading, vehicle life cycle management, and patients' data protection in hospitals. One can notice that these applications are all expanding in the "cyber world" (where information is only a digitalized value)

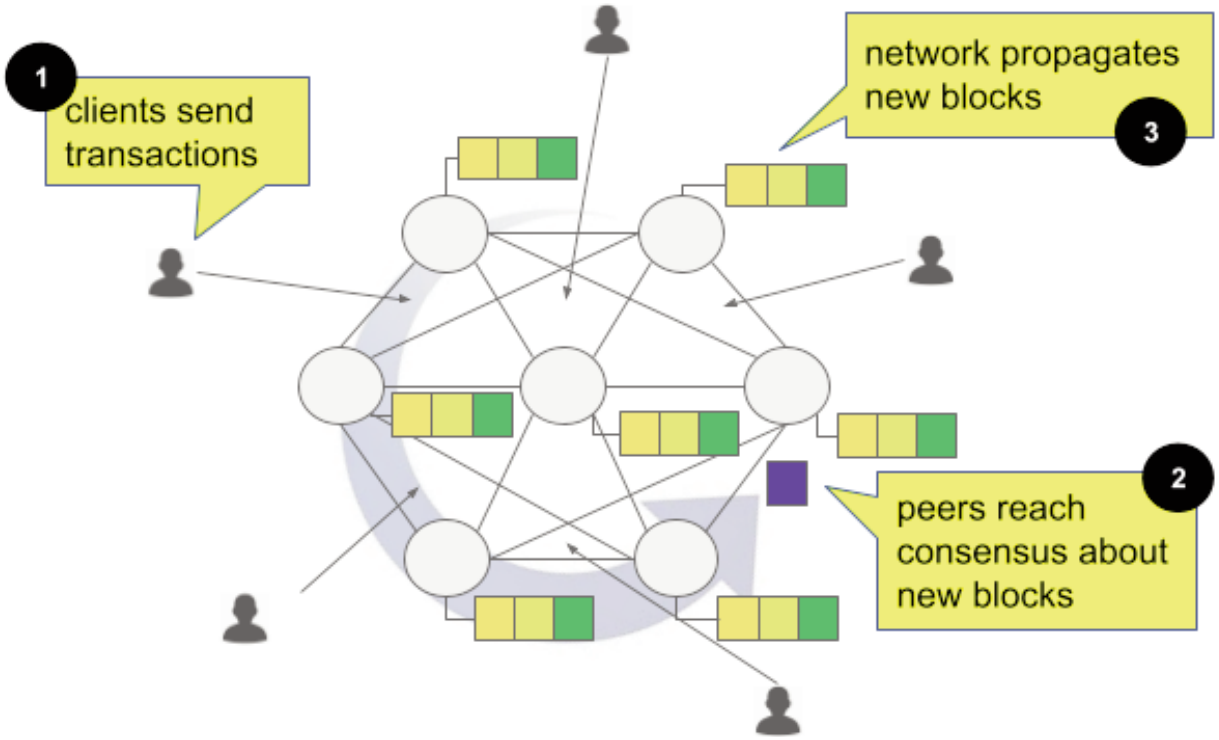


Figure 1: Blockchain's primary mechanism

and integrating into the "physical world" (where information concerns concrete elements and physical quantities). This finding introduces a new challenge (and many opportunities) that we can synthesize in the following statements:

- Legal metrology needs blockchains once many processes involving the trade of goods, people's health, public safety, and the environment will become blockchain-based applications;
- Blockchains need legal metrology support since much real-world information demands its translation into measurements of physical quantities.

This article proposes the concept that there is a beneficial symbiotic relationship between legal metrology and blockchains. We present evidence that supports this idea by describing some research findings regarding blockchain-based applications in scopes involving measuring systems under regulation. These examples demonstrate that blockchains can enhance legal metrology activities, reducing costs and improving their efficiency. Furthermore, blockchains depend on reliable information from the real world, and measuring systems under legal control are the most indicated devices to fill this gap. We conclude that blockchains can be an essential tool to accelerate legal metrology's digital transformation, leading its activities to a new technological level.

2 Blockchains in a nutshell

One can define blockchains as a distributed append-only data structure (called a *ledger*) that can store data and self-executed software called smart contracts [10], [11], [13]. These features make blockchains not only a storage solution but also a complete service-oriented platform. Moreover, blockchains provide a mechanism to reach trust among parts that do not trust each other without the need for a third trusted party (TTP). This last aspect leads to the two main reasons for adopting blockchains: a) there is no available TTP, or b) the cost regarding a TTP is prohibitive [14].

A blockchain implementation relies on a network of peers from independent organizations to ensure information reliability. Figure 1 illustrates a blockchain's primary mechanism, which consists of clients sending transactions to the network that organizes these transactions in blocks and replicates these blocks among all the participating peers. The process of deciding the next block is called consensus. The network also assures the transaction order by cryptographically linking each block to the previous one, creating a "chain of blocks".

According to Cachin and Vukolic [10], four technical disciplines work as cornerstones in a blockchain's architecture: cryptography, consensus, replication, and business logic. Cryptography is essential to assure the

authenticity and integrity of information on each transaction since senders sign their requests, and peers also sign every block on validation. Consensus is a canonic problem in Computer Science, and it is essential to determine the transactions' total order and each block content [12]. In turn, replication is the key to propagate blocks and achieve data consistency in all the peers. Finally, business logic comes from smart contracts, which are, in practice, pieces of software embedded into the blockchain. Smart contracts provide a flexible mechanism to automate workflows, implementing the blockchain model business.

Nowadays, there is a diversity of blockchain implementations which we call platforms [15], [16]. Adopting a blockchain platform is usually a wise decision due to the complexity of implementing a blockchain from scratch. However, each blockchain platform introduces its particularities and even its own working philosophy. There are two main platform categories in practical terms: permissioned (or private) and non-permissioned (also known as public) blockchains [10], [13]. The difference is that the former requires the identification of each peer taking part in the consensus, and the latter does not. This difference also impacts the consensus mechanism in the network. Permissioned blockchains can adopt voting-based consensus protocols, which generally perform better than proof-based consensus protocols. In contrast, non-permissioned blockchains constitute free-access platforms that are highly decentralized and ideal for cryptocurrency wallets and trading applications [10], [12].

Voting-based consensus protocols depend on a quorum of peers responsible for deciding the order of the transactions and generating any new block. Currently, fault-tolerant consensus protocols are the most promising alternative, especially regarding reliability and performance. One classifies these protocols into crash-fault tolerant (CFT) and byzantine-fault tolerant (BFT) [12]. In practical terms, we can say that a BFT consensus is more reliable than CFT since the former includes all the features of the latter. However, BFT is also more complex and resists collusion attacks of no more than a third of the peers integrating the consensus quorum, while CFT tolerates no more than a half of compromised peers.

3 Why legal metrology needs blockchains

Trust is an essential requirement in legal metrology. It is also the precise intersection point with blockchain technology. Although legal metrology has efficient methods for obtaining measurements with low uncertainty, digital information processing can be a problem when measurements and legally relevant information are targets of cyberattacks by malicious entities [6], [17], [18].

Different countries have different concerns about the cybersecurity of measuring instruments. For instance, the USA may worry about cyberterrorism against critical infrastructures that depend on sensors and the reliability of meters. On the other hand, Europe often discusses privacy issues once meters can expose sensitive consumer information. In many developing countries, measurement fraud is the principal challenge that demands continuous action on the part of the notified bodies. In all these scopes, blockchains can effectively increase the reliability of measuring instruments and protect legally relevant software and parameters.

Another aspect is the fast digital transformation in legal metrology [7], increasing the demand for new disruptive technologies to reduce uncertainty and enhance the protection of measuring instruments [4], [6]. As discussed above, blockchain is one of these technologies, and it is difficult to disagree with this claim. However, there are many questions and doubts about how we should use blockchains to improve legal metrology effectively.

The first widespread blockchain-based application is Bitcoin [15], proposed in 2008. In the last decade, blockchain thrives consistently within cryptocurrencies, and only some years ago, people started to wonder about using blockchains in other areas besides finances. In 2017, we published the first technical work suggesting that blockchains could help improve legal metrology activities [19]. In 2018, independent publications from the PTB and INMETRO proposed the first practical blockchain-based applications and experiments regarding legal metrology [20], [21]. In the same year, NIST published a technical report about blockchains but did not suggest any practical use in the metrology field [13]. Since then, different ideas have explored blockchain's properties in applications involving the management of smart meters, simplifying type approval, and field surveillance of instruments under regulation [18], [22]–[24]. In the following subsections, we present a short overview of these works.

3.1 Starting from the trivial applications

The most elementary blockchain feature is stored data. Further, this storage is distributed, decentralized, and immutable. When one considers these properties, the first idea is to use blockchains to maintain sensitive data under the scope of legal control of instruments and measurements [20]. Thus, blockchains can work as repositories for meters' legally relevant parameters,

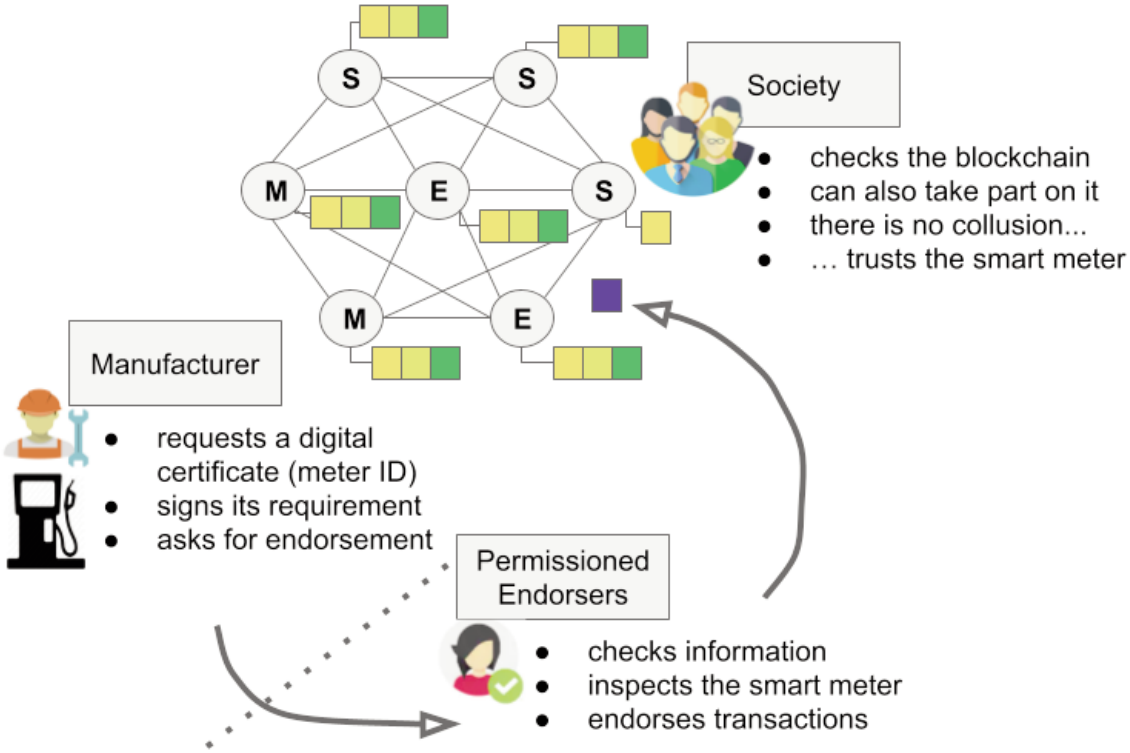


Figure 2: Blockchain-based PKI for smart meters (Moni et al. [23])

calibration certificates, and software updates for smart meters.

A practical initiative involving blockchains and legal metrology is already happening in the European Metrology Cloud (EMC) project scope [7]. The EMC includes several European National Metrology Institutes (NMIs) and establishes a reference architecture related to digital transformation in metrology. The project foresees the adoption of permissioned blockchains as an alternative in digital processes that demand trust. Thiel and Weztlich [8] explicitly mention the management of administrative identities and event logbooks.

3.2 Public-Key Infrastructure for measuring instruments

A Public-Key Infrastructure (PKI) is a mechanism for managing digital certificates, constituting a classic solution model for applications using cryptographic directives intensively (e.g. digital signature) [20], [23]. Its traditional implementation is hierarchical and relies on Certification Authorities (CAs). Essentially, a CA's function is to issue and verify digital certificates, attesting that a given public key belongs to a respective entity.

CA-based PKIs are often costly due to the need for management, verification, and revocation of digital certificates. Consequently, the traditional implementation could not be suitable in scenarios with a large number of low-cost devices (e.g., IoT devices and measuring instruments). In contrast, a blockchain-based PKI can constitute a cheaper alternative to provide the same services without depending on CAs [23]. In a blockchain-based PKI, if a device has its public key stored in the ledger, other participants can access it and check the authenticity and integrity of any signed information. Further, the immutable ledger provides irrefutability without the need for a digital certificate.

Figure 2 depicts a blockchain-based PKI architecture implemented by Moni et al. [23]. In their proposal, Permissioned Endorsers (e.g. notified bodies) are responsible for checking any new measuring instrument, extracting its public key, and inserting it into the blockchain. Once the public key is there, the instrument can sign any legally relevant information using the respective private key. Any entity with access to the blockchain can invoke a smart contract to verify this signature without the need for a CA or any other TTP.

This kind of application can be essential for smart meters. Different instruments already use public-key cryptography to ensure the integrity and authenticity of measurements and legally relevant data. However, without digital certificates, one cannot claim the irrefutability of a measurement performed by an instrument under legal control. A blockchain-based PCI can bridge this gap practically and efficiently.

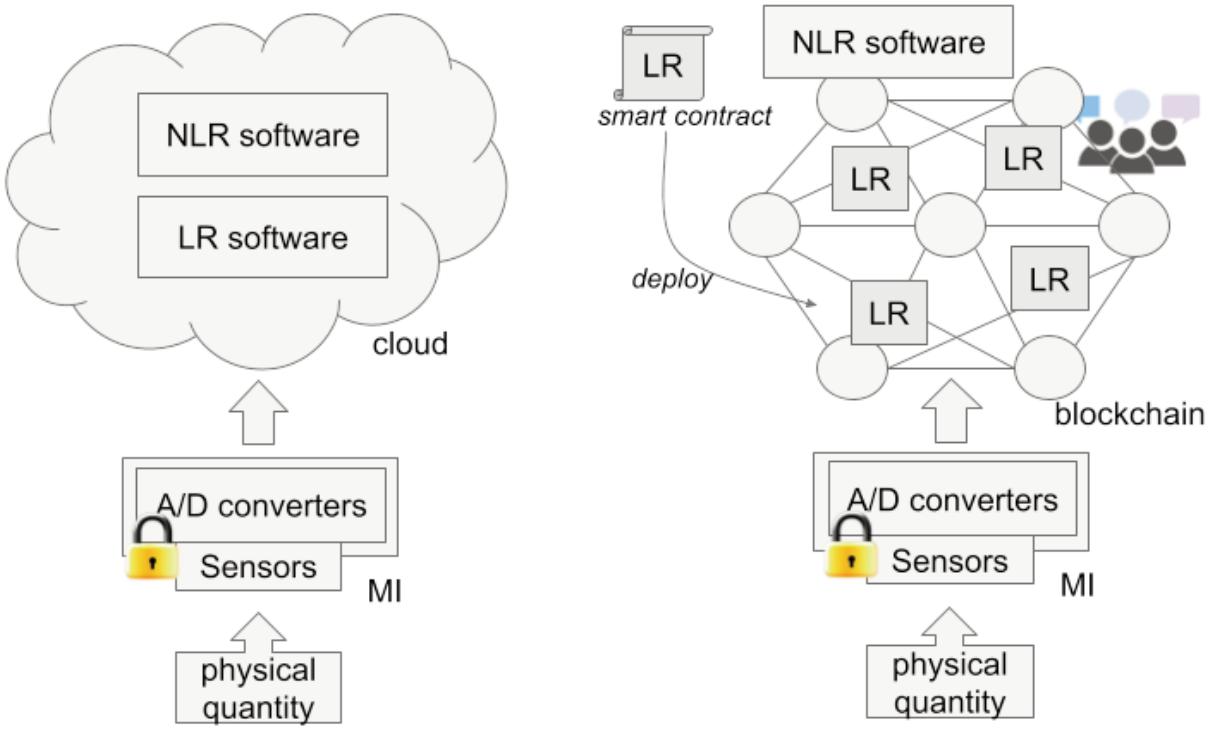


Figure 3: Cloud-based DMS versus blockchain-based DMS (Melo et al.,[21])

3.3 Distributed measuring systems

Recently, several works have discussed solutions that use remote computational resources to run legally relevant software in measuring applications [21], [25]. We name this kind of instrument Distributed Measuring Systems (DMS). A DMS has exciting properties when compared to traditional measurement instrument architectures. It reduces software evaluation complexity while allowing manufacturers to take advantage of up-to-date computing technologies (e.g. cloud computing and virtualization).

A DMS using blockchains introduces even more novel possibilities: one can implement legally relevant software as smart contracts, turning the blockchain into a software protection tool. Also, blockchain can reduce costs related to the metrological supervision of meters, including marketing and field surveillance [21].

Figure 3 summarizes a comparison between a cloud-based DMS as described in Opperman et al. [25] and a blockchain-based DMS implemented in Melo et al. [21]. Essentially, both have the same structure regarding relying on a "tiny" smart meter that gathers raw data, signs it and sends it to the blockchain. The difference happens after the meter sends the data. The cloud process data and provides measurements using legally (LR) and non legally relevant (NLR) software modules installed as a cloud service but still under the control of one specific entity (i.e. the cloud service owner). In contrast, the blockchain-based DMS implements LR and NLR software as smart contracts. Different peers from independent organizations execute the same smart contracts (this procedure is part of the blockchains redundancy) and must agree about the exact measurement result. Further, smart contracts are written into the ledger, ensuring its integrity and protection against tampering.

A blockchain-based DMS works as follows. The manufacturer implements its measuring instrument from two basic modules: a secure hardware module that senses a physical quantity and sends it to the blockchain in the format of a transaction, and a smart contract that implements the measurement computation (usually performed by the legally relevant software). After proceeding with type approval for both modules, the notified body writes the smart contract on the blockchain, so any hardware module in use can submit its transactions. The blockchain is responsible for performing the entire measurement computation. It also ensures software integrity since the code becomes an immutable, legally relevant smart contract in the ledger.

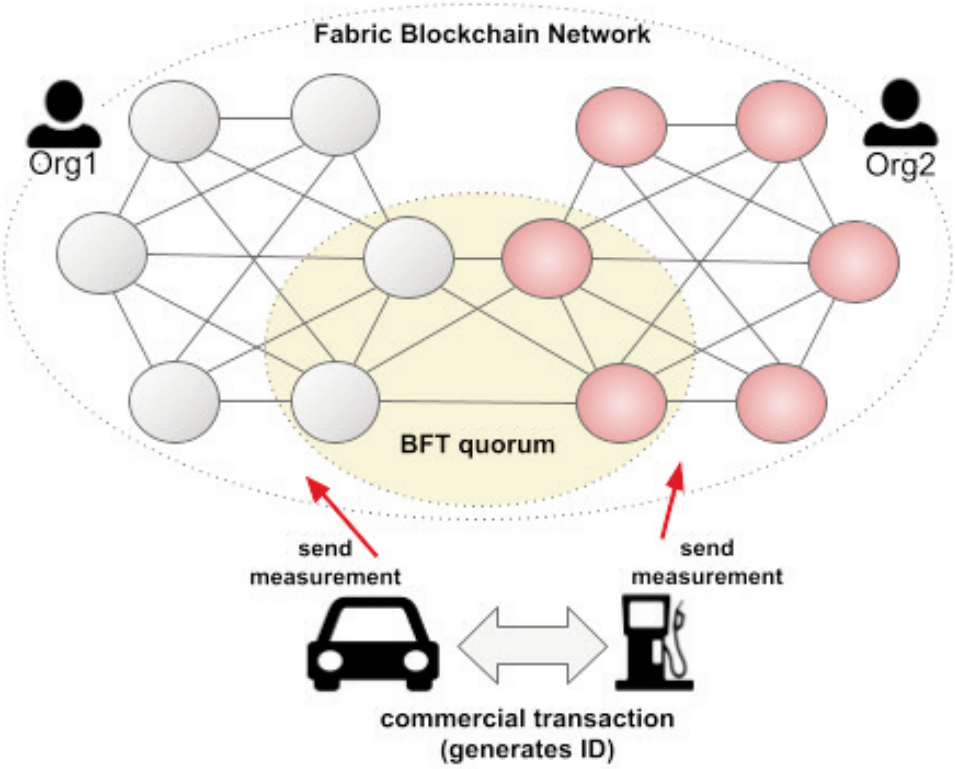


Figure 4: Field surveillance of fuel dispensers using blockchains (Melo et al.[22])

3.4 Legally relevant software update

Manufacturers that develop legally relevant software for instruments under legal control need to submit each new software version to a type approval process. Software designers can employ different mechanisms to ensure that the meter receives only duly approved software versions. However, blockchains can constitute an efficient solution [20]. In this application, manufacturers program their meters to search for (and accept only) software updates published on the blockchain. Notified bodies are responsible for uploading any new software version to the blockchain. Meanwhile, the users of the meters can follow software updates by consulting the blockchain and checking whether their device complies with the latest approved version.

3.5 Field surveillance using blockchains

Regrettably, fraud in measurements is a disseminated practice, and the problem occurs mainly due to the profitable income that malicious entities can earn [6], [26]. Many times, fraud is very sophisticated in terms of technological resources and surreptitious behavior [17].

Fuel dispensers are a typical example of fraud where malicious entities collude among themselves and can even corrupt notified bodies' agents. Leitao et al. [17] analyze the reality of fuel dispensers in Brazil and describe more than 20 different strategies of electronic fraud, most of which are hard to detect and expose even by experienced technicians. Moreover, Rodrigues Filho and Gonçalves [26] estimate that in Brazil alone, fraud in fuel measurements generate losses to society in the order of USD 300 million per year.

One of our recent works uses blockchains as a tool to improve field surveillance of fuel dispensers [22]. The core idea behind this proposal is to involve different entities in metrological supervision activities. The blockchain serves as a reliable platform to store information from various sources. For instance, one expects that the fuel dispensers log any refilling event into the blockchain. But drivers can do the same by using vehicular embedded sensors to estimate the fuel amount on each refilling. Although these sensors do not have enough accuracy and precision, their information becomes valuable after a large number of events. Furthermore, entities that participate as stakeholders in the blockchain can perform their statistical analysis by implementing smart contracts. Blockchains provide vital protection against collusion attacks, something that inhibits much fraudulent behavior. Figure 4 shows our implementation design using the Hyperledger Fabric platform and BFT consensus.

3.6 Management of proficiency testing

Proficiency Testing (PTs) are methods for evaluating the performance of a set of participants - usually laboratories or entities that perform metrological tests - based on pre-established criteria. They are an essential tool in verifying the competence demonstrated by these laboratories in carrying out tests, trials, and experiments.

Blockchains can provide an efficient platform for managing PTs by automating performance evaluation processes and providing secure information storage. We can implement this application as follows. The PT promoter (i.e. the organization responsible for leading the PT) publishes a cryptographic public key on the blockchain. Each participant generates its inter-comparison results, encrypts the respective measurements using the promoter's public key, and writes them on the blockchain. After this step, participants cannot change their measurements anymore. Once all the participants have provided their (encrypted) measurements, the promoter publishes the private key. This action triggers a smart contract that automatically decrypts each participant's measurements and computes the PT final result. Further, this result can pass by auditing at any moment since the ledger permanently stores all information that influences it.

4 Why blockchains need legal metrology

Although most people clearly understand why blockchains are necessary to legal metrology, few people notice that the opposite is also true: blockchains need legal metrology. This dependency will become more evident over the coming years due to an essential group of actors: the blockchains' oracles [27]. In the blockchain ecosystem, oracles are trustable entities that feed the blockchain network with information from the external world. This information is necessary for different purposes, but two are the more relevant: a) manage the binding between tangible assets and their digital representation; and b) provide information to smart contracts' decision processes [28], [29].

4.1 Measuring instruments can work as oracles

Blockchains are very good at managing digital assets (e.g. a cryptocurrency wallet, a document, a certificate). Still, these assets are often a digital representation of something in the physical world: a tangible asset. Many times, this tangible asset is also a physical asset. When this happens, oracles will need measurements to describe the physical asset and provide information about it. We can illustrate this concept from the following blockchain-based applications:

- Energy trade: Several works have proposed blockchains as a platform for free trading among microgenerators in a smart grid. However, the blockchain needs a "physical attestation" about the existence of the traded energy amount. In practice, this attestation will emanate from a smart energy meter that works as an oracle and informs the blockchain how much energy the seller indeed produced.
- Properties trade: People can be interested in buying or renting a property (e.g. an apartment) using blockchains. Proposals related to this kind of application usually explore the opportunity of creating platforms for direct interaction among sellers and buyers without the need for a TTP. However, buyers or renters typically ask for specific information such as the property size, its conservation state, or the exact position to determine the incidence of natural light. Smart meters and IoT devices can provide all this information, serving as reliable oracles.
- Controlled drugs traceability: This application is fascinating since it can manage the complete life cycle of controlled medications (i.e. production, distribution, and consumption). Again, the processes involved require measurements from different physical quantities. For instance, production labs can use meters that attest to the proportions of each chemical component. In turn, inspection labs can use X-ray instruments to verify solid-state chemistry properties. In practice, different kinds of measuring systems feed the blockchain with information about the product (i.e. the physical asset).

Things are very similar when we talk about smart contracts decision processes. The difference is that smart contracts can demand information that does not describe the physical asset but determine specific conditions which are relevant to complete a transaction. Again, these conditions can depend on reliable measurements. The examples below help to understand this dependency:

- Trade of chilled food: Blockchain applications can support smart contracts that determine the food's price according to its conservation temperature. In practice, a thermometer monitors the food temperature during its transportation. Temperature variations (i.e. the temperature exceeds a specific threshold) impact the product's final price.
- Monitoring of patient conditions: One can apply smart contracts in blockchain-based monitoring

health systems to log the need for specific medical procedures due to the patient's condition. Body sensors (e.g. sphygmomanometer, oximeter) can provide real-time information to a smart contract that triggers notifications or alarms on an abnormal situation. This registry protects both patients and healthy staff once it is immutable evidence that justifies the medical procedures.

4.2 Assuring oracles' reliability

Measuring instruments shall perform oracles in different blockchain-based applications, implementing legally relevant features in many of these scenarios. Consequently, these meters can also demand metrological control and supervision. At first glance, one can suppose that the necessary activities will be the same as those that notified bodies already apply on verifying measuring instruments in typical applications. However, this belief can be inaccurate. One must consider the fact that different factors can impact oracles' reliability, many of them demanding a deeper analysis.

First of all, blockchains can ask for new features that standard smart meters do not implement. Since these features can influence legally relevant functions, they can also impose new technical requirements and measuring instrument directives. There is a good chance that NMIs will need to implement new regulatory programs to contemplate different classes of oracles in completely new technical environments. A second exciting aspect is that blockchains can create a new business segment for smart meter manufacturers. When we evaluate the growing blockchain expectations, we notice that the number of applications will increase in the more diverse business segments. Wherever blockchain applications manage physical assets, oracles will be necessary, and smart meters will satisfy this need.

5 Challenges and research opportunities

Blockchain is still a young technology. Thus there are many doubts and concerns about how this technology will change until it reaches maturity. This uncertainty also affects any application in the legal metrology field. Unavoidably, we must deal with these issues before blockchain applications become a more predictable alternative. At the same time, these challenges constitute singular opportunities for research and investigation by metrology scientists worldwide. In the following subsection, we highlight four of these challenges: consensus, performance, privacy, and oracles' authentication.

5.1 What consensus should we use?

So far, practically all works about blockchains and applications in legal metrology suggest permissioned blockchains as the most suitable alternative. Thiel and Weztlich [8] discuss integrating blockchains to the EMC architecture reference and justify the choice for permissioned blockchains by arguing that in the EMC (i) there is not a TTP, (ii) there are multiple and unknown users, and (iii) users can be untrustworthy. In the experiments developed by INMETRO and the PTB, permissioned blockchains were a premise in all the scenarios investigated. This aspect is relevant because it directly impacts the blockchain consensus.

In a permissioned blockchain, one relevant question is about adopting CFT or BFT consensus. As we discussed above, BFT could imply interesting security properties in a truly decentralized blockchain network. Many practical scenarios in legal metrology can demand this kind of consensus to ensure fairness on deciding about transactions order and new blocks. However, its deployment is still a challenge. Most permissioned blockchain platforms do not implement BFT consensus natively. On the other hand, solutions using CFT consensus are more disseminated, as is the case of the Raft protocol. Some of our published experiments already use Raft to coordinate consensus among servers in Germany and Brazil. A necessary next step is a comparison among CFT and BFT alternatives.

5.2 Will my blockchain network perform correctly?

Performance is perhaps the blockchain bottleneck at the moment. The available blockchain platforms process a relatively low number of transactions per second (tps) compared to standalone solutions. Further, blockchain has serious scalability problems, which means that we cannot increase performance by simply adding more peers. This limitation is related to intrinsic properties from the consensus protocol. Although voting-based consensus protocols (suitable for permissioned blockchains) perform better than proof-based ones, they are still far less efficient than centralized solutions.

Just to give an idea about numbers, famous permissionless blockchains platforms such as Bitcoin and Ethereum 1.0 can do around 7 and 30 tps, respectively. In a permissioned blockchain, we have Hyperledger Fabric delivering around 2 000 tps in a benchmark environment [16], although, in our deployment, we

obtained a value of approximately 400 tps [18], [21], [22]. Even so, in practice, these performance rates can be enough to implement tailored applications. We can exemplify this reasoning from the findings of our previous work, where we design a blockchain application to meet the demand of a hypothetical vehicle speed DMS, counting on 1,000 speed meters and a vehicular flow greater than 2 500 vehicles/hour [21].

One can safely affirm that, in the coming years, performance will be one of the leading research topics about blockchains. We also can expect that blockchain platforms will present increasing performance and address larger-scale applications.

5.3 Will blockchains ensure my data's privacy?

Privacy is a big question when one talks about blockchains. Firstly, we need to remember that the first blockchain practical implementations strongly incentivized the information publicity philosophy. People usually trust Bitcoin because anyone can verify each transaction and audit any wallet (although their owners theoretically stay anonymous). However, this concept is far from being mainstream in terms of information management. Privacy is mandatory in most practical scenarios, especially in times of laws and regulations like the General Data Protection Regulation (GDPR).

Measurement privacy is a concern in legal metrology contexts, especially when there is the risk of personal sensitive information exposure [25]. That happens with smart energy meters that can reveal peoples' domestic habits or body sensors monitoring health data. Thus if we intend to use blockchain to store sensitive information, we need to discuss how to implement this feature. The solutions, though, are not trivial since they conflict with blockchain's "open" properties (e.g. auditability, transparency) with privacy constraints (e.g. secrecy, access control).

Access control is a feature that many permissioned blockchain platforms already include by default. For instance, in Hyperledger Fabric, peers can compose different channels (i.e. different ledger instances) and define specific access policies for each of them [16]. However, privacy policies can demand more restrictive constraints than access policies. In this case, cryptography directives are the more suitable alternative. The PTB has developed a pioneer investigation line that embraces fully homomorphic encryption systems for privacy assurance [18], [24]. These mechanisms enable the data computation in the cryptographic domain (i.e. we can mathematically operate over data without decrypting it), having applications in cloud systems and blockchains. Despite its promising aspects, this study faces tough challenges since homomorphic encryption still demands a significant spend of computational resources and can be prohibitive in many practical scenarios.

5.4 How can I prove that my meter is a reliable oracle?

People working on any activity related to smart meter manufacturing who pay attention to Section 4.1 will probably ask themselves how to transform these meters into blockchain oracles. This question is relevant, especially when one considers that oracles work before the blockchain information flow, so the blockchain security directives do not apply to these devices [27]. At the same time, if oracles are not trustable, neither is the blockchain. This finding has deep implications for evaluating the reliability of blockchains. Blockchains will need independent mechanisms to attest to the reliability of oracles, including their authentication.

Initially, we must remember that legal metrology already establishes guidelines and recommendations to protect legally relevant measuring instrument components and attest to their reliability. However, thinking of oracles as isolated trustable devices transforms them into a TTP, which blockchains do not want to depend on. Oracles will probably be redundant and complementary devices, so blockchain decisions will rely on information corroborated by a set of oracles instead of an isolated oracle [30].

There is already scientific work proposing oracle authentication protocols, some of which are based on voting protocols [28], [29]. However, to the best of our knowledge, no research discusses integrating smart meters into practical protocols of mutual authentication. This investigation is undoubtedly a remarkable topic that metrology scientists can address in their studies over the coming years.

5.5 The need for an inter-NMI blockchain network

When we consider so many possibilities and opportunities regarding blockchain-based applications in metrology, it is natural to conclude that scientists and metrologists will need a proper environment to experiment with solutions. Aiming to spread this idea, the PTB and INMETRO have worked together on behalf of an inter-NMI blockchain network [23]. Figure 5 describes this proposal as a permissioned blockchain network. The NMIs integrating the network need to provide peers to implement applications of common interest to other participants. The NMIs can also

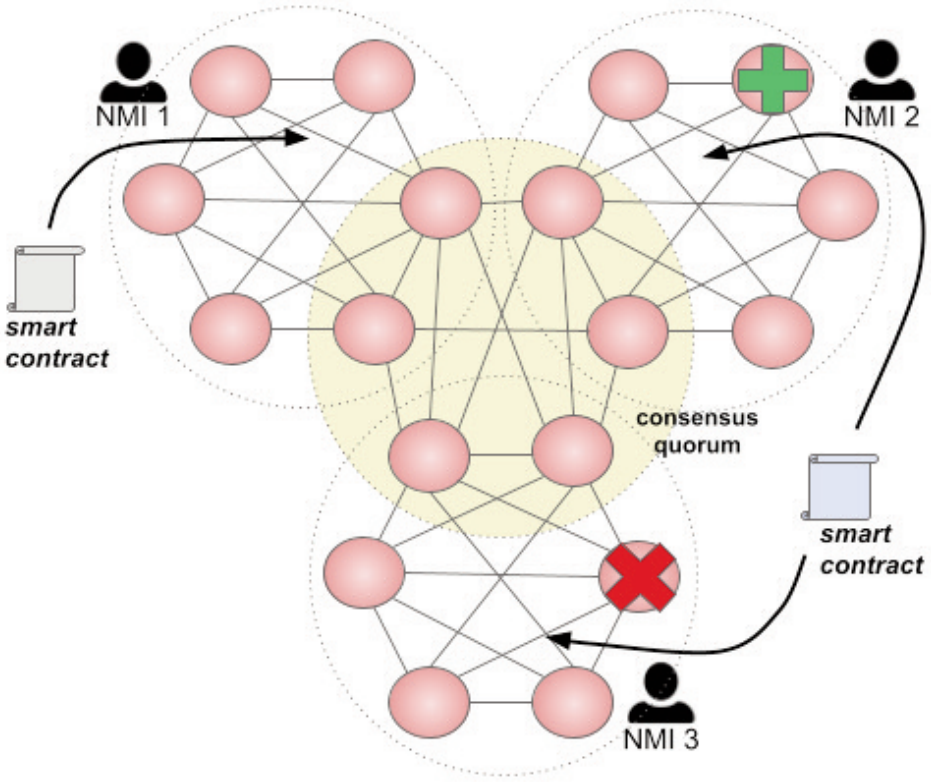


Figure 5: The concept of an inter-NMI blockchain network (Moni et al. [23])

participate in the consensus quorum (probably a voting-based alternative: CFT or BFT).

We visualize the inter-NMI blockchain network as a smart contract-oriented platform. Thus the participants can write and implement their applications by using smart contracts as a development base. Moreover, the network is decentralized. Each participant can manage their peers independently, adding or removing peers according to their needs.

The inter-NMI network is a great initiative that opens up opportunities for collaboration and contributions worldwide. For more details, please check the work of Moni et al. [23]. If your institution is interested in joining the network, we encourage you to contact us for more details about the project.

6 Conclusions

In this article, we have presented the main concepts that bind legal metrology to blockchain technology. Blockchain is a tool to accelerate digital transformation in many segments. The demand for blockchain-based applications will increase over the coming years, and legal metrology can also take advantage of that. Moreover, blockchains also will require help from legal metrology to manage physical assets correctly. This advantageous and mutual interdependency can strengthen the trustworthiness of blockchains and boost digital transformation in legal metrology processes that essentially depend on information immutability, reliability, and decision automation. ■

7 References

[1] E. V. Dudukalov, V. D. Munister, A. L. Zolkin, S. A. Galanskiy, e S. G. Rudnev, "Metrological support integration in conditions of digital transformation", *J. Phys. Conf. Ser.*, vol. 1889, nº 3, p. 032012, 2021, doi: 10.1088/1742-6596/1889/3/032012.

[2] T. Mustapää, P. Nikander, D. Hutzschenreuter, e R. Viitala, "Metrological challenges in collaborative sensing: Applicability of digital calibration certificates", *Sens. Switz.*, vol. 20, nº 17, p. 1–19, 2020, doi: 10.3390/s20174730.

[3] T. Mustapaa, J. Autiosalo, P. Nikander, J. E. Siegel, e R. Viitala, "Digital Metrology for the Internet of Things", in *GIoTS 2020 - Global Internet of Things Summit, Proceedings*, 2020, p. 1–6. doi: 10.1109/GIOTS49054.2020.9119603.

[4] A. Oppermann, S. Eickelberg, e J. Exner, "Toward Digital Transformation of Processes in Legal Metrology for Weighing Instruments", in *Proceedings of the 2020 Federated Conference on Computer Science and Information Systems, FedCSIS 2020*, 2020, vol. 21, p. 559–562. doi: 10.15439/2020F77.

[5] M. Peterek e B. Montavon, "Prototype for dual digital traceability of metrology data using X.509 and IOTA", *CIRP Ann.*, vol. 69, nº 1, p. 449–452, 2020, doi: 10.1016/j.cirp.2020.04.104.

[6] A. E. R. Rincon, W. S. Melo, C. M. Farias, e L. F. R. C. Carmo, "Securing Smart Meters through Physical Properties of their Components", *IEEE Trans. Instrum. Meas.*, vol. 70, p. 1–11, 2020, doi: 10.1109/TIM.2020.3041098.

[7] F. Thiel, "Digital transformation of legal metrology - The European Metrology Cloud", *OIML Bull.*, vol. 59, nº 1, p. 10–21, 2018.

[8] F. Thiel e 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, p. 39. doi: 10.1051/metrology/201901001.

[9] A. Ustundag e E. Cevikcan, *Industry 4.0: Managing The Digital Transformation*. Cham, Switzerland: Springer, 2018. doi: 10.1007/978-3-319-57870-5.

[10] C. Cachin e M. Vukoli , "Blockchain Consensus Protocols in the Wild", in *31 International Symposium on Distributed Computing*, 2017, p. 16. doi: 10.4230/LIPIcs.DISC.2017.1.

[11] H.-N. Dai, Z. Zheng, e Y. Zhang, "Blockchain for Internet of Things: A Survey", *IEEE Internet Things J.*, vol. 6, nº 5, p. 8076— – 8094, 2019.

[12] Y. Xiao, N. Zhang, W. Lou, e Y. T. Hou, "A Survey of Distributed Consensus Protocols for Blockchain Networks", *IEEE Commun. Surv. Tutor.*, vol. 22, nº 2, p. 1432–1465, 2020.

[13] D. Yaga, P. Mell, N. Roby, e K. Scarfone, "Blockchain Technology Overview", 2018. doi: 10.6028/NIST.IR.8202.

[14] K. Wüst e A. Gervais, "Do you Need a Blockchain?", in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 2018, p. 45–54. doi: 10.1109/CVCBT.2018.00011.

[15] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", *Www.Bitcoin.Org*, 2008. doi: 10.1007/s10838-008-9062-0.

[16] E. Androulaki *et al.*, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains", Porto, Portugal, 2018. doi: 10.1145/3190508.3190538.

[17] F. O. Leitão, M. T. Vasconcellos, e P. C. R. Brandão, "Hardware and Software Countermeasures on High Technology Fraud at Fuel Dispensers under the Scope of Legal Metrology", in *IX Simposio Internacional "Metrologia 2014"*, Havana, 2014, p. 1–10.

[18] D. Peters *et al.*, "IT Security for Measuring Instruments: Confidential Checking of Software Functionality", in *Advances in Intelligent Systems and Computing*, vol. 1129 AISC, Springer, Cham, 2020, p. 701–720. doi: 10.1007/978-3-030-39445-5_51.

[19] W. S. Melo Jr., A. Bessani, e L. F. R. C. Carmo, "How Blockchains can help Legal Metrology", in *SERIAL '17 Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*, New York, New York, USA, 2017, p. 1–2. doi: 10.1145/3152824.3152829.

[20] D. Peters, J. Wetzlich, F. Thiel, e J. Seifert, "Blockchain Applications for Legal Metrology", in *IEEE International Instrumentation and Measurement Technology Conference*, Houston, Texas, USA, 2018, p. 6.

[21] W. S. Melo Jr., A. Bessani, N. Neves, A. O. Santin, e L. F. R. C. Carmo, "Using Blockchains to Implement Distributed Measuring Systems", *IEEE Trans. Instrum. Meas.*, vol. 68, nº 5, p. 1503–1512, 2019, doi: 10.1109/TIM.2019.2898013.

[22] W. S. Melo, L. V. Tarelho, B. A. Rodrigues, A. N. Bessani, e L. F. R. C. Carmo, "Field surveillance of fuel dispensers using IoT-based metering and blockchains", *J. Netw. Comput. Appl.*, vol. 175, nº February 2021, p. 102914, 2020, doi: 10.1016/j.jnca.2020.102914.

[23] M. Moni, W. Melo, D. Peters, e R. Machado, "When measurements meet blockchain: On behalf of an inter-nmi network", *Sensors*, vol. 21, nº 5, p. 1–24, 2021, doi: 10.3390/s21051564.

[24] A. Yurchenko, M. Moni, D. Peters, J. Nordholz, e F. Thiel, "Security for Distributed Smart Meter : Blockchain-based Approach , Ensuring Privacy by Functional Encryption", in *Proceedings of the 10th International Conference on Cloud Computing and Services Science - CLOSER*, 2020, p. 292–301. doi: 10.5220/0009377702920301.

[25] A. Oppermann, F. G. Toro, F. Thiel, e J.-P. Seifert, "Secure Cloud Computing: Reference Architecture for Measuring Instrument under Legal Control", *Secur. Priv.*, vol. 1, nº 3, p. 1–26, 2018, doi: 10.1002/spy2.18.

[26] B. A. Rodrigues Filho e R. F. Gonçalves, "Measuring the economic impact of metrological frauds in trade metrology using an Input-Output Model", *IFIP Adv. Inf. Commun. Technol.*, vol. 488, 2016, doi: 10.1007/978-3-319-51133-7.

[27] K. Mammadzada, M. Iqbal, F. Payman Milani, L. García-Bañuelos, e R. Matulevi ius, *Blockchain Oracles: A Framework for Blockchain-Based Applications (SLR Protocol and Results)*. University of Tartu, 2020. doi: 10.15155/re-112.

[28] J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, e A. Kastania, "Astraea: A decentralized blockchain oracle", in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, p. 1145–1152. [Online]. Disponível em: http://arxiv.org/abs/1808.00528

[29] F. Zhang, E. Cecchetti, K. Croman, A. Juels, e E. Shi, "Town Crier: An authenticated data feed for smart contracts", in *23rd ACM Conference on Computer and Communications Security, CCS 2016*, 2016, p. 270–282. doi: 10.1145/2976749.2978326.

[30] L. Ma, K. Kaneko, S. Sharma, e K. Sakurai, "Reliable decentralized oracle with mechanisms for verification and disputation", in *7th International Symposium on Computing and Networking Workshops, CANDARW 2019*, 2019, p. 346–352. doi: 10.1109/CANDARW.2019.00067.

DIGITAL TRANSFORMATION

National metrology law as a driver for digital transformation

S. Golubev, A. Kuzin
Federal Agency on Technical Regulating and Metrology (Rosstandart)

OIML-PTB WEBINAR

DIGITAL TRANSFORMATION IN LEGAL METROLOGY

5 MAY 2021

1 Introduction

The term "digital transformation" in metrology, and in particular in legal metrology, has many different interpretations. There is also no precise definition as to what the result of digital transformation should be, and who will be interested in the final product.

Nowadays nobody is surprised by the opportunity to exchange a passport or driver's license, or obtain a visa or any other state service via the Internet. Moreover, sales of goods are increasingly moving to the Internet. The share of online sales in the consumer sector has exceeded 10 % and continues to grow. All this is possible thanks to the digital infrastructure of modern society.

In the Russian Federation, digital transformation and its practical results are currently understood as a similar infrastructure that is accessible to all participants of the national system for ensuring the uniformity of measurement results [1–7].

In these terms, the current goal of digital transformation in legal metrology is to develop an infrastructure where all users and participants may perform their legal metrology tasks.

The technical component of such an infrastructure is a digital platform that operates with data on standards, measuring instruments, reference materials, and other technical objects in legal metrology.

The legal component is to ensure the legal significance of all actions performed on the digital platform, and the key issue is that for practical use, *all data on a digital platform must be coherent.*

For example, the data available for a measuring instrument is required to be automatically linked to the data of all the instruments used for its calibration, and for that these data must also exist in a digital platform.

2 Tasks

To achieve the above-mentioned goal, it is necessary to resolve **three tasks**:

1) **The first** task is the development of a technical platform, i.e. the main technical component of the planned infrastructure.
2) **The second** task is the motivation of the participants, or users of the legal metrology system, to work in the newly created infrastructure, and the National Metrology Law [8] is the best driver to do so. In the absence of a legislative driver, the transition of users to a digital platform can take several years or even a decade. The legislation allows for such a transition to take place in the shortest possible time.
3) **The third** task is to ensure the legal significance of the data stored in the digital platform. Without this, the creation of such an infrastructure and platform will only create a new inconvenience for users. There are also some examples when so-called "digitalization" merely generates a duplication of actions previously carried out in the digital environment. Of course, such bad practices should be excluded, and the motivation of users should be based not only on legal requirements, but also on their convenience.

The next step was to select the legal metrology tasks to be implemented in the new digital infrastructure. For Russia we selected nineteen tasks, of which the following are the main ones:

- verification of legally regulated measurement instruments;
- establishment of the traceability chain from the SI (or other recognized standards when they correspond) down to the end user;
- definition of type approval procedures;
- certification of reference materials.

In the Russian Federation, legal metrology is mainly based on the verification procedure of measuring instruments. Now this procedure is in many ways close to the traditional understanding of calibration. Usually, the result is not only a conclusion as to the suitability or unsuitability of the measuring instrument, but also

Figure 1 Number of standards and measuring instruments in the Russian Federation

information about its performance, e.g. the measurement errors. The transfer of SI units from level to level down to the end user is also largely implemented through a chain of verifications.

Verification is the most widespread task in the field of legal metrology in the Russian Federation. By different estimations, about 50–60 million verifications are carried out in the Russian Federation per year. The task of storing and processing such a large amount of data is very difficult, however, Rosstandart made this decision. Through the information on the verification of measuring instruments, Rosstandart receives data about all measuring instruments used in the field of legal metrology in the Russian Federation (Fig. 1, Fig. 2).

At this stage, it is also very important to estimate the required capacity of the technical platform being created. This will play a crucial role in choosing its implementation.

The platform should be capable of processing about 500 verifications from 2000 verification authorities per minute. This means that at peak performance it should be able to process several thousand verifications per minute.

Year	amount of data
2016	18 911 671
2017	23 985 401
2018	20 923 616
2019	22 201 182
2020 (introduction of the digital platform in September 2020)	44 071 968

Figure 2 Volume of verification data on the platform per year

As this data is often used for legal actions, for example in legal courts, and another important technical issue is that the legal significance of the data on the platform requires, first of all, digital signatures. In the case of verifications, this is the signature of the verification authority. Also, the information must be protected against unauthorized changes, including hacker attacks.

3 Strategy for realization

Developing a digital infrastructure consists of two parallel threads.

The first thread is the development of legislation that ensures the recognition of the digital platform, and the second thread is the development of the digital platform itself.

The legislation comprises firstly the national law on metrology, and secondly a number of other legislative and technical acts. The technical platform comprises a software product and server capacities. One very important but also very challenging task for a project leader is the coordination of these two threads.

There are three important decisions that should be taken to organize this project.

The first issue for the development process is the question of who will do it, either a specialized outsourced company or internal resources (for a national metrology body it is the NMI). If the choice is made in favor of an outsourced company, the obvious advantage of this solution is the higher professional competence of specialized organizations. Also, the direct cost of this development initially appears to be lower; however, our practice has shown that the specifics of metrology are so complex that professional organizations have not been able to deal with it for two years. In addition, although the cost of external development initially seemed smaller, in practice it soon began to grow. For example, changes in legislation require changes to the platform, which incurs a cost. Therefore, in Russia the decision was taken to use the internal capabilities of VNIIMS (one of the Russian NMIs).

The second issue was about the order of execution of the two threads. A simpler option was to first develop a technical platform, and then prepare changes to the legislation. However, in this case, the period of digital transformation would greatly increase. In addition, when developing changes to the legislation, many issues were found in practice, which once recommended by our colleagues, were incorporated into the technical platform. So, it is possible to move these two streams in parallel, and this appears to be the most reasonable way of proceeding.

Table 1 Approximate timescale of coordination of the technical platform development and the changes in legislation in the Russian Federation

Timescale	Legislation	Technical platform
2016–2017		Development by outsourced company
2017 (Mid)	First draft of a new law	
2017–2018	Discussions with professional company and experts	Use of the developed platform by Rosstandart
2018	Discussions with federal bodies and in government	Decision to continue developing by NMI
2018–2019		Customizing the platform for actual tasks
2019	Official movements	Successful integration of the platform by Rosstandart
2019-12-27	Signed by President	
2020-01-30		Deployment of the platform for all users
2020	Development of 18 documents for law realization	
2020-09-24	Came into force	Became the sole possibility to work in the legal metrology area
2020–ongoing		Improvement of the platform

The third issue concerned changes to the legislation. To ensure a softer transition to the digital infrastructure, at the first stage it is easier to allow work both using the digital infrastructure and in the old way (i.e. paper certificates, etc.). In this case, after some time, it will be necessary to re-adopt changes to the law that oblige users to work solely on a digital platform. However, in this case, the information collected through the technical platform will not be fully up-to-date. Therefore, it is harder (but from some points of view more efficient) to make it mandatory for participants to switch to a digital platform. This decision should be reflected in the national law on metrology, and in our opinion serves as a driver for digital transformation.

4 Practical realization in the Russian Federation

Table 1 shows an approximate timescale of the coordination of the technical platform development and the changes in legislation in the Russian Federation.

The technical platform development by the outsourced company was started a short time previously.

However, during the testing and implementation of the product received, the federal agency and several organizations revealed the problems mentioned above. In 2019, the technical platform was developed and successfully implemented in the Federal Agency. Shortly afterwards, the platform developed was also integrated by all the participants and stakeholders.

As practice has shown, the three-step cycle of developing technical legislation in the Russian Federation takes about three years:

- the first step in the development cycle is to work out the legislative framework with the professional community;
- the second step is agreement by the federal bodies, authorities and government;
- the third step is the official one, when the draft is officially sent to Parliament for adoption and subsequent signature by the President of the Russian Federation.

The time required for the new provisions to come into effect was 270 days. This time was initially used for the development of lower-level government and ministerial acts. It was also the last call for the stakeholders to join in via the technical platform.

The changed law came into effect on 24 September 2020. From that moment on, all the participants involved in ensuring the uniformity of measurements in legal metrology in Russia were required to work solely within the scope of the newly developed digital infrastructure.

From the moment the new law was officially adopted, paper certificates, as well as other confirmations of metrological services, were no longer sufficient, and the data collection about the technical legal metrology infrastructure was started from this moment.

The technical platform contains both password-protected and open portals. The open portal is used by

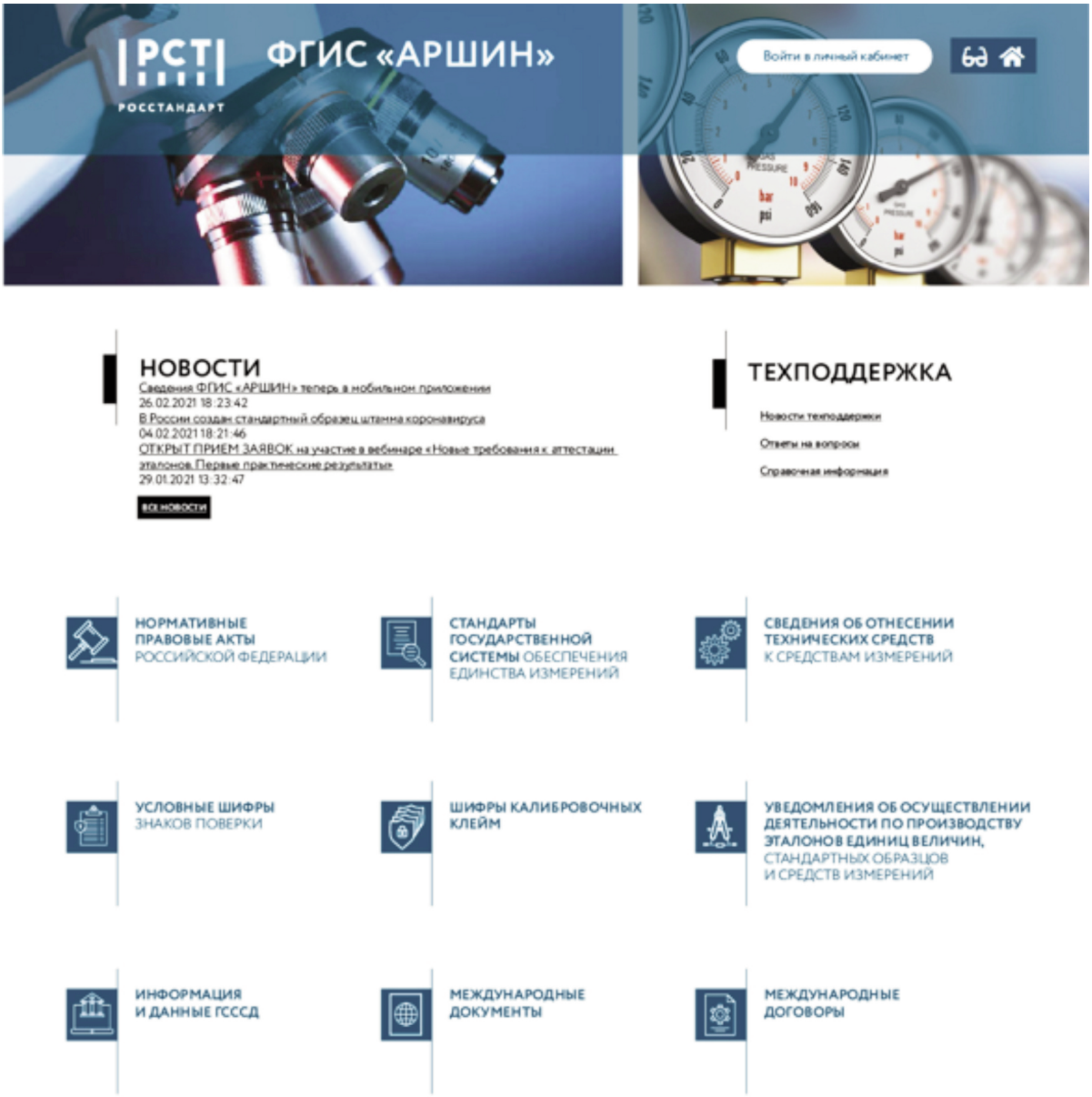


Figure 3 Main login page to the platform

the public to obtain information in the field of legal metrology in Russia (including all applicable international documents, e.g. OIML Recommendations in both the Russian and English languages). For example, it is possible check the verification of measuring instruments by their serial number and type approval index. The website address is https://fgis.gost.ru/fundmetrology/registry [9] (see Fig. 3).

In total, the technical platform has 19 modules for the same number of main tasks. Working with the system is quite convenient, as various information search facilities are available.

For large organizations that perform many metrological tasks, the mechanism of packet data transmission is implemented. This can be achieved both through files of a specific format, and through a special API of the technical platform.

The important issue is whether the system contains information about metrological tasks completed before 24 September 2020. During the preparation of the draft law, it was decided not to require the participants of the digital infrastructure to post all the information about previously performed services, which were accepted in the "old" paper format. Indeed, entering all this data into a digital platform would be a burden on the enterprises and seems to be unreasonable for them. On the other hand, Rosstandart required its organizations to enter all the information starting from 2010. This

explains why there are about 50 million verifications per year, but in total the platform contains more than 300 million verification datasets.

All the datasets on the platform are not just a volume, they are structured and coherent (or interconnected). Of course, this approach creates a large number of technical challenges. For example, there are many requests, such as "I can't send verification information, because my verification instrument or reference material or guideline is not on the technical platform". A support service for such requests was established, and all requests are processed fairly quickly.

It should be emphasized once again that at the implementation stage, a huge amount of work was done to digitize all the information concerning the verification of instruments. The key operator of the technical platform, VNIIMS, managed to accomplish this in just 270 days, which was probably the most resource-intensive action achieved by them. The success of the entire project depended, among other things, on large-scale efforts to resolve this problem.

5 Current participants of the developed infrastructure

There are four key groups of participants in new infrastructure:

- federal agency for technical regulation and metrology;
- national accreditation system;
- verification authorities;
- manufactures and users of measuring instruments.

The measuring instrument users are not only companies and authorities, but also individuals. This is a very important point, because the key objective of the law on metrology in Russia is, among other things, the protection of citizens. Now, with the help of a mobile application (Fig. 4), if desired anyone can, for example, check the verification of scales in a supermarket, fuel dispensers at gas stations, or the water meter in their house or apartment. Therefore, this project has also had an important social effect.

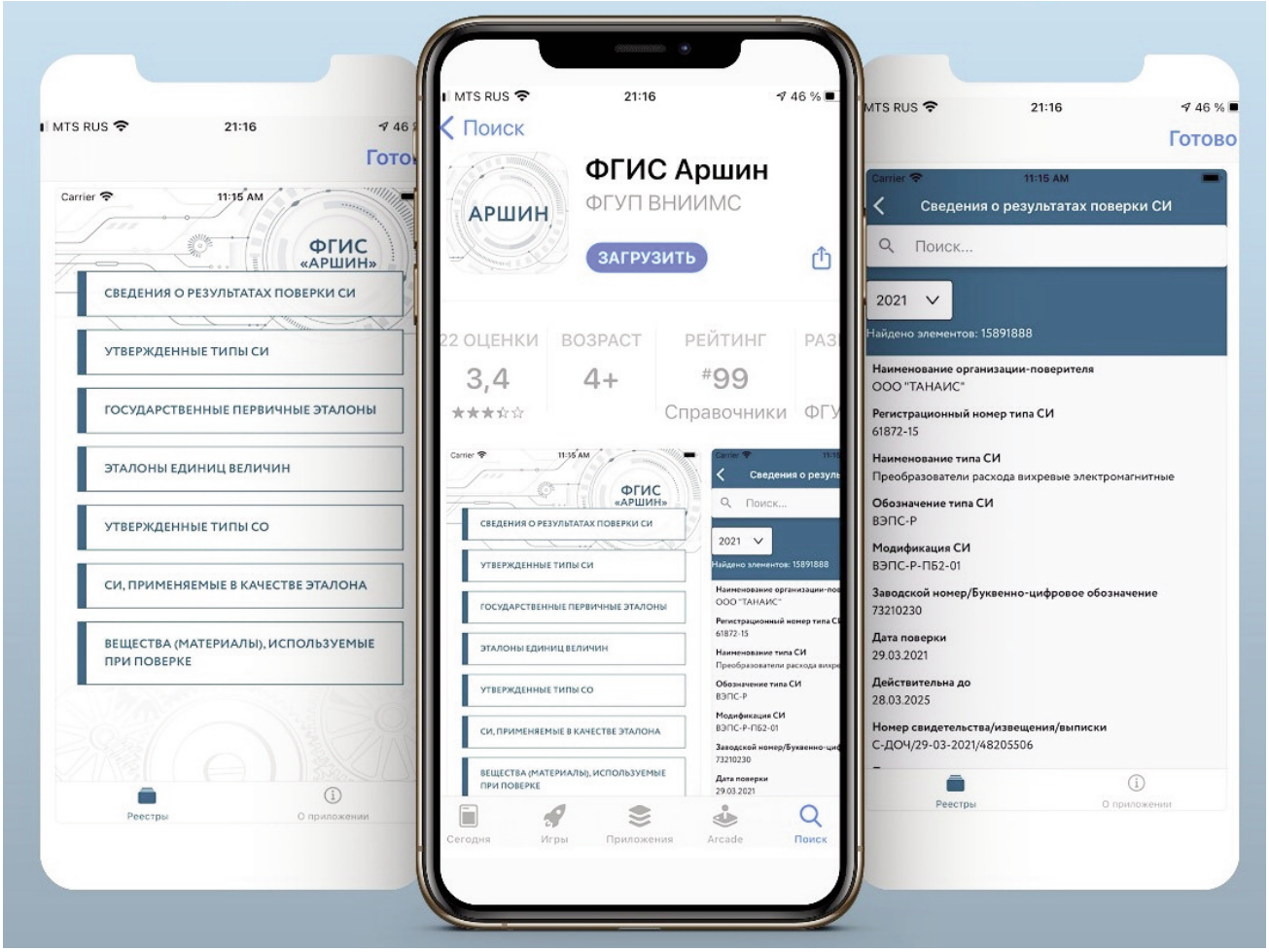


Figure 4 Mobile application for the platform

Sometimes, transformation processes meet strong resistance for execution, but perseverance and commitment to the accepted concept is the key to success. The project described here has produced important results in terms of the data obtained using the platform.

For example, it is already possible to obtain key data about the traceability of various measuring instruments to national primary standards from existing datasets. This will provide valuable input not only for legal metrology, but also for scientific metrology, and might be one of the keys for a primary standards development strategy.

Also, this data is very important for metrological supervision. Measuring instruments whose verification period has expired and for which no new verifications have been registered can easily be obtained from the platform. Targeted response measures can be applied for the organizations which own these instruments. For accreditation supervision, data about organizations performing a suspiciously large number of metrological tasks is also important. They can also focus on such cases and respond to them.

6 Practical results and conclusion

The digital infrastructure in legal metrology has many benefits for all users (legal authorities, manufactures and instrument users):

- For the national metrology body, it of course provides the most current data about the technical means used in legal metrology. It is difficult to overestimate the practical significance of these data, or when the array of data will be more or less complete (note: it is necessary to take into account the remark about the data prior to 2020).
- All traceability schemes of measuring instruments and verification tools will also be created and made available through the platform.
- An environment for risk-oriented metrological supervision, as one of the tasks of Rosstandart, will make the digitization process very efficient.
- For the verification authorities, this is an opportunity to work with the results in real time. Accordingly, this allows them to increase their customer focus. The problem of forged or fake documents in metrology also exists. Many authorities are regularly required to prove their innocence related to such fake information, but thanks to the data on the platform, this problem has now been eliminated.
- Another key benefit is that due to human error, the results of the metrological tasks sometimes have to be canceled, and this can lead to legal consequences. For the authorities, this entails a revocation of their certificates and involves extra costs for the correction of the mistakes. Now the system either does not allow such errors, or (at worst) allows them to be detected earlier.
- In addition, the system proposes automated tracking of verification periods.
- Lastly, users may analyze the market and locate the most appropriate verification authority.

S. Golubev A. Kuzin
Federal Agency on Technical Regulating and Metrology (Rosstandart)

7 References

[1] Lebedeva I.O. Changes in legislation and some updates in the verification unit of FGIS ARSHIN, Glavniy metrolog, 2021, No. 1, p.54.

[2] Krasavin I.V. Federal digital system of Rosstandart "ARSHIN". From user to developer, Mir izmereniy. No. 2, 2021, p. 10-14.

[3] Krasavin I.V. Talk "Current state in further development of the FGIS ARSHIN in digitalization context", All-Russian conference "Metrology in the service of quality", https://www.youtube.com/watch?v=Qb5-yxpi3IY.

[4] Lebedeva I.O. Federal law #496: how will the changes affect the input of verification data in the FGIS "ARSHIN", Glavniy metrolog, 2020, No. 5, p.74.

[5] Krasavin I.V., Piliugin A. Ju. The FGIS "ARSHIN" as a driver of digital transformation to ensure the uniformity of measurements, Glavniy metrolog 2020, No. 4, p.15.

[6] Lebedeva I.O. The FGIS "ARSHIN": how does the upgraded module "Verifications" works, Glavniy metrolog, 2020, No. 4, p.96.

[7] Androshuk Ju.M., Pashaev B.M., Kozmina E.V. Standards, verification schemes, the FGIS "ARSHIN" and their joint use, Glavniy metrolog, 2020, No. 3, p.66.

[8] The law on ensuring the uniformity of measurements, Russian Federation. http://www.consultant.ru/document/cons_doc_LAW_77904/

[9] Internet homepage https://fgis.gost.ru/fundmetrology/registry

DIGITAL TRANSFORMATION

Evolution of the European Metrology Cloud

Jan Nordholz, Maximilian Dohlus, Jasper Gräflich, Alexander Kammeyer, Martin Nischwitz, Jan Wetzlich, Artem Yurchenko, Florian Thiel

Physikalisch Technische Bundesanstalt (PTB), Germany

OIML-PTB WEBINAR

DIGITAL TRANSFORMATION IN LEGAL METROLOGY

5 MAY 2021

Abstract

Legal metrology regulations define the processes in the lifecycle of metrological instruments such as conformity assessment of new device series, verification of devices in the field, and updates to device software. The European Metrology Cloud (EMC) is an initiative by the Physikalisch-Technische Bundesanstalt (PTB) to build a platform for the digitization of existing and future processes. It provides stakeholders in legal metrology with a single point of contact to interact seamlessly, to initiate new processes using their own databases, and to reintegrate the resulting data or certificates. As the EMC has now been in development for three years and its base functionality is ready for testing on a larger scale, we present its overall architecture and key aspects of its security design, we describe how to join the network, and we showcase the opportunities of the growing platform.

Introduction

The purpose of legal metrology is to ensure correctness of measurements "in the field" by establishing a chain of trust among many different stakeholders: from the manufacturer of a device to its user, from the NMI to the market surveillance, following regulatory frameworks such as those published by WELMEC for the European market. By design, these regulatory systems require a lot of data collection, data exchange and communication between stakeholders within regulated processes.

Until now, data has been exchanged using a plethora of channels, even in the course of a single process, such as sending paper forms and USB thumb drives by mail, emailing attachments, and uploading data to file hosting services. Yet, even in cases where data is exchanged in digital form, the transport is often insecure and missing machine-readable metadata that would be needed for more automated process handling. While there are instances of more modern systems, e.g. the DEMOL system of the German market surveillance agencies used to apply for reverification of measuring devices, those services are in no way unified. While each of these solutions provides a step up from solely paper-based applications, their heterogeneity implies that each stakeholder would have to implement a large number of interfaces in order to be able to interact with all these services. The growing number of such localized digitization efforts makes it infeasible for stakeholders to incorporate and maintain all these services within their own ecosystems. In order to resolve these issues, a unified data platform is needed that can encompass all related data and allow for seamless data transfers and process execution while still maintaining compliance with regulatory demands on the one hand as well as data security and privacy of the participants on the other.

The European Metrology Cloud (EMC) is the vision of the PTB to create a common digital platform where all stakeholders can seamlessly interact, share data and engage in legal metrology processes. Its initial conception [1] and important technical decisions [2] have been described in previous issues of the OIML Bulletin. At its core, the EMC is designed as a distributed cloud where each participating stakeholder owns and runs one server installed with a common software stack, an "EMC node". Each of these nodes acts as a gateway for its respective stakeholder to start new or react to existing legal metrology processes and to exchange data with other stakeholders. The development of this software stack and the realization of exemplary legal metrology processes on top of this infrastructure has been the main focus of the EMC project. Obviously, the data shared among stakeholders for certain types of processes – such as the type examination for a new device series – is highly confidential, so maintaining high security and privacy standards is a vital aspect of the overall design.

After three years of development, the core system architecture of the EMC node is now ready for deployment and the first sample processes have been transformed into digital form. The EMC provides a number of unique features ensuring security and data sovereignty to all its participants:

- a decentralized blockchain based PKI, providing secure identities for all stakeholders (see Section II / Identities);
- a decentralized, encrypted logging system, also based on blockchain technology;
- secure authentication encompassing the whole EMC system using a specialized security dongle, currently under development (see Section II / Authentication);
- fine-grained data access policies specified by each node-owner individually;
- a simple (i.e. human readable) language for smart-contracts generation to mimic the previously analog-based legal procedures in the digital realm;
- a way for stakeholders to introduce additional services related to measuring devices; and
- a harmonized data-schema to minimize data transformations and to ensure data consistency throughout the EMC network.

In the following sections we present our platform, discuss its merits, and identify those areas where more work is needed. We invite more stakeholders to join our nascent network and collaborate in its further development. In Section I, we describe the network topology of EMC, how processes are started and advanced, and how queries and responses travel through the network. In Section II, we provide an overview of our security mechanisms and how privacy of past and ongoing processes is maintained. Section III explains how data can be exchanged between the existing stakeholder databases and the EMC network. In Section IV, we identify opportunities how the EMC could be connected to or made compatible with other service infrastructures, and describe possible extensions of the concept to other applications beyond legal metrology. Finally, we present the future direction of the project and invite interested parties to join the EMC test network in Section V.

I. Network

Today, the term "cloud" often evokes the mental image of large centralized server farms that are provided to customers in the form of IaaS (infrastructure as a service) or even SaaS (software as a service) to run their software, as is the case with Amazon EC2 or Microsoft Azure. In case of the EMC, this image of a cloud could not be further from the truth. The EMC was explicitly designed as a fully decentralized network, comprising a set of equal nodes, each located at a participating stakeholder (see Figure 1). Each node is integrated into its stakeholder's institutional network, so data can be easily transferred between the stakeholder's existing databases and their local EMC node. Communication among EMC nodes is performed over encrypted connections built on top of the modern, low-overhead WireGuard VPN technology.[1] The combined EMC nodes thus form a closed network. These design decisions have two key advantages:

- No honeypot: There is no central data storage or "master controller" that could attract malicious activity. The data is dispersed over all nodes, and additionally needs only to be stored as long as the corresponding process is incomplete (we explore this aspect further in Section II);
- Tightly controlled accessibility: Each stakeholder interacts with the EMC—including the upload and download of data – only through their own node, which is accessible via the node's own minimal web interface or the stakeholder's integrated user interface solution (see Section IV). In either case, all requests to the EMC are protected by a flexible authentication concept (see "Authentication" in Section II). EMC nodes communicate with each other only through encrypted and integrity-protected channels, which reduces the threat of an external attacker breaking into these connections to almost zero.

The data in the EMC is organized as a relational database (for a discussion of its structure, see Section III). The central concept is the "digital representation" of individual measuring instruments and of instrument types. Using this digital representation, stakeholders can modify the data or start different processes, depending on their role: a device manufacturer could upload updated documentation (such as a user manual), a device owner could start a process to roll out an available firmware update to all applicable devices, and a conformity assessment body could issue a certificate and attach it to the instrument type it pertains to.

For all these activities, the common root of trust of the EMC network is a set of distributed ledgers (often called "blockchains") that are shared by all nodes. These ledgers are used to record changes to the network itself, such as the addition of a new node or the creation or removal of user identities at one of the nodes, as well as

1 Therefore, the EMC node is usually a part of the institution's outward-facing server systems and as such is commonly placed in a "Demilitarized Zone" (DMZ).

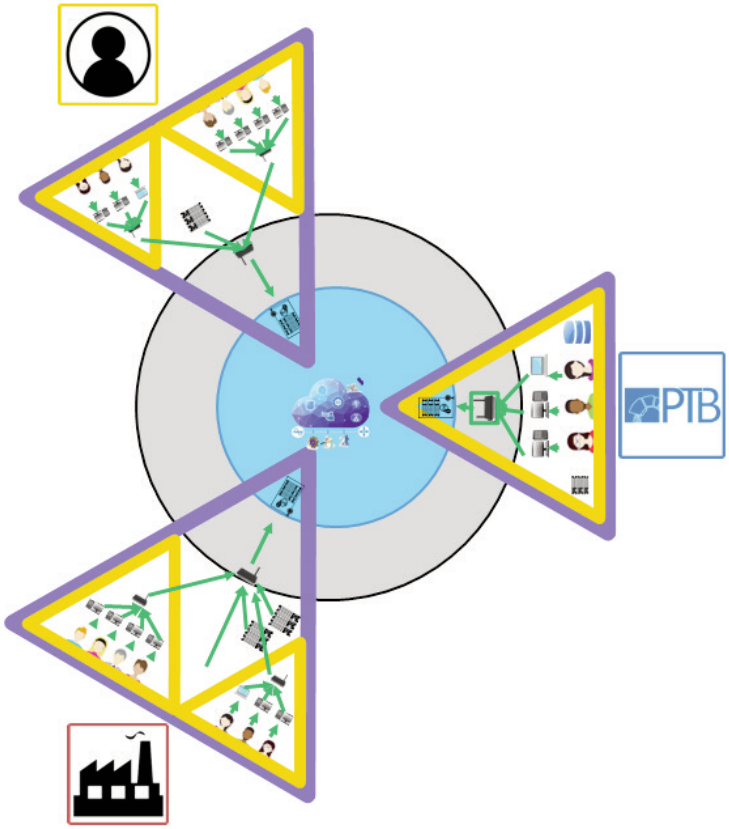


Figure 1: Visualization of the EMC network. Stakeholder networks (violet triangles), themselves possibly consisting of several subnetworks (yellow triangles), are connected with each other to form the EMC network (inner, blue circle) with an EMC node acting as a gateway for each stakeholder.

the advancement of legal metrology processes. They thus play a pivotal role in maintaining security and privacy of the whole system, which we investigate in Section II.

II. Security and privacy

The EMC needs to be secure against fraud and theft of intellectual property. For this, the system contains various protective measures which can be used by the stakeholders and dynamically scaled according to their own security requirements. Every node maintains a separate database and has complete sovereignty over its data. A stakeholder can decide freely which data sets and documents to upload to the EMC node, who should have access to these pieces of information, and when to remove them again from the EMC.

In contrast to other ledger-based networks such as Ethereum and the global cryptocurrency Bitcoin, where anybody can participate in the network and obtain a copy of the ledger, the EMC network is a "permissioned" network where the participating institutions know each other and adding a new member is not an arbitrary event. Instead, the action of joining a new node into the EMC network must be confirmed by a consensus among all existing participants. This consensus is then recorded in the distributed ledger, which is also used to store the cryptographic identity of the new node, thus adding the node to the set of participants. For the synchronization of the ledger among all nodes, the EMC uses the "Raft" algorithm [3]. Once a node has learned from the ledger that the consensus for joining the new node is complete, it will establish VPN connectivity with the new node and include it in further network queries, ledger updates and process notifications.

As already elaborated in the previous section, attacks on these encrypted node-to-node network connections are very unlikely to succeed. The only connections that a node responds to are from authenticated users, registered measuring instruments and integrated service components (see Section IV) – all of these are strongly authenticated and protected by a transport encryption layer. In addition, stakeholders whose EMC activity is entirely performed on site could limit the valid origins for these connections to their internal network, thus completely eliminating network-based attack vectors towards their node.

Identities

As all actions in the EMC have potential legal impact, all requests and all records stored into the distributed ledgers have to be cryptographically signed. A signature identifies the signed data as having originated from the person in possession of the cryptographic key that was used for the signature. The framework to support this scheme, including the mapping from keys to identities and identities to organizational structures, is called a "Public Key Infrastructure" (PKI) and is usually realized as a tree-like hierarchy with a universally-trusted entity acting as the root of trust. As the EMC network is inherently without such a leader, the PKI of the EMC is instead realized as a federation, where each node maintains and publishes its own tree of identities and corresponding keys. If a stakeholder prefers, the identities on such a tree could even be pseudonyms, as long as the stakeholder is able to reconstruct the real persons that participated in a process under such a pseudonymous identity in case of a legal dispute. Just like modifications to the set of nodes, additions and removals of identities are published throughout the EMC network through the distributed ledger.

Privacy

While each stakeholder has sovereignty over their node and the data they upload to it, the EMC as a distributed system records all identities and processes (realized as so-called "smart contracts") on a blockchain. The blockchain is implemented in a flat hierarchy, i.e. all nodes in the network take part in the "Raft" distribution algorithm and are therefore able to read the (meta-)data of each block. This is vital for the distribution of changes to the network and the set of identities (see Section I above), yet the storage of process advancement requires special treatment.

The actual data files that a stakeholder supplies to a running process (such as source code, documentation, firmware packages, etc.) are only referenced by a cryptographic checksum and not themselves stored in the ledger; however, the ledger contains metadata (e.g. the type of process, the ID of the measurement device type involved, etc.) for all processes that have taken place or are currently ongoing in the system. Hiding these pieces of information from other participating stakeholders, most importantly from competitors, is highly desirable.

To this end, ledger blocks which contain process metadata are encrypted using a "threshold encryption" scheme [4]. Each time a smart contract is initiated, all participating stakeholders perform a distributed key generation algorithm resulting in a shared public key and unique secret key shares for each stakeholder. If the threshold of stakeholders specified during the key generation algorithm collaborate, they can sign and encrypt data as a group. With threshold signatures, it is no longer possible to trace the individual identities of the signers, yet it is ensured that enough stakeholders have agreed to the execution of the smart contract and thus to the advancement of a particular process to its next stage.

Authentication

Many scientific studies [9,10,11] show that even a secure network can be compromised by employee inattention. The damage is often proportional to the employee's position in the company. Such mistakes often happen without malicious intent, but because of insufficient security awareness. As a result, the employee's digital identity could be abused. While we can confirm our identity in the real world using various physical methods, our digital identity is often protected merely by a combination of a username and a password. The disadvantage of a password is that it can be copied using a variety of ways, e.g. tricking the user into entering it into a crafted web page ("phishing"), monitoring the keystrokes using a malicious program (a "trojan"), or even simply watching them type.

For this reason, two-factor authentication was introduced, which requires a second form of authentication. Often, this is realized as proving that the user is in *possession* of something (such as a mobile phone which they use to receive a TAN via SMS) in addition to the *secret knowledge* they have (the password). The use of a second factor makes identity theft much more difficult (but not impossible, since the device used for the *possession* factor can also be stolen). Therefore, settings with even higher stakes make use of *inherent properties* of the authenticating user, i.e. biometrics such as a fingerprint, iris images or the palm vein structure. Nowadays, support for biometric authentication is already available in a wide range of smartphones.

In order to protect the cryptographic keys that represent the user in the federated PKI with this multitude of authentication factors, the EMC endorses the use of so-called "key dongles". These dongles are small USB devices built to protect the set of stored cryptographic keys from unauthorized use: when the system asks the dongle to generate a cryptographic signature, the dongle will in turn ask the user to confirm the action by presenting the necessary factors, which – depending on the physical size and the complexity of the device – might be a simple button press, entering a PIN, or using a fingerprint scanner [5]. The integration of such dongles into web-based authentication schemes has been made comparatively easy through the development of the FIDO2 protocols, which have been accepted as a standard by the W3C [6].

But even with all these authentication factors in place and with the cryptographic keys stored in a dedicated dongle, the threat remains that an attacker could infiltrate the user's workstation. A determined attacker could maliciously modify the browser so that it displays the intended EMC operation to the user, but submits a different operation to the dongle for the signature and submission to the network. Although such attacks are very difficult, they are not impossible. A possible solution could be to display the operation on the dongle before authorization, similar to how smartphone banking apps ask the user to check the details of a wire transfer as part of the confirmation process.

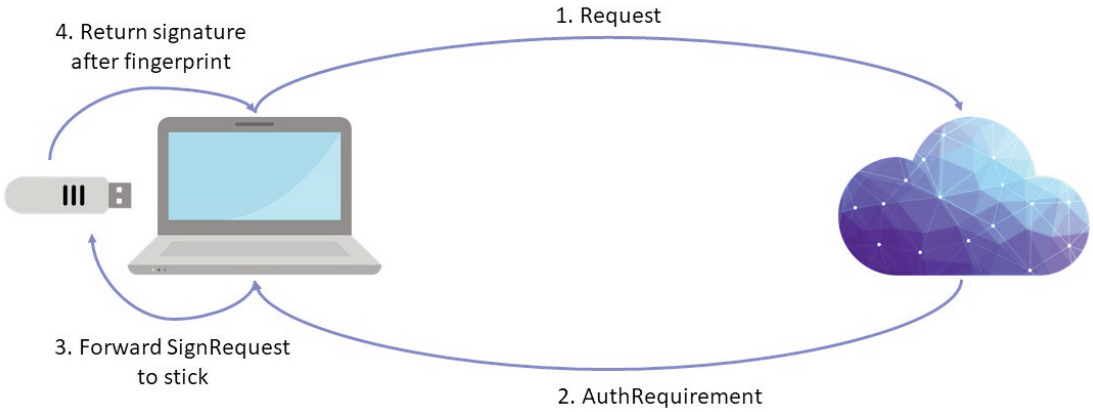


Figure 2: Sample EMC request involving the proposed key dongle. After a user requests a certain resource from the EMC network (1), the node that owns the requested resource replies with the level of user authentication (i.e. the set of factors) required to access this resource (2). The browser on the user's device forwards the set of factors to the dongle (3), which asks the user to confirm the request and provide the necessary factors. After the user has confirmed the request, the dongle uses its stored cryptographic key to sign the request (4). The request is now complete and can be resent to the remote node, which will check the signature against the user's key stored in the EMC PKI and respond with the desired resource.

Often, use-cases for secure authentication of processes may vary greatly in the scope of their required level of security. Additionally, users of such a system might be less willing to accept complex or time-consuming authentication processes especially for tasks performed many times a day. As such, there is no simple, all-encompassing answer to the question of how much security is actually necessary for performing actions in the EMC network. The answer will depend on the kind of action, but it will also most likely be different for different stakeholders. To mitigate this issue, the EMC will offer a dynamic security level, that allows (within certain guidelines) to assign different levels of authentication security to different actions within the EMC. Mostly, this is done by varying the number or type of requested authentication-factors. Another aspect is that in most shared data-systems, each participant has to trust in the effectiveness of all other participant internal identity management and authentication policies. One key feature of the EMC is that the required level of security for access to their data must be specified by each organization individually but will affect every user trying to access their data instead of being limited to the internal identity management. Under this assumption we see our task in providing the possibility to demand the highest level of security, but also support other levels which might increase the overall usability.

We believe that a dongle with support for various, individually requestable authentication factors and equipped with a display would fit these demands perfectly. Depending on the action, the data items and the stakeholders involved, the EMC network could request a different level of user confirmation, ranging from a simple button press (e.g. when requesting the status of an ongoing process) to a combination of several strong factors (e.g. when starting a new type examination process). As such a device is not available on the market, the PTB has created a spinoff project with the company Nitrokey, a German specialist in the field of two-factor authentication solutions, in order to jointly develop such a flexible key dongle. This development will not exclude other options, but is meant to showcase the ideal combination of a strong, but flexible and highly usable authentication solution.

III. Data integration

One of the main problems when trying to share data between different stakeholders is that data can only be interpreted if sufficient metadata is provided. For example, the value *9.81* is meaningless unless its context

and physical units (SI units) are provided as well, i.e. meter per second squared (m/s^2) for gravitational pull or cubic meters per second (m^3/s) for flowrate. Similarly, a given date such as *June 6, 2021* could refer to the last time a measuring device has been checked by market surveillance or to the end of the current calibration period.

From these examples, it is obvious that data without context is meaningless. Each stakeholder stores their data in a format (in database terms: schema) individual to that stakeholder and its internal usage, meaning these schemata are tailored to the individual needs of a given stakeholder. This can make it hard to exchange data because for each data transfer between two stakeholders, the data would need to be transformed from the sender's to the receiver's schema.

While data integration research suggests a number of solutions to this issue, none of these is precise and efficient enough to be applied in the context of legal metrology or would require extensive human interaction. Additionally, this work of matching schemata would have to be performed for each and every pair of stakeholders, which would grow quadratic in the number of stakeholders. Given the potentially high amount of work necessary for each individual schema-matching task and the potential number of stakeholders that are active in legal metrology in Europe, this approach is infeasible.

To mitigate this issue, the EMC defines a unified schema that defines a standard representation and structure for those (and only those) data fields that are necessary for the execution of legal metrology and related processes. With this approach, each stakeholder only has to develop a single schema translation: from their own individual data representation to the common "unified" one specified by the EMC. This unified schema directly induces a generalized taxonomy of values and terms within the realm of legal metrology and uses the standardized notation of the "digital SI" (D-SI, [7]) for the handling of physical units.

The further development of this unified schema is envisioned as a community process among the stakeholders involved in the EMC: the PTB offers a schema definition wiki[2] that allows for multi-party harmonization based on an integrated voting system. Within that unified schema, a unique name is provided to all data attributes as well as a unified data structure that encompasses and connects these items.

Another aspect of shared data-systems such as the EMC is to ensure data integrity. Going back to the original example, it may be that the mentioned value of 9.81 is stored redundantly at multiple locations. That means, if one instance of that value is changed, say to 9.82, these datapoints are now in an inconsistent state as they still refer to the same object. To avoid the negative effect a loss in data integrity might have on how processes can be performed on that data (e.g. a measurement might have to be repeated using a different parameter), the EMC provides an automated way to detect and repair data errors of this type.

IV. Interconnectivity

The EMC was designed with accessibility and interoperability in mind. Different methods exist for users, measuring devices and services to connect to and interact with the EMC. We will now visit each of these categories step by step.

The core services of an EMC node, such as the local data storage or the ledger subsystem, are accessible via a REST API which expects and returns JSON objects. These are standard methods used in many web services today. The node also offers a minimal web-based user interface which allows users interactive access to most API functions. However, we acknowledge that most stakeholders already have their existing in-house user interface that allows efficient navigation of their custom database. Stakeholders are therefore free to integrate the functionality of the EMC node as exported by its REST API into their own user interface: this way, interaction with processes in the EMC can be integrated much more tightly into existing workflows and disruption for employees is as small as possible.

As smart measuring devices with direct network connectivity become more and more common, the EMC also supports direct data exchange with these devices. To this end, the EMC offers a special device interface that can be used to couple such measuring devices with the EMC. This interface supports the OPC-UA protocol [8] or regular REST/JSON queries and allows the EMC to query and update certain device information such as conformity assessment data, and to push firmware updates to the device. Like many other aspects, this interface is not designed to replace or exclude other (possibly proprietary) protocols – in fact, many legacy devices do not offer such connectivity at all, and even those that do might only support much simpler protocols. In the case of these simpler protocols, stakeholders are free to implement a "connector" service that translates between the EMC and the measuring device.

In a very similar fashion, the EMC node also supports connecting to existing stakeholder services and

2 https://wiki.metrologycloud.eu/doku.php?id=start; see also the main page of the EMC: https://metrologycloud.eu

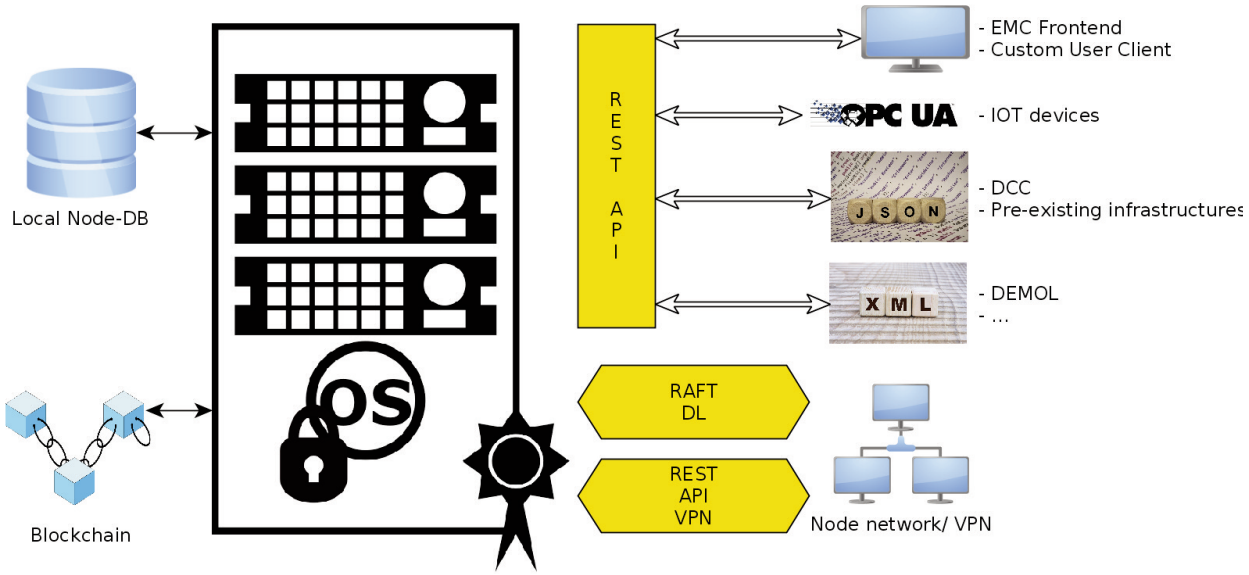


Figure 3: Visualization of connections to and from an EMC node. The "Raft" distributed ledger synchronization protocol uses its own protocol; all other components interact with the node using REST-style API calls.

infrastructures as an automated processing step. One notable example of this is the "DEMOL" web service of the German market surveillance organizations, which enables device owners to digitally request a reverification. This obviates the need for market surveillance agents to manually transform the incoming EMC process for a device reverification into their own workflow. Instead, the EMC directly performs the callout to DEMOL through a corresponding tailor-made "service connector" component.

Beyond legal metrology

The Digital Calibration Certificate (DCC) is a standard developed at the PTB for the digital and machine-readable representation of a calibration certificate, including a cryptographic signature to prove its authenticity. In a first step towards supporting applications beyond legal metrology, the digital representation of measuring instruments in the EMC has been extended to also allow users to upload a DCC. As it is very easy to check the structural integrity of a DCC and to extract individual pieces of information, it becomes possible to build derivative workflows, e.g. where the uncertainty ranges of all measuring instruments that are being used for a new measurement or calibration are automatically extracted from the EMC for inclusion in a new certificate.

Likewise, the Digital Certificate of Conformity (DCoC) is a planned specification for the digital representation of the CoC, again with a digital signature for authenticity verification. As soon as the specification is complete, we will add support for the integration of DCoC elements in the digital representation as well.

Finally, the architecture of the EMC has several striking similarities to GAIA-X, the European initiative to develop a generic European cloud service and data infrastructure. Like GAIA-X, the EMC was designed with security, federation and data sovereignty in mind. While GAIA-X is currently under development and in an early design phase, the EMC will eventually be extended to cooperate with services in the GAIA-X ecosystem. The exact form of interaction will not only depend on the details of the technical realization of the GAIA-X specifications, but also on the desire of the stakeholders in legal metrology to exchange data between the "walled garden" EMC and the more open, unrestricted GAIA-X environment.

V. Conclusion

The European Metrology Cloud has now reached a stage where the basic feature set is complete. The focus will in the future no longer lie in the development of the architecture, but in the creation of digital representations ("smart contracts") for more processes in legal metrology and in the integration of more stakeholders with their databases, infrastructures and existing digital services. The PTB has created the technological foundation, but the further steps cannot be performed by the PTB alone; in order to bring the EMC into productive use, input from stakeholders across the legal

metrology ecosystem is required. In parallel, the PTB group will continue its work towards compatibility with the upcoming GAIA-X standards and with new generations of smart and distributed measuring instruments.

The architecture of the EMC node has been developed as a group of modular microservices, which are perfectly suitable for reuse in other cases where similar requirements exist. The extension of the EMC towards other aspects of metrology already demonstrates how easily adaptable the system is.

We invite all interested parties who would like to learn more or to set up a node to contact us. We will gladly provide more information on the node API and how to integrate the node into the stakeholder infrastructure. ■

Bibliography

[1] F. Thiel, "*Digital transformation of legal metrology - the European Metrology Cloud*", OIML Bulletin, vol. LIX, January 2018, pp. 10-21

[2] M. Dohlus, M. Nischwitz, A. Yurchenko, R. Meyer, J. Wetzlich, F. Thiel, "*Designing the European Metrology Cloud*", OIML Bulletin, vol. LXI, April 2020, pp. 8-17

[3] D. Ongaro, J. Ousterhout, "*In search of an understandable consensus algorithm*", 2014 USENIX Annual Technical Conference

[4] L. T. Brandão, M. Davidson, A. Vassilev, "*NIST Roadmap Toward Criteria for Threshold Schemes for Cryptographic Primitives*", NIST Internal or Interagency Report (NISTIR) 8214A, National Institute of Standards and Technology, 2020

[5] C. Harrell, "*Getting a biometric security key right*", Yubico Company Blog, November 2020, https://www.yubico.com/blog/getting-a-biometric-security-key-right/

[6] The FIDO Alliance, "FIDO2: Moving the World Beyond Passwords", https://fidoalliance.org/fido2/

[7] D. Hutzschenreuter, F. Härtig, W. Heeren, T. Wiedenhöfer, A. Forbes, C. Brown et al., "*SmartCom Digital System of Units (D-SI)*", DOI 10.5281/zenodo.3816686

[8] OPC Foundation, "OPC Unified Architecture", https://opcfoundation.org/about/opc-technologies/opc-ua/

[9] K. Hughes-Lartey, M. Li, F. E. Botchey, Z. Qin, "Human factor, a critical weak point in the information security of an organization's Internet of things", Heliyon Journal, Volume 7 Issue 3, 2021

[10] S. L. Pfleeger, M. A. Sasse, A. Furnham, "From Weakest Link to Security Hero: Transforming Staff Security Behavior", Journal of Homeland Security Emergency Management, Volume 11 Issue 4, 2014, pp. 489-510

[11] N. Sebescen, J. Vitak, "Securing the human: Employee security vulnerability risk in organizational settings", Journal of the Association of Information Science and Technology, Volume 68 Issue 9, 2017, pp. 2237-2247

To contact the Authors

Jan Nordholz
Physikalisch Technische Bundesanstalt (PTB)
Abbestr. 2-12, 10587 Berlin, Germany
Email: jan.nordholz@ptb.de

Maximilian Dohlus .....maximilian.dohlus@ptb.de
Jasper Gräflich.....jasper.graeflich@ptb.de
Alexander Kammeyer .....alexander.kammeyer@ptb.de
Martin Nischwitz .....martin.nischwitz@ptb.de
Jan Wetzlich.....jan.wetzlich@ptb.de
Artem Yurchenko.....artem.yurchenko@ptb.de
Florian Thiel.....florian.thiel@ptb.de

Physikalisch Technische Bundesanstalt

DIGITAL TRANSFORMATION

The future of metrology – digitalization of metrology in METAS

Dr.-Ing. Federico Grasso Toro
METAS, Switzerland

Abstract

Since the redefinition of the SI in May 2019, the metrology community has started defining how metrology will evolve during the current century. Significant updates of existing metrological services and metrological services required by the digital age can be conceived under the term "digital" metrology. How will digitalization affect current and future metrological services? This article tries to clarify terms and organize ideas to identify a clearer path for the evolution of metrology.

Introduction

During the last few years, the term "digitalization" has been associated with innovation, but it has also been associated with tasks that are not at all the intention underneath. Since the terms are still confusing for most people, here are a few key terms to keep in mind:

Digitization: "…the representation of an object, image, sound, document or signal (usually an analog signal) by generating a series of numbers that describe a discrete set of its points or samples…"

Digitalization: "the use of digital technologies to change a business model and provide new revenue and value-producing opportunities; it is the process of moving to a digital business."

Digital transformation: "The total and overall effect of digitalization."

A simple example: from maps to Google Maps

The creation, evolution and ongoing deployment of the mobile phone tool known as Google Maps disrupted the map industry. While paper maps still exist, the new options and features included in the dynamic and real-time updated maps in our pockets provide users new services that old analog map-manufacturers cannot provide. To scan an analog map into a digital file would be only to "digitize" it. Nevertheless, to create a tool as powerful as Google Maps, with its multi-layer on-line services mean to "digitalize" a map.

Digitalization of metrology

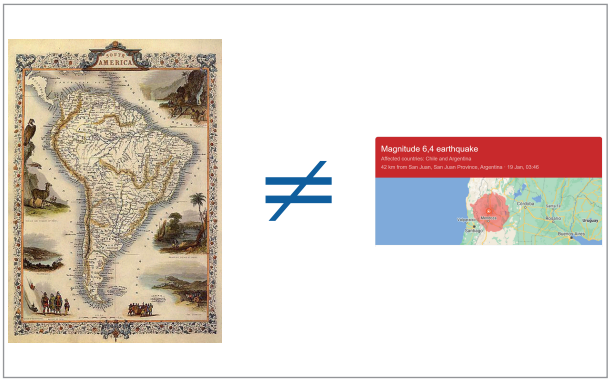
To make METAS a leading actor in the future of digital metrology, it is our duty to proactively create, evolve and apply new approaches, new tools and new services. All current efforts to digitize work in METAS, towards paperless and mostly digitally recorded information, has much more to do with "Technology and Operation" in METAS, while the digitalization of metrology has more to do with innovative research and development opportunities in METAS laboratories.

Current trends

Now that we know what the digitalization of metrology may entail, we can focus on current digital trends, but most importantly on trends that are the most significant and pressing for the future of metrology. The worldwide metrology market is estimated to reach, thanks to these digitalization efforts, $ 14 Billion by 2027.

Innovative efforts and their pressing metrological needs:

Digital industry: an interesting example from the Joint Audit Cooperation (JAC) is the "sustainable factory" concept, including modules for self-recycling and auto-efficient systems within industrial lines, requiring "digital thread" for traceability purposes and new types of certification for industrial modules including industrial internet of things (IIoT).



A scanned map (digitized) does not have Google Map features or dynamic information (digitalized)

Smart City requires new metrologies, such as measuring sensor networks metrology and Urban Metabolism Metrology (© Smart City Verein Bern)

Smart City: a Bosch and Intel concept for smart cities includes 24/7 real-time monitoring systems with air quality alerts for specific city sectors. These new modular sensor networks will require "digital trust" for their collected data, as well as new methods to certify said modules. Ongoing research aims to establish a new metrology called "urban metabolism metrology", converging metrological and legal metrology requirements.

Digital Identification: based on pattern recognition technologies from fingerprint, gait and other person-identifiers, a new emerging metrology sometimes called "human metrology" will require traceability of results and verification of processes related to person recognition.

Trustworthy AI: new methods to verify data quality will be required to achieve reasonable and trustworthy data-driven decisions from innovative systems aided by artificial intelligence (AI) and machine learning (ML) techniques, also described as "AI metrology".

Digitalization of metrology and the metrology of digitalization

While other institutes of metrology are trying to catch up with these digital trends, here in METAS we are aiming to prepare ourselves before the innovation storm to come, dividing on-going trends into two clear sets of research and development opportunities: The digitalization of metrology and the metrology of digitalization.

Digitalization of Metrology in METAS

Data science approaches, including big data, artificial intelligence, machine learning, will allow new innovative measuring systems. Existing regulations and guidelines are being updated to establish clear procedures to streamline innovation, allowing the creation of additional value for "digital" metrological services.

This first set of research and development opportunities entails:

- the inclusion of features such as integrity, availability and quality of measurement data from sensor networks;
- the digitalization of calibration data, reports and certificates; and
- the establishing of data governance policies, towards improving internal traceability and complying with FAIR (Findable, Accessible, Interoperable and Reusable) principles for Open Science.

METAS is currently working in collaboration with other NMIs to develop, test and deploy these new tools required by the digitalization of current metrological services (e.g. Digital Calibration Certificates, KCDB-API).

Metrology of Digitalization in METAS

By including metrology approaches to all new digital trends and technologies, the future institutes of "digital" metrology will ensure the placing on the market of innovative measuring systems, as one of the main actors in the Quality Infrastructure updated process.

This second set of research and development opportunities entails:

- Data science techniques for quantitative imaging, reliability of AI algorithms;
- Simulation and virtual measurement devices (e.g. digital models, digital shadows and digital twins);
- Certification and calibration of Industry 4.0.

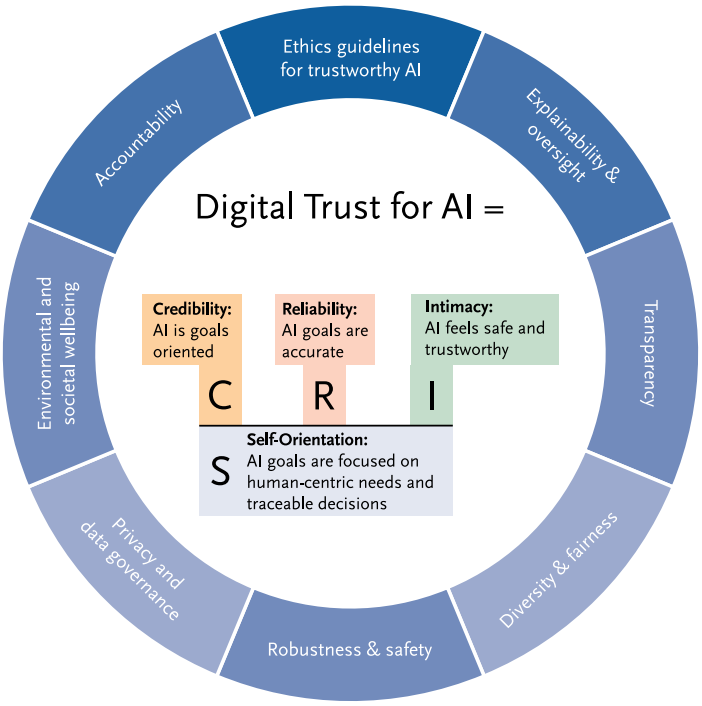
METAS is currently establishing national and international collaborative efforts, bringing our competences to EURAMET TC-IM working group "Metrology for Digital Transformation" (WG M4D).

Digitalization in METAS

This article is the first of a series of METInfo articles that will introduce the ongoing evolution of metrology in METAS.

Topics in follow up articles will include:

- Interdisciplinary framework of METAS Laboratories for in-novation in research and development;
- Update Metrological Services by/with digital technologies;
- New METAS Data Governance Policy, towards better data-driven decision making in METAS; and
- Potential Research Topics for Digital Services for innovative/complex systems in METAS laboratories.



Metrology of Digitalization – Digital trust for AI: A new interesting opportunity is using metrological approaches towards developing trustworthy AI

Contact:

Dr.-Ing. Federico Grasso Toro

Scientist research and development
federico.grasso@metas.ch
+41 58 387 02 94

FUEL DISPENSERS

New generation of system for the metrological control of fuel dispensers

Jaromír Markovič[1], Jozef Živčák[2], Milan Sága[3], Tomáš Kliment[1], Štefan Král[1]

[1] Slovak Legal Metrology, Hviezdoslavova, 31, 97401, Banská Bystrica, Slovakia

[2] Faculty of Mechanical Engineering, Technical University of Košice, Letná 9/B, 042 00 Košice, Slovakia

[3] Faculty of Mechanical Engineering, University of Žilina, Univerzitná 8215/1, 010 26 Žilina, Slovakia

Abstract

This article presents the new generation of the system for the metrological control of fuel dispensers. The new system is the result of research and development and subsequent practical implementation in the Slovak Legal Metrology Institute. The new generation of the system uses a high degree of automation, intelligent image processing, elements of artificial intelligence, and the application of innovative construction materials. The system enables metrological control of a wide range of measuring systems with a focus on the credibility and reliability of measurement results, measurement accuracy, and reducing the dispensers' shutdown time during their metrological control. The added value is the ease use of the system and the short training time needed for metrological staff to use it.

1 Introduction

Fuel dispensers that are used to measure the volume of liquids sold at fuel stations are included in the category of measuring systems for the continuous and dynamic measurement of quantities of liquids other than water. The metrological and technical requirements applicable to measuring systems for the continuous and dynamic measurement of quantities of liquids other than water, which are subject to legal metrological control, are set out in OIML R 117-1 [1], which is also used as a normative document in the conformity assessment of dispensers placed on the EU market in accordance with Directive 2014/32/EU for measuring instruments [3]. OIML R 117-1 includes metrological and technical requirements for dispensers for diesel, petrol (gasoline), LPG, AdBlue, washer fluids, etc.

Industrial practice is increasingly taking advantage of automation. Its benefits also extend to the field of metrology, in the form of streamlining frequently repetitive processes, and contribute to checking the reliability of the measurement results. Trends in the field of automation enter into all fields of industry, including metrology.

The idea of applying these trends to the area of metrological control services for measuring instruments used at fuel stations is based on the requirements of the practice and on the activities of the Research and Development Department of the Slovak Legal Metrology Institute, which as the main researcher of this project cooperated with leading Slovak technical universities.

The purpose of the article is to present a new generation of a compact system to perform metrological control, mainly the verification of dispensers used at fuel stations (a system for metrological control of fuel station dispensers hereinafter referred to as "MCoFD system"). The new MCoFD system has several previous versions, from which it differs by a significantly higher degree of automation and a wider range of provided services [4].

The aim of the research project was to create a measuring system that is capable of verifying all the dispensers available at fuel stations, using elements of artificial intelligence as a means of automation and acceleration of measurement processes, and whose size is compact enough and suitable to fit into commonly available commercial vehicles up to 3.5 T. The design process took into account the use of electrical systems in potentially explosive atmospheres with regard to the safety of use of the MCoFD system. Figure 1 shows the MCoFD system that can be built into a commercial vehicle to create a mobile technology. The individual subsystems are described in the following chapters.

2 Mechanical part of the MCoFD system

The design of the MCoFD system takes into consideration the weight of the total system, as well as whether it is sufficiently strong and rigid. The weight of the total system was designed to not exceed 3.5 T including the weight of the driver and the vehicle, as the maximum load capacity of a commercial vehicle. In addition, it

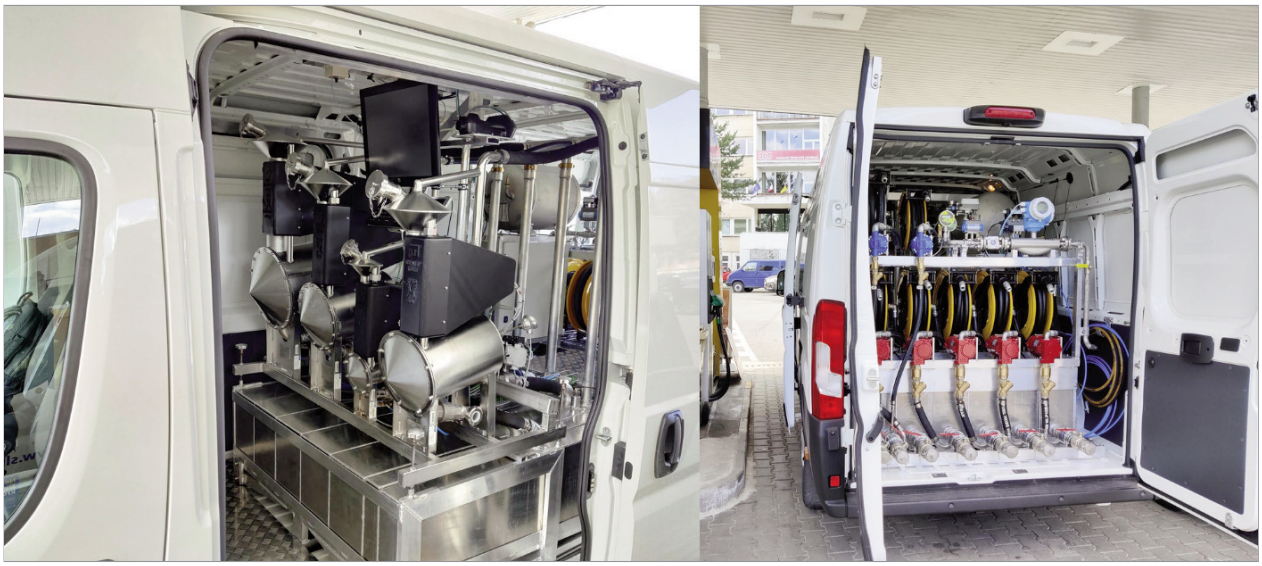


Fig. 1 MCoFD system as a part of the vehicle for verification

was required that the MCoFD system can be easily installed into the cargo space of commonly available commercial vehicles with only minimal modifications. Such a complex measuring system for the verification of all kinds of measuring systems includes a lot of sensors, tanks, standard vessels, pumps, hose systems, etc. According to the reasons mentioned above, it was not always possible to use ordinary materials (e.g. steel). Collecting tanks and the supporting structure frame were the most suitable parts to save weight. The supporting structure frame includes three parts: the main frame (Fig. 2), the frame for LPG technology and the frame for standard vessels.

The collecting tanks and the support frame system were made of aluminium alloy with a density equal to one third of the density and with a failure strength equal to half of the failure strength in comparison with commonly used steels. In this way, it was possible to reduce the weight of the entire construction by up to 350 kg. For safety reasons, simulation strength analyses of the supporting structure frame and collecting tanks were performed. The simulations were focused on:

- the static loading - for full collection tanks during the verification process;
- the quasi-dynamic load in the direction of the vehicle's motion (at the force equal to 0.8 g) - behavior of the system during vehicle braking;
- the quasi-dynamic load in the direction perpendicular to the vehicle motion (at a force equal to 0.4 g) - behavior of the system while moving round curves in the road.

The simulation results showed high safety factors (values of 4 and higher) [5] in all cases. The results of the main frame static loading simulation are shown in Fig. 2.

The 3D model of the MCoFD system as a compact measuring system is shown in Fig. 3.

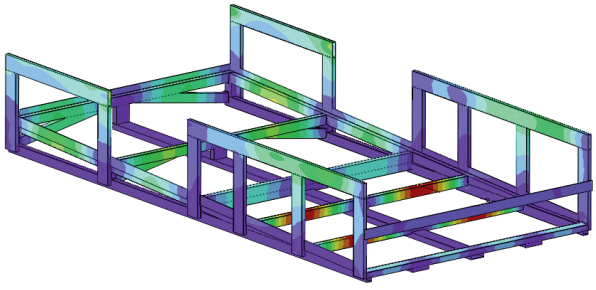


Fig. 2 Simulation of the static loading of the main frame

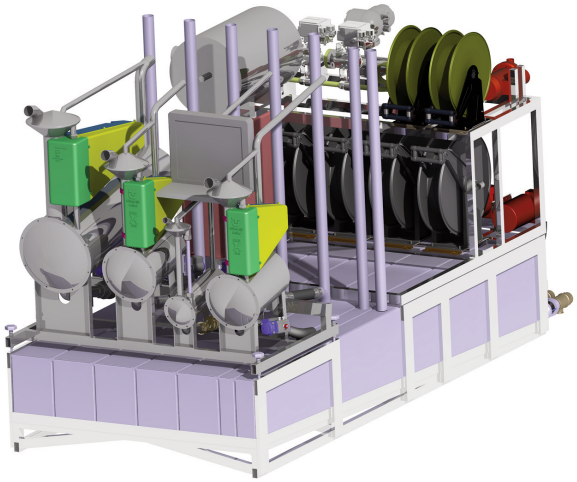
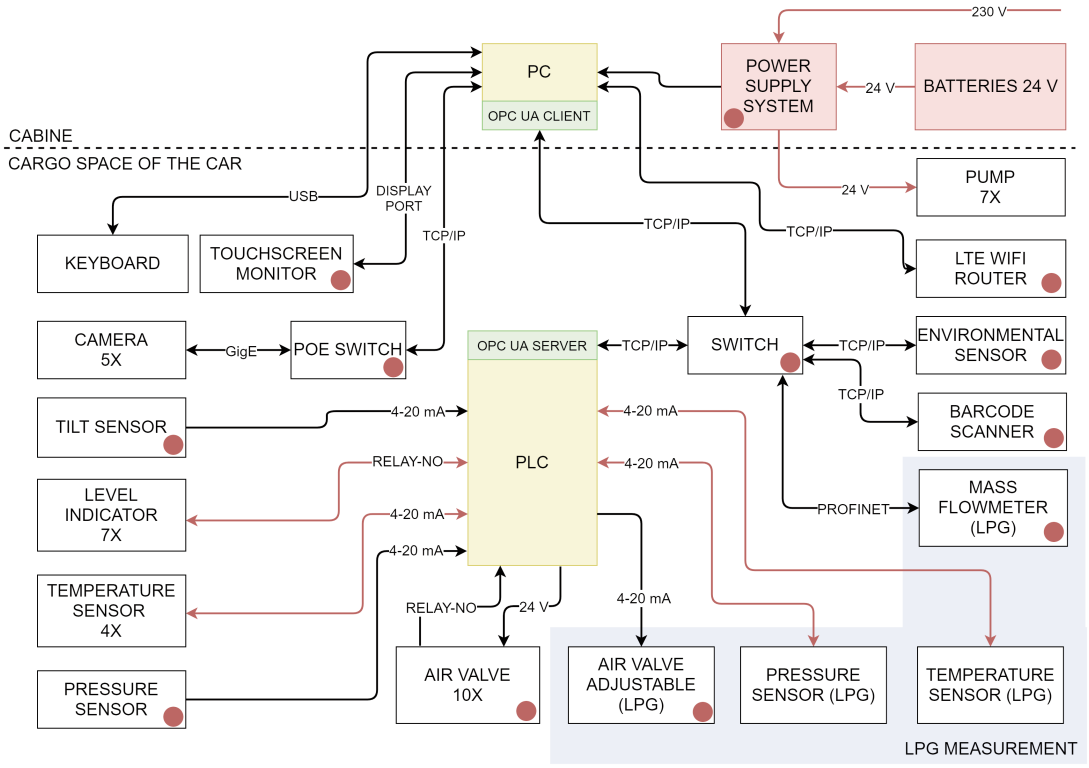


Fig. 3 Compact MCoFD system (3D model)



Note: Red circle is 24 V power supply from power supply system.
Red connection means that the power supply is via intrinsically safe barrier.

Fig. 4 The block diagram of the electrical system

3 Electrical system and software solution

The electrical system for the MCoFD system is designed to be energy independent. The power supply system uses four batteries with a total capacity of 200 Ah at 24 V. The power supply system includes converters, batteries, and a diode switch.

After connecting to the external 230 V power supply, the diode switch switches the power supply from the batteries to the converters and the batteries start the charging process. The entire electrical system with the batteries was designed to cover 15 hours of operation of the MCoFD system pumping 6 000 L of liquid (at a temperature of 20 °C inside the cabin) or 15 hours of operation pumping 4 500 L of liquid (at a temperature of 0 °C inside the cabin). The block diagram of the electrical system is shown in Fig. 4.

The MCoFD system is operated by the technician using software that runs on a PC and together with a PLC forms the control part at the highest level. The PC and the PLC communicate together via the OPC UA communication protocol [6], where the PLC is the server and the PC is the client. The OPC UA is a secure and an independent way of exchanging data between a PC and a PLC. Based on this data exchange, the control of air operated valves and the collection of data from all the sensors (except the cameras) can be performed and provides a high degree of automation. The PLC also checks the control parameters and includes regulatory algorithms.

The MCoFD system uses intelligent image processing to read the dispenser indicated data and the liquid volume in standard vessels.

The image processing is performed by cameras, which are connected to the PC via a POE switch. Sensors such as a barcode scanner (used to identify the measuring instrument from the verifier's instrument database), the environmental sensor (temperature, pressure and humidity) and the mass flow meter communicate with the PLC through the TCP/IP protocol via a switch. All the valves used are air operated with electrical control and use a compressed air tank. The pressure inside the compressed air tank is measured continuously. The control valve, used to adjust the flow when measuring LPG, is controlled by a 4 – 20 mA signal, while the start/stop valves are controlled by a 24 V signal. Each start/stop valve contains a pair of sensors with a relay output for monitoring its end position. These valves are used to empty the standard vessels into collecting tanks or for the verification of

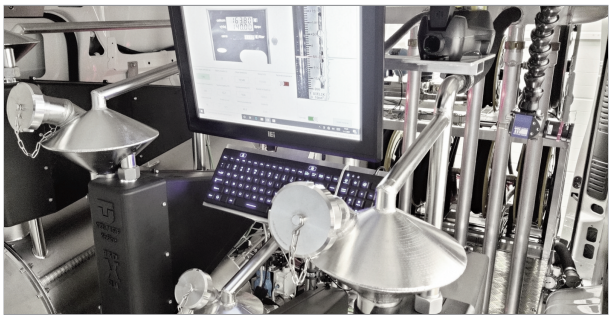


Fig. 5 The user interface of the MCoFD system with touch screen monitor

LPG dispensers. Approximately 90 % filling of the collecting tanks is indicated by level indicators. For the purpose of verification of dispensers with a temperature compensation function, the temperature of the liquid in standard vessels is measured. A two-axis tilt sensor is used to put the standard vessels into the equilibrium position. For the purpose of verification of LPG dispensers, the MCoFD system uses a thermometer and a pressure gauge with a current 4 – 20 mA output.

The LTE WiFi router connects the MCoFD system to the measuring instruments database of the verification authority via the GSM. This connection can be used to upload the measurement data to the cloud that is under the control of the verification authority. The user interface of the MCoFD system is shown in Fig. 5.

4 Measurements

The MCoFD system is a complex measuring device suitable for the verification of all available dispensers located at a fuel station. The MCoFD system uses the following measuring principles:

- the volume measurement of a liquid using standard vessels at atmospheric pressure (diesel, petrol, AdBlue and washer fluid),
- the volume measurement of a liquid using a standard mass flow meter in a closed loop (LPG).

All measurements are highly automated. The volume of liquid in the standard vessels, as well as the reading of the volume indicated by the indicating device of the fuel dispenser, is done by means of intelligent image processing.

Measurements that are not based on image processing but that directly affect the measurement of the volume of liquid are controlled by the PLC (see Fig. 4). These measurements include the following:

- the measurement of the titling of the standard vessels in two axes;
- the measurement of the temperature of the liquid (temperature compensated volume);
- the measurement of the temperature, pressure and humidity of the environment;
- the measurement of the volume of liquid by means of a mass flow meter in the closed-loop (LPG);
- the measurement of the temperature in the closed-loop (LPG);
- the measurement of the pressure in the closed-loop (LPG).

The measurements that are important in the automation process but that do not directly affect the measurement of the volume of liquid are following:

- the indication of the liquid level in the collecting tanks;
- the measurement of the pressure in the compressed air tank - for correct operation of the air-operated valves;
- the measurement of the voltage of batteries;
- the monitoring of the position (opened/closed) of the air-operated valves;
- the reading of the barcode from the measuring instruments - for unambiguous identification of the measuring instruments in the database of the verification authority.

4.1 Measurement of liquid volume using standard vessels at atmospheric pressure

The measurement is performed by the volumetric method with a fixed start. The system allows to choose from four standard vessels in order to ensure the verification of the dispenser in its full measuring range.

The configuration of the standard vessels for the MCoFD system is shown in Fig. 6. The standard vessels

Fig. 6 Configuration of standard vessels for the MCoFD system

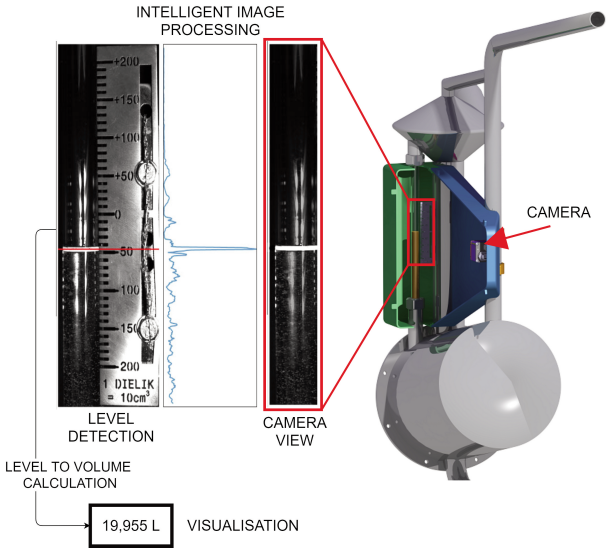


Fig. 7 Reading of the volume of liquid in standard vessels by means of intelligent image processing

and their shape were designed to reduce the formation of foam on the surface of the liquid during the measurement process. This allows the time for reading the received volume of liquid to be reduced.

Reading of the volume of liquid from standard vessels is performed by means of intelligent image processing (Fig. 7).

The camera scans the image of the level indicator (Fig. 7 - camera view), which is used as the input to the correlation-derivation algorithm (Fig. 7 - intelligent image processing). The algorithm determines the location of the line of the level indicator and based on the specified sensitivity performs the conversion to volume (Fig. 7 - level to volume calculation). The issue of edge detection and machine vision is discussed in general in [7]. In this way, the volume is measured continuously within the scale range. The metrology personnel only check the value recognized by the algorithm.

Several measurement principles have been considered in the design process of volume measuring. The advantage of the chosen principle is significantly better measurement dynamics in comparison with other principles. For example, a radar level transmitter needs some time to stabilize the indicated value and its electronics are sensitive to the temperature influence. Measuring the volume of liquid by means of the optical principle (camera) has another significant advantage, namely the possibility of visual control of the measurement results.

Intelligent image processing is also used for reading the indicated value from the dispenser indicating device. Digitizing of results using optical character recognition (OCR) as part of the automation process is useful for their subsequent processing. Intelligent image processing is a powerful tool and a future trend in the field of legal metrology. Image recognition can be used in difficult conditions and the following three factors have the most influence on image recognition:

- fuel stations use dispensers from different manufacturers and with different indication devices;
- ambient lighting conditions - if the dispensers are placed outdoors, a wide range of lighting conditions may occur;
- indicating devices of dispensers have a plastic or glass protective cover that is a source of light reflections.

The illustration of OCR digitization of the indicated value displayed by the indicating device is shown in Fig. 8.

In most cases, light reflections on the covers of the indication device prevent reliable image processing. The camera with a Polarsens chip can capture a four-directional polarization image (0°, 45°, 90° and 135°) in one shot by the four-directional polarizer, which can remove the reflections.

If some indication devices display the indication in a certain polarization, it is possible to select another polarization that does not suppress the displayed indication.

The image without reflections is then the input into the OCR algorithm, which uses elements of artificial intelligence, namely convolutional neural networks with deep learning [8]. The output is not only the recognized value, but also the probability with which this value was recognized. In this automated process, the technician only checks the recognized value.

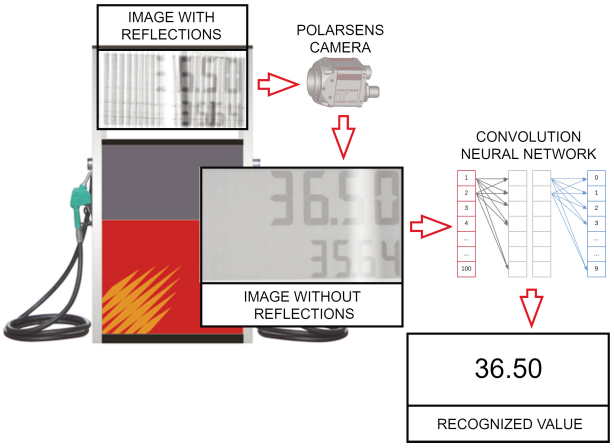


Fig. 8 Illustration of OCR digitization of the indicated value displayed by the indicating device

4.2 Measurement of liquid volume using standard mass flow meter in a closed loop (LPG dispensers)

The measurement is performed by the volumetric method with the fixed start and is carried out using a mass flow meter (Fig. 9).

After connecting the LPG dispenser to the MCoFD system, the measurement process is fully automated. The technician enters the required flow rates and volumes at which the measurements shall be performed. The software user interface on the basis of which the LPG verification is performed is shown in Fig. 10.

The PC and PLC automatically control the verification process based on the steps as shown in Fig. 12.

Figure 13 shows an example of the regulation process of the required flow rate, which is achieved by means of an electro-pneumatic positioner and operated by the control algorithm implemented in the PLC.

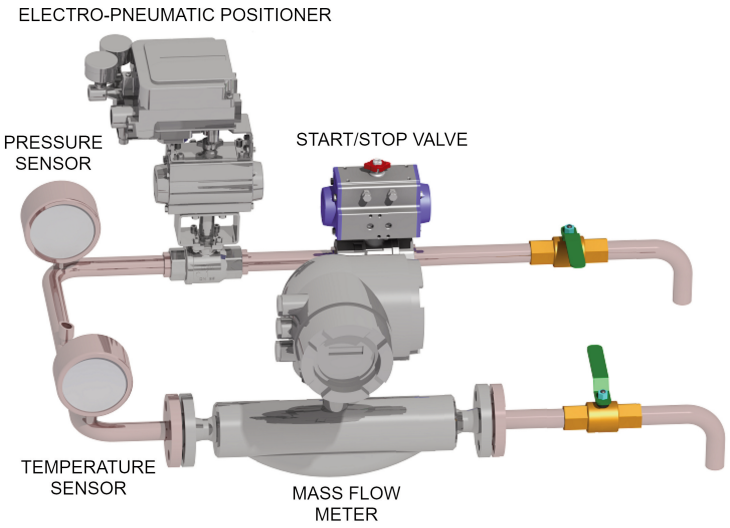


Fig. 9 Standard measuring system for the continuous and dynamic measurement of quantities of LPG as a part of the MCoFD system

5 Credibility of measurement results

An important aspect of verification is the credibility of the measurement results. The MCoFD system uses three control levels of measurements results credibility:

- the use of intelligent data processing - the technician is not the only one who reads the values from the measuring instruments;
- in case the technician changes the recognized value indicated by the measuring instrument, the change is recorded;
- the recording of witness photography with all key measurement information: values displayed by the indicating device of the dispenser, values indicated by the level indicator of the standard vessels, temperature compensation values, time and place of the measurement, etc.

A witness photography from the measurement is shown in Fig. 11.

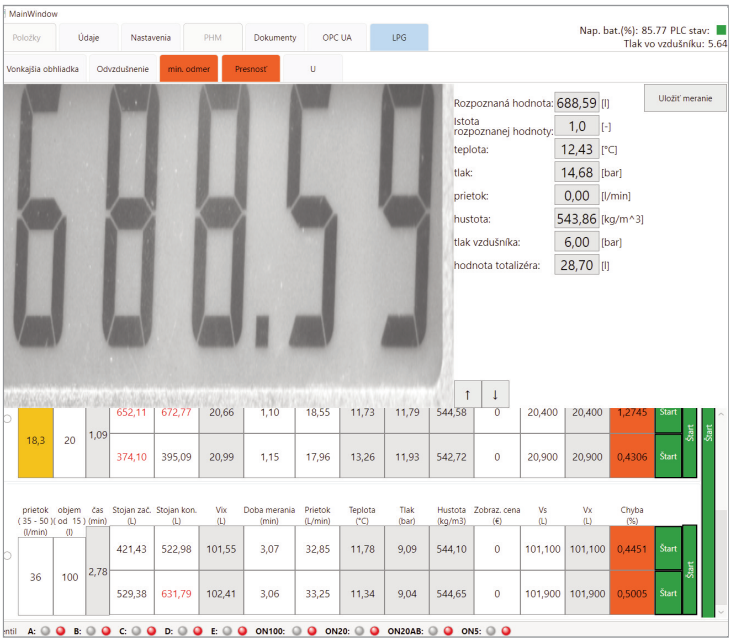


Fig. 10 Software user interface for verification of the LPG dispenser

6 Technical data of the MCoFD system

The MCoFD system is suitable for the verification of dispensers used on fuel stations with a flow rate of up to 200 L/min. It includes dispensers for the following liquids:

- standard hydrocarbon fuels (without temperature compensation);
- standard hydrocarbon fuels (with temperature compensation);
- liquefied petroleum gas (LPG);
- washer fluids;
- AdBlue – uric acid.

The following documents can be issued as result of the metrological control of dispensers:

- verification certificate;
- calibration certificate;

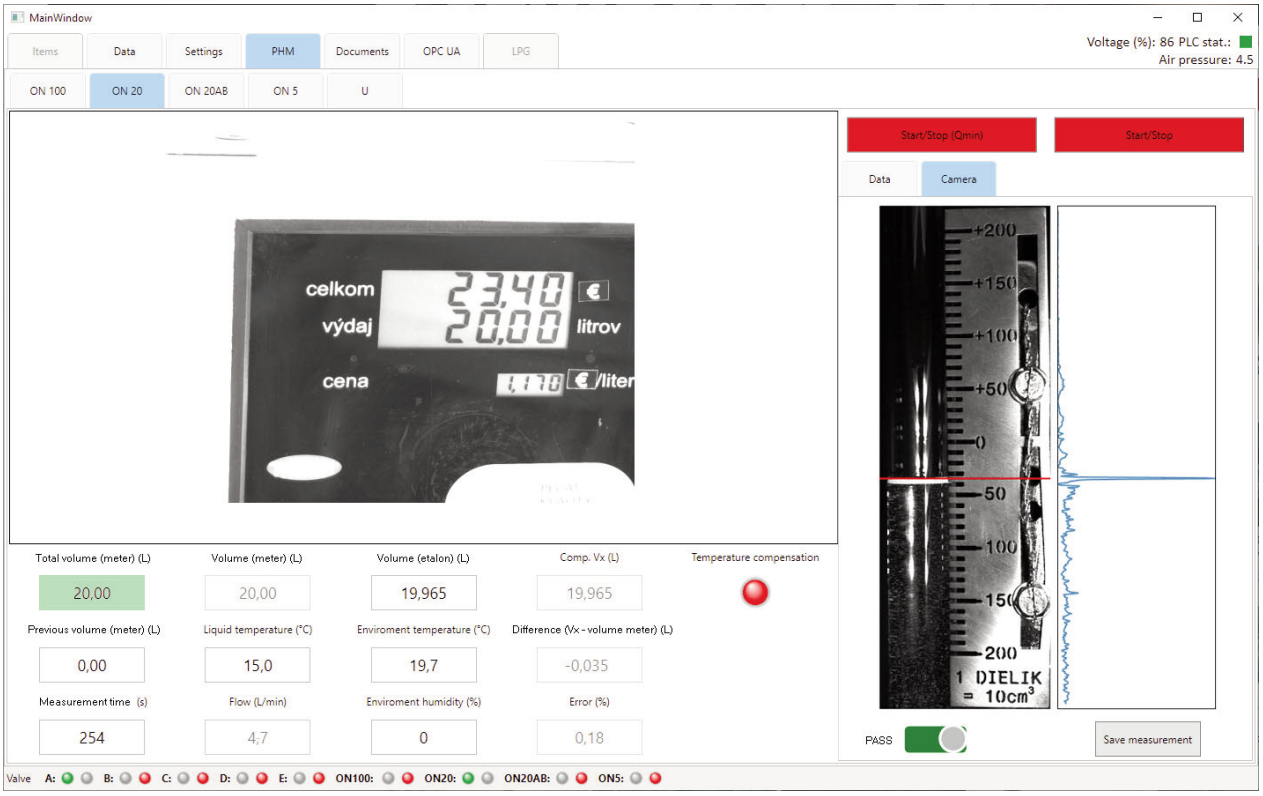


Fig. 11 Witness photography as the control of the credibility of measurement results

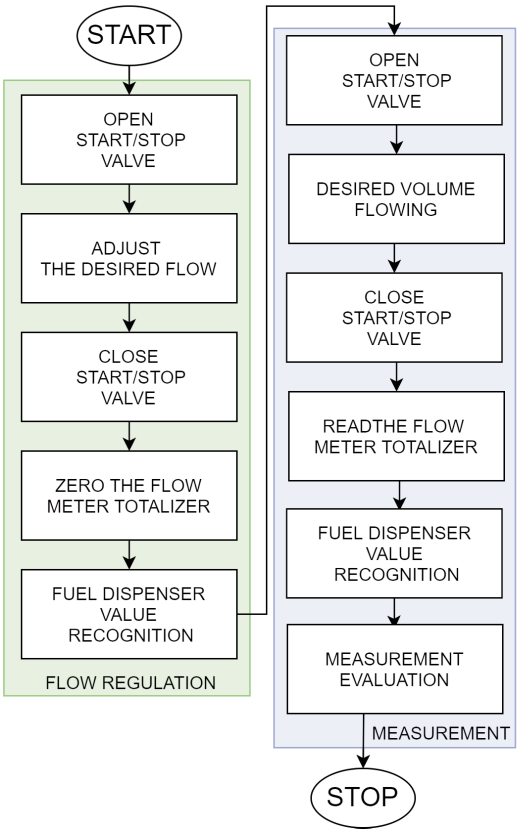


Fig. 12 Fully automated verification process for LPG dispensers

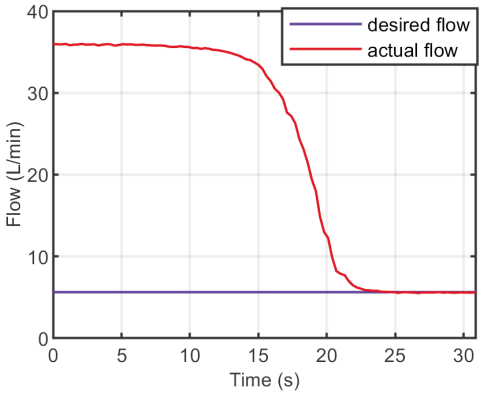


Fig. 13 Example of the regulation process of the required flow rate (the flow rate is regulated from 36 L/min to 5.25 L/min)

- receipt concerning the volume of liquid used during the metrological control;
- confirmation regarding the metrological control realization.

The MCoFD system has four standard vessels and the characteristics of the standard vessels and of the collection tanks are given in Table 1.

The expanded uncertainty of the determination of the error on indication of the volume conforms to the requirements of OIML R 117-2 [2].

Table 1 Characteristics of standard vessels and collection tanks

Standard measure	Specification	Nominal capacity (L)	Measuring range (L)	Collection tanks capacity (L) and their number
ON5	Washer fluids	5	4.95 – 5.05	90 (1 ×)
ON20AB	AdBlue	20	19.8 – 20.2	110 (1 ×)
ON20	Hydrocarbon fuels	20	19.8 – 20.2	240 (5 ×)
ON100	Hydrocarbon fuels	100	99 – 101	

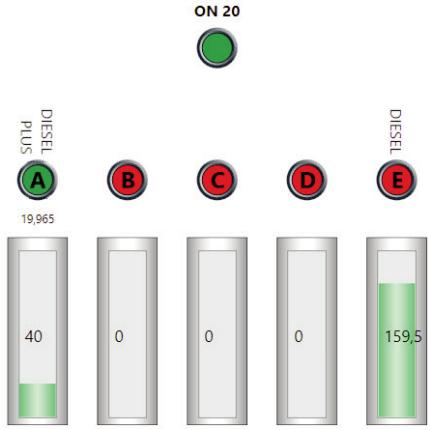


Fig. 14 Sorting of the liquids into separate collection tanks according to the kind of liquid (screenshot taken from the user interface)

Table 2 Technical data of the MCoFD system

Feature	MCoFD		
Power supply	Batteries	Externally	Charging
	24 V	~230 V	yes
Temperatures	Operating	Charging	
	–20 °C ~ +60 °C (external temperature)	–10 °C ~ +40 °C (cabin temperature)	
Collection tanks	Volume		
	240 L	110 L	90 L
	Pcs		
	5	1	1
	Pump		
	50 L/min	30 L/min	30 L/min
	Approximate time to empty the entire tank		
	5 min	4 min	3 min
Connectivity	GSM, WiFi		

After the measurement of the volume by means of standard vessels, the liquid can be transferred to the specified collection tank and the standard vessels can be used again. In the case of hydrocarbon fuels, two standard vessels (ON20 and ON100) are connected to five collection tanks. This allows the individual liquids (petrol, diesel, etc.) to be sorted as shown in Fig. 14.

The collection tanks for hydrocarbon liquids can be emptied using pumps with a flow rate of 50 L/min. The collection tanks for the washer fluids and AdBlue can be emptied using pumps with a flow rate of 30 L/min. All collection tanks also have the possibility to be emptied by gravity (Fig. 15).

Other technical data are given in Table 2.

Fig. 15 Ways of emptying the measured liquids (by gravity or pump)

7 Conclusion

Fuel dispensers are one of the most frequently used measuring instruments in business relations worldwide. Therefore, they require special attention. This was the main motivation for the development of a new generation of systems for the metrological control of dispensers used at fuel stations. The aim of the project was to develop and produce the MCoFD system for the verification of a wide range of dispensers in order to increase the credibility and efficiency of verification. The new MCoFD system enables the shutdown duration of dispensers during their metrological control to be shortened, thereby reducing financial losses for the seller.

The MCoFD system uses automation by means of intelligent image processing, complex data collection, and monitoring of accompanying quantities and their evaluation.

The new system has passed the phase of complete testing and is already in use in the Slovak Republic. The MCoFD system was presented to owners of fuel stations and received a positive response. Based on this positive response, the distribution of the design or even of the final product itself to countries expressing potential interest is being considered.

The development and production of the MCoFD system is the result of a research team that also included experts in the field of legal metrology – Miloš Ujlaky, Peter Cintula, Tomáš Kováč, Rastislav Bánik, Branislav Florek (Slovak Legal Metrology Institute) and experts in the field of science and research – Teodor Tóth (Faculty of Mechanical Engineering, Technical University of Košice) and Ľuboš Kučera (Faculty of Mechanical Engineering, University of Žilina).

The composition of the research team was balanced and allowed the theoretical knowledge of science and research from the university environment to be connected with the practical and technical knowledge from the field of legal metrology. This created a synergy of science and practice, which was a key factor in the design and realization of new MCoFD system. ■

References

[1] OIML R 117-1, *Dynamic measuring systems for liquids other than water, Part 1: Metrological and technical requirements*, Edition 2019 (E)

[2] OIML R 117-2, *Dynamic measuring systems for liquids other than water, Part 2: Metrological controls and performance tests*, Edition 2019 (E)

[3] Directive 2014/32/EU of the European Parliament and of the Council, 2014/32/EU, The European Parliament and the Council of the European Union, 2014.

[4] Slovak Legal Metrology, *Method for automated verification of a fuel dispenser and equipment for carrying out the method*, Slovak utility model no. 7735, 2014, Jul. 3. 2021.

[5] F. M. Burdekin, *General principles of the use of safety factors in design and assessment*, Engineering Failure Analysis, vol. 14, no. 3, pp. 420-433, 2007.

[6] OPC Foundation, *OPC Unified Architecture Specification – Part 1: Overview and Concepts*, Version 1.04, 2017.

[7] E. R. Davies, *Computer and Machine Vision*, 4th. ed, Cambridge, MA, USA: Academic Press, 2012.

[8] I. Goodfellow, Y. Bengio and A. Courville, Deep Learning, Cambridge, MA, USA: MIT Press, 2016.

SOFTWARE

ZKASP: ZKP-based attestation of software possession for measuring instruments

Luís T.A.N. Brandão, National Institute of Standards and Technology (NIST), USA
At NIST as a contractor from Strativia

Carlos E.C. Galhardo, National Institute of Metrology, Quality and Technology (INMETRO), Brazil

René Peralta, National Institute of Standards and Technology (NIST), USA

Abstract

Software-controlled measuring instruments used in commercial transactions, such as fuel dispensers and smart meters, are sometimes subject to "memory replacement" attacks. Cybercriminals replace the approved software by a malicious one that then tampers with measurement results, inflicting a financial loss to customers and companies. To mitigate such attacks, legal metrology systems often require regular device attestation, where an auditor checks that the device possesses ("knows") the approved software. However, current attestation methods usually require the software to be known by the auditor, thus increasing the risk of inadvertent leakage or malicious theft of proprietary information, besides facilitating its malicious adulteration. To address this issue, we propose that legal metrology systems consider the use of **z**ero-**k**nowledge **p**roofs **o**f **k**nowledge (ZKPoK), as a way of enabling attestation of possession of approved software, while ensuring its confidentiality from the auditor. To further provide publicly verifiable evidence of freshness, each such proof can be related to a fresh random value from a public randomness beacon. This article describes the basic conceptual idea, while also discussing pitfalls that should be avoided.

Keywords

Device attestation, Legal metrology, Proof of knowledge, Public auditability, Randomness beacon, Zero-knowledge proof.

Introduction

In modern society, measuring instruments are a cornerstone of many activity sectors, including trade, safety, the environment and health. For example, when filling up an automobile fuel tank, a customer trusts that the volume of fuel dispensed by the pump corresponds to the displayed measurement result. Given the importance of measurements in many economic activities, each country develops a "legal metrology" framework composed of laws and regulations that strive to ensure that measurements are accurate (agree with corresponding standard units), reliable (stable against environmental changes), and incorruptible (impervious to malicious manipulation).

While scientific metrology is the science of measurement, legal metrology can be defined as the "practice and process of applying a regulatory structure and enforcement to metrology" [OIML12]. Laws concerning measuring instruments are needed when measurement errors or fraud could affect commercial transactions, public safety, health-related measurements, or the environment [Kel19]. Most countries have at least one national metrological authority [OIML13] to enforce the metrological regulations and execute legal metrology procedures[1].

Each legal metrology authority enacts, through regulations, a set of software security requirements to mitigate attacks that modify the software embedded in measuring instruments. The embedded software must be approved by the metrological authority to be in use, i.e., must comply with requirements [PBMC+14]. The **integrity of the approved software** is one of the most critical concerns of software security regulation requirements [PPST15]. In legal metrology, measuring instruments must prove their software's integrity to a customer or an official auditor. The integrity check is typically obtained through a device attestation protocol.

A device attestation protocol allows a software-controlled device to make a reliable statement about its memory content. The device attestation has two

[1] European harmonized standards rely on Notified Bodies [Gal13].

Author's note: Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is neither intended to imply recommendation or endorsement by INMETRO or NIST, nor to imply that they are necessarily the best available for the purpose.

Editor's note: This paper will be presented at the CIML2021 Conference in Lyon, France in September 2021. The CIM Organization Committee has kindly given permission to the Editors of the OIML Bulletin to publish it in this Special Edition.

participants: the *verifier V* (the auditor), and the *prover P* (the instrument). The main goal is to enable *V* to check that *P* is a valid device – usually, that *P* has some embedded software trusted by *V*.

Device attestation is, in general, implemented as a challenge-response protocol [CGLH+11]. Figure 1 shows the five main steps:

(1) *V* creates a challenge for *P*, and
(2) sends it to *P*.
(3) *P* computes a response, and
(4) sends it to *V*.
(5) *V* verifies the validity of the response with respect to the challenge.

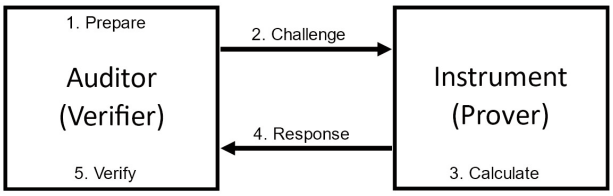


Fig. 1: Device attestation

Often, the response is the output of a hash function that uses the memory content and the challenge. If *P* is an honest prover (the statement about its memory content is `true`), it convinces the verifier about memory content. If *P* lacks the required memory content, it should not be able to convince *V*.

A device attestation protocol should reflect the current status of *P*. This property is called *freshness*. Several techniques can be used to ensure freshness:

- local randomness can be used to create a nonce controlled by the verifier [SPVK04];
- a pseudo-random number generator could determine a sequence of input memory blocks [CFPS09];
- including a monotonically increasing integer [ISZ17] to be hashed along with the code;
- session keys [KBGK17]; or
- timestamps from a real-time clock [ERT17].

In our approach, a public randomness beacon is used as an innovative source of time-bound and verifiable randomness.

A public randomness beacon is a time-stamped source of randomness [KBPB19]. It broadcasts, at regular time intervals, a fresh sequence of time-stamped random bits called a pulse. It has three critical properties: unpredictability, autonomy, and consistency. Unpredictability means no one can consistently predict the output bits provided. Autonomy means no one could alter the probability distribution of the output bits. Consistency means all users could rely on periodically new random bits [FIP11].

A proof that uses the randomness from a pulse has a lower bound in time, as it cannot be created before the pulse was publicly known. The time interval between the present moment, and this lower bound could be used as a quantitative measure of freshness. This freshness is publicly verifiable, as the randomness beacon stores each timestamped pulse signed and hash-chained in a publicly-readable database. Furthermore, a user can query the database to retrieve any previous pulse and its associated data [Che18].

Legal metrology tries to mitigate the malicious software replacement attack by requiring regular device attestation (software integrity verification), where an auditor checks that the device possesses ("knows") the original software by comparing it to a copy held by the auditor. However, the requirement of giving the auditor a view of the software has two important consequences: it impairs the protection of the manufacturer's intellectual property, and it constrains the set of possible auditors (i.e., to those allowed to see the software).

This paper argues that legal metrology frameworks should take advantage of state-of-the-art practical cryptography to provide an enhanced solution to the described attestation problem. In particular, the advanced solution, dubbed ZKASP, proposes the use of a **z**ero-**k**nowledge based **a**ttestation of **s**oftware **p**ossession for measuring instruments. By using a **z**ero-**k**nowledge **p**roof **o**f **k**nowledge (ZKPoK), the auditor, even if unacquainted with the approved software, can check whether a measuring instrument contains the approved software. This is a desirable property for legal metrology applications that have a dual requirement of confidentially and auditability of the embedded software.

In the proposed solution, the assurance of confidentiality becomes technical/cryptographic, instead of depending on a non-disclosure agreement by the auditor. Besides the official auditors, the customers can also run the protocol before a commercial transaction, to ensure that the instruments are able to prove knowledge of the correct software.

The proposed solution also enables freshness based on a "nonce", which is obtained from a public randomness beacon. The timestamped nonce creates an upper bound for the age of the proof, which can be publicly verified. This solution also prevents replay attacks, where a valid proof is maliciously repeated. Current public randomness sources, such as the NIST Beacon have a period of as low as a one-minute.

While the proposed solution is conceptually simple, it is important to avoid a number of pitfalls. For example, while the generation of a hash of the software requires knowledge of the software, a proof of knowledge of the said hash is not a proof of knowledge of the software. Thus, the ZKASP solution should simultaneously be succinct and require access to the full

software. Different mechanisms are possible depending on the legal metrology system model and the allowed interaction between various parties.

2 System model and building blocks

For a given type of measuring instrument, there are various parties in the system of interest:

- **Measuring instruments (a.k.a. provers):** the individual instruments that are required to provide a proof of knowledge of the approved software.
- **Auditors (a.k.a. verifiers):** those that interact with the measuring instrument to verify that the instrument "knows" the approved software. Usually these are official *auditors*, but in the proposed solution they can also be regular *customers*.
- **The authority:** a legal metrology authority (or notified body) providing public parameters that enable the device attestation protocol.
- **The randomness beacon:** an agreed trusted public randomness source [BeaconUS; BeaconBR; BeaconCL] that periodically outputs signed time-stamped random values.
- **The vendor/manufacturer:** the entity that is responsible for setting (and possibly updating) the embedded software in the measuring instruments.

Our proposal makes use of the following cryptographic primitives:

- **Signatures [FIPS 186-5].** Any party can create a pair (k, K) of keys: one private (k) for signing, and one public (K) for verification. Given any string M, the party can use its private key to compute a signature $\sigma \leftarrow \text{Sign}[k](M)$. Given M and σ, any party with the public key can verify authenticity: $\text{Verify}[K](\sigma, M) = \texttt{true}$. However, without the private key it is unfeasible for any party to compute σ that would pass the verification.
- **Hash function [FIPS 180-4].** A hash function H takes as input any string M, of arbitrary length, and outputs a (short) string $h = H(M)$. Any party can compute H. Given h it is unfeasible for any party to find an M such that $h = H(M)$. Given M it is unfeasible for any party to find another M' such that $H(M') = H(M)$. Furthermore (informally), $H(M)$ reveals no information about M (when the exact M is unpredictable).
- **ZKPoK [ZKProof]:** A ZKPoK (*Zero Knowledge Proof of Knowledge*) is a cryptographic method by which a party (the prover) can prove to another party (the verifier) that it knows a secret value x, but without disclosing x itself. For example, the prover may know the factorization of an RSA key N, and wish to prove this to a verifier without revealing the prime factors. The method must ensure that no prover can convince a verifier that it knows a secret if this is not the case.

Our proposal also makes use of various components of the infrastructure of the Internet, such as secure communication [RFC 8446] and public-key infrastructure [RFC 5280]. As for the public randomness server, our proposal is to use any server which is interoperable with the NIST Beacon. This server provides, every minute, a timestamped and cryptographically signed 512-bit random string. The signature authenticating these random strings can be verified off-line using the server's public key.

2.1 ZKPoK bound to time and identities

The type of ZKPoK we will use – let us call it Π – for proving knowledge of a secret S with a certain property P (i.e., that $P(S) = \texttt{true}$) is of the following basic form:

- The verifier sends an external challenge C to the prover[2].
- The prover replies with a value $\pi \leftarrow \Pi(C, S)$ that could only have been produced by someone who knows secret S satisfying P, and who simultaneously knows public C.
- Given π, the verifier can efficiently compute $\text{VerProof}(\pi, C)$, which returns $\texttt{true}$ if and only if the proof is valid.

Section 3.2 describes our solution, which amounts to designing the external challenge C and choosing a ZKPoK Π so as to ensure zero-knowledge, eliminate some attacks, and mitigate others.

It should not be possible to reuse the proof constructed by one instrument in order to produce a proof for a different instrument. It should also not be possible to use an old proof to construct a fresh proof, even if by the same instrument. More generally, a good solution must ensure that proofs are bound to the context in which they were produced.

To ensure this, we let the external challenge C be the hash of various strings that, together, specify the

[2] We call it "external" to avoid confusion with a common [internal] "challenge" step in the generation of π.

context. For example, the proof $\pi \leftarrow \Pi(C, S)$ becomes bound to the time t, and to the prover and verifier identities (ID_P , ID_V), if we require $C = (t, \mu_t, ID_P , ID_V)$, where μ_t is a random string produced at time t by a public source of randomness.

3 ZKASP protocols

3.1 Setup (initial deployment)

The typical setup setting for a ZKASP protocol is as follows:

- **Cryptographic keys.** All parties have private and public keys for a signature scheme. The j^{th} auditor's private/public key pair is (y_j, Y_j). The i^{th} instrument's key pair is (x_i, X_i). The authority's and vendor's key pairs are, respectively (a, A) and (v, V). The public key of each party is also used as its identity.
- **Software approval.** Through an agreed protocol during the *type approval* [OIML13], the authority approves the software S developed by a vendor for use with a type of measuring instrument.
- **Software commitment.** At time t_0, the authority publishes the hash $h = H(S)$ of the approved software S, along with a signature $\sigma_A = \text{Sign}[a](t_0 \| r_{to} \| h)$ by the authority, and a corresponding signature $\sigma_V = \text{Sign}[v](t_0 \| r_{to} \| h)$ by the vendor, where r_{to} is the most recent beacon randomness (from time t_0).[3]
- **Software deployment.** The vendor deploys the measuring instruments, each with a private–public key pair (x_i, X_i). Only the instrument knows its own secret key; the authority and the vendor both have a list of the public keys of all instruments.

3.2 The baseline ZKASP Protocol

In an attestation interaction, started at time t, between an auditor j and an instrument i:

1 **External challenge.** The auditor determines the current time t, locally generates a random value r'_t, and obtains the most recent random value r_t produced by a public randomness beacon. The auditor signs them together, obtaining $\sigma_j = \text{Sign}[y_j](t, r_t, r'_t, X_i)$ and then sends $C_t = (t, r_t, r'_t, X_i, Y_j, \sigma_j)$ to the instrument.

2. **Response.** The instrument starts by checking that the received X_i (inside C_t) is indeed the instrument's public key. Then it checks the validity of the auditor's signature σ_j.[4] If the verification fails, then the instrument aborts the interaction. Otherwise it produces the proof $\pi = \Pi(C_t, S)$, i.e., a $C_{t\text{-bound}}$ ZKPoK of "S satisfying $H(S) = h$". Finally, the instrument computes a signature $\text{Sign}[x_i](\pi)$ of π and sends (π, σ_i) to the auditor.
3. **Verification.** The auditor checks the validity of (π, σ_i), i.e., that $\text{VerProof}(\pi, C_t) = \texttt{true}$ and $\text{VerSign}[X_i](\sigma_i, \pi) = \texttt{true}$.
4. **Transfer.** The auditor can then transfer to the authority the tuple (C_t, π, σ_i). From a legal metrology standpoint, this is what we would call the "proof". Anyone can check the validity of a published tuple, including that it was requested by auditor j, and produced by instrument i after the beacon value r_t was generated. The latter requires using the beacon public key to check the validity of its output value r_t from a corresponding signed pulse.

The described protocol is agnostic to the ZKPoK technique used to prove knowledge of a hash pre-image. This may be based on a general-purpose ZKPoK technique to prove knowledge of the input of a function (a hash, in this case), which yields the output h. Details are beyond the scope of this paper. However, we note that computing such ZKPoK entails not only every step of the computation of $h = H(S)$, which processes every bit of S, but also a multiplicative overhead of the ZKP to prove a proper sequence of those steps.

3.3 A lightweight ZKASP protocol

It is conceivable that low-resource devices may be unable to efficiently perform the generic ZKPoK described in Section 3.2. For those cases, we describe a much more efficient approach, essentially based on a simple discrete-log ZKPoK (a Schnorr proof [Sch91]).

The tradeoff, as compared with the previous solution, is that it requires a more active role by the authority (or the vendor), and a corresponding synchronization by the auditor.

Elliptic curve parameters. The system uses global elliptic curve parameters [SP 800-186] agreed by every party. These include a cyclic group G_q of order q and generator G, e.g., based on `Curve25519` [RFC 7748], which can be the same as already used for signatures.

[3] This requires, on purpose, coordination between authority and vendor to sign the same element.

[4] An actual implementation can do more verifications, such as checking that the timestamp is acceptable.

Frequent fresh commitments. For this lightweight solution, we assume that a trusted party with knowledge of the software S periodically computes a secret value $h_t = H(r_t||S)$ and then commits to it by publishing $P_t = H(r_t||S) \cdot G$, where r_t is obtained from a public randomness service at time t. The operation represents a multiplication in the elliptic curve. Therefore, P_t is simply a point on `Curve25519`, which can be represented by a 256-bit integer.

Under standard cryptographic assumptions, the publication of P_t does not reveal h_t. Since P_t changes periodically (the frequency can be as high as once per minute), the knowledge of $h_t = H(r_t||S)$ can be used as a proxy for the knowledge of S. To prove knowledge of h_t, the following protocol suffices:

1. The auditor (verifier) requests a proof, sending the external challenge C_t as in Section 3.2, i.e., $C_t = (t, r_t, r'_t, X_i, Y_j, \sigma_j)$ to the instrument.
2. The prover makes the necessary checks, including that the embedded identifiers and the signature σ_j are valid. If any check fails then the instrument aborts. Then, the prover computes the hash $h_t = H(r_t||S)$ and the corresponding commitment $P_t = h_t \cdot G$.
3. Then the prover produces the proof π (a ZKPoK of the discrete-log of P_t):
   - selects a random number u and computes $U = u \cdot G$;
   - computes the internal challenge $c = H(C_t||U)$;
   - computes the answer $z = u + c \cdot h_t \bmod q$.

   The prover sends (π, σ_i) to the verifier, where $\pi = (U, z)$ and $\sigma_i = \text{Sign}[x_i](\pi)$
4. The verifier accepts if and only if $z \cdot G = U + (c \cdot P_t)$, where c is computed as also prescribed in step 3b for the instrument.

Note that U and $(c \cdot P_t)$ are points in the elliptic curve, and the last addition is an elliptic curve operation. This is known as a Schnorr proof and, under standard cryptographic assumptions, securely demonstrates knowledge of h_t, the discrete-log of P_t. By proxy, assuming that within the last minute the instrument did not receive the value h_t from an adversary, it follows that the instrument must have computed h_t based on the software S.

4 Discussion

ZKASP is a proposal for verifying the possession of software by measuring instruments, in a legal metrology framework. It makes essential use of a zero-knowledge proof of knowledge (ZKPoK) in combination with a public randomness server.

4.1 Foreseen ZKASP deployment

An adoption of the ZKASP approach is expected to be suitable for deployment in instruments with micro-controllers running without an operating system. These micro-controllers, used in "built-for-purpose measuring instruments" (a type P computer, as specified by WELMEC 7.2 [WEL19]), would be chosen to support a chosen ZKPoK implementation[5]. Instruments such as fuel dispensers (gas pumps), utility meters, grain moisture meters, and non-automatic weighing instruments (grocery store scales) are examples of measuring instruments that could benefit from ZKASP. It is worth noting that ZKASP is a hybrid device attestation protocol [SL16] that depends on software and specialized hardware to secure the instrument's secret signing key.

Concrete implementations are beyond the scope of this paper, but even in settings where the general ZKASP approach (a direct ZKPoK of a pre-image of the hash of a long software) may be too expensive (say, due to low resources of the micro-controller), it is possible to consider the lightweight version we described, based on a very efficient Schnorr proof (Section 3.3), albeit requiring a more active role by the authority and synchronization by the auditor.

4.2 ZKASP for a digital transformation of legal metrology

The European Union is under a digital transformation of the legal metrology infrastructure, known as The European Metrology Cloud [Thi18]. In the Metrology Cloud, the manipulation of sensors became an important attack vector [OETS18]. ZKASP can mitigate this attack vector, by having the computer play the role of verifier. It can perform the attestation of several sensors in its neighborhood area network [BSK10] and report the results to the Metrology Cloud.

The ZKASP approach can also be used to empower customers as verifiers. The authority can enable a system (e.g., a mobile application) that allows customers to communicate with instruments, run the device attestation, and report proofs. The authority can crowdsource the collected data to better direct the placement of market surveillance operations. In this scenario, the approved software should enforce a period between subsequent attestations to avoid denial of service attacks.

[5] General-purpose computers, running an operating system, are more flexible for other attestation approaches [PPST15].

5 Security considerations

5.1 Basic properties

Important security properties for the legal metrology system stem essentially from the underlying building blocks: ZKPoK and beacon randomness. Informally:

- **Completeness.** If every party is honest, then the system leads the auditors to obtain valid proofs from instruments, which can in turn be validated by the authority and even verified by the public.
- **Soundness.** A party without access to the software cannot produce a signature. This stems from the "extractability" property of the ZKPoK, i.e., that producing a valid proof implies being able to write down the full software string. Furthermore, the use of a signature also implies access to the secret key of the instrument names in the proof.
- **Zero-knowledge (with transferability).** By definition, the ZKPoK does not reveal any information (in a cryptographic sense) about the software. Actually, the use of the Fiat-Shamir technique (for a non-interactive proof) makes the proof transferable (meaning that one gains the ability to prove that someone has knowledge of the software). This however is an intentional feature.
- **Verifiable freshness.** The use of public randomness from a randomness beacon binds the proof to a public timestamped value trusted to be unpredictable before the timestamp. This means that no one could have generated the proof before said timestamps. This enables placing an upper bound on the age of a proof.

The use of a digital signature scheme is crucial for ZKASP, to provide authenticity of the author of a proof, which in turn avoids proxy attacks. Naturally, this relies on a trust model about public keys, which can be supported on a public key infrastructure and blockchains [MMACR19; MMPM20; PWTS18]. Furthermore, the legal metrology itself should promote a system of transparency, which may for example include making publicly accessible a list of the public keys of all measuring instruments.

A formal security analysis should consider an idealization of security, such as in the ideal-real simulation paradigm, e.g., in the universal composability (UC) framework [Can01].

5.2 Some adversarial considerations

The following paragraphs discuss what can(not) be achieved by an adversary without the software, with respect to forging proofs. The considerations are intended as clarifying comments to convey intuition about security properties. However, they are not a proof of security. Concrete protocols following the ZKASP approach (i.e., building on fresh, transferable ZKPs of software possession) should be accompanied by a specific formulation of the properties intended of the system model (possibly derived from a so-called ideal model) and how they are achieved by the proposed concrete protocol.

Goal: A malicious instrument, without the valid software, wants to produce a valid proof of correct software possession. For example, either an adversary has replaced the instrument's software, or the instrument has not undergone a mandatory software update.

Capabilities: The adversary (e.g., a malicious auditor) does not possess the software, but has access to honest instruments, being able to request valid proofs from them, with complete control over the corresponding challenges. The adversary is assumed to not be able to exfiltrate the private signing key from deployed measuring instruments.

Impracticable attacks: Two well-known attacks against device attestation protocols are proxy attacks and precomputing attacks [SL16]. They are prevented in ZKASP:

- **Pre-computing attack (trying to reuse old proofs):** A malicious auditor is able to interact with an honest instrument and thereby obtain many proofs. In an unprotected system the auditor could now try to reuse these proofs when in fact the instrument could have been corrupted and no longer possess the correct software. ZKASP prevents this forgery of younger proof ages, because of its binding to timestamped (unpredictable) beacon randomness. If at a time t (with precision in minutes) the instrument loses access to the software, from that moment onward it will not be able to produce a proof with an acceptable claim that it was produced after time t.
- **Proxy attack (trying to use proofs from others):** In unprotected attestation protocols, the adversary may try to act as a malicious instrument (without the approved software), evading the attestation by redirecting the external challenge to a nearby honest instrument, acting as a proxy. This is not possible in ZKASP, since the proofs of software possession (ZKPoK) produced by other honest instruments (with access to the software) are bound to the instrument's identity, and therefore will not be valid if claimed by other instruments.

5.3 Adversaries with the software

It is important to bear in mind that the ZKASP approach proposes a proof of possession, which is not equivalent to a proof about the entire memory of the instrument. For example, an instrument capable of retaining the correct software and additional malicious code will still be an instance of possession of the correct software.

Possible attacks in which the adversary possesses the approved software are out of scope for resolution in this paper. Yet, it is instructive to consider their possibility.

- **The compression attack:** in which the adversary compresses the approved software, adds a small malicious code in the instrument's memory [CFPS09].
- **The time-of-check to time-of-use attack (TOCTOU):** a malicious instrument can download the approved software just in time for attestation, but during all other times use a malicious software [NJRT20].
- **The collusion attack:** two malicious instruments have complementary pieces of the approved software; together they can reconstruct the entire approved software [YWZC07].
- **Proofs-as-a-service (PaaS):** An adversary that knows the approved software can create a proof that is bound to the public key of an instrument that does not possess the software. Then, this party could conceivably manipulate the corrupted instrument to simply sign the proof.

Yet, even the sole proof of possession addresses an important problem: it prevents malicious instruments oblivious of the confidential correct software to pose as honest. It is also a good application for enabling proof of proper software update. Possible attacks in which the adversary possesses the approved software do not break the semantics of the proof, although it shows one limitation of the ZKASP approach. The resolution of this case is out of scope of resolution in this paper, but for concrete schemes it is worth considering what complementing techniques may be possible to implement. For example:

- **System restrictions.** The compression attack can conceivably be avoided by a non-compressing software string that fills up the entire memory. The TOCTOU and collusion attacks may be mitigatable by hardware restricting the interaction capabilities of the instrument. While these are conceivable mitigations, ensuring the mentioned restrictions is not trivial in practice.
- **More sophisticated ZKPoK.** The described PaaS attack requires manipulating the instrument to sign a forged proof. Conceivably, this can be mitigated by a more sophisticated ZKPoK that would be verifiably bound also to the private key of the instrument, rather than only to the public key, in a way that prevents the malicious auditor from building the proof alone. In other words, the idea would be to require a much higher interaction between the holder of the key and the holder of the software. A proof of software possession would still be possible via an interactive secure computation between the instrument and the malicious auditor, each with the corresponding secret (private key and software, respectively). While this would not eliminate the possibility of the attack (after all, the pair of colluding parties knows the entire secret needed to produce the proof), it would increase the practical difficulty / deterrent for collusion.

6 Conclusions

This paper presented ZKASP, an approach for zero-knowledge based attestation of software possession, for measuring instruments in a legal context. It combines a zero-knowledge proof protocol, as well as randomness from a public beacon, to address challenges of device attestation. The zero-knowledge proof allows the verifier (auditor) to remain oblivious of the content of the software embedded in the audited instrument. The use of beacon randomness allows ensuring an upper bound on the age of each proof, which can be publicly verified. ZKASP is a proposal where cryptography meets metrology. It combines a privacy-enhancing cryptographic tool (zero-knowledge proofs) and verifiable randomness to enhance the security guarantees of a real use-case requirement (attestation of software possession) of legal metrology. Being a high-level proposal, there are various aspects that deserve a closer look.

The choice of concrete instantiation options can depend on the exact context, e.g., the computational power of the processing unit (often micro-controllers) of the measuring instruments. Interesting options concern the choice of hash function, which may vary between the widely recognized SHA family standard and other more-recent proposals of ZKP-friendly hashes. ■

References

[BSK10] R. Berthier, W. H. Sanders, and H. Khurana. "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions". In: *2010 First IEEE International Conference on Smart Grid Communications*. IEEE. 2010, pp. 350–355. DOI: 10.1109/SMARTGRID.2010.5622068.

[Can01] R. Canetti. "Universally composable security: a new paradigm for cryptographic protocols". In: *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*. 2001, pp. 136–145. DOI: 10.1109/SFCS.2001.959888.

[CFPS09] C. Castelluccia, A. Francillon, D. Perito, and C. Soriente. "On the difficulty of software-based attestation of embedded devices". In: *Proceedings of the 16th ACM conference on Computer and communications security*. 2009, pp. 400–409. DOI: 10.1145/1653662.1653711.

[Che18] S. Chen. "Why are countries creating public random number generators?" In: *Science Magazine* 28 (2018). DOI: 10.1126/science.aau6171.

[CGLH+11] G. Coker, J. Guttman, P. Loscocco, A. Herzog, J. Millen, B. O'Hanlon, J. Ramsdell, A. Segall, J. Sheehy, and B. Sniffen. "Principles of remote attestation". In: *International Journal of Information Security* 10.2 (2011), pp. 63–81. DOI: 10.1007/s10207- 011-0124-7.

[ERT17] K. Eldefrawy, N. Rattanavipanon, and G. Tsudik. "HYDRA: hybrid design for remote attestation (using a formally verified microkernel)". In: *WiSec'17: Proceedings of the 10th ACM Conference on Security and Privacy in wireless and Mobile Networks*. July 2017, pp. 99–110. DOI: https://doi.org/10.1145/3098243.3098261.

[FIP11] M. J. Fischer, M. Iorga, and R. Peralta. "A public randomness service". In: *Proceedings of the International Conference on Security and Cryptography*. IEEE. 2011, pp. 434–438. DOI: 10.5220/0003612604340438.

[Gal13] J.-P. Galland. "The difficulties of regulating markets and risks in Europe through notified bodies". In: *Eur. J. Risk Reg.* 4 (2013), p. 365. DOI: 10.1017/S1867299X00002634.

[ISZ17] A. Ibrahim, A.-R. Sadeghi, and S. Zeitouni. "SeED: secure non-interactive attestation for embedded devices". In: *WiSec'17: Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2017, pp. 64–74. DOI: https://doi.org/10.1145/3098243.3098260.

[Kel19] M. Kellermann. *Comprehensive Diagnostic Tool*. Annex to the QI Toolkit. The World Bank, 2019. Chap. 11, pp. 187–207. https://www.worldbank.org/en/topic/competitiveness/brief/qi.

[KBPB19] J. Kelsey, L. T. A. N. Brandão, R. Peralta, and H. Booth. *A Reference for Randomness Beacons: Format and Protocol Version 2. Draft NISTIR 8213*. 2019. DOI: 10.6028/NIST.IR.8213-draft.

[KBGK17] F. Kohnhäuser, N. Büscher, S. Gabmeyer, and S. Katzenbeisser. "Scapi: a scalable attestation protocol to detect software and physical attacks". In: *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2017, pp. 75–86. DOI: 10.1145/3098243.3098255.

[MMPM20] W. Melo, R. C. Machado, D. Peters, and M. Moni. "Public-Key Infrastructure for Smart Meters using Blockchains". In: *2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT*. IEEE. 2020, pp. 429–434. DOI: 10.1109/MetroInd4.0IoT48571.2020.9138246.

[MMACR19] W. Melo Jr, R. Machado, B. Abreu, L. F. R. da Costa Carmo, and R. Ramos. "Certificação Digital como Ferramenta de Segurança para Medidores Inteligentes". In: *Anais Estendidos do IX Simpósio Brasileiro de Engenharia de Sistemas Computacionais*. SBC. 2019, pp. 89–94. DOI: 10.5753/sbesc_estendido.2019.8641.

[NJRT20] I. D. O. Nunes, S. Jakkamsetti, N. Rattanavipanon, and G. Tsudik. "On the TOCTOU problem in remote attestation". arXiv: Cryptography and Security (cs.CR). 2020. arXiv:*2005.03873* (2020).

[OIML12] OIML. OIML D 1:2012: *Considerations for a Law on Metrology*. Organisation Internationale de Métrologie Légale. 2012. https://www.oiml.org/en/files/pdf d/d001-e12.pdf.

[OIML13] OIML. OIML V 1: *International vocabulary of terms in legal metrology (VIML)*. Organisation Internationale de Métrologie Légale. 2013. http://viml.oiml.info.

[OETS18] A. Oppermann, M. Esche, F. Thiel, and J.-P. Seifert. "Secure Cloud Computing: Risk Analysis for Secure Cloud Reference Architecture in Legal Metrology". In: *2018 Federated Conference on Computer Science and Information Systems (FedCSIS)*. IEEE. 2018, pp. 593–602. DOI: 10.15439/2018F226.

[PPST15] D. Peters, M. Peter, J.-P. Seifert, and F. Thiel. "A secure system architecture for measuring instruments in legal metrology". In: *Computers* 4.2 (2015), pp. 61–86. DOI: 10.3390/computers4020061.

[PWTS18] D. Peters, J. Wetzlich, F. Thiel, and J.-P. Seifert. "Blockchain applications for legal metrology". In: *2018 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*. IEEE. 2018, pp. 1–6. DOI: 10.1109/I2MTC.2018.8409668.

[PBMC+14] C. B. do Prado, D. R. Boccardo, R. C. Machado, L. F. da Costa Carmo, T. M. do Nascimento, L. M. Bento, R. O. Costa, C. G. de Castro, S. M. Câmara, L. Pirmez, et al. "Software Analysis and Protection for Smart Metering". In: *NCSLI Measure* 9.3 (2014), pp. 22–29. DOI: 10.1080/19315775.2014.11721691.

[Sch91] C.-P. Schnorr. "Efficient signature generation by smart cards". In: Journal of cryptology 4.3 (1991), pp. 161–174. DOI: 10.1007/BF00196725.

[SPVK04] A. Seshadri, A. Perrig, L. Van Doorn, and P. Khosla. "SWATT: Software-based attestation for embedded devices". In: *IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004*. IEEE. 2004, pp. 272–282. DOI: 10.1109/SECPRI.2004.1301329.

[SL16] R. V. Steiner and E. Lupu. "Attestation in wireless sensor networks: A survey". In: *ACM Computing Surveys (CSUR)* 49.3 (2016), pp. 1–31. DOI: 10.1145/2988546.

[Thi18] F. Thiel. "Digital transformation of legal metrology-The European Metrology Cloud". In: *OIML Bulletin* 59.1 (2018), pp. 10–21. https://www.oiml.org/en/publications/bulletin

[WEL20] WELMEC. Welmec 7.2: Software Guide (Measuring Instruments Directive 2014/32/EU). 2020. https://www.welmec.org/guides-and-publications/guides.

[YWZC07] Y. Yang, X. Wang, S. Zhu, and G. Cao. "Distributed software-based attestation for node compromise detection in sensor networks". In: *2007 26th IEEE International Symposium on Reliable Distributed Systems (SRDS 2007)*. IEEE. 2007, pp. 219–230. DOI: 10.1109/SRDS.2007.31.

[BeaconBR] INMETRO. *INMETRO Randomness Beacon*. https://beacon.inmetro.gov.br/.

[BeaconCL] UChile. *Randomness Beacon — RandomUChile*. https://random.uchile.cl/en/randomness-beacon/.

[BeaconUS] NIST. *NIST Randomness Beacon*. https://beacon.nist.gov.

[FIPS 180-4] National Institute of Standards and Technology (2015). *Secure Hash Standard (SHS)*. (U.S. Department of Commerce, Washington, D.C.) Federal Information Processing Standards Publication (FIPS PUBS) 180-4. Aug. 2015. DOI: 10.6028/NIST.FIPS.180-4.

[FIPS 186-5] National Institute of Standards and Technology (2015). *Digital Signature Standard (DSS)*. (U.S. Department of Commerce, Washington, D.C.) Draft Federal Information Processing Standards Publication (FIPS PUBS) 186-5. Oct. 2019. DOI: 10.6028/NIST.FIPS.186- 5-Draft.

[RFC 5280] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". In: *RFC*. Request for Comments 5280.5280 (May 2008), pp. 1–151. DOI: 10.17487/RFC5280.

[RFC 7748] A. Langley, M. Hamburg, and S. Turner. "Elliptic Curves for Security". In: *RFC*. Request for Comments 7748.7748 (Jan. 2016), pp. 1–22. DOI: 10.17487/RFC7748.

[RFC 8446] E. Rescorla. "The Transport Layer Security (TLS) Protocol Version 1.3". In: *RFC*. Request for Comments 8446.8446 (Aug. 2018), pp. 1–129. DOI: 10.17487/RFC8446.

[SP 800-186] L. Chen, D. Moody, A. Regenscheid, and K. Randall. Recommendations for Discrete Logarithm-Based Cryptography: Elliptic Curve Domain Parameters. (U.S. Department of Commerce) National Institute of Standards and Technology. Draft NIST Special Publication (SP) 800-186. Oct. 2019. DOI: 10.6028/NIST.SP.800-186-draft

[ZKProof] ZKProof (many contributors). *ZKProof Community Reference. Version 0.2*. Editors: D. Benarroch, L.T.A.N. Brandão, E. Tromer. 2019. https://zkproof.org.

OIML Certification System (OIML-CS)

Introduction

The OIML-CS is a system for issuing, registering and using OIML Certificates and their associated OIML type evaluation reports for types of measuring instruments (including families of measuring instruments, modules, or families of modules), based on the requirements of OIML Recommendations.

The OIML-CS comprises two Schemes: Scheme A and Scheme B. Competence of the OIML Issuing Authorities and their Test Laboratories is demonstrated through self-declaration under Scheme B and accreditation or peer assessment under Scheme A.

The aim of the OIML-CS is to facilitate, accelerate and harmonize the work of national and regional bodies that are responsible for type evaluation and approval of measuring instruments subject to legal metrological control. In the same way, instrument manufacturers, who are required to obtain type approval in some countries in which they wish to sell their products, should benefit from the OIML-CS as it will provide evidence that their instrument type complies with the requirements of the relevant OIML Recommendation(s).

It is a voluntary system and OIML Member States and Corresponding Members are free to participate. Participating in the OIML-CS commits, in principle, the signatories to abide by the rules of the OIML-CS that are established in OIML B 18:2018 *Framework for the OIML Certification System (OIML-CS)*. Signatories voluntarily accept and utilize OIML type evaluation and test reports, when associated with an OIML Certificate issued by an OIML Issuing Authority, for type approval or recognition in their national or regional metrological controls.

The OIML-CS was launched on 1 January 2018 and has replaced the former OIML Basic Certificate System and the OIML Mutual Acceptance Arrangement (MAA).

Further information can be found at:

https://www.oiml.org/en/oiml-cs

For enquiries regarding the OIML-CS, please contact the OIML-CS Executive Secretary Paul Dixon (executive.secretary@oiml.org).

OIML certificates

OIML certificates issued under Scheme A and Scheme B can be downloaded from the database on the OIML website at https://www.oiml.org/en/oiml-cs/certificat_view.

The database also includes certificates issued under the former OIML Basic Certificate System and the MAA. Although these two systems are no longer in operation, the certificates remain valid.

OIML Issuing Authorities, Utilizers and Associates

A summary of the approved OIML Issuing Authorities is published on the next page, followed by a summary of those Utilizers and Associates that have declared that they will accept OIML certificates and/or OIML type evaluation reports as the basis for a national or regional approval.

OIML Certification System (OIML-CS)

List of OIML Issuing Authorities and their scopes

The list of OIML Issuing Authorities is published in each issue of the OIML Bulletin and can be downloaded at www.oiml.org/oiml-cs/oiml-issuing-authorities

Updated: 2021-07-05

		R 21:2007	R 46:2012	R 49:2006	R 49:2013	R 50:2014	R 51:2006	R 60:2000	R 60:2017	R 61:2004	R 61:2017	R 75:2002	R 76:1992	R 76:2006	R 85:2008	R 99:2008	R 106:2011	R 107:2007	R 117:1995	R 117:2007	R 117:2019	R 126:1998	R 129:2000	R 134:2006	R 137:2012	R 139:2014	R 139:2018
AU1	National Measurement Institute Australia (NMIA)												■	■													
CH1	Federal Institute of Metrology (METAS)							■						■													
CN2	National Institute of Metrology, China (NIM)						■	■	■	■	■		■	■													
CZ1	Czech Metrology Institute (CMI)				■		■				■			■						■	■				■		
DE1	Physikalisch-Technische Bundesanstalt (PTB)				■		■	■	■	■		■		■													
DK2	FORCE Certification A/S				■	■	■	■	■	■	■			■			■	■					■	■	■		
FR2	Laboratoire National de Métrologie et d'Essais (LNE)			■	■		■	■	■					■								■					
GB1	NMO				■		■	■	■				■	■						■	■						
JP1	NMIJ/AIST							■	■				■	■					■	■	■						
NL1	NMi Certin B.V.	■	■	■	■	■	■	■	■	■	■		■	■	■			■	■	■	■		■	■	■	■	■
SE1	Research Institutes of Sweden (RISE)						■	■	■	■	■			■	■				■	■	■						
SK1	Slovak Legal Metrology (SLM)			■	■									■													

OIML Certification System (OIML-CS)

List of Utilizers, Associates and their scopes

The list of Utilizer and Associate scopes is published in each issue of the OIML Bulletin and can be downloaded at www.oiml.org/oiml-cs/utilizers-and-associates

Updated: 2021-06-29

1 = Scheme A only **5 = Scheme B only**
2 = Scheme A and MAA
3 = Scheme A and B
4 = Scheme A, B and MAA

		R 21:2007	R 35:2007	R 46:2012	R 49:2006	R 49:2013	R 50:2014	R 51:2006	R 58:1998	R 59:2016	R 60:2000	R 60:2017	R 61:2004	R 61:2017	R 75:2002	R 76:1992	R 76:2006	R 81:1998	R 85:2008	R 88:1998	R 93:1999	R 99:2008	R 102:1992	R 104:1993	R 106:2011
AU	National Measurement Institute, Australia (NMIA)				1	1					1					1	1								
BE	Federal Public Service Economy	3		3		3	3	3			1		3		3		1		3			3			3
CA	Measurement Canada										2	1			1		2								
CH	Federal Institute of Metrology (METAS)			1	2	2	1	1			2		1		1		2								1
CN	State Administration for Market Regulation (SAMR)							1			2	1	1	1		2	2								
CO	Superintendencia de Industria y Comercio (SIC)	3		3	4	4	3	3			2		3		3	2	2		3			3			3
CU	Oficina Nacional de Normalizacion (NC)	3	3	1		1	3	1	3	3	1	1	3	3	3		1	3	3	3	3	3	3	3	3
CZ	Czech Metrology Institute (CMI)					1		1						1			1								
DE	Physikalisch-Technische Bundesanstalt (PTB)	5		3	3	4	3	3			2		3		3		2					5			1
DK	FORCE Certification A/S				2	2	1	1			2	1	1	1			2								1
FR	Laboratoire National de Métrologie et d'Essais (LNE)	1		1	1	1	1	1			1		1		1	1	1		1			1			1
GB	NMO Certification	3			4	4	3	3			2		3			2	2		3						3
IN	Legal Metrology Division, Department of Consumer Affairs	3		3		4	3	3			2		3		3		2		3						1
IR	Iran National Standards Organization (INSO)				4	4					2	1				2	2								
JP	NMIJ/AIST										2	1				2	2								
KE	Weights and Measures Department		3	3	4	4		3			4	4	3	3		4	4		3						3
KH	National Metrology Centre (NMC)	3		3	3	3	3	3			1		3		3	1	1		3			3			3
KI	Ministry of Commerce, Industry and Cooperatives	5	5	5	1	1	5	1		5	1	1	5	5	5	1	1	5	5						5
KR	Korea Testing Certification (KTC)															2	2								
LV	LNMC Ltd. Metrology Bureau																								
NA	Namibian Standards Institution			3	4	4	3	3			2		3			2	2		3						3
NL	NMi Certin B.V.	3		3	3	4	3	3			2	1	3	3	3	1	2		3			3			3
NZ	Trading Standards (Ministry of Business, Innovation and Employment) (MBIE)				4	4	3	3			2					2	2		3						3
RU	VNIIMS																								
RW	Rwanda Standards Board	3	3	3	3	3		3	3	3	1	1	3	3		1	1					3	3	3	3
SA	SASO (Saudi Standards, Metrology and Quality Organization)			3		1						1					1								
SE	RISE Research Institutes of Sweden AB							3			2	1	3				2		3						
SK	Slovak Legal Metrology (SLM)				2	2											2								
TN	National Agency of Metrology (ANM)	3		3	2	2	3	3			2		3				2		3			3			3
UG	Uganda National Bureau of Standards (UNBS)			3	1	3					1	1				1	1								
US	National Conference on Weights and Measures (NCWM)										2														
ZA	NRCS: Legal Metrology				3	3		3			1					1	1		3						3
ZM	Zambia Metrology Agency	3		3	3	3	3	3			1		3		3	1	1		3			3			3

OIML Certification System (OIML-CS)

List of Utilizers, Associates and their scopes (Cont'd)

The list of Utilizer and Associate scopes is published in each issue of the OIML Bulletin and can be downloaded at www.oiml.org/oiml-cs/utilizers-and-associates

Updated: 2021-06-29

1 = Scheme A only
2 = Scheme A and MAA
3 = Scheme A and B
4 = Scheme A, B and MAA
5 = Scheme B only

		R 107:2007	R 110:1994	R 117:1995	R 117:2007	R 117:2019	R 122:1996	R 126:1998	R 128:2000	R 129:2000	R 129:2020	R 133:2002	R 134:2006	R 136:2004	R 137:2012	R 139:2014	R 139:2018	R 143:2009	R 144:2013	R 145:2015	R 146:2016	R 148:2020	R 149:2020	R 150:2020
AU	National Measurement Institute, Australia (NMIA)																							
BE	Federal Public Service Economy	3			3					3					3	3								
CA	Measurement Canada																							
CH	Federal Institute of Metrology (METAS)	1						1		1			1		1									
CN	State Administration for Market Regulation (SAMR)																							
CO	Superintendencia de Industria y Comercio (SIC)	3		3	3			3		3			3		3	3								
CU	Oficina Nacional de Normalizacion (NC)	3	3		3		3	3	3	3		3	3	3	3	3	3	3	3	3	3			
CZ	Czech Metrology Institute (CMI)				1	1									1									
DE	Physikalisch-Technische Bundesanstalt (PTB)	3			3	1				3			1	5	3									
DK	FORCE Certification A/S	1			1	1				1	1		3		1									
FR	Laboratoire National de Métrologie et d'Essais (LNE)	1			1			1		1			1		1	1								
GB	NMO Certification	3		3	3					3			3											
IN	Legal Metrology Division, Department of Consumer Affairs	3			3					3			1		3	3								
IR	Iran National Standards Organization (INSO)																							
JP	NMIJ/AIST			1	1	1																		
KE	Weights and Measures Department			3	3			3					3	3	3	3	3							
KH	National Metrology Centre (NMC)	3		3	3			3		3			3		3	3								
KI	Ministry of Commerce, Industry and Cooperatives		5	1	1							5	5		5	5	5							
KR	Korea Testing Certification (KTC)																							
LV	LNMC Ltd. Metrology Bureau							3					3											
NA	Namibian Standards Institution	3		3	3			3		3			3											
NL	NMi Certin B.V.	3		3	3	1		3		3			3		3	3	3							
NZ	Trading Standards (Ministry of Business, Innovation and Employment) (MBIE)	3		3	3					3			3											
RU	VNIIMS			3	3																			
RW	Rwanda Standards Board		3	3	3		3	3		3		3	3		3			3	3		3			
SA	SASO (Saudi Standards, Metrology and Quality Organization)				3																			
SE	RISE Research Institutes of Sweden AB			3	3																			
SK	Slovak Legal Metrology (SLM)																							
TN	National Agency of Metrology (ANM)	3		3	3			3		3			3		3	3								
UG	Uganda National Bureau of Standards			1	1	1							3		3									
US	National Conference on Weights and Measures (NCWM)																							
ZA	NRCS: Legal Metrology	3		3	3			3		3			3		3	3								
ZM	Zambia Metrology Agency	3		3	3			3		3			3		3	3								

COOMET

31st COOMET Committee meeting and Webinar "30 years to COOMET"

15–17 June 2021 (online)

VALERY HUREVICH, COOMET President
NADEZHDA LIAKHOVA, Head of COOMET Secretariat

2021 is the year of the 30th anniversary of COOMET's establishment because on 12 June 1991 the COOMET Memorandum of Understanding was signed in Warsaw, Poland.

On 15–17 June 2021 events took place associated with this anniversary date.

Working session

The Working session of the 31st COOMET Committee meeting was held on 15 June 2021, at which COOMET Committee members or their official representatives from 14 countries (Armenia, Azerbaijan, Belarus, Bulgaria, Georgia, Germany, Kazakhstan, Moldova, P.R. China, Russian Federation, Slovakia, Tajikistan, Turkey, Ukraine) took part.

Based on the discussion of events to improve the work of COOMET, the following resolutions and actions were adopted:

- the updated COOMET Document D2/2021 "COOMET Rules of Procedure" was approved (the amendments are related to establishing the possibility of holding COOMET events online and a more detailed procedure for voting on agenda items, possibility of an algorithm for making decisions on behalf of the COOMET Committee based on the results of electronic voting, as well as refining the work procedure with COOMET projects and approaches to drawing up and submission of the annual reports of COOMET structural bodies (CSBs), etc.);
- the updated COOMET Document D5/2021 "Model Regulations for COOMET Structural Bodies" was approved (requirements were set for a quorum at CBSs meetings, etc.);
- approach to conducting a survey to assess the effectiveness of the work of CSBs and a draft questionnaire prepared by the COOMET Secretariat were adopted (an online survey will be organized from June to October 2021 – respondents will be the COOMET Committee members and CSB members);
- COOMET criteria were adopted for COOMET member countries to be classified as countries with emerging metrology systems (CEEMS);
- the organizational structure of COOMET was updated (subcommittees were excluded from the structure of TC 1.5 "Length and angle" and TC2 "Legal Metrology" and meanwhile fields of activities in legal metrology were identified with simultaneous appointment of coordinators of those fields).

An updated membership of the Working Group for Strategy was approved at the meeting, and a decision was made to hold further consultation to define the positions of COOMET member countries on the issues concerning the possible change of the institutional status, criteria for membership in COOMET, issues of funding of COOMET activities (organizers: COOMET President and Secretariat, timeframe for consultations: from June to September 2021). It was agreed to hold an extraordinary online COOMET Committee meeting for preliminary discussion of a selection of the above issues in autumn 2021.

Preparation of the Final report and a Roadmap with proposals on the implementation of the tasks of the WG for Strategy will be completed in December 2021, so as to discuss the results obtained at the COOMET Committee meeting in 2022 and decide on the appropriateness of changing the institutional status of COOMET.

The issues were considered concerning the extension of the terms of office of the current Chairs of TC 1.6 "Mass and Related Quantities", TC 1.8 "Physical Chemistry", TC 1.10 "Thermometry and Thermal Physics", SC 4.2 "COOMET Informational Resources" and SC 4.3 "Raising Proficiency Level and Work with Young Metrologists".

New Chairs of TC 1.3 "Electricity and Magnetism" (Marina Yarmolovich, BelGIM, Belarus), TC 2 "Legal Metrology" (Yuriy Kuzmenko, Ukrmetrteststandart, Ukraine) and SC 1.6.2 "Force" (Aleksandr Tsiporenko, Ukrmetrteststandart, Ukraine) were appointed until June 2025, and an updated list of COOMET auditors on

peer reviews of QMS of COOMET NMIs/DIs was approved (new auditor: Viktoriya Skachyok, BelGIM, Belarus).

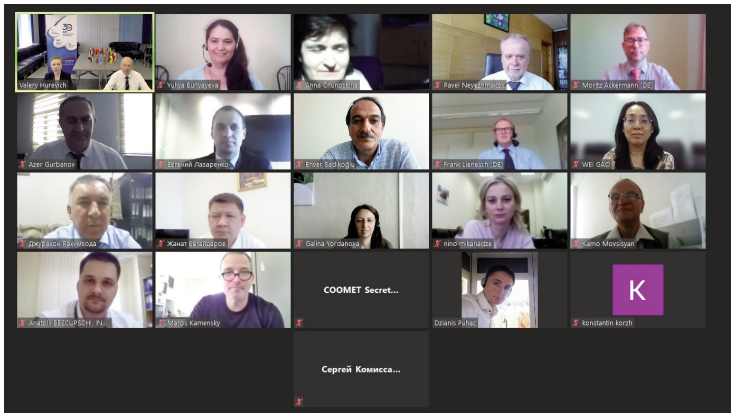
For their considerable personal contribution to the work and activities of COOMET, the Distinguished Title "Honorary Metrologist of COOMET" was given to the following experts of the organizations of COOMET member countries: Azer Gurbanov (Azerbaijan); Petr Krivonos (Belarus); Teodor Birsa (Moldova); Nikolay Moiseev (Russia).

The COOMET Committee approved the nominees for the positions of COOMET Vice-Presidents, proposed by COOMET President for a new term of his office (from 2021 to 2024), namely:

Direction of activities	Name of COOMET Vice-President
Cooperation in the field of measurement standards. Joint scientific research	Evgeny Lazarenko (Russia)
Cooperation in the field of legal metrology	Frank Lienesch (Germany)
Cooperation in the field of development and peer review of quality management systems	Nino Mikanadze (Georgia)
Cooperation with regional metrology organizations. Information and knowledge transfer	Pavel Neyezhmakov (Ukraine)
Cooperation with countries with emerging metrology systems	Zhanat Begaidarov (Kazakhstan)

Plenary session

The Plenary session of the 31st COOMET Committee meeting was held on 16–17 June 2021, at which representatives of 18 COOMET member countries (Armenia, Azerbaijan, Belarus, Bosnia and Herzegovina, Bulgaria, Georgia, Germany, Kazakhstan, Kyrgyzstan, Lithuania, Moldova, P.R. China, Russian Federation, Slovakia, Tajikistan, Turkey, Ukraine, Uzbekistan) took part. Representatives of international organizations (BIPM, OIML) and regional organizations (APMP, APLMF, EURAMET, WELMEC, SIM, NCSL International and EASC) also participated in the meeting and gave presentations on their activities in 2020–2021.



The COOMET President presented a report on the results of activities for the three years during which he had performed his duties as President, and about the tasks of COOMET for his new term of office. The Head of the COOMET Secretariat presented the Annual report with an analysis of COOMET activities in 2020–2021.

The COOMET Committee approved the updated Roadmap for the implementation of resolutions related to the redefinition of the SI base units for 2021–2025 as a COOMET Program P6/2021.

In addressing the issue of the implementation of the CIPM MRA, information about the 42nd and 43rd JCRB meetings was presented, as well as a report on the activities of the COOMET Joint Committee for Measurement Standards (with an analysis of the current state of preparation, review and publication in the KCDB of CMC entries of NMIs and DIs of COOMET member countries and implementation of the COOMET Program of comparisons).

The annual report on the activities of the Quality Forum and TC 3.1 "Quality Forum Technical Committee" was also presented, which included information about the implementation of the document "Policy and Plan of COOMET TC 3.1 "Quality Forum Technical Committee" related to the transition to ISO

17034:2016 and ISO/IEC 17025:2017 for peer reviews of QMS of COOMET NMIs and Dis", results of the peer reviews of the QMS of Russian, Kazakhstan, Belarusian and Ukrainian NMIs/DIs and the schedule of peer reviews of the QMS of other NMIs/DIs for 2021.

During the COOMET Committee meeting, the issues of cooperation in the field of legal metrology were also considered. The Committee approved the Work Program of TC 2 "Legal Metrology" for 2021–2023 (COOMET P3/2021) and also supported proposals of TC2 in terms of optimization of the structure of TC 2. In particular, the following fields of cooperation within TC 2 were endorsed:

- "Measuring devices in legal metrology" (coordinator: M. Shabanov, BelGIM, Belarus);
- "Measuring systems in legal metrology" (coordinator: A. Krichevets, DP NDI "Systema", Ukraine);
- "Medical equipment with measuring functions" (coordinator: N. Raymjonov, UzNIM, Uzbekistan);
- "Conformity assessment of measuring instruments" (coordinator: I. Pototskiy, Ukrmetrteststandart, Ukraine);
- "Digitalization in legal metrology" (coordinator: P. Ulbig, MEN, Germany).

At the next TC 2 meeting (28–29 September 2021) the concept of further work and the subject of cooperation in the above fields will be discussed.

With regard to COOMET activities in 2020–2021 the following can be highlighted:

- Holding of a COOMET webinar "Role of measurement uncertainty in conformity assessment decisions in legal metrology" (6 April 2021, number of participants – over 120).
- Update of information about the legal metrology systems in COOMET member countries in view of the latest changes in the legislation and its posting on the COOMET web-portal:
  (https://www.coomet.net/activities/legal-metrology/lm-in-coomet-countries/).
- Preparation of a COOMET Plan for translation of OIML publications into Russian (a draft plan is an integral part of the Work Program of TC2 for 2021–2023) – currently work on translation of the following publications has started: OIML D 1:2020, ILAC-G24/OIML D 10:2007, OIML D 11:2013, OIML D 30:2020, OIML D 31:2019, OIML D 32:2018, OIML D 33:2019, OIML R 75-3:2006, OIML R 125:1998, OIML R 137-1/2:2012 with Amendment to OIML R 137-1/2 (2014), OIML R 137-3:2014, OIML G 14:2011. The translation of OIML publications should be the highest priority for TC2, since translations prepared by COOMET can further be used for the development of COOMET Recommendations and/or be put into working practice in COOMET member countries by issuing national normative legal acts or national standards.
- Translation of the UNIDO-OIML Brochure "Certification of measuring instruments".

Following the discussion of COOMET activities in the field of information and training of metrologists, the Committee approved the Work Program of TC 4 "Information and training" for 2021–2023 (COOMET P4/2021) and adopted the Plan of training activities of COOMET for 2021.

The COOMET Committee adopted the Schedule of updates of COOMET publications for 2021–2024 and approved the following COOMET publications, prepared and updated in 2020–2021:

- Recommendation R/GM/11:2021 "Regulations for Comparisons of Measurement Standards from the NMIs/DIs of COOMET";
- Recommendation R/GM/12:2021 "Rules of Maintaining of Foregoing COOMET Program of Comparisons";
- Recommendation R/GM/7:2021 "Procedure for an Intra-regional Review of Calibration and Measurement Capabilities of COOMET NMIs/DIs and an Inter-regional Review of Calibration and Measurement Capabilities of NMIs/DIs of Other RMOs";
- COOMET Recommendation "Temporary rules and procedure for peer reviews of quality management systems of National metrology institutes/Designated institutes (QMS of NMIs/DIs) during the COVID-19 pandemic" (new);
- Information material "About remote calibrations of measurement standards of COOMET NMIs" (new);
- Information material "Organization of the sphere of state regulation in the field of legal metrology in the COOMET member countries" (new);
- COOMET Document D5.18/2021 "Regulation on the COOMET Quality Forum",

as well as updated regulations on a number of COOMET Technical Committees (TC 1.1 "General Metrology" (General Questions Concerning Measurements), TC 1.4 "Flow Measurement", TC 1.9 "Ionizing Radiation and Radioactivity", TC 4 "Information and Training").

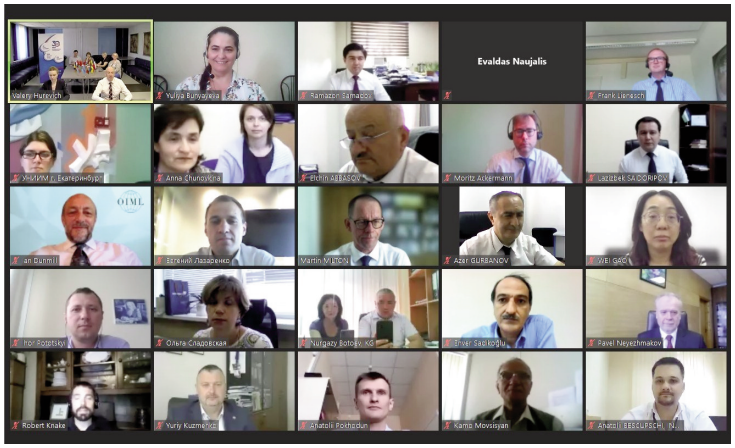
The Committee highlighted the relevance of work on the preparation of a Concept for application of digital technologies in metrology within COOMET (COOMET project 825/BY/21) and requested the COOMET Secretariat to organize an online meeting of the WG for the project in June–July 2021.

The Committee supported the proposal of the COOMET Secretariat, in which firstly COOMET Committee members are requested to send videos on issues of metrology, and secondly the organizers of COOMET training events are requested to record webinars, all of

which will be posted on the official COOMET YouTube channel.

Representatives of national metrology organizations, which are COOMET members, presented information about the state of metrological activities in their countries.

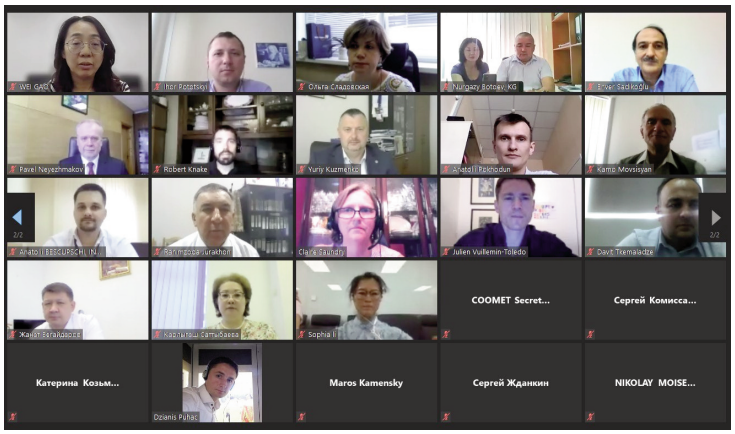
In view of the resolution adopted at the Working session to hold the 32nd extraordinary COOMET Committee meeting on 26 October 2021 (online on the Zoom platform), it was agreed that the dates and format of the 33rd meeting will be specified in October 2021 (taking into account the situation with the Covid-19 pandemic).



Webinar "30 years to COOMET"

On the occasion of the 30th Anniversary of COOMET's establishment, a webinar "30 years to COOMET" was held on 15 June 2021. The following reports were presented during the webinar:

- The history of COOMET's creation and development (V. Belotserkovsky (Russia), N. Zhagora (Belarus) - Former COOMET Presidents);
- Results of COOMET's cooperation in 2012–2017 (V. Krutikov, Russia - Former COOMET President);
- 30 years cooperation of PTB within COOMET - a personal view (M. Kochsiek, Germany);
- The role of COOMET in the development of the metrology infrastructure of countries and economies with emerging metrology systems on the example of Uzbekistan (L. Saidoripov, Uzbekistan);
- COOMET & GEOSTM: success story for organization and persons (N. Mikanadze, Georgia);
- Contribution of NMIs of COOMET member countries to the implementation of the CIPM MRA and to BIPM activities (M. Milton, Director of the BIPM);
- COOMET and the OIML: 30 years of cooperation and future opportunities (A. Donnellan, Director of the BIML);
- COOMET: results, strategy and prospects of cooperation (V. Hurevich, COOMET President, Belarus);
- Digital transformation of the system for ensuring the uniformity of measurements in the Russian Federation (E. Lazarenko, Russia);
- Digital SI and challenges of modern metrology (P. Neyezhmakov, Ukraine).



Over 80 specialists from 14 countries (Azerbaijan, Belarus, Georgia, Germany, Kazakhstan, Kyrgyzstan, Lithuania, Moldova, P.R. China, Russian Federation, Slovakia, Tajikistan, Ukraine, Uzbekistan) took part in the Webinar, as well as representatives of EURAMET and EASC. ■

COOMET

Ninth International Competition: "The Best Young Metrologist of COOMET 2021"

21–22 April 2021 (online)

PROF. PAVEL NEYEZHMAKOV,
COOMET Vice-President
MRS. YULIYA BUNYAYEVA,
National COOMET Secretariat in Ukraine

The Ninth International Competition "The Best Young Metrologist of COOMET" was held online from 21–22 April 2021.

The history of the competition dates back to 2005, and is open to specialists up to and including the age of 35 who work in the field of scientific and applied metrology at NMIs or other metrology institutions of COOMET Member Countries, independently of their academic degree and position.

In 2013, following the first four successful Competitions, when organising the Fifth Competition it was decided to expand the boundaries by inviting young metrologists from other regional metrology organizations to participate. English was chosen as the Competition language, as it was acceptable to all the participants, and English is also the second working language in COOMET.

Following the results of the Fifth Competition, in which 25 young metrologists from COOMET, EURAMET, AFRIMETS, and APMP took part, it was decided to allow representatives from other RMOs to participate in every second Competition.

The Ninth International Competition "The Best Young Metrologist of COOMET 2021" therefore included participants representing other RMOs. Taking into account the COVID-19 situation, it was decided to hold the competition online via the Zoom platform since this platform allows polls and votes (including secret votes) to be held, and it also provides the possibility to organize simultaneous interpretation.

Organizing the Competition is one of the areas of activities of COOMET TC 4 *Information and Training*. TC 4 also developed COOMET Recommendation R/GM/18:2020 *Procedure for the International Competition "The Best Young Metrologist of COOMET"*. According to this Recommendation, full texts of the competitors' papers with abstracts and registration forms are submitted at least one year and two months before the date of the competition. After the end of the acceptance period, the papers are sent for consideration to the members of Scientific Committee, and the abstracts are posted on the information resources of COOMET.

For the Ninth Competition, 18 papers were selected from COOMET (Belarus, Kazakhstan, Germany, Russia, Ukraine), EURAMET (Italy), and SIM (Colombia, Mexico).

The Scientific Committee includes representatives of International (BIPM, OIML) and Regional (COOMET, AFRIMETS, EURAMET, SIM) metrology organizations, namely:

- *Chairperson of the Scientific Committee* – Pavel Neyezhmakov (COOMET, Ukraine);
- *Members of the Scientific Committee* – Valery Hurevich, Nikolay Zhagora (COOMET, Belarus), Sergey Golubev, Anna Chunovkina (COOMET, Russia), Nino Mikanadze (COOMET, Georgia), Andrey Surzhykov (COOMET, Germany), Chingis Kuanbayev (BIPM), Ian Dunmill (BIML), Mohamed Amer (AFRIMETS, Egypt), Maria Luisa Rastello (EURAMET, Italy), Aigar Vaigu (EURAMET, Estonia), Rodrigo Felix (SIM, Brazil);
- *Secretary of the Scientific Committee* – Ekaterina Kozmina (COOMET, Russia).

The evaluation of the papers was carried out according to five criteria, grouped into two categories – innovation of the paper (relevance and scientific novelty of the paper (implementation); practical significance of the paper; practical use and implementation of the results of the paper), as well as the quality of its design and presentation.

The winners of the competition are determined by two nominations: in the field of scientific metrology and in the field of applied metrology.

Each member of the Scientific Committee, during and/or after hearing each participant's presentation, assigned points from 1 to 5 for each of the five criteria and entered them into an Excel table.

After hearing all the papers presented in the Competition, each member of the Scientific Committee then entered the final point for each participant in the online summary table (Google Forms).

After the evaluation and after assigning the final points, a lively discussion took place. The following participants were recognized as being the winners of the Ninth Competition:

- Gianluca Milano (EURAMET, INRIM, Italy) for the best report in the field of scientific and fundamental metrology;
- Mutaib Zackaria (COOMET, PTB, Germany) for the best report in the field of applied metrology.

Special nominations for second and third places were awarded to the following participants:

- Gleb Belotelov (COOMET, VNIIFTRI, Russia) – second place;
- Rustam Tukhvatullin (COOMET, VNIIR, Russia) – third place.

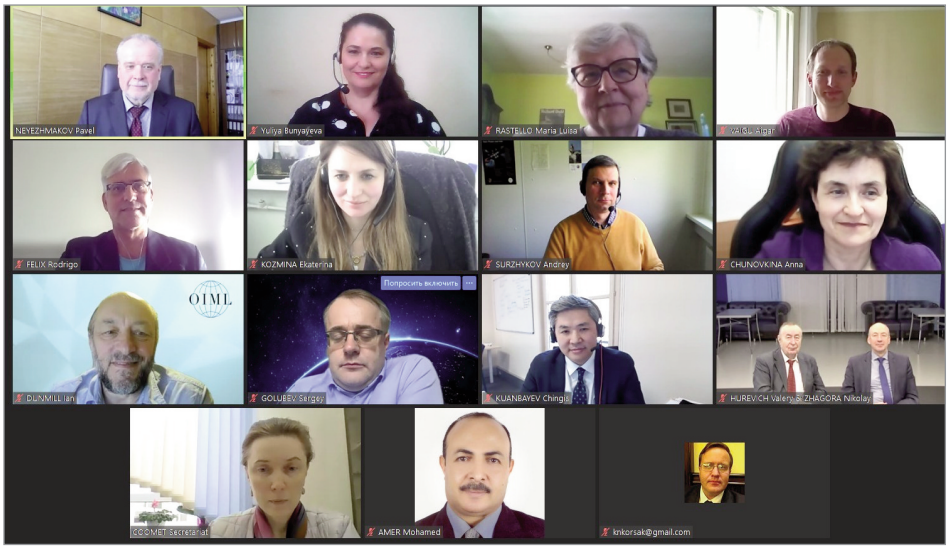
All nine Competitions have very clearly shown that this regional activity has a very high standard, and consists not only in demonstrating one's own capabilities but also in building friendship as well as developing and intensifying scientific and personal contacts between young scientists around the world. Another remarkable result of the series of Competitions is the continuously increasing quality of the papers and presentations.

Meanwhile, all the young scientists who participated in the Competition have taken the opportunity to demonstrate their professional skills and to exchange knowledge and experience. They accepted the challenge and the Scientific Committee, after a meticulous evaluation of the work presented, expressed confidence that many of the young metrologists would become the leading scientists of the future and the pride of their NMIs.

We would like to thank the Head of the COOMET Secretariat Nadezhda Liakhova (BelGIM, Belarus) and the Chairperson of COOMET SC 4.3 *Raising Proficiency Level and Work with Young Metrologists* Ekaterina Kozmina (VNIIMS, Russia) for their technical and organizational support in the competition.

Prof. Pavel Neyezhmakov
CIPM Member
COOMET Vice-President
Chairperson of TC 4 *Information and Training*
General Director of the NSC *Institute of Metrology*
(Kharkov, Ukraine)

Mrs. Yuliya Bunyayeva
National COOMET Secretariat in Ukraine
Secretary of TC 4
COOMET Coordinator in the BIPM CBKT Programme
Head of the Scientific & Research Laboratory of the International Cooperation and Information Technologies of NSC *Institute of Metrology*
(Kharkov, Ukraine)



Promotion of the OIML Bulletin: Become a Mentor

The OIML Bulletin is one, if not the only, international publication dedicated to legal metrology topics.

In accordance with CIML Resolutions 2019/30 and 2020/21, there is a clear desire for the Bulletin to be an attractive publication for legal metrology worldwide, and for it to be an excellent advertisement for our Organisation.

This can be achieved through long-term planning of the future editions and identification of key topics of high interest, for instance, legal control of measuring instruments in the fields of energy, health and the environment, where important aspects such as new technology, legal requirements, or test/verification procedures will be addressed.

In addition, support is sought from CIML Members and Corresponding Member Representatives who are ready to take on the responsibility of acting as "**Mentors**" for certain key topics / editions and technical articles. These are not necessarily expected to be written by the "**Mentors**" themselves, but by experts that a "**Mentor**" has identified and contacted.

In order to identify key topics of significant interest and "**Mentors**" to lead them, it was proposed by the CIML President that the BIML prepares, and makes publicly available on the OIML website, a plan for the upcoming eight to ten editions of the Bulletin.

The table on the following page is intended to be "dynamic", i.e. proposed key topics may be moved to other editions depending on available "**Mentors**" and authors for technical articles. The table can also be found at www.oiml.org/en/publications/bulletin/future-editions.

All CIML Members and Corresponding Member Representatives are encouraged to support the OIML Bulletin, to share their legal metrology experiences with the legal metrology community worldwide, and to take responsibility either as a "**Mentor**" for one of the next editions of the Bulletin, or by promoting it at TC/SC/Project Group meetings, RLMO meetings, CEEMS AG meetings, and other opportunities.

CIML Members and Corresponding Member Representatives who would like to be a "**Mentor**" for a specific edition / key topic, or who would like to suggest that a new key topic be added to the list, are asked to contact the BIML (chris.pulham@oiml.org).

Edition	General key topic	Mentor	Article submission #1	Article submission #2	Article submission #3	Other
October 2021	Health		Medical instruments / devices with metrological functions			
2022	(Metrology for protecting the) Environment					
	National / Regional Metrology Systems					
	Measurement related to traffic	PTB/ METAS	Speed meters (overview of current technologies)	Soot particle measurement	Smart metering, e-vehicle charging	
	Training of inspectors / verification officers		E-Learning material already available	Revised OIML D 14		
	Pre-packages / Statistical control	Some RLMOs?	Theoretical principles / basics	Various systems in different regions	Report on OTE 2022 in Bad Reichenhall (DE)	
	Intellectual property		Role of patents in legal metrology			

Trust your measurements!

CIM2021 Programme

The **International Metrology Congress will be held on 7-9 September in Lyon (France),** in partnership with Measurement World exhibition and on the same dates and location as Global Industrie exhibition.

The Congress is dedicated to the best industrial practices, and advances in R&D applied to measurements, analysis and testing processes: this unique meeting is the meeting between science, industry and institutional organisations of metrology.

> "This year marks the 20th event in this tremendous series, and it includes more than ever currents trends and a sneak preview into future innovations. The three tracks represent the global grand challenges. The metrology community supports the development of solutions for these challenges, in particular by ensuring that we can trust in measurements!"
>
> Sascha Eichtaedt, PTB (Germany) and Daniel Jullien, Digiplant Consulting (France), co-chairs of the CIM2021

What's new ?

- **Industry 4.0, Green Deal and Health**: the three main tracks for 2021
- The CIM2021 will also be an opportunity for new experiences with a **hybrid part,** videos and live presentations will be available on a dedicated platform
- The **Metrology Village** in the heart of Measurement World and for the first time associated to Global industrie. The topics linked to Industry 4.0 are common. The exhibition gives new opportunities to meet professionals and develops solutions.

The programme

The International Metrology Congress includes **200 technical presentations and 6 Round Tables:**

This is the opportunity to discover recent advances in various technical fields:

- mechanics, electromagnetism, flow, temperature, photonics, chemistry, biology but also data, AI, statistics, quantum technologies…
- And their implication in the key applications, also in the measurement process: quality, accreditation, conformity and risks, cost optimisation…

Topics to be developed during the Round Table session:

- Metrology in the **digital age**
- The role of **Metrology and Quality infrastructures** in the transition to Industry 4.0
- **Shopfloor measurement** challenges
- **Trust in health measurement**: new challenges
- **Industry emissions**: metrology support to achieve the new requirements
- New skills for the **future of metrology**

The repartition of the participants is:

- **70 % of industrial end-users** from all sectors and from laboratories
- 30 % organisations, academics and researchers

Link to the full programme:
https://www.cim2021.com/programme-congres-international-metrologie-2021.html

ORGANISERS, PARTNERS AND SPONSORS

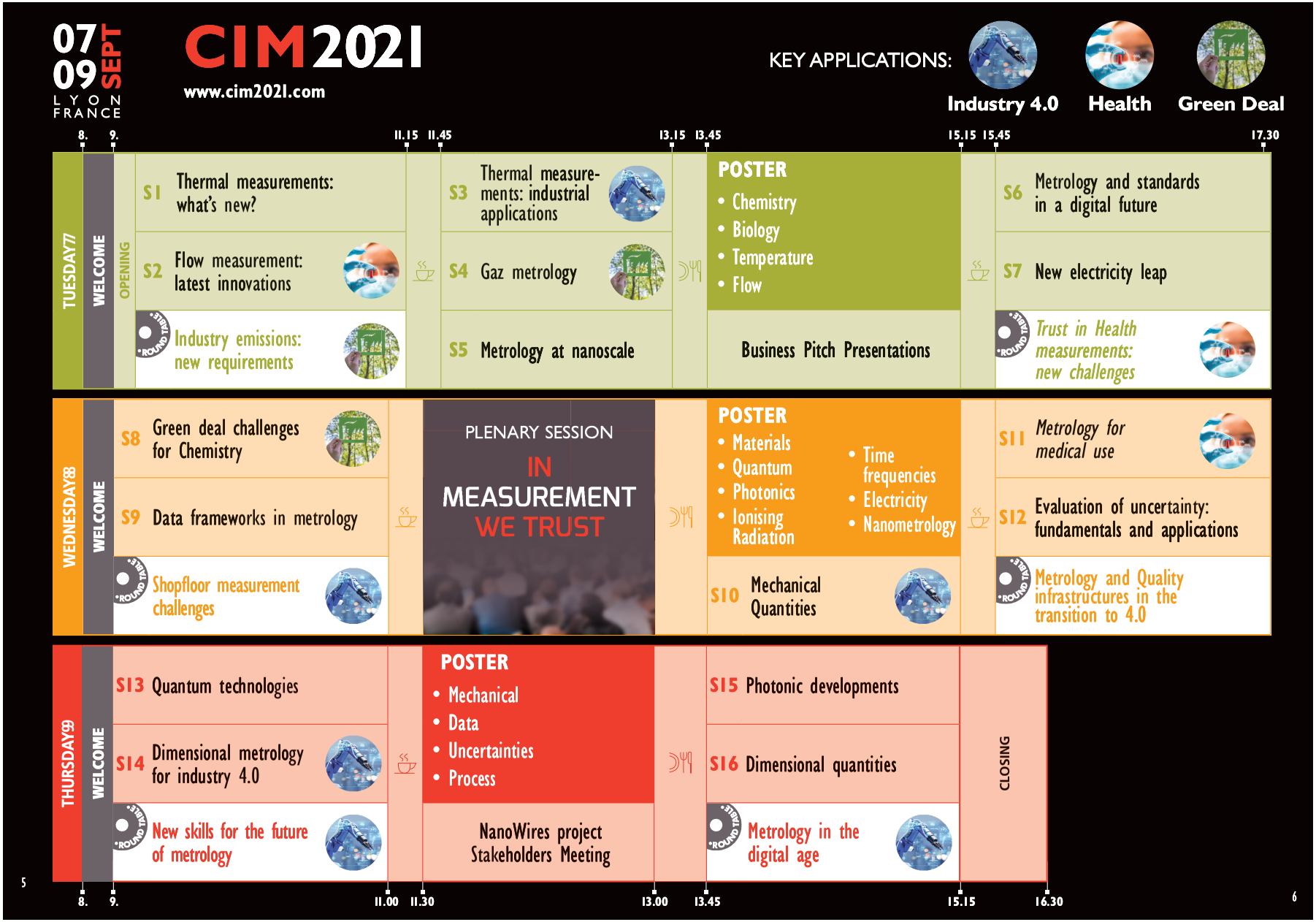
The congress is organised by the Collège Français de Métrologie with the support of:

BEA METROLOGIE, BIPM, CETIAT, CETIM, COFRAC, DIGIPLANT CONSULTING, EUROPEAN ACCREDITATION, EURAMET, EVALU8TION (GB), INERIS, PTB (DE), LNE, NPL (GB), NCSLi (US), OIML, STELLANTIS, SPF ECONOMIE (BE), STIL Marposs, TRESCAL, UNIVERSITE de BOURGOGNE.

And with the contribution of: BIPM, CETIAT, EURAMET, LNE, POLYWORKS EUROPA and TRESCAL.

Press information:

04 67 06 20 36 - info@cfmetrologie.com
https://www.cim2021.com


07 09 SEPT
LYON FRANCE
CIM2021
www.cim2021.com
KEY APPLICATIONS:
Industry 4.0
Health
Green Deal
8. 9. 11.15 11.45 13.15 13.45 15.15 15.45 17.30
TUESDAY77
WELCOME
OPENING
S1 Thermal measurements: what's new?
S2 Flow measurement: latest innovations
ROUND TABLE
Industry emissions: new requirements
S3 Thermal measurements: industrial applications
S4 Gaz metrology
S5 Metrology at nanoscale
POSTER
• Chemistry
• Biology
• Temperature
• Flow
Business Pitch Presentations
S6 Metrology and standards in a digital future
S7 New electricity leap
ROUND TABLE
Trust in Health measurements: new challenges
WEDNESDAY88
WELCOME
S8 Green deal challenges for Chemistry
S9 Data frameworks in metrology
ROUND TABLE
Shopfloor measurement challenges
PLENARY SESSION
IN
MEASUREMENT
WE TRUST
POSTER
• Materials
• Quantum
• Photonics
• Ionising Radiation
• Time frequencies
• Electricity
• Nanometrology
S10 Mechanical Quantities
S11 Metrology for medical use
S12 Evaluation of uncertainty: fundamentals and applications
ROUND TABLE
Metrology and Quality infrastructures in the transition to 4.0
THURSDAY99
WELCOME
S13 Quantum technologies
S14 Dimensional metrology for industry 4.0
ROUND TABLE
New skills for the future of metrology
POSTER
• Mechanical
• Data
• Uncertainties
• Process
NanoWires project Stakeholders Meeting
S15 Photonic developments
S16 Dimensional quantities
ROUND TABLE
Metrology in the digital age
CLOSING
5
8. 9. 11.00 11.30 13.00 13.45 15.15 16.30
6

CFM / CIM 2021 Conference - 8 September 2021, 15:30-17:30

Round Table - Leader: Anthony Donnellan, BIML Director

The role of Metrology and Quality infrastructures in the transition to Industry 4.0

What is Industry 4.0

Launched in Germany in the early 2010's, the initiative "Industry 4.0" has been adopted by many countries, sometimes with specific branding. The concept describes how the production processes should be re-organised in order to integrate new technologies such as IIoT (Industrial Internet of Things), AI (Artificial Intelligence), additive manufacturing, cobotics, etc. The expected benefits include an increase in productivity maintenance efficiency, cost reductions, and energy efficiency. Metrology, as a part of the industrial process, is also impacted from acquisition, processing, to decision making.

Key areas

Key areas to be explored include: How do IOs coordinate to promote the benefits of engagement with Industry 4.0 initiatives? What are the most important needs in economies when it comes to metrology and standards? How does improved Quality Infrastructure advance trade opportunities and people's quality of life?

The role of International Organisations

International Organisations (IOs) also have a key role to play in this revolution. Their normative and process standards contribute to the development and realisation of policies to create a fair environment to encourage trade and stimulate innovation.

This Round Table will see several actors from IOs and other organisations sharing their views on the role of Industry 4.0 initiatives, their impact on the development of Quality Infrastructure and examples of collaboration.

The role of the OIML

The CFM and the CIM event have a long history both in France and as an international event. Equally, the OIML also has a long and proud history of supporting the CFM and the CIM event.

CIM2021 provides a unique opportunity to bring together metrology practitioners, laboratory operators, policy makers, regulators, industry experts and academics from the fields of legal, scientific and industrial metrology.

The legal metrology community expects the OIML to play a key role in events such as CIM2021 and to assume a leadership role in order to advance and promote legal metrology. Leading a Roundtable discussion at CIM2021 meets these needs.

The OIML, and indeed any organisation, can only realise its potential by talking to its stakeholders, listening to their needs, by embracing technological developments and by monitoring industry and consumer trends. The CIM2021 event provides an excellent platform to do this in a very concentrated period of time.

Through the OIML's participation in CIM2021 and through the Round Table that it is leading, we are able to discuss options and potential solutions that will benefit not only industry but also the Members of the OIML. This includes participation in the OIML Certification System (OIML-CS) which is our international certification system in which measuring instrument manufacturers and measurement test laboratories participate.

Round Table experts

Accreditation – EA: Maureen Logghe, ILAC: Erik Øhlenschlæger ■ Industry Association – CECIP: Tim Hamers
Industry – Siemens: Thomas Engel, STIL Marposs: Cosimi Corleto ■ Metrology – BIPM: Andy Henson, OIML: Anthony Donnellan
Standardisation – ISO: Cristina Draghici ■ Trade and economic development – UNECE: Mika Vepsäläinen

Further information

To participate, please visit the event website at https://www.cim2021.com/round-tables-sessions.html

info

The OIML is pleased to welcome the following new

Member State:

- Ukraine

CIML Members

- Spain:
  Mr. Jose Angel Robles Carbonell
- Thailand:
  Mr. Wattanasak Sur-iam

Committee Draft

Received by the BIML, 2021.02 – 2021.04

Revision of OIML D 5: Principles for the establishment of hierarchy schemes for measuring instruments	4 CD	TC 4/p2	SK	2021-06-15

OIML meetings

28 September 2021
CEEMS AG meeting

30 September 2021
RLMO Round Table meeting

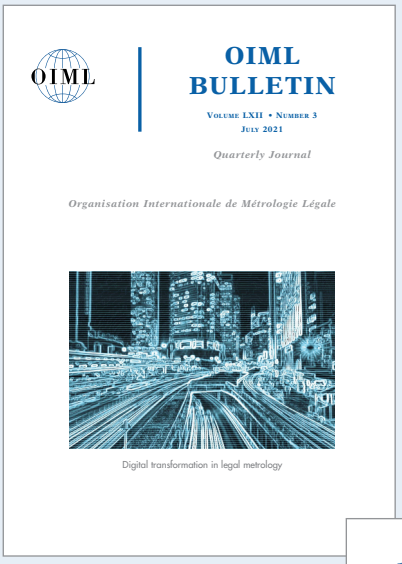
18-22 October 2021
16th International Conference on Legal Metrology and 56th CIML Meeting

www.worldmetrologyday.org
World Metrology Day Website

Bulletin online

Download the OIML Bulletin
free of charge

www.oiml.org/en/publications/bulletin



Call for papers

OIML Members
RLMOs
Liaison Institutions
Manufacturers' Associations
Consumers' & Users' Groups, etc.

- Technical articles on legal metrology related subjects
- Features on metrology in your country
- Accounts of Seminars, Meetings, Conferences
- Announcements of forthcoming events, etc.

The **OIML Bulletin** is a forum for the publication of technical papers and diverse articles addressing metrological advances in trade, health, the environment and safety - fields in which the credibility of measurement remains a challenging priority. The Editors of the Bulletin encourage the submission of articles covering topics such as national, regional and international activities in legal metrology and related fields, evaluation procedures, accreditation and certification, and measuring techniques and instrumentation. Authors are requested to submit:

- a titled, typed manuscript in Word or WordPerfect either on disk or (preferably) by e-mail;
- the paper originals of any relevant photos, illustrations, diagrams, etc.;
- a photograph of the author(s) suitable for publication together with full contact details: name, position, institution, address, telephone, fax and e-mail.

Note: Electronic images should be minimum 150 dpi, preferably 300 dpi.

Technical articles selected for publication will be remunerated at the rate of 23 € per printed page, provided that they have not already been published in other journals. The Editors reserve the right to edit contributions for style, space and linguistic reasons and author approval is always obtained prior to publication. The Editors decline responsibility for any claims made in articles, which are the sole responsibility of the authors concerned. Please send submissions to:

The Editor, OIML Bulletin
BIML, 11 Rue Turgot, F-75009 Paris, France
(chris.pulham@oiml.org)