20th IMEKO TC10 Conference
“Measurement for Diagnostics, Optimization and Control to Support Competitiveness and Innovation”
Lisbon, Portugal, September 28–29, 2026

The New Inmetro Seal as a Digitally Verifiable Conformity Mark: Digital Verification, Fraud Detection and Quality Infrastructure

Leonardo Batista Paiva

National Institute of Metrology, Quality and Technology (Inmetro), Professional Master’s Program in Metrology and Quality, Duque de Caxias, Brazil. e-mail: Lbpaiva@inmetro.gov.br

***Abstract* — This paper examines the new Inmetro seal as a digitally verifiable conformity mark and as a visible market-facing expression of quality infrastructure outcomes in Brazil. Building on the problem of information asymmetry and on recent discussions about label credibility, digital traceability, and verifiable conformity information, it argues that the seal acquires a new functional role when combined with app-based digital verification. In this configuration, the seal no longer operates merely as a static conformity sign; it becomes a practical mechanism for authentication, traceability, and fraud detection.**

Methodologically, the study adopts a qualitative exploratory case-study approach combining documentary analysis of official Brazilian sources with a structured benchmark against international digital conformity, product-identification, and anti-counterfeiting approaches. The analysis is grounded in Inmetro Administrative Order No. 314/2025 and in official documentation on “Inmetro na Palma da Mão” (Inmetro’s mobile authentication app). The paper proposes a conceptual sequence linking quality infrastructure, conformity assessment, trust, seal, digital verification, fraud detection, and consumer/industry value. It concludes that digitally verifiable conformity marks have the potential to strengthen consumer protection, improve market confidence, and represent an important innovation in the interface between quality infrastructure and end users.

Keywords* — *quality infrastructure; conformity assessment; trust; conformity mark; digital verification; fraud detection; consumer protection; Inmetro.

I. INTRODUCTION

In regulated markets, product compliance is often not directly observable before purchase or use. This creates information asymmetries that can weaken trust, distort competition, and increase exposure to fraud [1]. Recent research shows that labels and digital product information are only effective when they are accurate, substantiated, and supported by credible institutional arrangements [2]–[5]. Against this background, this paper examines the new Inmetro seal as a **digitally verifiable conformity mark** embedded in Brazil’s quality infrastructure. It argues that, when combined with app-based authentication and secure identification features, the seal moves beyond static signalling and becomes a practical mechanism for digital verification, fraud detection, and market-facing trust. This framing is especially relevant to IMEKO TC10 because it connects conformity assessment, digital transformation, and diagnostics-oriented verification in a concrete regulatory setting [7]–[10].

This issue has become more pressing in environments marked by counterfeiting, misleading claims, and fragmented signalling systems. Recent studies indicate that trust in labels depends strongly on credibility, transparency, and institutional support, while digital traceability systems are increasingly associated with fraud prevention, compliance verification, and stronger trust formation [3], [4]. In parallel, UNECE’s work on digital conformity credentials frames conformity information as something that can be structured, authority-linked, and digitally verifiable [5].

The case study concerns the National Institute of Metrology, Quality and Technology (Inmetro), the central executive body of Brazil’s national metrology and quality system [6]. The analysis investigates how its new seal transforms conformity assessment outcomes into a digitally verifiable and market-facing trust mechanism.

II. OFFICIAL AND REGULATORY BASIS OF THE INMETRO SEAL

According to official information, the Inmetro conformity seal is intended for products with assessed conformity and is used by manufacturers, importers, and service providers that obtain certification or registration within the Inmetro system [6]. The official service page identifies Inmetro Administrative Orders (Portarias)

Inmetro nº 422/2021, 218/2021, 230/2021, and 231/2021 as part of the regulatory basis governing the service [6].

A decisive recent step was Inmetro Administrative Order No. 314/2025, the 2025 amendment to the conformity-mark requirements for selected regulated products and services, introduced to integrate these regulated objects into **"Inmetro na Palma da Mão" (Inmetro's mobile authentication app)** [7]. The official text states that the initiative was developed by Inmetro in cooperation with Casa da Moeda do Brasil (CMB), the Brazilian Mint, a federally owned public company specialized in secure printing and related security solutions [7], [8].

The 2025 amendment to the conformity-mark requirements also provides a concrete technical basis for the paper. For the covered product categories, the seal must be indelible, resistant to removal, abrasion, chemicals, and weathering, self-destructive upon attempted removal, and equipped with visible and invisible security elements, a QR code authenticable by smartphone, and a human-readable alphanumeric code for contingency reading [7]. Official Inmetro communication further states that the new seal is linked to the Institute's database and designed to reinforce consumer protection and anti-fraud action [8], [9].

These regulatory and technical characteristics constitute the primary evidence used in the functional decomposition and comparative analysis presented in the following sections.

III. METHODOLOGY

This study adopts a qualitative exploratory case-study approach based on documentary analysis and structured benchmarking. This design was selected because the new Inmetro seal represents a recently implemented regulatory and technological innovation for which consolidated longitudinal performance data are not yet available. The analysis therefore focuses on the architecture, intended functions, institutional basis, and trust mechanisms of the system rather than on ex-post impact measurement.

The documentary corpus comprises Inmetro Administrative Order No. 314/2025, official Inmetro publications describing the conformity seal and the "Inmetro na Palma da Mão" mobile authentication app, and institutional information on the role of Inmetro and the Brazilian Mint. International specifications and publications concerning digital conformity credentials, standardized product identifiers, digital product information, and QR-code-based anti-counterfeiting systems were used for comparative purposes.

The documents were examined according to ten comparative dimensions: (i) presence of a physical mark or data carrier; (ii) linkage to conformity assessment; (iii) smartphone-based access; (iv) authoritative verification source; (v) physical security layers; (vi) tamper-evident or self-destructive removal; (vii) unique digital identification; (viii) consumer fraud reporting; (ix) linkage to regulatory enforcement; and (x) interoperability. The Inmetro model was then compared with three adjacent approaches: the UNECE Digital Conformity Credential, GS1 Digital Link, and protected QR-code anti-counterfeiting approaches described in the literature.

The comparison does not assume functional or legal equivalence among these approaches. Instead, it identifies shared design principles and distinctive characteristics concerning the connection between physical products, digital identities, conformity evidence, authoritative data sources, and end-user verification. Based on this analysis, the paper develops a conceptual framework linking quality infrastructure, conformity assessment, trust, digital verification, fraud detection, and market value.

IV. CONCEPTUAL FRAMEWORK: FROM QUALITY INFRASTRUCTURE TO DIGITALLY VERIFIABLE CONFORMITY

The paper proposes the following analytical sequence:

Quality infrastructure → conformity assessment → trust → seal → digital verification → fraud detection → consumer/industry value

In this framework, quality infrastructure provides the institutional and technical foundation, while conformity assessment converts this foundation into verified compliance. Trust represents the intended systemic outcome, and the seal functions as its visible market-facing expression. Digital verification enables the seal to be authenticated against an authoritative source, while fraud detection protects the integrity of the conformity signal. The final stage represents the potential value generated for consumers, industry, and regulators.

The framework distinguishes between a static conformity sign and a digitally verifiable conformity mark. A conventional conformity mark primarily communicates that conformity assessment has taken place. A digitally verifiable mark adds an interactive layer by allowing end users to authenticate the mark and access information linked to an official source. The framework therefore treats digital verification as the connecting mechanism between the physical conformity mark and fraud-detection functions.

This analytical sequence is summarized in Fig. 1.

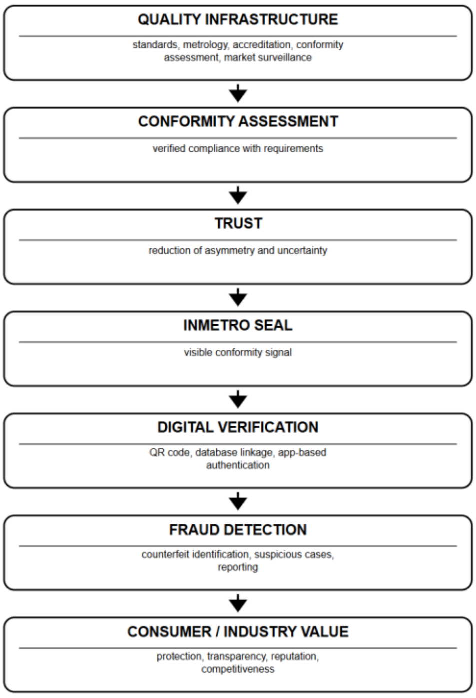

Fig. 1. Conceptual framework linking quality infrastructure, conformity assessment, trust, digital verification, fraud detection, and consumer/industry value.

V. DIGITAL VERIFICATION, AUTHENTICATION, AND FRAUD DETECTION

"Inmetro na Palma da Mão" offers a concrete example of digital transformation in conformity marking. Inmetro's official launch communication states that the app allows consumers to verify the authenticity of regulated products through smartphone-readable security elements and to use the system as a practical anti-fraud and consumer-protection tool [8]. The first implementation covers motorcycle helmets, fire extinguishers, and CNG cylinders, with progressive expansion planned for other regulated products and services [7], [8].

The verification process connects a physical conformity mark to information maintained in an official institutional environment. By scanning the QR code with a smartphone, the user can check whether the seal corresponds to a record recognized by Inmetro. A human-readable alphanumeric code provides an alternative verification mechanism when automatic reading is unavailable or unsuccessful [7]. This dual-access design reduces dependence on a single reading channel and increases the accessibility of the verification process.

The new seal also combines digital verification with physical security features. According to the regulatory requirements, the seal must be indelible, resistant to removal, abrasion, chemicals, and weathering, and self-destructive when removal is attempted [7]. It also includes visible and invisible security elements intended to make copying, reuse, and unauthorized reproduction more difficult. The QR code therefore does not operate as an isolated security mechanism, but as one layer within a broader physical and digital protection architecture.

This distinction is important because a conventional QR code may provide access to a digital resource without necessarily proving that the code or the physical object is authentic. In the Inmetro model, authentication depends on the combination of the physical seal, its security characteristics, the digital identifier, and verification against an official database. The effectiveness of the system is therefore based on the consistency between the physical mark and the authoritative digital record.

The app also creates a user-facing channel for identifying and reporting suspicious cases. When a seal cannot be authenticated or appears inconsistent with the product or service to which it is attached, the user can report a possible irregularity. This function extends the role of the conformity mark beyond communication of compliance and introduces an additional source of information for market-surveillance and enforcement activities [8], [9].

Analytically, the seal can therefore be understood as a hybrid artefact that combines a regulated physical conformity mark, a digital authentication interface, an official verification source, and a gateway for suspected-fraud reporting. For TC10 purposes, this architecture supports a form of diagnostics for market integrity: it enables authenticity checking, anomaly indication, and escalation of possible fraud. UNECE's conformity-credential logic points in a similar direction by treating conformity information as digitally verifiable evidence linked to authoritative issuers and compliance schemes [5].

VI. COMPARATIVE ANALYSIS OF DIGITALLY ENABLED VERIFICATION APPROACHES

To To assess the distinctive characteristics of the new Inmetro seal, the proposed model was compared with three adjacent approaches: the UNECE Digital Conformity Credential, GS1 Digital Link, and QR-code-based anti-counterfeiting systems described in the literature. These approaches were selected because they represent complementary mechanisms for linking physical products, digital identities, authoritative information, and user-facing verification.

The comparison does not assume that the selected approaches are legally or functionally equivalent. The Inmetro seal is a regulated conformity mark embedded in a national quality infrastructure, whereas the benchmark cases primarily address digital conformity evidence, standardized identification, interoperability, or product authentication. The purpose of the comparison is therefore to identify shared design principles and distinctive institutional and technological features.

The UNECE Digital Conformity Credential provides digitally verifiable assessments of products, facilities, or organizations against published standards and regulations. Such credentials may include information on the conformity assessment body, accreditation, assessment criteria, measured performance, and conformity determination. The model is strongly oriented toward machine-readable evidence, interoperability, and independent verification of conformity claims [5], [11].

GS1 Digital Link provides a standardized method for encoding product, location, and logistics identifiers, including GTINs, batch numbers, and serial numbers, in barcodes that can be scanned and connected to online information. Its main contribution lies in standardized identification and in the connection between physical objects and digital resources [12]. GS1 specifications also allow digital signatures to be encoded in two-dimensional barcodes or RFID data carriers to support product authenticity and brand protection [13].

QR-code-based anti-counterfeiting systems focus more directly on product authentication. However, conventional QR codes can be copied and reproduced unless they are combined with additional physical, cryptographic, or database-based security layers. Recent studies therefore propose textured, hidden, or protected QR codes that make unauthorized replication more difficult [14], [15]. Reviews of traceability technologies similarly indicate that QR codes alone do not provide strong protection against counterfeiting and should be combined with complementary authentication mechanisms [16].

Table 1. Comparison of digitally enabled product-verification approaches.

Feature	**Inmetro**	**UNECE DCC**	**GS1**	**QR-based systems**
physical mark/carrier	yes	not required	carrier	yes
conformity link	direct	direct	not inherent	usually no
smartphone access	yes	possible	yes	yes
verification source	inmetro db	issuer / cab	owner / resolver	system operator
security layers	yes	not specified	not inherent	depends
tamper evidence	yes	no	no	usually no
unique digital id	yes	yes	yes	yes
consumer fraud reporting	yes	not inherent	not inherent	depends
regulatory enforcement link	direct	depends	not inherent	limited
interoperability	emerging	strong	strong	limited

DCC: Digital Conformity Credential; **DL:** Digital Link; **DB:** database; **CAB:** conformity assessment body.

Each source was coded according to the comparative dimensions defined in Section III, and the resulting feature profiles were compared using a qualitative categorical and functional-equivalence matrix. Table 1 summarizes the comparison.

The comparative implications of these results are discussed in Section VII.

VII. DISCUSSION

The comparative analysis indicates that the distinctive feature of the new Inmetro seal is not the use of a QR code alone, but the integration of functions that are commonly distributed across separate product-identification, digital conformity-credential, and anti-counterfeiting systems. GS1 Digital Link provides standardized connections between physical products and digital resources; the UNECE Digital Conformity Credential emphasizes structured and independently verifiable conformity evidence; and protected QR-code systems focus primarily on preventing unauthorized reproduction. The Inmetro model combines elements of these three functions within a national regulatory architecture, together with physical tamper resistance, visible and covert security elements, official-database verification, smartphone access, and consumer fraud reporting.

From a quality infrastructure perspective, the findings indicate that trust depends not only on the presence of a conformity mark, but also on whether the mark can be checked, linked to credible evidence, and supported by an authoritative institutional framework. The seal therefore functions as a market-facing interface through which conformity-assessment outcomes become visible, accessible, and actionable, moving from static conformity signalling toward a verifiable trust architecture.

This transition is relevant to the TC10 scope. The app does not perform diagnostics in the conventional industrial sense of monitoring equipment condition or identifying technical failures. However, it supports a form of diagnostics for market integrity by enabling authenticity checks, identification of suspicious cases, and escalation of possible fraud. In this context, digital verification contributes to reliability, risk assessment, market surveillance, and decision support.

The potential benefits extend to consumers, legitimate industry, and regulators. Consumers gain access to authoritative information and become less dependent on visual inspection alone. Legitimate manufacturers and service providers may benefit from stronger reputational protection and fairer competition. Regulators may receive additional information for surveillance and enforcement through user-generated fraud reports and verification activity.

These benefits, however, are not automatic. The effectiveness of the system will depend on database accuracy, app availability, user awareness, cybersecurity, clarity of verification results, response time, interoperability, and the institutional capacity to investigate reported cases. A digitally verifiable seal may fail to strengthen trust if users do not understand how to use the app, if the database is incomplete, or if suspicious reports are not processed effectively.

The comparison also reveals opportunities for further development. UNECE and GS1 approaches place strong emphasis on interoperable identifiers, structured data, and machine-readable conformity information. Publicly available documentation on the Inmetro model currently emphasizes authentication, physical security, and fraud reporting more strongly than interoperability or standardized digital conformity evidence. Future integration with international identifiers, digital credentials, and product-information architectures could extend the value of the seal beyond consumer authentication and support supply-chain verification, automated compliance checking, and cross-border recognition.

This study is limited by the recent implementation of the initiative and by its qualitative documentary design. It does not measure actual reductions in fraud, app adoption, user experience, enforcement outcomes, cybersecurity performance, or economic impact. The conclusions are therefore based on documentary evidence, functional decomposition, and structured benchmarking rather than ex-post performance data. Future empirical research should assess how consumers and economic operators interact with the app, the frequency and nature of authenticity checks, the number and treatment of reported suspicious cases, institutional response times, and measurable effects on consumer trust, fair competition, and regulatory efficiency.

VIII. CONCLUSION

This paper examined the new Inmetro seal as a digitally verifiable conformity mark within Brazil's quality infrastructure. Through documentary analysis and structured benchmarking, the analysis indicates that its main innovation lies not in the QR code alone, but in the integration of physical security, unique identification, official-database verification, mobile access, regulated conformity assessment, and fraud reporting.

The proposed framework shows how quality-infrastructure outcomes can be translated into a market-facing and interactive verification mechanism. In this architecture, the conformity mark moves beyond static signalling and supports authentication, traceability, market-integrity diagnostics, and regulatory decision-making.

The Inmetro case therefore provides a relevant example of digital transformation in conformity assessment. Its actual effectiveness will depend on adoption, data reliability, cybersecurity, interoperability, and institutional response capacity, which should be evaluated through future empirical research.

REFERENCES

[1] **G. A. Akerlof**, "The market for 'lemons': Quality uncertainty and the market mechanism," *The Quarterly Journal of Economics*, vol. 84, no. 3, pp. 488–500, Aug. 1970, doi: 10.2307/1879431.

[2] **OECD**, *Leveraging Digital Business Models, Tools and Technologies for Reliable Environmental Information and Consumer Engagement in the Circular Economy*, OECD Digital Economy Papers, no. 377. Paris, France: OECD Publishing, 2025, doi: 10.1787/33c6e2bc-en.

[3] **J. Cromwell, C. Turkson, M. Dora, and F. A. Yamoah**, "Digital technologies for traceability and transparency in the global fish supply chains: A systematic review and future directions," *Marine Policy*, vol. 178, Art. no. 106700, 2025, doi: 10.1016/j.marpol.2025.106700.

[4] **I. Kovač, D. Dunković, and B. Kovač**, "Greenwashing and consumer skepticism toward eco-labels in Croatia: Challenges and policy directions," *British Food Journal*, 2025, doi: 10.1108/BFJ-02-2025-0122.

[5] **United Nations Economic Commission for Europe**, "Conformity Credential," *UN Transparency Protocol Specification*. [Online]. Available: https://untp.unece.org/docs/specification/ConformityCredential/. [Accessed: 15-Jul-2026].

[6] **National Institute of Metrology, Quality and Technology**, "Selo de Conformidade" and "Competências," Governo Federal. [Online]. Available: https://www.gov.br/inmetro/pt-br/assuntos/regulamentacao/avaliacao-da-conformidade/selo-de-conformidade; https://www.gov.br/inmetro/pt-br/acesso-a-informacao/institucional/competencias. [Accessed: 13-Apr-2026].

[7] **Brasil**, *Inmetro Administrative Order No. 314/2025* [*Portaria nº 314, de 29 de maio de 2025*], amending the conformity-mark requirements for selected regulated products and services, *Diário Oficial da União*, May 30, 2025. [Online]. Available: https://www.in.gov.br/en/web/dou/-/portaria-n-314-de-29-de-maio-de-2025-632890915. [Accessed: 04-Apr-2026].

[8] **National Institute of Metrology, Quality and Technology**, "Governo Federal lança 'Inmetro na Palma da Mão'," Governo Federal, May 30, 2025. [Online]. Available: https://www.gov.br/inmetro/pt-br/centrais-de-conteudo/noticias/governo-federal-lanca-201cinmetro-na-palma-da-mao201d. [Accessed: 07-Apr-2026].

[9] **National Institute of Metrology, Quality and Technology**, "'Inmetro na Palma da Mão': campanha institucional reforça proteção ao consumidor," Governo Federal, Sep. 17, 2025. [Online]. Available: https://www.gov.br/inmetro/pt-br/centrais-de-conteudo/noticias/201cinmetro-na-palma-da-mao201d-campanha-institucional-reforca-protecao-ao-consumidor. [Accessed: 07-Apr-2026].

[10] **IMEKO TC10**, "Authors," *20th IMEKO TC10 Conference*. [Online]. Available: https://www.imekotc10-2026.sztaki.hu/authors.php. [Accessed: 02-Apr-2026].

[11] **United Nations Economic Commission for Europe**, "Technical Specifications," *UN Transparency Protocol*. [Online]. Available: https://untp.unece.org/docs/specification/. [Accessed: 10-Jul-2026].

[12] **GS1**, "GS1 Digital Link." [Online]. Available: https://www.gs1.org/standards/gs1-digital-link. [Accessed: 10-Jul-2026].

[13] **GS1**, *GS1 Digital Signatures Technical Implementation Guideline: Using Digital Signatures to Support Brand Protection and Product Authenticity*. [Online]. Available: https://www.gs1.org/standards/gs1-digital-signatures/current-standard. [Accessed: 10-Jul-2026].

[14] **T. Wang, H. Zheng, C. You, and J. Ju**, "A texture-hidden anti-counterfeiting QR code and authentication method," *Sensors*, vol. 23, no. 2, Art. no. 795, Jan. 2023, doi: 10.3390/s23020795.

[15] **G. Nicoletta, M. D. L. Bruno, P. Yu, Z. Wang, M. P. De Santo, R. Caputo, and A. Ferraro**, "Anti-counterfeiting tags with camouflaged QR codes on nanocavities, using polymer-dispersed liquid crystals," *Advanced Materials Technologies*, vol. 10, no. 12, Art. no. 2402055, 2025, doi: 10.1002/admt.202402055.

[16] **S. P. Gayialis, E. P. Kechagias, G. A. Papadopoulos, and D. Masouras**, "A review and classification framework of traceability approaches for identifying product supply chain counterfeiting," *Sustainability*, vol. 14, no. 11, Art. no. 6666, 2022, doi: 10.3390/su14116666.