TU Delft | OPEN Publishing

Research article

Journal of Standardisation

Dynamic Certifications for Dynamic Standards Leveraging ENTRUST's Real-time Conformity Certificates to Strengthen Regulatory Compliance with the GDPR, MDR, CRA and NIS2

Adrian Quesada Rodriguez [1,2,*], *André Cardozo Sarli* [3], *Renáta Radócz* [1], *Sébastien Ziegler* [1], *Augusto Díaz-Ordóñez González* [1], *Antonio Skarmeta* [4], *Jesús García Rodríguez* [4], *Gilson Javier Delgado Rodríguez* [4]

[1] Mandat International, Geneva, Switzerland

[2] ETSIT, Universidad Politécnica de Madrid, Spain

[3] UDG Alliance, Geneva, Switzerland

[4] Dept. Ingeniería de la Información y las Comunicaciones
Facultad de Informática, University of Murcia, Spain

Abstract: Recent developments in the European healthcare landscape and the rapidly evolving technologic ecosystem have led to the adoption of a new range of regulations that, amongst other key features, increasingly depend on standardization, and recognize the viability of certifications for demonstrating regulatory compliance. This paper examines shortcomings in existing guidelines and standardization approaches, while showcasing the results of both the ENTRUST project, as well as the Europrivacy and Interprivacy certification schemes, as potential ways forward to enable a streamlined approach to regulatory compliance with cybersecurity and privacy requirements through modular and ICT-supported third-party certification. It presents some perspectives regarding the potential of this approach in broader standardization activities and identifies key advantages of the proposed model for the various players in the healthcare sector.

Keywords: medical devices, dynamic certification, conformity, regulatory compliance, privacy, ICT

Highlights:

1. The European Union's complex web of regulations (GDPR, MDR, CRA, NIS2) creates significant cybersecurity and compliance challenges for connected medical devices.
2. Authoritative guidance tends to be static and fragmented, failing to keep pace with the rapidly evolving technology and threat landscape in digital healthcare.
3. The ENTRUST project introduces a novel, automated framework using Zero Trust principles to continuously assess the security of medical devices throughout their entire lifecycle.
4. The ENTRUST model demonstrates cross-sector scalability beyond healthcare, offering a blueprint for real-time accountability in other high-integrity domains such as finance and autonomous transportation
5. This article presents the opportunities arising from the shift from traditional, periodic audits towards dynamic certification models that provide real-time, continuous trust verification.
6. Integrating automated solutions with adaptable certification schemes like Europrivacy offers a practical and scalable path to ensuring ongoing regulatory compliance.

* Corresponding author:
aquesada@mandint.org

Submitted: 01-09-2025
Revised: 07-01-2026
Accepted: 09-01-2026
Published: 09-11-2026
Peer review: double blind

This work is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence

DOI:
https://doi.org/10.59490/jos.2026.8348

ISSN: 2772-9249

How to cite: Quesada Rodriguez, A., Cardozo Sarli, A., Radócz, R., Ziegler, S., Díaz-Ordóñez González, A., Skarmeta, A., García-Rodríguez, J., Delgado Rodríguez, G. J. (2026). Dynamic Certifications for Dynamic Standards Leveraging ENTRUST's Real-time Conformity Certificates to Strengthen Regulatory Compliance with the GDPR, MDR, CRA and NIS2. *Journal of Standardisation, 5*. https://doi.org/10.59490/jos.2026.8348

©2026 the authors published by TU Delft OPEN Publishing on behalf of the authors.

Abbreviations:

- AI: Artificial Intelligence
- ATL: Actual Trust Level
- CB: Certification Body
- CC: Conformity Certificate
- CE: Conformité Européenne (European Conformity mark)
- CMD: Connected Medical Device
- CRA: Cyber Resilience Act
- EA: European Accreditation
- ECCP: European Centre for Certification and Privacy
- EDPB: European Data Protection Board
- EEA: European Economic Area
- EN: European Standard
- ENISA: European Union Agency for Cybersecurity
- ESO: European Standardization Organization
- EU: European Union
- EUCC: European Common Criteria-Based Cybersecurity Certification Scheme
- EUCS: European Cybersecurity Certification Scheme for Cloud Services
- FSCA: Field Safety Corrective Action
- FV: Formal Verification
- GDPR: General Data Protection Regulation
- ICT: Information and Communications Technology
- IoMT: Internet of Medical Things
- IVD: In-Vitro Diagnostic device
- IVDR: In Vitro Diagnostic Medical Devices Regulation
- JTC1: Joint Technical Committee 1 (ISO/IEC)
- MD: Medical Device
- MDCG: Medical Device Coordination Group
- MDR: Medical Devices Regulation
- ML: Machine Learning
- NIS2: Network and Information Systems Directive (recast)
- PAS: Publicly Available Specification
- PDE: Products with Digital Elements
- PHG: Personal Health Gateway
- PMS: Post-Market Surveillance
- PUF: Physically Unclonable Function
- RoT: Root of Trust
- RTL: Required Trust Level
- SE: Secure Element
- TAF: Trust Assessment Framework
- ToE: Target of Evaluation
- TPM: Trusted Platform Module
- VC: Verifiable Credential
- W3C: World Wide Web Consortium

1 Introduction

The European healthcare system has been transformed by the advent of Connected Medical Devices (CMDs) and interconnected information systems. While this brought significant advancements in patient care, the increased connectivity also resulted in a significant rise in cybersecurity challenges. In Europe, CMDs are regulated through a web of different regulations depending on the services, such as health data within the GDPR or Cybersecurity with NIS2 Directive, but specifically through Medical Device Regulation and In Vitro Device Regulation. However, this regulatory landscape requires a continuous alignment of technical, legal and organizational processes.

Certification rises as a viable method to demonstrate compliance, but its traditional model, which is focused on a point-in-time compliance assessment is not well equipped to manage a reality with increased new cybersecurity threats, risks assessment requirements and regulatory demands. To address these challenges, this paper proposes a concept of a dynamic certification, based on the ENTRUST project. This dynamic certification leverages continuous technical assessments that are adapted to different regulations and requirements by relying on certification schemes (Europrivacy and Interprivacy).

Methodologically, this paper follows a conceptual and analytical research approach grounded in regulatory analysis, standardization practice, and evidence emerging from an ongoing European research and innovation project. While empirical validation through large-scale deployment is outside the scope of this contribution, the arguments presented are supported by established regulatory mechanisms, recognised certification schemes, and concrete technical architectures currently under implementation.

To this end, in Section 2 we provide a general overview of the regulatory quagmire and traditional certification models. We proceed to address the implications of multi-source

regulations and overlapping standards (Section 3), to propose a lifecycle-based automated trust assessment framework for connected medical devices (Section 4), and outline how such a framework can support and be integrated with a dynamic standardization and certification model (Section 5).

2 An increasingly certification-aware regulatory framework

Over the past decades, the European healthcare landscape has experienced a significant evolution with the widespread implementation of Medical Devices (MD), Connected Medical Devices (CMDs), and In-Vitro Diagnostic (IVD) devices (see the European Medical Technology Industry in figures, MedTech Europe, 2023). In parallel, hospitals and the various stakeholders involved in health service provision have benefitted from digital transformation processes which now enable highly integrated and interconnected healthcare ecosystems. These advancements have positively impacted most healthcare services, easing the adoption of remote consultations, diagnostics, treatment, and patient monitoring, increasing quality of care with the promise of ever-increasingly personalized medicine.

On the other hand, the massive adoption of CMDs poses significant cybersecurity challenges, with global healthcare ecosystems facing mounting pressure to enhance the safety, security and trustability of the "Internet of Medical Things" (IoMT) (on the subject see Hemanth et al., 2021; Ziegler et al., 2024) and its associated technologies[1] in an increasingly decentralized point of care environment. Conversely, the increased connectivity and digitalization of critical health services have greatly augmented the potential impact of cyberthreats, data breaches, and disruptions to patient care.

In recognition of these challenges, governments and regulatory authorities have proposed and implemented a sequence of stringent cybersecurity regulations and data protection frameworks. In the European context, Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR); Regulation (EU) 2024/2847, the Cyber Resilience Act (CRA); Regulation (EU) 2017/745, the Medical Devices Regulation (MDR); and the revised Directive (EU) 2022/2555 (NIS2) represent the manifestation of the supervisory objective to address these emerging challenges. Additionally, these regulations introduce innovative alternatives for regulatory compliance validation through an alignment with standards and certification.

The GDPR includes specific dispositions to guide the processing and protection of personal data, including robust security measures and requiring the adoption of a privacy-by-design[2], risk-based approach to ensure the lawful, transparent and secure processing of such data. In a parallel spirit to other EU laws, particularly of the new legislative framework, the GDPR includes strong and flexible options for the demonstration of regulatory compliance[3]. Indeed,

[1] Particularly in a context where software is increasingly contemplated as potentially falling under the medical device classification (Beckers et al., 2021; EMA, 2018; MDR, 2021)

[2] Privacy by design is principle that foster the idea that technical and organizational measures should be implemented at the earliest stages of development of technologies or data processing to safeguard privacy and data protection rights from the start.

[3] The approach followed by GDPR-based certifications (and particularly under the relevant EDPB guidance for EU Data Protection Seals) differs from the approach found in other regulatory frameworks such as the Medical Device Regulation, the Machinery Directive, the Radio Equipment Directive, and the Construction Products Regulation, in that GDPR-based certifications are always issued by accredited third-party certification bodies to demonstrate compliance of data processing activities with the totality (or a sub-section) of the Regulation (depending on the scope of the certification scheme), whereas many EU product regulations allow for a mix of conformity assessment procedures, which include third-party certification and self-certification by manufacturers,

Articles 42 and 43 of the GDPR establish certification mechanisms[4] as valid methods to demonstrate regulatory compliance of personal data processing activities with the regulation's privacy and cybersecurity requirements. This is an alternative to a usually required comprehensive third-party examination of the legal, organizational and technical measures in place. Furthermore, Article 46 defines approved certification mechanisms as providing an "appropriate safeguard" for international data transfers, and (provided they are coupled with binding and enforceable commitments from the data enforcer) they may enable controllers or processors to carry out legitimate international transfers of personal data upon this basis.

The Cyber Resilience Act (CRA) bolsters this framework by defining mandatory cybersecurity requirements for products with digital components[5] placed on the European Union Market. It complements the GDPR's requirements through the introduction of a dedicated security-by-design approach and requires the performance of vulnerability assessments by manufacturers as well as the provision of lifecycle-oriented security updates. As in the case of the GDPR, the CRA includes mandatory certification provisions with varying levels of scrutiny depending on the product's classification[6] for both hardware and software products.

It should be observed that the CRA formally excludes medical devices. However, we still argue that its provisions are relevant for Medical Device developers as they represent the state-of-the-art in cybersecurity legislation and serve as important guidelines for implementation. Furthermore, in view of the complexity of new MD and their requirements for integration, this regulation is still applicable for information systems, that though not directly connected to MD, support the digital infrastructure behind them. Therefore, a strong alignment by design, even for medical devices, is recommended.

In parallel, stakeholders will need to take in consideration the obligations set by the EU AI Act. The AI Act introduces classification mechanisms for high-risk AI systems[7], a category under which many CMDs fall, especially those performing diagnosis or therapeutic interventions. The

depending on the risk classification of the product. This flexibility and focus on data processing activities permits the development of adaptive schemes such as Europrivacy (see section 4).

[4] Including the specification of both nationally-valid and EU-wide valid certification schemes, both for sector-specific and for generic data processing activities. This paper will focus its attention on the specific case of Europrivacy (Europrivacy, n.d.) due to its research background, its status as the first EU Data Protection Seal to have been recognized by the European Data Protection Board (EDPB), and its modular and flexible approach (Ziegler et al., 2022).

[5] While excluding MDs and IVDs from its scope, its dispositions are complementary to IoMT and innovative healthcare ecosystems, particularly as it concerns the cybersecurity infrastructure supporting them, and also non-MD-based products and solutions (e.g. wellness applications) which are increasingly contemplated as part of the quality of care strategy for the various medical stakeholders (e.g. insurance providers, caregiver organizations, etc.). (Alslaity et al., 2022; Boardman, 2021; ISO, 2021; WHO, n.d.)

[6] The CRA categorizes products into different classes based on their cybersecurity risk and functionality and specifies the level of granularity and stringency of the assessment in line with this categorization: for "Critical Annex IV products" (which present the highest risk) it requires an European Cybersecurity Certification (currently being developed by ENISA (European Union Agency for Cybersecurity, n.d.)); for "Important Class II products" (those with fundamental cybersecurity functions or with a high potential for adverse effects if compromised) it requires a third-party conformity assessment to be performed; for "Important Class I products" (cybersecurity-sensitive software and network management tools) it requires self-assessment with harmonized standards or, in their absence, third-party conformity assessment).(Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA Relevance), 2024).

[7] The specific rules for high-risk systems have an extended transition period until 2 August 2027.

AI Act requires stringent risk assessment and mitigation, elements to facilitate traceability and detailed documentation, among other requirements that are important for both deployment and certification.

The Medical Device Regulation acts as *lex specialis* for the design, manufacture and placement on the EU market of medical devices. To this end, it requires a lifecycle-wide risk management and security-by-design approach, mandating the performance of risk assessments, vulnerability management, and the deployment of appropriate technical and organizational techniques to ensure patient safety and cybersecurity. The MDR also supports and clarifies the route towards CE[8] marking certification[9] of medical devices in Europe (including software-based MDs).

Lastly, the NIS2 (Second iteration of the Network and Information Systems Directive) reinforces the EU's cybersecurity landscape by establishing particular obligations on essential entities (including the healthcare sector), expanding on organizational requirements like risk management, corporate accountability, enhanced incident reporting obligations, business continuity planning, and supply chain security management. As its scope is particularly oriented on maintaining integrity and availability of key services across the Union, and given the wide range of entities bound by its requirements, Art. 24 of NIS2 acknowledges European Cybersecurity certification schemes[10] as means to demonstrate compliance with its requirements, in alignment with the Cybersecurity Act[11]. While the NIS2 primarily applies to organizations rather than specific products, many connected medical devices (once integrated into critical healthcare infrastructure) are indirectly affected by its dispositions due to the cybersecurity obligations placed on the entities that operate them.

The Cybersecurity Act, in turn, defines three assurance levels (commensurate with the level of risk associated with the intended use of the ICT product, service or process) that can be specified by such schemes, namely:

a) Basic: providing assurance that the products, services and processes for which the certificate is issued have been evaluated at a level intended to minimise the known basic risks of incidents and cyberattacks.
b) Substantial: which builds upon the basic assurance level with the addition of an evaluation regarding the risk of incidents and cyberattacks carried out by actors with limited skills and resources.

[8] CE marking is a conformity mark indicating that a product sold within the European Economic Area (EEA) meets EU health, safety, and environmental protection standards.

[9] The MDR classifies devices in various classes (I, IIa, IIb, and III) based on risk, and defines two pathways for certification: self-certification for Class I devices and Third-party assessment by a notified body (as defined under Annexes IX, X or XI) for some Class I devices (sterile devices, devices with a measuring function or reusable surgical instruments) and with increasing depth of assessment for devices in Classes IIa, IIb and III. (Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on Medical Devices, Amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and Repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA Relevance.), 2017).

[10] In particular it makes reference to ENISA's European Cybersecurity Certification and its candidates (Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 Laying down Rules for the Application of Regulation (EU) 2019/881 of the European Parliament and of the Council as Regards the Adoption of the European Common Criteria-Based Cybersecurity Certification Scheme (EUCC) (Text with EEA Relevance), 2025; European Union Agency for Cybersecurity, n.d.) It is important to note that through the Cybersecurity Act, ENISA has taken a central role in defining and promoting cybersecurity certification schemes across the Union.

[11] (Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 2019).

c) High: which further expands the assurance level to consider also the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources, and an assessment of their resistance to such threats using penetration testing.

It is relevant to note that the Act requires that certifications with a High assurance level are generally issued only by a national cybersecurity certification authority, certifications with a Substantial assurance level may be granted by accredited conformity assessment bodies, which may also grant those certifications conveying Basic assurance, however, depending on the dispositions of the implemented scheme, Art. 53 of the Act recognizes the viability of conformity self-assessment under the sole responsibility of the manufacturer or provider of products, services or processes.

Whilst these regulations are generally seen as complementary (the MDR prioritizes patient safety, the CRA acts as a horizontal baseline for digital products, NIS2 enforces institutional resilience and the GDPR protects personal data rights), their interactions[12] raise a number of challenges for traditional compliance approaches, particularly within the healthcare sector. Among these challenges we can cite:

1. Navigating a web of overlapping obligations
2. Demanding a continuous risk-based approached rather than a static checklist
3. Compliance must be observed during the whole lifecycle of products and services and according to different obligations.
4. Requiring higher levels of alignment between technical, legal and organizational processes.
5. A wider chain of risk for healthcare operators, due to the cumulative risk from the interconnected systems they use.

Table 1 below illustrates this complex regulatory landscape:

Table 1: Regulatory landscape overview

Regulation	Primary scope	Interaction with medical devices	Core cybersecurity/ data protection focus	Role of certification
MDR (EU) 2017/745	Product safety and clinical performance	Direct (lex specialis for MDs)	Security-by-design; patient safety; lifecycle risk management (Annex I, GSPR 17.2)	Mandatory conformity assessment (CE marking); primarily pre-market
CRA (EU) 2024/2847	Horizontal product cybersecurity	Indirect; formally excludes MDs where MDR applies	Vulnerability management; security updates; state-of-the-art benchmark	Mandatory certification for critical PDEs; reference baseline for cybersecurity

[12] For example, interaction of the CRA with the MDR involves complex "lex specialis" exemptions that can create ambiguity regarding vulnerability reporting timelines. This fragmentation often leads to compliance silos, where a device might be clinically certified under the MDR but lack the dynamic vulnerability management processes envisioned by the CRA, creating a "compliance gap" that dynamic certification aims to bridge.

NIS2 (EU) 2022/2555	Entity-level cybersecurity resilience	Indirect via healthcare providers (essential entities)	Risk management; incident reporting; supply-chain security	Certification schemes recognised as due-diligence mechanisms
GDPR (EU) 2016/679	Personal data protection	Applies to data processing performed by or via MDs	Confidentiality, integrity, availability of personal data (Art. 32)	Voluntary certification mechanisms (Arts. 42–43)

In this evolving regulatory environment, effective risk management activities must be tailored to address and evaluate the full lifecycle of the various products, services or processes involved in these new healthcare models. This requires common technical, legal and organizational compliance approaches, which have been increasingly achieved through the support of the various involved stakeholders, towards the definition of best practices (DIGITALEUROPE, 2024; International Medical Device Regulators Forum, 2023; MedTech Europe, 2023) and the specification of public and private standards[13], which may in turn bring forth further improvements to currently existing guidelines and upcoming regulatory developments[14] at the national, regional and international level.

3 Identified shortcomings in currently applicable EC cybersecurity guidance

Originally established by the European Commission to facilitate the cooperation and compliance of interested stakeholders with applicable regulatory frameworks[15], the Medical Device Coordination Group (MDCG) (European Commission, 2024), addresses key issues from the medical devices sector, from Notified Body oversight, standardization, market surveillance and international matters.

As part of these activities, and with the goal of reducing the administrative burden of the new regulations for manufacturers and healthcare delivery hospitals, the MDCG has issued an extensive range of endorsed documents and reference, non-binding guidance, which effectively became a key reference point towards the clarification of regulatory requirements for solution

[13] Including (International Electrotechnical Commission, 2020a, 2020b, 2021; ISO, 2004, 2007, 2009, 2019a, 2019b, 2020, 2022a) and in particular on the process and requirements of audit and certification activities, see (ISO, 2011b, 2011a, 2015). Also it is of relevance to acknowledge that in the European context the New Legislative Framework (NLF) policy approach to product placement in the EU market is closely aligned with standardization activities, enabling manufacturers to meet essential regulatory requirements by applying harmonized standards (officially published in the Official Journal of the European Union), with the result that a successful third-party certification (or self-certification if the applicable legislation enables it) enables a presumption of compliance, e.g.: (European Commission, 2021).

[14] Also considering the steady entry into force of the AI act, within which connected medical devices may fall under the high-risk classification whenever AI is introduced as a safety component of the medical device or the AI is itself a medical device.

[15] Mainly the MDR and IVDR, but considering also the potential alignment with the GDPR, the NIS2 and with the CRA.

providers and deployers alike[16]. In the specific area of compliance with cybersecurity and privacy requirements for medical devices, it published the dedicated Guidance on Cybersecurity for Medical Devices (European Commission, 2020).

Key takeaways of this document include the reiteration of the need for lifecycle-wide cybersecurity; the incorporation of security measures and clinical safety considerations; the clarification of the secure by design approach to be pursued in MDs; the necessity to define and communicate the minimum IT requirements for safe performance of the device; the clarification of joint stakeholder responsibilities; an encouragement to align with broader regulations and standards for compliance demonstration[17]; a clarification of security-relevant documentation; and the recognition of the need for post-market surveillance (PMS) to enable manufacturers to monitor and address emerging risks and potentially trigger field safety corrective actions (FSCAs)[18].

Despite its relevance in clarifying applicable cybersecurity requirements for Internet of Medical Things, and together with the regulations, several limitations still undermine its work. A gap analysis performed by a selection of current (2023-2025) projects funded under the Horizon Europe call "Enhancing cybersecurity of connected medical devices" (HORIZON-HLTH-2022-IND-13-01)[19] identified a number of open issues (Taylor et al., 2024), namely:

1) The existence of fragmented lifecycle considerations, with unclear guidance on the responsibilities of manufacturers and especially healthcare delivery organisations across each lifecycle stage, particularly relevant in emerging multi stakeholder scenarios. Furthermore, limited specificity of the guidance on user environment transitions or practical, step-by-step processes for each stage limit usability.
2) Potential enhancements to both the regulations and the guidance to better address complex supply chains and legacy systems. Of particular relevance in an operational environment where third-party sub-components and libraries are usually incorporated, and for use-cases where the devices continue in operation following the finalization of official vendor support.
3) A misalignment between the principles of security, privacy, and patient safety, with no direct mapping regarding how breaches in confidentiality, integrity or availability may harm the patient; furthermore, it lacks guidance regarding the necessary balancing of strong security measures with immediate patient safety options (e.g. emergency overrides) which are necessary in real-world situations. Additionally, the guidance presents limited precision regarding the integration of cybersecurity threat modelling into the clinical risk assessment practices.

[16] Unlike other bodies tasked with a similar coordination and clarification function, like the European Data Protection Board, the MDCG's enforcement authority is limited due to the non-binding nature of the guidance it generates. While MDCG is not a standardization body, the relevance of its guidance for implementers is still notable.

[17] It is noteworthy that chapter 6 of this document also includes guidance in harmonizing the MDR and IVDR with GDPR, NIS and the CRA, although this section is rather limited.

[18] Which are to be reported to competent authorities as per MDR/IVDR requirements.

[19] The call counts with six EU funded projects, and among those, the ENTRUST project (European Commission, n.d.; ENTRUST n.d.).

4) Remaining need for harmonization with the state-of-the art[20]: the 2019 version of this guidance remains the latest published by MDCG[21], and predates newer EU regulatory efforts described in the first section of this paper, as well as older versions of relevant standards. This is further complexified by the ever-evolving threat panorama, where advanced threats and technologies (e.g. AI/ML driven devices/attacks) are not sufficiently covered.

This last point, and particularly the need to harmonize MDCG guidelines with relevant standards and certification avenues available today are especially relevant. Indeed, industry stakeholders have expressed a need for "recipes", practical case studies, and role-specific examples (for manufacturers or system integrators), all part of the necessary education and capacity-building processes[22] expected from authoritative sources[23]. To this, we may add that the MDCG guidelines could benefit from a longer and clearer assessment on how the MDR integrates and harmonizes with the other relevant EU regulations such as the GDPR, CRA, NIS2 and the AI Act.

The results of this gap analysis serve to showcase some of the limitations to the MDCG guidance, which also affect traditional standardization processes. In particular, slow adaptation to technological and jurisprudential evolution, fragmentation and overlapping frameworks (as well as harmonization difficulties amongst local, regional, national and international authorities, in the specific case of guidance), amongst others.

The above-mentioned limitations of the MDCG guidance are also echoed in recent academic literature. Han et al. (2024), based on interviews with 28 regulatory professionals across the medical device industry, emphasize challenges such as the complexity of legal language, fragmentation of oversight bodies[24], and the need for a centralized regulatory database in Europe. Amaral et al. (2024) perform a comparative review of regulatory systems in the EU, US and Japan and identify a “medical device lag” associated with the delay in the approval and adoption of medical devices. Lie et al. (2020) explore how software development practices are met by emerging regulatory demands upon the classification of software as an “active medical device” and propose a potential alignment of development cycles with compliance needs through agile methodologies (and DevOps in particular).

The observations on the current limitations of regulatory guidance such as the MDCGs cybersecurity document point to a broader need for emerging standardization processes to overcome structural inertia and recognize stakeholders’ need for agile, interoperable and

[20] Which resonates with similar perspectives from (Freyer et al., 2024; Granlund et al., 2021; Schwartz et al., 2018), which noted the potential uncertainty generated by harmonized standards, the potential gaps on cybersecurity risk recognition in MDs, and the need to acknowledge legacy systems and organizational processes on the manufacturing supply chains.

[21] With no current plan for its update (see https://health.ec.europa.eu/document/download/f588a5c8-57af-48aa-808f-1d9c02f4925a_en?filename=mdcg_ongoing-guidance.pdf)

[22] The authors also noted challenges in establishing common terminology between healthcare practitioners and technology service providers.

[23] Of particular relevance for SMEs seeking to enter the market and/or deploy compliant systems, as standards and certification criteria can provide officially validated “checklists” to support and exemplify the pathway for adequate and safe technology adoption.

[24] Noted by the author as a “regulatory quagmire”, reinforced by the proliferation of notified bodies in Europe vis-à-vis a central agency like the FDA in the US.

responsive compliance validation frameworks in face of the increasingly complex regulatory landscape.

These limitations are visible, for example, in the temporal gap between the publication of MDCG cybersecurity guidance (last updated in 2019) and the subsequent adoption of major regulatory instruments such as the 2022 NIS2 Directive, the 2024 Cyber Resilience Act, and the 2024 AI Act. As a result of this gap, manufacturers and healthcare providers must reconcile newer lifecycle and incident-response obligations with guidance that predates these regulatory developments, often without clear procedural alignment.

In this context, emerging standardization processes should evolve in step with contemporary development practices, and recognize the value of rapid iteration, continuous delivery and embedded compliance as pathways to operationalize regulatory requirements. By doing so, standards may shift from retrospective checklists towards becoming dynamic compliance tools for governance, particularly through their operationalization via frameworks like ENTRUST. This perspective directly informs the discussion in Section 4, where we explore how a dynamic standardization and certification model can be made actionable.

4 The ENTRUST Approach: Automated Trust Assessment and Lifecycle Oversight

The recommendations by MDCG regarding post-market surveillance and cybersecurity vigilance[25] are particularly relevant to this paper, as they touch upon the feasibility of performing continuous conformity assessment and vulnerability management in medical devices upon their deployment, particularly given the previously noted issues regarding clarity of the requirements for the various stakeholders involved in an MD's lifecycle in a modern healthcare environment.

As previously noted, Taylor et al. (2024) mention that vulnerability management (identifying weaknesses and determining appropriate actions throughout a device's lifecycle) "has been explored very little with regard to medical devices." The authors observed that regulations impose obligations manufacturers cannot fulfil independently of healthcare delivery organization, such as minimizing risks based on deployment environments. Indeed, these practices are partially addressed by current standards in their dispositions regarding life-cycle risk management for medical devices, as found in ISO 13485:2016 (International Organization for Standards [ISO], 2016) (Clauses 8.21 & 8.2.2)[26] and ISO 14971:2019[27] (ISO, 2019b), however no comprehensive framework is currently available which integrates these obligations with broader device security and performance monitoring requirements[28].

In the concluding remarks of the gap analysis, the authors highlight the need to note a potential way forward through the endorsement of Toolkit solutions capable of supporting, which introduce dynamic conformity assessment and vulnerability management throughout the

[25] And in alignment with MDR art. 83.

[26] Which has been recognized as a harmonized standard under the MDR (European Commission, 2021).

[27] Also mentioned in ISO/TR 20416:2020 (ISO, 2020b) as part of the guidance on post-market surveillance for product safety and performance enhancements.

[28] ISO 14971:2019's (ISO, 2019b) approach to risk management is largely focused on patient safety rather than on cybersecurity threat management, and ISO 13485:2016's (ISO, 2016) guidance does not directly address an evolving cybersecurity panorama where vulnerability monitoring, incident response coordination, and software patching protocols must be considered.

lifecycle of CMDs enablers. The ENTRUST approach presented below puts this idea into practice by applying a Zero Trust mindset and introducing a structured way to assess and verify device trustworthiness. The ENTRUST project (European Commission, n.d.) (ENsuring Secure and Safe CMD Design with Zero TRUST Principles), is a research and innovation action project within the Horizon Europe programme (HORIZON-HLTH-2022-IND-13-01), which seeks to enhance the security, privacy and trustworthiness of connected medical devices by introducing, amongst other enablers, a dynamic trust assessment model capable of continuously evaluating the security status of these devices across their life-cycle.

A core innovation of ENTRUST lies in its Zero Trust Approach, by which each connected medical device must continuously demonstrate its trustworthiness rather than being trusted by default. To operationalize this idea, ENTRUST introduces the Trust Assessment Framework (TAF), which dynamically evaluates the trustworthiness level of each CMD during enrolment and operation through the calculation of their Actual Trust Level (ATL), which is compared with their Required Trust Level (RTL). In this context, trust refers to cybersecurity properties verifiable through a remote attestation process, such as operational-integrity, safety or resilience, rather than to broader sociotechnical notions of trust discussed in AI ethics and governance. Thus, trustworthiness can be formally measured and used to manage the technological solution according to quantified policies: devices may carry out a specific interaction with the digital system only when they fulfil the required trustworthiness policy.

Concretely, the TAF computes the Actual Trust Level (ATL), based on real-time attestation evidence such as trusted-computing base integrity check, attestation results, and detected anomalies. This ATL is then compared against the Required Trust Level (RTL), which is determined from the device's protection profiles, and reflects the threats, vulnerabilities, and security requirements associated to the device and its deployment environment. For the full technical details, we refer to ENTRUST (n.d.).

By performing these comparisons continuously, the TAF provides ongoing oversight across the device's lifecycle. When a device's ATL falls below its RTL, for example due to a failed attestation, newly detected vulnerability, or suspicious behaviour, the TAF automatically triggers appropriate countermeasures to restore trust, such as temporarily isolating the device. This dynamic process ensures that emerging risks are addressed as soon as they appear, strengthening system resilience and supporting real-time conformity with regulatory and cybersecurity requirements. This trust assessment model is conducted in three phases:

1) Risk assessment and trust quantification: the initial assessment of the device is carried out during manufacturing, associating devices with Required Trust Level and attestation policies based on its security posture, known threats and vulnerabilities, and requirements from its protection profiles[29]. This assessment is subsequently refined and revalidated in the pre-deployment and runtime phase using domain-specific risk recalculations and runtime attestation device and used as the baseline for trust evaluation.
2) Deployment: this phase entails the authentication, onboarding, and enrolment of the device into the domain, as well as the generation of the required cryptographic material, that can be used to provide trustworthiness evidence. Also, the Required Trust LeveL

[29] Each device operates under a Protection Profile which defines the specific security and attestation requirements it should meet. This profile is established during manufacturing and dynamically updated in response to newly identified threats or failed attestations, and may be based, e.g., in an extension of Manufacturer Usage Description files (Matheu et al., 2019)

(RTL) calculated during the manufacturing stage is updated accordingly by the Risk Assessment component, followed by the updating of the Trust Policy and the Trust Model Templates.

3) Continuous attestation, mitigation and countermeasures: CMDs are required to provide cryptographic guarantees of identity, integrity, and trust-relevant information, which is validated by the TAF and results in the computation of an Actual Trust Level (ATL), if a device's ATL falls under the RTL, the TAF triggers corrective security actions.

The validity of the device trust assessment is guaranteed through the application of Formal Verification (FV), which uses mathematical and cryptographic proofs to define the device's inherent security and its initial Required Level of Trustworthiness (RTL)[30].

The core metrics (TAF, RTL and ATL) and methodologies for the Zero Trust operational architecture were co-created by the partners with an iterative design process, that included an analysis of the status quo in the medical device domain, a review of existing standards and regulations, and the integration of feedback from real-world use case partners. The mathematic and cryptographic proofs were designed using Subjective Logic, which was specifically chosen due to its theoretical grounding and flexibility in allowing the aggregation of trustworthiness evidence from other sources (such as remote attestation and AI-based Misbehaviour Detection). These design choices were continuously refined based on feedback from technical partners and use case demonstrators, ensuring the resulting framework addressed practical healthcare needs.

4.1. Defining Trust and Trustworthiness in a Zero-Trust Architecture

When explaining the operational mechanics of the Trust Assessment Framework (TAF), it is crucial to distinguish between "trustworthiness" as an objective property and "trust" as a subjective decision. Following the taxonomy established in ISO/IEC TS 5723:2022 (ISO, 2022a), trustworthiness refers to the verifiable ability of a system to perform as expected under given conditions (encompassing characteristics such as security, safety, reliability, and privacy). In contrast, trust is the belief or confidence that a user (or another system) places in the device based on evidence of its trustworthiness.

Critically, scholars such as Tartaro (2024) have argued that technical standards often attempt to encode trustworthiness as purely neutral metrics, potentially ignoring that the definition of "acceptable risk" is inherently value-laden and context-dependent. A device deemed "trustworthy" in a general ward may not meet the higher risk threshold required for an ICU setting. The ENTRUST project acknowledges this challenge. The TAF does not automate the ethical decision of whether a device should be trusted in a sociological sense; rather, it seeks to automate the quantification of technical trustworthiness (e.g., patch status, encryption integrity, behavioral anomalies) using Subjective Logic. This yields an "Actual Trust Level" (ATL) that serves as transparent, auditable evidence, allowing human operators or automated policies to make informed trust decisions aligned with the specific risk appetite (or "value system") of the healthcare context.

4.2. Establishing the Root of Trust at Manufacturing

[30] This foundational trust is reinforced by Software Verification (including techniques like fuzzing and malware scanning) to establish a secure operational baseline, often summarized as a "golden hash". The assessment results are formalized in Protection Profiles, which act as the immutable, verifiable blueprints against which the device's runtime performance is continuously measured, assuring the enduring correctness of the initial assessment.

The validity of the dynamic trust assessment is predicated on an initial, immutable anchor established during the manufacturing phase. ENTRUST relies on a hardware-based Root of Trust (RoT) provisioning process to guarantee this baseline. During manufacturing, a unique, immutable cryptographic identity[31] is assigned to the device. This process is governed by Formal Verification methods, which utilize mathematical proofs to verify that the device's boot code and initial configuration strictly adhere to the specified "Protection Profile".

This creates a "Golden State": a cryptographically signed baseline of the device's hardware and software integrity. The RoT ensures that the device's identity cannot be cloned and that its initial software load has not been tampered with. Any subsequent deviation from this state during operation (e.g., malware injection, unauthorized firmware modification) breaks the cryptographic chain of trust rooted in the hardware, causing the device's Actual Trust Level (ATL) to degrade immediately. Thus, the correctness of the initial assessment is guaranteed not by manual inspection, but by the cryptographic binding of the device's physical identity to its certified software state.

This approach and its various stages are then completed with a dynamic certification model, that leverages conformity certificates that are issued by TAF when the verification and attestation phases are confirmed. W3C specifications, including the Verifiable Credential (VC) data model, are not harmonized standards under EU law, although they may be channelled through ISO/IEC JTC1, as W3C is a PAS submitter. Their use here is due to the strong interoperability focus of this technology for verifiable data, enhanced because the specifications are being widely adopted in contexts such as self-sovereign identity and EU initiatives such as eIDAS 2.0 and the European Digital Identity Wallet.

These certificates are cryptographically bound to each specific device and follow a privacy-by design principle, revealing only the necessary information (attested attributes) in each usage. Particularly, privacy-preserving Attribute-Based Credentials are proposed for the issuance and presentation of Conformity Certificates, enabling selective disclosure of trust attributes associated with the device. To increase flexibility, these CCs are represented following the W3C's Verifiable Credential format, and alternatives such as the use of Physically Unclonable Function (PUF)-based authentication are proposed for lower-end devices for which the performance of complex cryptographic operations may not be feasible. This flexibility will allow covering varied use cases, balancing privacy features with computational efficiency.

This dynamic certification process is supported by a blockchain infrastructure that maintains an immutable, verifiable log of security assessments, and is further validated by an AI-based anomaly detection solution which identifies deviations and triggers certification revocation or re-validation if necessary.

Although standards like ISO 14971 (ISO, 2019b) focus on safety and others like ISO/IEC 27001 (ISO, 2022b) address cybersecurity, few frameworks integrate both dimensions comprehensively. ENTRUST's approach demonstrates that while individual standards may remain domain-specific, their harmonized implementation—enabled by dynamic certification tools—can achieve the integrated outcomes regulators are seeking.

To ensure real-world applicability and validate its dynamic certification framework, the ENTRUST project is currently implementing four pilot demonstrations across six diverse

[31] Typically, a private key generated within a Secure Element (SE), Trusted Platform Module (TPM), or Physically Unclonable Function (PUF)

healthcare scenarios. These pilots are designed to test and refine ENTRUST's capabilities across a spectrum of real-world healthcare environments, namely:

1) Dynamic trust assessment in ECG monitoring portable devices and complex stationary devices in a hospital setting: where the project applies real-time trust assessment and swarm attestation to portable and stationary ECG devices in a cardiology clinic, ensuring integrity in complex hospital networks.
2) Ambient intelligent system for supporting independent and safe living: where ENTRUST supports trustworthy and secure access to devices in home and institutional care through Personal Health Gateways (PHGs), thus enhancing autonomy and data protection.
3) Digital assistance towards enhancing the health and well-being of patients and carers (in smart ambulance systems): which integrates legacy and wearable devices with secure update pipelines with continuous attestation and trust management during patient transport.
4) Compliant protection of wearable devices for mental health monitoring and integrity of accompanying data: ENTRUST will ensure software updates in a zero-trust manner to enhance privacy of the device and patient.

These pilots are expected to showcase measurable outcomes, and as such, they represent a necessary step to validate the potential of the ENTRUST model for providing scalable, certifiable, and adoptable solutions within the European healthcare landscape. In line with their expected activities, the demonstration of ENTRUST's solutions and pilots presents interesting avenues to expand the trustworthiness of certifications granted to medical devices[32].

Indeed, the project seeks to bridge security and privacy standardization gaps by aligning with EU cybersecurity standards while harmonizing its approach with the requirements found in the various regulatory frameworks that recognize certification as a mechanism to demonstrate regulatory compliance. In this context, the project's enablers present interesting avenues to enhance and support traditional certification processes (either towards supporting claims of compliance in real-time or for triggering non-compliance-based re-certification processes).

As a final element to consider at this stage, properly distinguishing between benefits already observed in existing dynamic certification schemes and those expected from the application of ENTRUST's technical enablers. While schemes such as Europrivacy already demonstrate the

[32] Including the situations when Medical Devices incorporate open-source components. Indeed, an integral part of ENTRUST is not only to use but to generate open-source software. As such, the project has considered the benefits and challenges. ENTRUST's dynamic assessment model provides a valuable pathway for addressing potential certification issues in these contexts by enabling traceability, vulnerability scanning, and real-time monitoring of open-source artefacts.

While the W3C is not an official European Standardization Organization (ESO) like CEN or CENELEC, there is a well-established pathway for W3C specifications (such as the Verifiable Credentials Data Model used by ENTRUST) to become Harmonized European Standards. The W3C is an approved PAS (Publicly Available Specification) Submitter to ISO/IEC JTC 1. This mechanism allows W3C Recommendations to be fast-tracked into International Standards; a precedent was set when the W3C's Web Content Accessibility Guidelines (WCAG) 2.0 were transposed into ISO/IEC 40500:2012 (ISO, 2012).

Once adopted as an ISO/IEC standard, the Vienna Agreement allows CEN/CENELEC to adopt the text as a European Standard (EN), as was done with EN 301 549 for accessibility. If this EN is subsequently cited in the Official Journal of the EU (OJEU), it grants a presumption of conformity with EU legislation. Alternatively, recent regulations like the EU AI Act and the CRA empower the European Commission to adopt "Common Specifications" where harmonized standards are absent, potentially referencing widely adopted technical specifications like those from the W3C directly to ensure interoperability.

feasibility of modular, updateable certification criteria, ENTRUST extends this model by introducing automated trust evidence and continuous surveillance mechanisms whose operational effectiveness is currently being validated through pilot deployments.

The project results showcased in this paper suggest that dynamic certification aided by automated mechanisms has the potential to address several shortcomings of static conformity assessment models, provided that appropriate governance, auditability, and oversight mechanisms are maintained. That being said, the extent to which these approaches can be generalized will depend on sector-specific risk profiles, regulatory expectations, and the maturity of supporting technical infrastructures.

5 Towards a dynamic standardization and certification model, the case of Europrivacy and Interprivacy

The ENTRUST project brings together 20 partners from different countries and expertise, including technology development, healthcare, regulatory compliance, academia and certification. This multidisciplinary collaboration is supported by partners with dedicated experience and involvement in the development of European standards and regulations. As previously noted, the project seeks to operationalize the integration of security and privacy enhancing systems onto connected medical devices, validating these actions through various pilots, and integrate these solutions with the Europrivacy and Interprivacy certification models as part of its conformity assessment tools and processes. These models are further described in section 4.1. Before examining these models in detail, it is necessary to revisit and highlight the need for certification as a critical mechanism for ensuring trust, transparency and compliance (Ziegler et al., 2022). As noted in the previous sections, emerging regulations impose highly dynamic compliance obligations, creating challenges for businesses, regulators, and certification bodies alike. It is a common criticism[33] that compliance models guided or supported by the results of generally adopted standardization processes may result in one-time certifications that follow a multi-year-long review cycle and often struggle to keep pace with regulatory updates, emerging risks, and evolving jurisprudence (see for instance Ruohonen et al., 2025; Marotta & Madnick, 2021).

Traditional certification models are typically rigid and periodic, requiring organisations to undergo manual, resource-intensive audits at fixed intervals. This approach, while providing an initial compliance snapshot, lacks mechanisms for continuous validation, leading to several critical shortcomings, ranging from compliance lag, lack of real-time monitoring, high costs and inefficiencies, and regulatory disconnection. These serious shortcomings highlight the need for a shift towards a dynamic certification mechanism.

[33] The limitations of traditional, "point-in-time" certification models are well-documented in regulatory science literature and economic analysis. Research by MedEnvoy Global (2025) analyzing FDA 510(k) and PMA pathways indicates that the static certification process for high-risk devices can incur costs ranging from $1 million to $4 million per device and delay market entry by 18 to 30 months. In the context of cybersecurity, this latency is critical; a study by MedTech Europe (2023) highlighted that the administrative burden of recertification for post-market software changes discourages rapid patching, creating a "Patching Paradox" where regulatory compliance inadvertently increases security exposure windows. Furthermore, Marinovic et al. (2018) describe an "over-certification trap" where firms in static regimes over-invest in signaling compliance rather than improving dynamic quality. Dynamic certification aims to dismantle this paradox by replacing manual recertification with automated, continuous monitoring that validates security updates against pre-defined protection profiles in real-time.

By dynamic standardization we refer to a standardization process and governance model which departs from traditional and often slow standard drafting and update methods, for the adoption of an agile approach where the standard of reference for the certification itself is not only modular but also subject to a continuous improvement approach. Using the regulatory framework (and latest developments in the jurisprudence, technique and best practice) as a baseline, dynamic standardization enables the continuous evolution of criteria through permanent (and procedurally specified) communication processes between certification bodies, regulators and technical communities.

By dynamic certification we refer to the shift from one-size-fits-all certification pathways toward modular, adaptive certification processes and dynamic methodologies that are tailored to match the characteristics and contextual requirements of the Target of Evaluation (ToE), and that, upon being granted, ensure that each granted certification can continuously evolve and remain relevant to showcase real-world conditions, technological change, and regulatory developments to data subjects and interested stakeholders. A dynamic certification provides continuous feedback to a dynamic standard, which can be generated on the basis of real-time evidence thus ensuring the standards always respond quickly to incidents, trends and industry needs. Furthermore, a dynamic certification process facilitates oversight by software and human auditors (through machine-readable and verifiable conformity profiles), which reaffirms the model's compliance with the regulatory requirements for certifications to be provided by third-parties, integrating and securing the validity of this dynamic approach within the traditional audit process (e.g. ISO 19011/17021-1 (ISO, 2011a)) in the form of technology-enhanced continuous surveillance of each granted certification.

Unlike previous models based on static and one-time certification, a dynamic certification mechanism uses automated tools to keep assessment continuously up to date. It relies on real-time audit logs and AI-driven risk assessments that allow the mechanism to adapt requirements as conditions change. A dynamic approach to certification enables leveraging continuous trust verification mechanisms (as proposed by ENTRUST) during the certification maintenance stages, serving as automated certification surveillance solutions, which ensure ongoing regulatory alignment and enable a more transparent certification process towards the data subjects. These processes are relevant because of their adaptability and flexibility, as they rely on modular criteria and hybrid frameworks that can address multiple regulatory requirements at once.

Dynamic certification can also generate opportunities to solution providers, certification bodies, standardisation development organizations and researchers to closely work and align with regulations and legislators, as the systems and methodologies constantly generates rich data and evidence that can support regulatory processes.

To give examples, Europrivacy and Interprivacy are representatives of this dynamic standardization and certification approach. They are designed to provide scalable, recognized, and technology-agnostic compliance solutions. They provide (1) real-time certification updates based on evolving laws, jurisprudence, and enforcement trends, (2) automated assessment tools to generate verifiable compliance reports, and (3) a modular, extendable architecture that ensures cross-domain applicability.

5.1 Understanding Europrivacy and Interprivacy

The development of Europrivacy (n.d.) and Interprivacy (n.d.) marks a fundamental shift in how data protection certification is approached, moving from static and region-specific certifications to dynamic and globally scalable models.

Europrivacy and Interprivacy are certification schemes. They function as standards that can be triggered by interested parties in order to assess the compliance of their data processing activities with major data protection regulations such as the GDPR. Their difference is in reach and scope. Europrivacy allows certification within Europe and Interprivacy is its international counterpart and includes regulations such as CBPR Framework and APEC Privacy Framework (see below). The goals of these certifications are to reduce legal and financial risks, simplify compliance management, facilitate international data transfers and value certification.

The Europrivacy Certification Scheme was developed within the European research program and formally recognized in October 2022 by the European Data Protection Board (EDPB) as the first official European Data Protection Seal under Article 42 of the GDPR. It was further accredited in March 2024 by European Accreditation (EA), enabling certification bodies to issue legally recognized Europrivacy certifications.

Europrivacy plays a crucial role in legal compliance as it enables certification bodies accredited under Art.42 GDPR to audit and certify data processing activities. Europrivacy is also recognised across EU jurisdictions, ensuring harmonized enforcement, and its extension capabilities allow organizations to incorporate national- and domain-specific regulations.

With the increasing demand for internationally recognized data protection certifications, the European Centre for Certification and Privacy (ECCP) leveraged its expertise from Europrivacy to create Interprivacy, a globally applicable certification framework. Interprivacy was developed to overcome jurisdictional fragmentation by providing a neutral and interoperable certification mechanism that aligns with:

- Convention 108+ (Council of Europe)
- General Data Protection Regulation
- Global Cross-Border Privacy Rules (CBPR) System

Interprivacy builds upon Europrivacy's foundation and provides flexible certification pathways, including Interprivacy for standard international compliance, and Interprivacy+, an enhanced solution with additional compliance checks. Crucially, while Europrivacy is formally recognized under Articles 42 and 43 of the GDPR as an EU Data Protection Seal, Interprivacy is designed as a separate, voluntary international framework. Because Interprivacy does not seek formal EDPB approval under Art. 42, it avoids the specific procedural constraints of the European regulatory "lock-in," allowing for broader, more agile adoption in jurisdictions outside the EEA.

Both frameworks utilize a dynamic certification model that combines universal and specialised certification approaches, meaning their criteria can be updated dynamically based on jurisprudence, technological evolution, and policy changes. Both Europrivacy and Interprivacy are designed for cross-sector application, enabling compliance with multiple regulatory frameworks, including:

- Healthcare & Medical Devices
- Cybersecurity & Digital Services
- Artificial Intelligence & Emerging Technologies, including the EU AI Act.

- Financial Services & Cross-Border Data Flows

Within the ENTRUST project, Europrivacy and Interprivacy guide the research towards a real-time dynamic certification approach, which is herein discussed.

5.2 Dynamic certification models

Dynamic certification models have emerged in response to the challenges of regulating and overseeing compliance in complex, high-risk, and rapidly evolving systems. Unlike traditional certification approaches (often rigid and static), these models leverage real-time data, modular standards, and continuous oversight to keep pace with technological and regulatory change. For example, Quigley et al. (2025) proposed a framework based on blockchain for real-time monitoring of maritime environmental compliance (specifically MARPOL) using smart contracts and IoT integration. Bakirtzis et al. (2023) suggest the implementation of codified checks and balances that include embedded regulatory constraints for autonomous systems such as Unmanned aerial vehicles and ground-based robots. These approaches exemplify the shift towards dynamic frameworks where certifications evolve alongside the system they assess, and auditors are increasingly supported by monitoring and context-aware risk evaluation solutions.

One of the most groundbreaking aspects of Europrivacy and Interprivacy is their ability to integrate automated compliance mechanisms, transforming certification from a static, periodic process into a continuously verifiable framework. Instead of relying on manual audits at set intervals, the adoption of modular frameworks tailored to match the Target of Evaluation and its contextual technical and organizational framework, allowing for the use of machine-generated compliance reports to serve as verifiable certification evidence. AI-driven risk assessments deployed by the certification owner's technical and research providers further enhance compliance by detecting potential non-conformities in real time, minimizing regulatory exposure while ensuring ongoing adherence.

Beyond automation, real-time surveillance mechanisms track compliance status and trigger audits or recertifications when anomalies are detected. Unlike traditional models that require scheduled reassessments, these frameworks dynamically respond to:

- Regulatory changes or new legal interpretations.
- Evolving jurisprudence and enforcement practices.
- Security incidents that impact data processing integrity.

Another major innovation is their modular criteria, which are continuously expanded and aligned with the expected requirements and protection profiles across multiple regulatory sectors. Traditional certification models struggle to remain relevant across industries, but Europrivacy and Interprivacy adapt dynamically, incorporating risk-based compliance benchmarks for cybersecurity, medical devices, and artificial intelligence governance. Their ability to extend certification scope beyond privacy laws makes them a cornerstone for cross-sector compliance in an increasingly complex regulatory environment.

Both Europrivacy and Interprivacy have been designed with sufficient technical, organizational and procedural elements to integrate seamlessly with ENTRUST's real-time trust models, which define Required Trust Levels (RTL) for data processing activities. Instead of viewing certification as a one-time attestation, ENTRUST enables continuous trust assessment, dynamically adjusting compliance requirements based on evolving risks. Europrivacy and Interprivacy support this by acknowledging the validity of ENTRUST's automated policy

enforcement, AI-driven auditing, and blockchain-based certification proofs, as enablers to support compliance efforts, empowering Certification Bodies[34] and reassuring Data Subjects[35] through auditable, transparent and explainable systems.

When paired with legally recognized dynamic standardization and verifiable technical enablers, dynamic certification thus signifies a step evolving beyond a simple demonstration of compliance. It becomes a mechanism to actively contribute to resilience, support accountability, and foster adaptability, thereby promoting long-term, multistakeholder trust in connected healthcare systems.

6 Conclusions

The European healthcare sector's rapid digitalization and interconnectivity bring forth an increasing need for robust cybersecurity and data protection mechanisms. The European regulatory environment has evolved to address this need, and increasingly relies on standards to provide clarity, and on certifications to demonstrate compliance.

This is not to say that the current regulatory panorama is perfectly aligned with the emerging needs. Guidance generated by the various authorities presents gaps that still need to be addressed, and which call for more detailed, up-to-date and practically-oriented frameworks which can adapt to evolving threats whilst remaining transparent and understandable by all stakeholders.

Lifecycle-wide oversight of compliance has become the gold standard, and traditional one-time or static certification models are insufficient ways to address the need for real-time response to security threats, regulatory updates, and transparency and trust-generation needs of connected and aware data subjects. Dynamic certification models offer solutions for continuous trust assessment and real-time conformity verification and are compatible with the solutions that are being developed by state-of-the-art research projects such as ENTRUST.

The integration of technical enablers and dynamic certification solutions showcases how cross-sector collaboration can produce improved standards that better meet market and regulatory requirements. This is evidenced by the ENTRUST pilot outcomes, which demonstrate that integrating real-time telemetry into standardization criteria significantly reduces the 'Patching Paradox' (where regulatory delay increases vulnerability windows) common in static models. Ongoing collaboration amongst regulators, industry stakeholders, healthcare providers and certification providers is essential to ensure the viability of these emerging standardization pathways and certification methodologies. In our scenario, for instance, this integration allows a harmonization between a rights-oriented regulation of the GDPR with products and services-oriented dispositions, which are the IVDR, MDR, the NIS2, CRA, Cybersecurity Act and AI ACT. As such, it also facilitates integration with the New Legislative Framework. The approach taken by Europrivacy and Interprivacy provides a promising reference point for other standardization initiatives.

[34] Including for example the initial certification (and subsequent re-certification) decision(s) and the intermediary certification surveillance activities, based upon which the CB and its auditors may take better informed decisions (such as triggering a control audit upon a major breach).

[35] For example, as proposed by the ANASTACIA H2020 project's Dynamic Privacy and Security Seal (see https://cordis.europa.eu/project/id/731558), which sought to provide an easy to understand GUI on the subject of certification which accurately reflected the inputs from automated enablers.

Moreover, the benefits of the ENTRUST framework have potential beyond healthcare. Highly regulated sectors such as finance, banking, and domains involving the use of AI systems (such as manufacturing and transportation) are facing similar pressures in cybersecurity, compliance, and the demand for real-time accountability. The underlying "Patching Paradox" (where administrative burdens delay critical security updates) is a systemic issue in all highly regulated ICT environments. By replacing manual audits with automated, Subjective Logic-based assessments, the model provides the same real-time resilience for financial services or smart manufacturing that it offers to medical ecosystems. In this context, ENTRUST's model, anchored in continuous trust evaluation, AI-driven auditing, and blockchain-based evidence, can help these sectors maintain ongoing compliance across the lifecycle of digital systems.

Finally, ENTRUST's dynamic certification approach (grounded in real-time data and lifecycle-wide trust assurance) is built to be reproducible, offering opportunities for application in different sectors and in larger scale. This can be a practical example for European and International research and standardization efforts. For example, the ENTRUST approach could be leveraged to support EU-wide assurance levels, especially under schemes like EUCS or EUCC being developed by ENISA. Notably, the current review of the Cybersecurity Act (currently under public consultation) may provide opportunities to incorporate dynamic certification models such as ENTRUST's onto future official EU-wide assurance frameworks.

Grant

This work is supported by the ENTRUST project (Horizon Europe, Grant Agreement No. 101095634).

Contributor Statement

Adrian Quesada Rodriguez: Writing original draft, presentation (EURAS Conference), review and editing

André Cardozo Sarli: Writing original draft, literature research, review and editing.

Renáta Radócz: Visualization, review and editing

Sébastien Ziegler: Supervision, support for the funding acquisition, review and editing

Augusto Díaz-Ordóñez González: Literature research.

Antonio Skarmeta: Conceptualization, Funding acquisition, Methodology, Project Administration, Investigation, Validation, review and editing.

Jesús García Rodriguez: Project administration, investigation, validation, review and editing.

Gilson Javier Delgado Rodriguez: Conceptualization, investigation, validation, review and editing.

Use of AI

During the preparation of this work, the authors used Google AI Search, Gemini and Claude in order to perform background research and to proofread and enhance the readability of the output text. After using these tools/services, the authors reviewed, edited, made the content their own and validated the outcome as needed, and take full responsibility for the content of the publication.

Acknowledgements

We also acknowledge the contributions of parallel Horizon Europe projects for their collaborative inputs on the gap analysis of MDCG 2019-16.

Conflict Of Interest (COI)

There is no conflict of interest

References

Alslaity, A., Orji, R., Oyebode, O., Fowles, J., Steeves, D., & Suruliraj, B. (2022). Mobile Applications for Health and Wellness: A Systematic Review. *Proceedings of the ACM on Human-Computer Interaction*, *6*(EICS), 1-29. https://doi.org/10.1145/3534525

Amaral, C., Paiva, M., Rodrigues, A. R., Veiga, F., & Bell, V. (2024). Global Regulatory Challenges for Medical Devices: Impact on Innovation and Market Access. *Applied Sciences*, *14*(20), 9304. https://doi.org/10.3390/app14209304

Bakirtzis, G., Carr, S., Danks, D., & Topcu, U. (2023). Dynamic Certification for Autonomous Systems. *Communications of the ACM*, *66*(9), 64–72. https://doi.org/10.1145/3574133

Beckers, R., Kwade, Z., & Zanca, F. (2021). The EU medical device regulation: Implications for artificial intelligence-based medical device software in medical physics. *Physica Medica*, *83*, 1–8. https://doi.org/10.1016/j.ejmp.2021.02.011

Boardman, S. (2021). Creating wellness apps with high patient engagement to close the intention–action gap. *International Psychogeriatrics*, *33*(6), 551–552. https://doi.org/10.1017/S1041610220003385

Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 Laying down Rules for the Application of Regulation (EU) 2019/881 of the European Parliament and of the Council as Regards the Adoption of the European Common Criteria-Based Cybersecurity Certification Scheme (EUCC). (2025). http://data.europa.eu/eli/reg_impl/2024/482/2025-01-08/eng

DIGITALEUROPE. (2024, December 13). Strengthening healthcare cybersecurity: Focus on implementation, not new legislation. *DIGITALEUROPE*. Retrieved March 4, 2025, from https://www.digitaleurope.org/resources/strengthening-healthcare-cybersecurity-focus-on-implementation-not-new-legislation/

ENTRUST. (n.d.). *Secure & Safe Connected Medical Devices*. Retrieved March 5, 2025, from https://www.entrust-he.eu

European Medicines Agency (EMA). (2018, November 26). *Medical devices* [Text]. https://www.ema.europa.eu/en/human-regulatory/overview/medical-devices

European Commission. (n.d.). *ENsuring Secure and Safe CMD Design with Zero TRUST Principles (ENTRUST). CORDIS.* Retrieved March 5, 2025, from *https://cordis.europa.eu/project/id/101095634*

European Commission. (2020, January 7). *Guidance on Cybersecurity for medical devices* (*MDCG 2019-16 Rev. 1)*. https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf

European Commission. (2021, July 19). *Commission implementing decision (EU) 2021/1182 of 16 July 2021 on the harmonised standards for medical devices drafted in support of Regulation (EU) 2017/745 of the European Parliament and of the Council*. https://eur-lex.europa.eu/eli/dec_impl/2021/1182/oj

European Commission. (2024, July 26). Medical Devices—Dialogue between interested parties. https://health.ec.europa.eu/medical-devices-dialogue-between-interested-parties_en

European Union Agency for Cybersecurity. (n.d.). *About EU Cybersecurity Certification*. ENISA. Retrieved May 19, 2023, from https://certification.enisa.europa.eu/about-eu-cyber-certification_en

Europrivacy. (n.d.). Europrivacy Certification. Retrieved April 28, 2022, from https://europrivacy.com/en/frontpage

Freyer, O., Jahed, F., Ostermann, M., Rosenzweig, C., Werner, P., & Gilbert, S. (2024). Consideration of Cybersecurity Risks in the Benefit-Risk Analysis of Medical Devices: Scoping Review. *Journal of Medical Internet Research*, *26*, e65528. https://doi.org/10.2196/65528

Granlund, T., Vedenpaa, J., Stirbu, V., & Mikkonen, T. (2021). On Medical Device Cybersecurity Compliance in EU. *2021 IEEE/ACM 3rd International Workshop on Software Engineering for Healthcare (SEH)*, 20–23. https://doi.org/10.1109/SEH52539.2021.00011

Han, Y., Ceross, A., & Bergmann, J. (2024). More than red tape: Exploring complexity in medical device regulatory affairs. *Frontiers in Medicine*, *11*, 1415319. https://doi.org/10.3389/fmed.2024.1415319

Hemanth, D. J., Anitha, J., & Tsihrintzis, G. A. (Eds.). (2021). *Internet of Medical Things: Remote Healthcare Systems and Applications*. Springer International Publishing. https://doi.org/10.1007/978-3-030-63937-2

International Electrotechnical Commission. (2020a, July 27). *IEC 60601-1-6:2010 Medical electrical equipment—Part 1-6: General requirements for basic safety and essential performance—Collateral standard: Usability*. https://webstore.iec.ch/publication/67381

International Electrotechnical Commission. (2020b, June 17). *IEC 62366-1:2015 Medical devices—Part 1: Application of usability engineering to medical devices*. https://webstore.iec.ch/publication/67220

International Electrotechnical Commission. (2021, September 21). *IEC 80001-1:2021 Application of risk management for IT-networks incorporating medical devices—Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software*. https://webstore.iec.ch/publication/34263

International Medical Device Regulators Forum. (2023, April 13). *Medical Device Cybersecurity Guide*. https://www.imdrf.org/working-groups/medical-device-cybersecurity-guide

International Organization for Standardization. (2004). *Health informatics—Point-of-care medical device communication—Part 20101: Application profiles—Base standard* (ISO/IEEE 11073-20101:2004). https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/03/63/36347.html

International Organization for Standardization. (2007). *Health informatics — Use of mobile wireless communication and computing technology in healthcare facilities — Recommendations for electromagnetic compatibility (management of unintentional electromagnetic interference) with medical devices* (ISO/TR 21730: 2007). https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/04/48/44865.html

International Organization for Standardization. (2009). *Medical device software—Part 1: Guidance on the application of ISO 14971 to medical device software* (IEC/TR 80002-1:2009). https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/41/54146.html

International Organization for Standardization. (2011a). *Guidelines for auditing management* systems (ISO 19011:2011). https://www.iso.org/standard/50675.html

International Organization for Standardization. (2011b). *Information technology—Security techniques—Guidelines for information security management systems auditing* (ISO/IEC 27007:2011). https://www.iso.org/standard/42506.html

International Organization for Standardization. (2012). *Information technology — W3C Web Content Accessibility Guidelines (WCAG) 2.0* (ISO/IEC 40500:2012). https://www.iso.org/standard/58625.html

International Organization for Standardization. (2015). *Conformity assessment—Requirements for bodies providing audit and certification of management systems—Part 1: Requirements* (ISO/IEC 17021-1:2015). https://www.iso.org/standard/61651.html

International Organization for Standardization. (2016). *Medical devices—Quality management systems—Requirements for regulatory purposes* (ISO 13485:2016). https://www.iso.org/standard/59752.html

International Organization for Standardization. (2019a). *Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines* (ISO/IEC 27701:2019). https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/16/71670.html

International Organization for Standardization. (2019b). *Medical devices—Application of risk management to medical devices* (ISO 14971:2019). https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/27/72704.html

International Organization for Standardization. (2020a). *Medical devices—Guidance on the application of ISO 14971* (ISO/TR 24971:2020). https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/44/74437.html

International Organization for Standardization. (2020b). *Medical devices — Post-market surveillance for manufacturers* (ISO/TR 20416:2020). https://www.iso.org/standard/67942.html

International Organization for Standardization. (2021). *Health software—Part 2: Health and wellness apps—Quality and reliability* (ISO/TS 82304-2:2021). https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/81/78182.html

International Organization for Standardization. (2022a). *Trustworthiness—Vocabulary* (ISO/IEC TS 5723:2022). https://www.iso.org/standard/81608.html

International Organization for Standardization. (2022b). *Information security, cybersecurity and privacy protection—Information security management systems—Requirements* (ISO/IEC 27001:2022). https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/08/28/82875.html

Interprivacy. (n.d.). *The international data protection certification scheme*. https://www.interprivacy.org/

Lie, M. F., Sánchez-Gordón, M., & Colomo-Palacios, R. (2020). DevOps in an ISO 13485 Regulated Environment: A Multivocal Literature Review. *Proceedings of the 14th ACM / IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM),* 1–11. https://doi.org/10.1145/3382494.3410679

Marinovic, I., Skrzypacz, A., & Varas, F. (2018). Dynamic certification and reputation for quality. *American Economic Journal: Microeconomics, 10*(2), 58–82. https://doi.org/10.1257/mic.20160282

Marotta, A., & Madnick, S. (2021). Convergence and divergence of regulatory compliance and cybersecurity. *Issues in Information Systems, 22*(1), 10–50. https://doi.org/10.48009/1_iis_2021_10-50

Matheu, S. N., Hernández-Ramos, J. L., Pérez, S., & Skarmeta, A. F. (2019). Extending MUD Profiles Through an Automated IoT Security Testing Methodology. *IEEE Access*, *7*, 149444–149463. IEEE Access. https://doi.org/10.1109/ACCESS.2019.2947157

MedEnvoy Global. *(2025, November 18). How much does it cost to sell medical devices in Europe?* https://medenvoyglobal.com/blog/how-much-does-it-cost-to-sell-medical-devices-in-europe/

MedTech Europe. (2023, May). *MedTech Europe's vision for cybersecurity in the medical technology ecosystem—Position paper*. https://www.medtecheurope.org/resource-library/medtech-europes-vision-for-a-resilient-medical-technology-ecosystem-position-paper/

Quigley, W. C., Rahouti, M., & Weiss, G. M. (2025). *A Secure Blockchain-Assisted Framework for Real-Time Maritime Environmental Compliance Monitoring (Version 1)*. arXiv. https://doi.org/10.48550/ARXIV.2503.08707

Regulation (Eu) 2017/745 Of The European Parliament And Of The Council of 5 April 2017 on Medical Devices, Amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and Repealing Council Directives 90/385/EEC and 93/42/EEC, 117/1 OJ L (2021). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on Medical Devices, Amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and Repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA Relevance.), 117 OJ L (2017). http://data.europa.eu/eli/reg/2017/745/oj/eng

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (2019). https://eur-lex.europa.eu/eli/reg/2019/881/oj

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA Relevance) (2024). http://data.europa.eu/eli/reg/2024/2847/oj/eng

Ruohonen, J., Hjerppe, K., & Kang, E.-Y. (2025). A mapping analysis of requirements between the CRA and the GDPR. arXiv. https://doi.org/10.48550/arXiv.2503.01816

Schwartz, S., Ross, A., Carmody, S., Chase, P., Coley, S. C., Connolly, J., Petrozzino, C., & Zuk, M. (2018). The Evolving State of Medical Device Cybersecurity. *Biomedical Instrumentation & Technology*, *52*(2), 103–111. https://doi.org/10.2345/0899-8205-52.2.103

Tartaro, A. (2024). Value-laden challenges for technical standards supporting regulation in the field of AI. *Ethics and Information Technology, 26*(4). https://doi.org/10.1007/s10676-024-09809-y

Taylor, S., Gilje Jaatun, M., Bernsmed, K., Androutsos, C., Frey, D., Favrin, S., Rodrigues, J., Milojević, D., Karras, D., Siachos, I., Epiphaniou, G., Moukafih, N., Messinis, S., Rallis, I., Protonotarios, N., Gedeon, P., Castillo, A., Maple, C., Matragkas, N., … Katzis, K. (2024). A Way Forward for the MDCG 2019-16 Medical Device Security Guidance. *Proceedings of the 17th International Conference on PErvasive Technologies Related to Assistive Environments*, 593–599. https://doi.org/10.1145/3652037.3663894

World Health Organization (WHO). (n.d). *Quality of care*. Retrieved March 5, 2025, from https://www.who.int/health-topics/quality-of-care

Ziegler, S., Huamani, A. M. P., Miteva, S.-M., Quesada Rodriguez, A., & Radocz, R. (2022). Europrivacy Paradigm Shift in Certification Models for Privacy and Data Protection Compliance. In S. Schiffner, S. Ziegler, & A. Quesada Rodriguez (Eds.), *Privacy Symposium 2022* (pp. 73–84). Springer International Publishing. https://doi.org/10.1007/978-3-031-09901-4_5

Ziegler, S., Radócz, R., Quesada Rodriguez, A., & Matheu Garcia, S. N. (Eds.). (2024). *Springer Handbook of Internet of Things*. Springer International Publishing. https://doi.org/10.1007/978-3-031-39650-2