Towards a Holistic Certification Approach for IoT Trust and Identity Management Framework – The ERATOSTHENES approach

Konstantinos Loupos, INLECOM INNOVATION, Athens, Greece

Harris Niavis, INLECOM INNOVATION, Athens, Greece

Konstantinos Ntafloukas, INLECOM INNOVATION, Athens, Greece

Jesús García-Rodríguez, University of Murcia, Murcia, Spain

Antonio Skarmeta (Author), University of Murcia, Murcia, Spain

George Athanasiou, DIADIKASIA Business Consulting S.A., Athens, Greece

Sokratis Vavilis, INLECOM INNOVATION, Athens, Greece

Nektarios Hatzichristodoulou, DIADIKASIA Business Consulting S.A., Athens, Greece

Abstract

With countless devices influencing our daily lives and a variety of industries, the Internet of Things (IoT) has created a new era of interconnectedness. However, this extensive connectivity has also increased the potential attack surface, making people and their devices more susceptible to cyberattacks, which are becoming more frequent and sophisticated, making security maintenance extremely difficult. The huge variety of devices is one of the main obstacles to IoT security. The capabilities, interfaces, processing power, and architectures of these devices, which come from various manufacturers, differ significantly. Implementing a consistent security approach is practically impossible due to this heterogeneity. In a setting this dynamic, traditional, conventional security measures are useless. Furthermore, a lot of IoT devices are resource-constrained, which makes it difficult to put strong security measures in place and leaves them vulnerable to attacks. The IoT ecosystem complexity adds another level of challenge. Data exchange and secure communication protocols are necessary for integrating platforms and devices. Another major issue is handling the enormous volumes of data produced. Sensitive data can be compromised, and user privacy is at risk in the absence of appropriate security procedures and data governance plans. Additionally, new, decentralized security models are required due to the growth of edge computing. Due to its distributed nature, it is more difficult and necessitates creative methods for access control and data protection. Another serious risk is supply-chain vulnerabilities. Adversarial assaults are one of the new hazards brought about by IoT systems' growing reliance on AI and machine learning. Alongside these difficulties, a rising legacy of susceptible devices is produced by the short lifespan of certain IoT devices and the absence of reliable update procedures. Interoperability is hampered and comprehensive security management is extremely difficult due to the lack of common security protocols across the broad IoT ecosystem. Lastly, traditional security boundaries are blurred and new attack vectors are introduced with potentially serious real-world repercussions when IT/OT networks combine, in industrial IoT.

The ERATOSTHENES project is developing a security framework for IoT devices to address challenges like device heterogeneity, limited resources, evolving cyber threats, and privacy

concerns. The framework is distributed, automated, auditable, and privacy-respectful. It includes dynamic trust management, decentralized identity management, and lifecycle management of IoT devices. The project has been validated through three industrial use cases: V2X communication security, remote patient monitoring, and industrial network security with disposable IDs. The framework dynamically assesses device trustworthiness, manages identities, and provides a secure basis for managing trust-related information. It leverages blockchain technology and AI threat analysis models to enhance security. The ERATOSTHENES project aims to create a more secure and trustworthy IoT ecosystem by addressing key security and privacy challenges. In this direction, the ERATOSTHENES project orchestrates a novel distributed, automated, auditable, yet privacy-respectful, Trust and Identity Management Framework and Reference Architecture. Its vision is to dynamically and holistically manage IoT devices in a lifecycle approach, strengthening trust, identities, and resilience in the entire IoT ecosystem while supporting the enforcement of the NIS2 directive, GDPR and the European Union's Cyber Resilience Act.

In this position paper, we discuss the overall cyber security challenges aligned with its research and industrial vision and results and its contribution over a targeted certification approach. This incudes diving into particular use cases and highlighting the cascading challenges of daily threats in operations and processes of IoT devices, networks and infrastructures.

1. Introduction

The Internet of Things (IoT) has brought a new era of interconnected devices and seamless data exchange. IoT has recently given rise to an era of ubiquitous interconnectivity, deploying devices on a massive scale that directly or indirectly impact various industrial sectors. Several key industries benefit from IoT technology, such as the automative sector (e.g., connected vehicles), or healthcare sector (e.g., remote patient monitoring). Despite the benefits that IoT introduces to various industries, mainly applicable to enhanced operational efficiency, it comes with certain security challenges. Indeed, the deployment of IoT devices contributes to the development of an environment ruled by enhanced interoperability and interconnectivity, but at the same time leads to a sharp increase of the attack surface, with the creation of numerous IoT-enabled attack paths [1]. At the same time, the complexity of the situation is further intensified by the vast heterogeneity of IoT devices. These devices originate from multiple vendors and feature diverse capabilities, interfaces, processing power, and architecture. This variability makes it challenging to implement a standardized security approach. Traditional, one-size-fits-all security solutions prove ineffective in such a dynamic and ever-evolving environment. Moreover, the resource limitations of many IoT devices hinder the deployment of robust security measures, making them attractive targets for attackers. The growing complexity of IoT ecosystems further amplifies these challenges. Integrating diverse devices and platforms requires secure communication protocols and reliable data exchange mechanisms. Additionally, handling the vast amount of data generated by these devices presents another significant concern. Without effective security protocols and strong data governance strategies, user privacy is at risk, and sensitive information may be exposed.

Both past events and research studies highlight the need for the development of a holistic approach purely aligning with the management of IoT device lifecycle. For example, during the Mirai Botnet Attack (2016), the Mirai malware infected thousands of IoT devices by exploiting weak default passwords. These compromised devices formed a botnet that launched massive Distributed Denial-of-Service (DDoS) attacks, taking down major websites (e.g., Netflix) [2]. Furthermore, the Amazon Ring camera hacks of 2019 were a series of incidents where hackers gained unauthorized access to Ring security cameras, operating as IoT devices, allowing them to spy on and even communicate with users through the device's two-way audio [3]. These hacks raised significant concerns about privacy and security vulnerabilities in Ring devices. Similarly, research studies emphasize the necessity of robust lifecycle management for IoT devices, which include secure onboarding, regular firmware updates, and secure decommissioning processes to mitigate potential vulnerabilities throughout a device's operational life, while the adoption of decentralized security frameworks that leverage blockchain technology are considered as key [4].

Apart from the detailed concerns, as described above, emerging trends in IoT security certification require further investigation. For example, blockchain technology provides decentralized and tamper-resistant recordkeeping, enhancing trust and transparency in IoT security certification. By utilizing blockchain, certification processes can ensure the immutability and auditability of records, simplifying the validation of security claims for IoT devices and systems. Furthermore, consensus algorithms play a significant role in defining the network's security properties and efficiency, as the cornerstone of blockchain [5, 6]. Indeed, emerging trends highlight the importance of automated and continuous certification. By leveraging continuous monitoring, real-time threat intelligence, and automated assessment tools, certification processes become more agile and adaptive, ensuring that certified devices uphold their security posture over time. As concerns about data privacy continue to rise, emerging trends in IoT security certification are placing greater emphasis on privacy-centric approaches. Certifications that incorporate privacy-by-design principles, data minimization, and user consent management are gaining importance in ensuring compliance with regulations like GDPR. At the same time, AI and ML algorithms can analyze vast amounts of data and identify potential security risks, enabling more efficient and proactive certification approaches. Last, as the IoT landscape grows, the interoperability and standardization of security certification frameworks become increasingly essential. Emerging trends focus on creating common standards and frameworks that facilitate the seamless integration of certified devices and systems across various domains and regions.

It is clear that a comprehensive solution must cover the different phases, from initial bootstrapping of security mechanisms during device manufacturing, to its secure deployment, operation and decommissioning. The ERATOSTHENES project tackles the complex security challenges of the IoT, with a focus on managing the entire lifecycle of these networks, with a specific focus on distributed trust management and digital identity solutions. The focal point is the development of a Trust and Identity Management Framework for IoT devices, distributed and operating across the entire network, addressing different steps of the lifecycle of the participant devices. Additionally, the framework is auditable, enabling transparent tracking and verification of actions. Finally, it is privacy-respectful, prioritizing user data privacy and control. By effectively managing the lifecycle

of IoT devices, this framework aims to strengthen trust, identities, and overall resilience within the IoT ecosystem. This aim and the approaches taken in the project are aligned with NIS Directive, GDPR and Cyber-Resilience Act. This white paper seeks the dissemination of knowledge related to the analysis of such challenges and potential recommendations, supporting the enforcement of such regulations and standardization activities and highlighting the needs for certification.

2. Overview of ERATOSTHENES Project

The ERATOSTHENES project addresses the intricate security challenges of the IoT, by focusing on comprehensive lifecycle management, with an emphasis on distributed trust management and digital identity solutions. At its core, the project develops a Trust and Identity Management Framework that operates across the entire IoT network, covering various stages of a device's lifecycle. This framework is auditable, ensuring transparent tracking and verification of actions, and privacy-conscious, prioritizing user data protection and control. By effectively managing IoT device lifecycles, it aims to enhance trust, identity security, and overall resilience.

2.1 ERATOSTHENES architecture

The ERATOSTHENES architecture, as shown in Figure 1, has been meticulously designed for adaptability across multiple industrial domains. It is structured to accommodate various use cases, specific requirements, and the unique characteristics of different application environments. The architecture envisions an environment with multiple independent (but potentially collaborating through information exchange) domains, serving to group operations depending on physical or logical criteria. These domains are organized based on physical or logical criteria to streamline operations. The components of the structure architecture will act within the device, pertain to a specific domain, or operate across multiple ones to enable global functionalities.

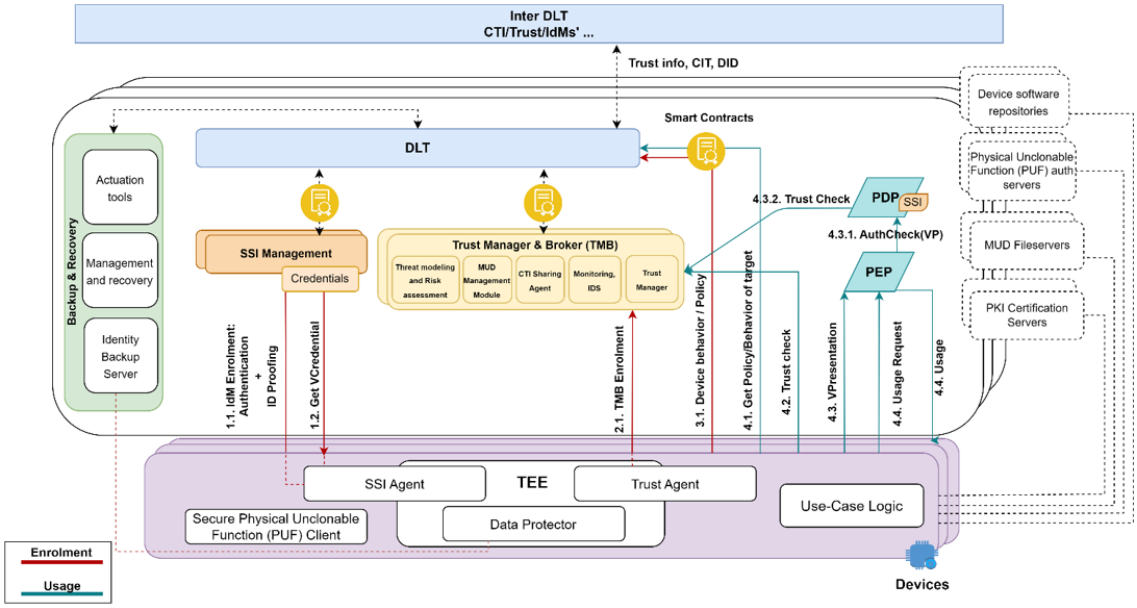

Figure 1. ERATOSTHENES architecture

The main features of ERATOSTHENES architecture are based on identity management grounded in self-sovereign principles. Specifically, by utilizing Self Sovereign Identity (SSI) Agents within devices, it enables to handle credentials, ensuring security and privacy while integrating key infrastructural components like SSI Management. To further strengthen identification security and cryptographic fingerprinting, the approach incorporates Physical Unclonable Function (PUF)-based authentication. Trust Management & Broker (TMB) integrates essential components to establish a trust framework built on zero-trust principles. Devices engage with this framework through Trust Agents, while the Trusted Execution Environment (TEE) serves as a foundational anchor of trust, reinforcing both device security and identity management. In addition to identity and trust, architecture also addresses device lifecycle management through various supporting tools, including backup, recovery, secure data storage, and management solutions (such as actuation tools, recovery mechanisms, and data protection). It also incorporates Manufacturer Usage Description (MUD) files and Cyber Threat Intelligence (CTI) sharing to enhance security configurations and enable coordinated responses to cyber threats. The entire ecosystem is powered by Distributed Ledger Technologies (DLTs), serving as verifiable data registries enhanced with smart contracts. Notably, key information, such as Cyber Threat Intelligence (CTI) and identity data—can be shared across domains through inter-DLT mechanisms, enabling collaboration and fostering a globally interconnected ecosystem with strengthened security.

3. ERATOSTHENES Project and certification activities

The rapid growth of IoT has drastically increased the number of connected devices, bringing significant security and privacy challenges across various industries. As these devices become deeply integrated into critical systems and everyday life, their vulnerabilities can have widespread consequences. To address these risks, the European Union's Cyber Resilience Act (CRA) introduces strict requirements to establish a cybersecurity baseline for IoT products throughout their entire lifecycle. By placing responsibility on manufacturers to secure devices throughout their entire lifecycle, the CRA seeks to ensure that devices are secure by design, fit for purpose, and protected against emerging threats. Additionally, cyber incidents and cyber-threat intelligence must be shared across ecosystems aiming for a widespread improvement on the security of solutions and the achievement of a collaborative cyber-shield. In order to achieve that, the CRA sets to:

- Facilitate the secure development of digital products and their components.
- Define cybersecurity rules for placing products on the market.
- Define requirements for the design, development, and production of products.
- Define requirements for the processes for handling vulnerabilities.
- Establish rules on market surveillance and enforcement.
- Establish different proof of conformity processes (self-declaration, third-party assessment) depending on the category the products fall in.

The CRA's scope and impact on IoT devices makes it very relevant to ERATOSTHENES. Lifecycle management, threat detection, sharing and mitigation techniques, secure identification, timely security update. Are all relevant to the goals of the regulation. To illustrate the implications of the CRA in the project, we use the Intelligent Transport System pilot in ERATOSTHENES as a reference in the context of the challenges and scenarios in a real-world use case. The CRA is a very horizontal piece of legislation with common cybersecurity requirements for all products, regardless of sector or field of application. Most of the devices involved in the pilot would most likely fall under the CRA scope (e.g., IoT nodes, OBUs and road-side units, gateway etc.). Indeed, Article 2 of the CRA text says that the regulation applies to products with digital elements made available on the market, which includes a direct or indirect logical or physical data connection to a device or network.

3.1 Industrial Challenges and certification activities

Deeper into our analysis, we focus on an indicative and highly challenging environment such as this of connective vehicles as a reference pilot of the ERATOSTHENES project. As the CRA recently came into force and its obligations are still further away in the future, even though the text is stable, many aspects will be delegated to implementing acts. Thus, the analysis herein presented might need to be revised when the details and the actual application of the CRA will occur after a transition period. In addition, ERATOSTHENES remains a research project, and we do not claim to perform any conformance test, nor do we plan to undergo a certification process within the context of this exercise. In fact, the complex issue of conformity assessment of such solutions remains a gap in the regulation's context. Thus, we discuss here the pilot and its use cases in the context of the CRA to bring a better understanding of the project impact being developed in close alignment with the reality of the industry, the law, and its evolution, in order to facilitate the adherence to such regulatory context. The ERATOSTHENES architecture and its components can be a step toward alignment with the CRA and its implementation, and particularly for the core roles covered by lifecycle management and information sharing.

The number of connected devices in the automotive industry has grown over the years, and this increase comes along with the evolution of the hardware and software that is integrated into vehicles and infrastructures. Modern vehicles can interact with other connected devices to retrieve information about other vehicles or infrastructures (e.g., vehicles, smart traffic lights, smart speed signs, etc.) to make driving more comfortable and advise for the best possible decision while supporting smart-city and smart-connectivity trends. However, this progress is also accompanied by concerns of the automotive industry about possible cyber threats and the safety reduction of pedestrians or drivers. This connection can be exploited by cyber criminals to carry out attacks remotely, modifying the vehicle behavior or hindering its function. The 155 and 156 of the United Nations regulations are proof of this worry, standardizing cybersecurity and a software update process that the manufacturers must follow on their products [7]. In this situation, the pilot deals with the interaction of the vehicle with the infrastructure devices, where a vehicle will be the victim of attacks. This illustrates the deployment methodology followed in a highly distributed scenario, as well as the way in which the technologies developed during the ERATOSTHENES project can detect bad behaviors in the network, identify the potential malicious actors and finally, be able to

deal with a cyber-attack. The pilot focuses on two scenarios or use cases: The first use case is focused on the secure communication between the vehicle and its exterior devices on the road (i.e., V2X). The scenario uses a vehicle that communicates through an OBU with a smart traffic light. The vehicle will act according to the inputs that it receives from this infrastructure device. A second vehicle fitted with an OBU is also present. The aim of this additional vehicle, and the third actor in the scenario, is to send conflicting/malicious messages to the first vehicle, trying to destabilize the previous established communication between the first vehicle and the infrastructure (smart traffic light). The second use case faces one of the most challenging and newest worries of the automotive world which is the remote software updates.

3.1.2 Industrial Applications and the link to CRA

The CRA aims to embed cybersecurity as a fundamental consideration in the design, development, and production of products with digital components. As emphasized in various policy discussions, its successful implementation would ensure a security-by-design approach for all manufacturers selling products in the EU market. This goal can be achieved by enforcing essential cybersecurity requirements and ensuring that products are free from known vulnerabilities before reaching consumers. Industrial challenges start with the secure bootstrapping and enrolment of the devices in a network (for example involved in V2X communication) into a security domain. Similarly to the essential requirements of the CRA, the certifications and security assets introduced during manufacturing will be key during this process and serve as a root of trust for the process. Additionally, we need to highlight the operation and monitoring of such devices in a secure way leaning on the results of such enrolment. This relates to several pillars and topics within the CRA, but especially on the provisions about lifecycle and vulnerability management. If, for instance, a rogue device injects false traffic control data with the aims of performing harmful actions to the connected vehicles, the ERATOSTHENES framework, will be able to detect it, and inform about it in a privacy preserving manner through the exchange of Cyber-Threat Intelligence (CTI). Of course, when a vulnerability is detected, one or more digital products within the systems might no longer be compliant with the CRA or at least be impacted by a “known exploited vulnerability”. As the CRA requires market operators to act throughout the product’s lifecycle providing support, updates, or mitigation measures, the automated CTI sharing will be key in starting (and completing) such processes.

What is more, the analysis goes a step further, covering the vulnerability handling process. In particular, it takes into account the essential requirement established by the CRA on the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the time the product is expected to be in use. Once vulnerability is identified, the manufacturer must take immediate action to address the issue. This may involve bringing the product or manufacturing processes into compliance or, if necessary, withdrawing or recalling the affected product. The ERATOSTHENES framework allows for not only the detection and notification of vulnerabilities, but also automated collection and application of mitigation measures thanks to the application of CTI sharing techniques and the application of extended Manufacturer Usage Description files. This enables the identification and handling of any anomalous behavior while helping security domains comply with cybersecurity regulations.

The second set of challenges involves remote software updates for example again in the automotive sector and is particularly one of the key potential outcomes of a vulnerability handling process. Again, the CRA is explicit in the obligation to support and update digital products, especially in case of vulnerabilities. The ERATOSTHENES framework provides tools for addressing these processes, and particularly for the management of the lifecycle of the device in a secure manner taking advantage of secure execution, monitoring, trust and strong identity management. Particularly, as mentioned above, the usage of the extended MUD file emerges as a key solution for many of the challenges established. Each actor can, collaboratively, contribute, update and provide a state of the security of the system.

The application of the MUD file (and its expressiveness extensions along with Threat MUDs as proposed in ERATOSTHENES) meets the spirit of many of the regulatory provisions contained in the CRA text. Such a tool would help with the dispatching of newly discovered vulnerabilities as well as their mitigation. The enforcement of the latest MUD file policies would support the creation of evidence of a secure state of the system, providing a basis to build on for notification and reporting purposes.

The legislation emphasizes that market operators should systematically document key cybersecurity aspects of products with digital elements, including any known vulnerabilities and relevant information from third parties. They are also required to update the cybersecurity risk assessment of their products as needed. Additionally, the CRA introduces detailed notification and reporting requirements for exploited vulnerabilities and major incidents, featuring new elements such as a Single Reporting Platform and a Single Point of Contact for manufacturers. The extended MUD file further strengthens collaboration among stakeholders, promoting a more cohesive approach to IoT security. These measures align with the need for cooperation among key entities involved in vulnerability management and incident response, such as Computer Security Incident Response Teams (CSIRTs), ENISA, and Single Points of Contact. Ideally, the extended MUD file could also serve as a foundation for conformance documentation, whether self-assessed or verified by a third party.

3.1.3 Further Challenges

While this position paper gives an overview of the CRA and some potential recommendations and approaches that may help in the context of the regulation, there remain challenges that should be addressed for a successful implementation of the regulation act with high impact on the digital security in the European Union. First, it is necessary to tackle potential issues regarding the awareness and knowledge of relevant stakeholders with respect to the CRA. The scope of the CRA, whether it applies to specific products, or how it interacts with other relevant security standards and regulations might not be fully clear to all groups such as different market operators. This document aims to serve as a small step to improve awareness through the contextualization of some of the CRA in the technological scope of the ERATOSTHENES project and a real-world pilot. On another note, while the timeline for the CRA adoption is becoming clearer with its coming into force in December 2024 and foreseen obligations starting at 2027, the availability of standards, standardization requests and relative official decisions will result in a complex schedule and

deadlines that relevant stakeholders should be prepared to address. Some organizations will have to deal with their structural complexity both in terms of the size of their portfolio or the complexity of the product with digital elements they develop, requiring more time to adapt the development process in line with the CRA. This is also true for time needed to adapt to the essential requirements related to the processes' organizations will need to adopt. Lastly, it is necessary to clarify and enable the processes for showing conformance or certification within the scope of the CRA for all relevant stakeholders. While the issue of certification is challenging in itself, the issue is further exacerbated in the scenarios of complex supply chains, where several manufacturers and integrators may be involved in the creation of a product with digital components, and the distribution of responsibility will not be trivial.

3.2 Gaps and Challenges Summary

- *Lack of Adaptive Certification Models*

Current certification frameworks struggle with adaptability to emerging IoT threats. Traditional static evaluation processes do not accommodate real-time risk assessment or continuous security validation. There is a need for more dynamic, AI-driven certification mechanisms that can adjust security assurance levels based on evolving threat intelligence [8].

- *Fragmented IoT Supply Chain and Compliance Complexity*

IoT ecosystems consist of diverse components sourced globally, each with its own security posture. Existing certification schemes do not account for the end-to-end security of interconnected devices, making it difficult to validate overall system security. There is a need for a modular certification approach that ensures compliance across multi-vendor environments [9].

- *Inconsistent Security Metrics and Benchmarking*

Certification bodies use varying security evaluation criteria, creating inconsistencies in risk assessment. Standardized, quantifiable security metrics are required to ensure comparability across different certification schemes and geographies [10].

- *Security of Legacy IoT Devices*

Many legacy IoT devices lack embedded security features, yet they remain operational in critical infrastructures. There are no well-defined certification pathways for integrating retrofitting security mechanisms into legacy systems. A structured certification framework for secure post-market cybersecurity enhancements is needed [11].

- *Regulatory Gaps in AI-Driven and Autonomous Systems*

As IoT devices increasingly incorporate AI and autonomous decision-making, current certification models do not evaluate AI security risks, adversarial machine learning attacks, or explainability in automated security enforcement. Future frameworks should integrate AI security validation mechanisms [12].

3.3 Bridging the gap to current security certification approaches

While current security certification approaches contribute to security requirements, they often come with certain limitations that ERATOSTHENES targets to address.

For example, *Common Criteria* (CC) is widely regarded as the foremost cybersecurity certification standard [13]. It establishes security functional and assurance requirements for a Target of Evaluation (TOE), which includes software, firmware, and/or hardware. These requirements are outlined through Protection Profiles (PPs) and documented in the Security Target (ST) description. Although CC is the leading standard, the cybersecurity community has identified certain limitations. For example, documenting the evaluation and collecting evidence, especially at higher EALs, can be both time-consuming and resource-intensive. Additionally, managing changes in a certified product during manufacturing may lead to market delays and substantial financial losses *ENISA* has developed the first European cybersecurity certification scheme based on Common Criteria (CC), known as the Common Criteria-based European Candidate Cybersecurity Certification Scheme (EUCC Scheme) [14]. The EUCC Scheme is intended to replace existing schemes under the Senior Officials Group Information Systems Security (SOG-IS) Mutual Recognition Agreement (MRA), introducing new elements and expanding its scope to all EU Member States. While this initiative marks an important step toward a unified and harmonized certification framework in Europe, the current document primarily focuses on the certification structure. Specific details regarding lifecycle processes, vulnerability management, and mechanisms for information sharing are only briefly addressed. Notably, the EUCC is the first European scheme developed under the Cybersecurity Act (CSA). In addition, other certification schemes are in progress, including the European Cybersecurity Certification Scheme for Cloud Services (EUCS), which already has a draft version, and future plans for a 5G certification scheme. The *Certification de Sécurité de Premier Niveau (CSPN)* is a French cybersecurity standard introduced by the National Cybersecurity Agency of France (ANSSI) in 2008 [15]. It ensures impartiality by requiring evaluations to be conducted by ANSSI-accredited auditors. The primary goal of CSPN is to assess whether products comply with their specifications, evaluating them against known vulnerabilities and subjecting them to rigorous security testing. CSPN complements the Common Criteria (CC) and serves as a preliminary, time-efficient, and cost-effective assessment before pursuing CC certification. However, CSPN is specific to France and does not operate under a Mutual Recognition Arrangement (MRA), limiting its role in fostering a harmonized cybersecurity certification framework. The *IoT Security Compliance Framework* is a structured set of security requirements and an evidence-gathering process designed to help organizations achieve assurance and demonstrate compliance [16]. It is based on the Best Practice Guidelines provided by the IoT Security Foundation (IoTSF). The certification issued under this framework has an unlimited validity period and is supported by documentation, including a best practice guide and a compliance checklist for vulnerability management. The recommended process follows the ISO/IEC 29147 standard. However, it is important to note that the framework does not cover post-certification risk analysis and management, which remain the responsibility of the developer or vendor. The *Eurosmart IoT Security Certification Scheme* (e-IoT-SCS) is specifically designed for Internet of Things (IoT) devices, aiming to achieve a high level of security

assurance as outlined in the Cybersecurity Act [17]. It underscores the importance of integrating strong security measures from the initial design and development phases. The scheme includes various processes, such as testing and inspecting samples from both the open market and manufacturing facilities, assessing production and service delivery, evaluating operational processes, and monitoring issued certificates. Additionally, a mandatory temporary mitigation/patching phase ensures an initial level of security before assessing the risks associated with each vulnerability. However, the framework does not specify technical mechanisms for communicating updates or newly identified vulnerabilities. Other schemes include the Singaporean *National IT Evaluation Scheme* (NITES) [18]. It is mandatory for suppliers of IT products to governmental agencies in Singapore. However, the NITES scheme specifications and requirements were not made public by the Cyber Security Agency (CSA). In Germany, the *ULD Datenschutz-Gütesiegel* certifies IT products for compliance with data protection and data security regulations [19]. It covers a broad range of products, including hardware, software, automated processes, and services. While minor modifications may qualify for a simplified certification process, significant changes require a complete recertification.

In 2019, the new EU cybersecurity regulation, the *Cybersecurity Act,* came into effect to establish a unified framework for the cybersecurity certification of ICT products, services, and processes. A key requirement of the Cybersecurity Act is the ongoing monitoring of compliance with European cybersecurity certificates or EU statements of conformity, including mechanisms to ensure continued adherence to specified cybersecurity standards. However, there is still a gap in the security lifecycle management framework, which would help monitor device security compliance while promoting collaboration among certification stakeholders, such as users, manufacturers, and certification. The *Network and Information Security 2 (NIS2)* Directive is an EU legislative act aiming to enhance cybersecurity across EU member states [20]. As a predecessor of NIS1, it establishes a common framework for safeguarding network and information systems in sectors critical to societal functions, such as energy, transportation, and digital infrastructure. The directive promotes cooperation and information sharing among EU member states to prevent and respond to cybersecurity incidents. Under the NIS Directive, member states must adopt national cybersecurity strategies and designate competent authorities responsible for implementing and enforcing its provisions. As the first EU-wide legislation on cybersecurity, the NIS Directive sought to establish a high common level of cybersecurity across Member States. However, its implementation faced challenges, leading to fragmentation within the internal market. To address growing digital threats and the rise of cyber-attacks, the European Commission proposed a replacement, NIS2. NIS2 aims to strengthen security requirements, improve supply chain security, streamline reporting obligations, and introduce more stringent supervisory measures and enforcement, including harmonized sanctions across the EU. The *General Data Protection Regulation (GDPR)* is a thorough data protection law introduced by the EU, which took effect in 2018 [21]. It outlines the rights and principles governing the processing of personal data of individuals within the EU. The GDPR applies to organizations that collect, store, or process the personal data of EU residents, regardless of the organization's location. Specifically, it requires organizations to implement suitable technical and organizational measures to ensure that data protection is integrated from the start and maintained by default.

3.4 ERATOSTHENES contribution

In overall ERATOSTHENES bridges the gap to existing approaches. As detailed above, the main issues originate from the lack of harmonization among the various existing certification schemes, the lack of a streamlined recertification process to ensure that security certificates remain up to date, the resource intensive and complex nature of existing solutions, and the modeling of dependencies due to the multi-layered supply chain ecosystem that further complicates security integration. ERATOSTHENES supports system composition by enabling the reuse of certification information from individual components to certify the entire system, as well as utilizing existing data to update the certificate, and automates the certification process by leveraging advanced tools and techniques that facilitate the identification of threats and evaluation of the security certification claims. Moreover, ERATOSTHENES enhances the cybersecurity evaluation process by providing tools to manage cybersecurity, identifying potential threats that could impact the certificate level, and streamlining the evaluation to focus on the most relevant areas, and emphasizes the importance of collaboration and information sharing among stakeholders within the security certification process.

ERATOSTHENES contributes to managing the IoT security lifecycle by integrating security profiles into the certification process. These profiles define the security properties and usage conditions for IoT devices. Manufacturers can implement mechanisms like MUD and threat MUD to manage security policies during device enrollment and facilitate agile mitigation or reconfiguration when new vulnerabilities are discovered. The framework integrates security information gathering into the device bootstrapping process, collecting details such as MUD, configuration, vulnerabilities, threats, and identity. This information helps assess device risks and determine whether it should be granted network access, as well as the necessary configuration if allowed. This ensures secure device configuration and minimizes attack surfaces. ERATOSTHENES also supports the NIS directive by developing a security information-sharing mechanism based on cyber threat intelligence (e.g., MISP), integrated with an Interledger solution to exchange trust and security information among stakeholders. This fosters collaboration, vulnerability disclosure, and secure software update management. Furthermore, ERATOSTHENES aids GDPR implementation by providing privacy-preserving solutions through a decentralized approach. It will develop decentralized identity management to support self-sovereignty and privacy, utilizing Decentralized Identifiers (DIDs), smart contracts, and context-aware identity management for individuals and devices. Secure communication channels between IoT devices and edge components will ensure privacy preservation and secure interactions.

4. Conclusion

The current outlook in the context of the CRA and cybersecurity regulation showcases the tendency and need for more general awareness as well as clarity on specific topics under the category of compliance and how to practically demonstrate it. There is also a sense of urgency within the ICT community, fueling the idea that the timeline of application of CRA should be well known by market operators and considered seriously, as CRA application is coming fast. The ERATOSTHENES project presents several approaches tightly related to security challenges in the

IoT world, and in particular in the context of the CRA. The work in lifecycle management, threat detection and sharing, and security configuration and mitigation capabilities is relevant to several requirements raised in the regulation such as vulnerability handling processes for assets with digital components. In this report, we give an overview of such relevance in the context of a real-world pilot, improving awareness around these topics. Further, in the upcoming weeks the consortium will build on this document to prepare observations regarding IoT security lifecycle as a report to ETSI technical committee. The work will involve the preparation of a more technical view on the discussed concepts, particularly in relation to the ERATOSTHENES architecture and components.

5. Acknowledgments

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement no 101020416. The authors acknowledge the research outcomes of this publication belonging to the ERATOSTHENES (101020416) project consortium

6. References

1. Loupos, K., H. Niavis, F. Michalopoulos, G. Misiakoulis, A. Skarmeta, J. Garcia, A. Palomares, H. Song, R. Dautov, and F. Giampaolo. *An inclusive lifecycle approach for IoT devices trust and identity management*. in *Proceedings of the 18th International Conference on Availability, Reliability and Security*. 2023.
2. Antonakakis, M., T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J.A. Halderman, L. Invernizzi, and M. Kallitsis. *Understanding the mirai botnet*. in *26th USENIX security symposium (USENIX Security 17)*. 2017.
3. Calacci, D., J.J. Shen, and A. Pentland, The cop in your neighbor's doorbell: Amazon ring and the spread of participatory mass surveillance, Proceedings of the ACM on Human-Computer Interaction 6 (2022) p. 1-47.
4. Pirbhulal, S., S. Chockalingam, A. Shukla, and H. Abie, IoT cybersecurity in 5G and beyond: a systematic literature review, International Journal of Information Security 23 (2024) p. 2827-2879.
5. Michalopoulos, F., S. Vavilis, H. Niavis, and K. Loupos, *Integrating a Hybrid Lightweight Consensus Algorithm in HyperLedger Fabric*, in *International Summit on the Global Internet of Things and Edge Computing*. 2024, Springer. p. 188-203.
6. Niavis, H. and K. Loupos. *Consenseiot: A consensus algorithm for secure and scalable blockchain in the iot context*. in *Proceedings of the 17th International Conference on Availability, Reliability and Security*. 2022.
7. UN Regulation No 156 – Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system [2021/388]. https://op.europa.eu/en/publication-detail/-/publication/ec74fcfc-8079-11eb-9ac9-01aa75ed71a1?utm_source=chatgpt.com, (accessed February 2025).
8. Baral, S., S. Saha, and A. Haque. *An Adaptive End-to-End IoT Security Framework Using Explainable AI and LLMs*. in *2024 IEEE 10th World Forum on Internet of Things (WF-IoT)*. 2024. IEEE.

9. Hamarsheh, A., An adaptive security framework for internet of things networks leveraging SDN and Machine Learning, Applied Sciences 14 (2024) p. 4530.
10. Villegas-Ch, W., R. Gutierrez, I. Sánchez-Salazar, and A. Mera-Navarrete, Adaptive Security Framework for the Internet of Things: Improving Threat Detection and Energy Optimization in Distributed Environments, IEEE Access (2024).
11. Matheu, S.N., J.L. Hernandez-Ramos, A.F. Skarmeta, and G. Baldini, A survey of cybersecurity certification for the internet of things, ACM Computing Surveys (CSUR) 53 (2020) p. 1-36.
12. Che, X., Y. Zheng, M. Zhu, Q. Li, and X. Dong. *A Domain-Adaptive Large Language Model With Refinement Framework For IoT Cybersecurity*. in *2024 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics*. 2024. IEEE.
13. Common Criteria: Official website for the Common Criteria for Information Technology Security Evaluation, a widely recognized security certification standard. . https://www.commoncriteriaportal.org/, (accessed February 2025).
14. EU Cybersecurity Certification Scheme on Common Criteria (EUCC). https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en, (accessed February 2025).
15. Certification de sécurité de premier niveau (CSPN), ANSSI. https://cyber.gouv.fr/decouvrir-les-solutions-certifiees, (accessed February 2025).
16. IoT Security Foundation (IoTSF). https://www.wallarm.com/what/iot-security-foundation-iotsf#:~:text=The%20IoT%20Security%20Foundation%20or,are%20on%20the%20lower%20side., (accessed February 2025).
17. Eurosmart IoT Certification Scheme: Information on the Eurosmart IoT Certification Scheme, which focuses on security certifications for smart devices. . https://www.eurosmart.com/, (accessed February 2025).
18. Singaporean National IT Evaluation Scheme (NITES). https://www.csa.gov.sg/, (accessed February 2025).
19. ULD Datenschutz-Gütesiegel. https://www.datenschutzzentrum.de/, (accessed February 2025).
20. NIS2 Directive: new rules on cybersecurity of network and information systems. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive, (accessed February 2025).
21. The General Data Protection Regulation (GDPR). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434, (accessed February 2025).