EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme

ANUM KHURSHID, REEM ALSAAIDI, MUDASSAR ASLAM, AND SHAHID RAZA, (Senior Member, IEEE)

RISE Research Institutes of Sweden, 114 28 Stockholm, Sweden
BCSS Security Engineering, Ericsson, 164 80 Stockholm, Sweden
Department of Cybersecurity, National University of Computer and Emerging Sciences (NUCES-FAST), Islamabad 44000, Pakistan
Department of Information Technology, Uppsala University, 752 36 Uppsala, Sweden

Corresponding author: Anum Khurshid (anum.khurshid@ri.se)

This work was supported in part by the Swedish Foundation for Strategic Research (SSF) Secure Software for the Internet of Things (aSSIsT) Project, in part by the Horizon 2020 (H2020) Cyber security cOmpeteNCe fOr Research anD InnovAtion (CONCORDIA) Project under Grant 830927, and in part by the Cybersecurity Knowledge Platform at Research Institutes of Sweden (RISE).

ABSTRACT The vulnerabilities in deployed IoT devices are a threat to critical infrastructure and user privacy. There is ample ongoing research and efforts to produce devices that are secure-by-design. However, these efforts are still far from translation into actual deployments. To address this, worldwide efforts towards IoT device and software certification have accelerated as a potential solution, including UK’s IoT assurance program, EU Cybersecurity Act and the US executive order 14028. In EU, the Cybersecurity Act was launched in 2019 which initiated the European cybersecurity certification framework for Internet and Communications Technology (ICT). The heterogeneity of the IoT landscape with devices ranging from industrial to consumer, makes it challenging to incorporate IoT devices in the certification framework or introduce a European cybersecurity certification scheme solely for IoT. This paper analyses the cybersecurity certification prospects for IoT devices and also places article 54 of the EU Cybersecurity Act in an international perspective. We conducted a comparative study of existing IoT certification schemes to identify potential gaps and extract requirements of a candidate IoT device security certification scheme. We also propose an approach that can be used as a template to instantiate an EU cybersecurity certification scheme for IoT devices. In the proposed template, we identify IoT-critical elements from the article 54 of the Cybersecurity Act. We also evaluate the proposed template using the ENISA qualification system for cybersecurity certification schemes and show its qualification on all criteria.

INDEX TERMS Internet of Things, IoT certification, security certification scheme, conformity assessment, EU agency for cybersecurity (ENISA), EU cybersecurity act.

I. INTRODUCTION

The Internet of Things (IoT) is defined as a network of embedded cyber-physical devices that sense and interact with their external environment. The IoT devices by design, generate, operate and transmit data and as a result, devices existing in the vicinity of people capture personal data.

As the number of devices around us increases, the threat to security, safety and privacy is ever greater than before. Hence, security of IoT devices has become a significant concern in the past decade due to the massive amount of data incorporated into cyberspace by IoT devices and the exponentially increasing security incidents involving vulnerable and unpatched IoT devices [1]. Typical IoT devices enable and incorporate commercial-off-the-shelf components in their underlying infrastructure. These components are
often not tested for existing vulnerabilities or enforcement of state-of-the-art security standards [2]. The consequence of these IoT vulnerabilities has resulted in compromise by adversaries affecting IoT devices from video cameras and smart locks to industrial safety systems [1], [3], [4], resulting in incidents of large-scale Distributed Denial-of-Service (DDoS) attacks [3], [5], [6]. Although the availability of security solutions in the market is rapidly increasing, without the enforcement of these mechanisms within devices, the improvement in the security posture of IoT devices cannot be guaranteed. Typically, cybersecurity certification schemes are at the forefront of efforts to establish minimum security requirements, that have to be enforced by vendors and manufacturers.

A cybersecurity certification scheme establishes baseline security, monitors for compliance and regulates the security throughout the IoT device lifecycle [7]. Among other obvious benefits of cybersecurity certification, is the increase in trust on the IoT devices based on compliance with security standards. The assurance of individual IoT device’s software and hardware components also enables their integration in the industry, automotive and medical use cases by meeting regulatory requirements [8]. Hence, establishing a certification framework, unified across the world has taken considerable priority within security and research bodies. However, creating and implementing cybersecurity certification in any domain is still a challenging feat with legal as well as technical considerations to be supported by laws, regulations and technical experts. To address the above challenges, the EU Cybersecurity Act [9], [10] along with efforts across the globe are initiated [11], [12], [13], [14], [15], [16].

In this paper, we present an overview of recent cybersecurity certification schemes and security standards for IoT which will serve as a means to construe the requirements for an EU cybersecurity certification scheme targeting IoT. It becomes imperative here to provide a formal distinction between a security standard and a cybersecurity certification scheme in context of IoT devices. Security Standards are documented procedures, product technical specifications, guidelines, precise criteria, defining the exemplary state of an IoT device. Whereas a Security Certification Scheme encompasses the entire procedure by which a third-party (ideally, trusted) gives a written/recognized assurance that the IoT device is in conformity with standards.

We also propose an approach (building blocks/template) to devise a Security Certification Scheme (SCS) targeting IoT devices. We design this template to assist the creation of a candidate for cybersecurity certification scheme targeting an IoT profile. Our study and proposed template focus on the EU Cybersecurity Act but leverage the efforts of NIST, initiatives from UK [17], Singapore [15], [18] and Finland [16] which aligns with our goal of IoT security through unified certification. We strengthen our proposed certification template by evaluating it against the criteria enlisted in the ENISA qualification system for a potential IoT device certification scheme [8].

A. CONTRIBUTIONS

The main contributions of this paper are listed below.

- A comprehensive study of IoT certification landscape, highlighting key advantages and shortcomings of existing schemes.
- We identify key elements of an IoT Security Certification Scheme (SCS) relevant to EU Cybersecurity Act.
- We propose a template that assists in creation of an eligible IoT Device SCS candidate for an EU cybersecurity certification scheme for IoT.
- We conduct an evaluation of the proposed Template using the well-formed ENISA qualification system and instantiate the Template demonstrating its application.

The rest of the paper is structured as follows. In Section II, we discuss recent literature and efforts towards IoT certification. In Section III, we discuss the EU Cybersecurity Act and the entities involved in the certification process. A comparative discussion about existing certification schemes is included in Section IV, followed by the gap analysis in Section V. We identify key elements and propose a template for IoT Device SCS in Section VI along with an example of instantiating an IoT Device SCS. The proposed template is evaluated in Section VII and the paper concludes with potential future directions in Section VIII.

II. RELATED WORK AND OUR SCOPE

The EU Cybersecurity Act entered into force on 27th of June 2019, strengthening the mandate of the EU Agency for Cybersecurity (ENISA) and launching the European cybersecurity certification framework for Internet and Communications Technology (ICT) digital products, processes and services [9], [10] (including IoT). Since 2019, the government of UK has launched several initiatives to ensure the security of consumer IoT devices [11] including their recent approach to IoT security using product assurance schemes [12]. The Executive Order 14028, has directed the National Institute of Standards and Technology (NIST) to initiate a labeling program on cybersecurity capabilities of IoT [13] and since 2022, NIST has already identified a baseline criterion for consumer IoT and labeling and conformity assessment considerations [14]. In addition to these, there are recent efforts towards unified labelling schemes for IoT security from Singapore [15] and Finland [16].

In our study of the existing IoT cybersecurity certification landscape, we have come across some recent relevant efforts towards identification of challenges related to IoT certification and some others that provide valuable perspectives to the establishment of unified IoT certification across domains and use cases. In this section, we only discuss the related literature on IoT certification published around the launch of the EU Cybersecurity Act and onwards, to stay as relevant as possible in comparison and to our goal of an IoT Security Certification Scheme (SCS) suitable for the EU cybersecurity certification framework.
The work by Matheu et. al is one of the first efforts in proposing risk-based automated assessment and testing methodology for the IoT [19]. It is closely followed by [20] which majorly contributes towards identification of requirements and challenges in establishing a cybersecurity certification framework for the IoT. This work is published in a time frame coinciding with the announcement of the EU Cybersecurity Act and builds on the cornerstone established by [19] that risk-based assessment and testing form the baseline for IoT cybersecurity certification methodology. This remains the common thread in surveys and studies that have followed, exploring the suitability of different security risk assessment and testing methodologies for the IoT infrastructure [21]. Alternatively, our contributions are formulated in the form of a template that can instantiate cybersecurity certification schemes for different IoT scenarios.

An overview of the different security frameworks and certifications internationally is presented in [22]. This research identifies how these international frameworks can be applied to IoT devices. Besides a study of the state-of-the-art, the primary focus of the work is towards labeling methods to convey the certification results indicating a security level to the IoT consumers. The comparisons and results of this work are based solely on the security labels, often isolating them from other IoT dependent factors. In our work, we take the analysis of the state-of-the-art in IoT certification, one step further ahead. In our proposed template, the focus is not on providing the ideal option for testing, evaluating and labeling, but presenting the range of possibilities for IoT security certification schemes to be tailored for different scenarios.

The most recent published work related to our work is the IoT focused systematic study exploring the integration and adaptation of different certification schemes to varying IoT application scenarios [23]. This work answers interesting questions like “What are the requirements that IoT environments expect from certifications?”, “What are the special requirements that different IoT application scenarios impose on certifications?”, and “Are current certifications able to meet the requirements imposed by IoT?”. Contrary to the valuable findings of this research, our work contributes a parent template that can be easily adapted to different IoT profiles to formulate a cybersecurity certification mechanism.

### A. SCOPE OF STUDY

In this section, we briefly summarize how the study was conducted, including the scope of the referenced documents. A comprehensive study of the EU Cybersecurity Act served as the starting point of our analysis. In order to visualize the IoT certification landscape and identify key building blocks, we conducted a systematic search for international cybersecurity certification efforts for IoT (or ICT in the broader context) and credible sources referenced in the EU Cybersecurity Act. Our search for existing certification schemes within EU and internationally, aimed at identifying initiatives either addressing the IoT domain or with potential for IoT suitability. They were thoroughly studied to formulate the requirements of an IoT Device SCS. The second step of our work was to instantiate an example of an IoT Device SCS from the template. The study of the following documents, reports, standards and certification schemes along with relevant IoT literature, assisted us in extracting only the most relevant features and requirements of cybersecurity certification for the constrained domain of IoT.

- Security evaluation standard: Common Criteria (CC) [24].
- Cybersecurity standards: ISO/IEC 17825 [25], ISO/IEC 27400 [26], NISTIR 8228 [27], NISTIR 8259 [28], [29], NISTIR 8259A [30], ETSI EN 303 645 [31], ISO/IEC 29147 [32], ISO/IEC 17065 [33], ISO/IEC 30111 [34].
- Cybersecurity certification schemes for IoT: Eurossmart (e-IoT-SCS) [35], NIST Cybersecurity Labeling [14], Finnish Cybersecurity Label [16], Singapore’s Cybersecurity Labelling Scheme [18], PSA Certified [36].
- State-of-the-art literature on IoT certification, security evaluation, etc. (e.g., [11], [12], [14], [21]).

### III. THE EU CYBERSECURITY CERTIFICATION WITH RESPECT TO IoT

The European Cybersecurity Act launched the European cybersecurity certification framework for Internet and Communications Technology (ICT) digital products, processes and services. A certification scheme, i.e., EUCC scheme (Common Criteria based European candidate cybersecurity certification scheme) is also proposed by ENISA that looks into the cybersecurity certification of ICT products [37]. It is based on the Common Criteria, the Common Methodology for Information Technology Security Evaluation, and corresponding standards, respectively. ISO/IEC 15408 and ISO/IEC 18045. Since this scheme targets the ICT domain in general which raises the question of its applicability to the dynamic IoT lifecycle and relevance of the outcome. The certification is currently voluntary and the European Commission intends to evaluate whether a mandatory certification is needed for specific categories of products and services [9], [10]. The main objective behind mandatory certification is to increase trust in ICT products which is vital for the European Digital Single Market. Hence, we are also not far from a mandatory certification for IoT products which are a part of ICT product category for now. The EU Cybersecurity Act facilitates the creation of risk-based certification schemes as an inclusive set of rules, cybersecurity standards, technical requirements and procedures decreasing the risk of fragmentation in the Single Market, enabling vendors to trade across the Union’s borders and supporting the users to understand the product’s security features. Currently, when we trust products, we trust in the goodwill of the manufacturer. ENISA’s efforts in certification are driven by the ultimate goal of increasing trust in devices and making products safer by shifting the trust anchor to EU-recognized certification bodies. The EU Cybersecurity Act emphasizes on categorizing products and services based on their usecases and computational capabilities. Such a categorization makes...
the task of identifying cybersecurity requirements, relevant standards, technical specifications, evaluation methods and assurance level relatively comprehensible. As per the EU Cybersecurity Act, a self-assessment process for a basic assurance level reduces the overhead of certifying trivial products [9], [10]. An EU-recognized certificate ideally falls in three levels of assurance that are adequate to the risk level associated with the intended use of the IoT device and mirroring the market needs (time, cost and performance). ENISA recommends using the existing technical specifications and standards (European and International) as guiding principles for setting the assurance levels, EU statement of conformity and a baseline for certification [8]. This enables a non-discriminatory certification scheme with common norms promoting international collaboration.

We summarize nine entities below which are defined in the EU Cybersecurity Act for the certification process. Figure 1 shows the certification process tailored for an IoT device.

A. CONFORMITY ASSESSMENT
In order to have regulated ICT products/services or processes, certain requirements regarding assurance of hardware or state of security features can be specified. Conformity Assessment is a procedure for demonstrating whether the ICT product/service/process meets those specific requirements.

B. ASSURANCE LEVELS FOR CERTIFICATES
According to Article 52 of the EU cybersecurity Act, three assurance levels are specified based on which a certificate can be issued to a product or service (Table 1). For a Basic assurance level, the evaluation activities should contain at least a technical documentation review or any alternative evaluation activity with an equal effect. The second level of assurance, i.e. Substantial level requires the evaluation activities to contain (i) a review that confirms the absence of known vulnerabilities, and (ii) tests that validate that the required security functionalities are correctly applied by the target device. The maximum level of assurance that an IoT device can require is High. The evaluation activities for a product requiring a high level of assurance should contain all the activities specified by Substantial level in addition to penetration testing of the IoT device or software to assess its resistance against skilled known attacks.

| Assurance Level | Description of Evaluation Activities |
|-----------------|--------------------------------------|
| Basic           | Evaluation activities to contain at least a technical documentation review. |
| Substantial     | Evaluation activities to contain: (i) a review to confirm the absence of known vulnerabilities and (ii) tests validating the correct implementation of required security functionalities. |
| High            | Evaluation activities to contain: (i) a review to validate the absence of known vulnerabilities, (ii) testing to ensure that required security functionalities are correctly applied and (iii) penetration testing to assess its resistance. |

C. CONFORMITY ASSESSMENT BODY (CAB)
A Conformity Assessment Body is responsible for performing the assessment procedure. According to the EU Cybersecurity Act, a CAB is an independent third party which is not the manufacturer or the provider of the product/service/process being assessed. The product manufacturer or service provider can apply for certification to any CAB in the Union. The IoT Device Security Certification Scheme should however identify whether the certificate is to be issued by a public or a private assessment body depending on the assurance level.

D. REQUIREMENT SPECIFICATIONS FOR CAB
The requirements of CABs that certify or that can certify the target should be specified in a document and created as a part of the certification components.

E. NATIONAL ACCREDITATION BODY (NAB)
A National Accreditation Body is responsible for accrediting CABs if they fulfill Requirement specifications for CAB mentioned above. The accreditation has a five-year validity and can be renewed on the same evaluation conditions.

F. SELF-ASSESSMENT
The Security Certification Schemes should enable the self-assessment feature in which the manufacturer/provider itself is responsible for the assessment of the target. Self-assessment can only be performed for Basic assurance level.

G. AN EU STATEMENT OF CONFORMITY
In case of Self-assessment by manufacturers, it is mandatory that they issue and submit an EU statement of conformity to ENISA and the National Cybersecurity Certification Authority (NCCA). This is a document declaring that the entity being certified fulfils the requirements of the SCS.

H. NATIONAL CYBERSECURITY CERTIFICATION AUTHORITY (NCCA)
A National Cybersecurity Certification Authority is a critically important entity stated in the EU Cybersecurity Act. It is held responsible for overseeing many aspects of the entire certification process. It should provide the NABs with expertise and information. It should validate CABs that fulfill the requirements set out in the scheme and authorize them to perform assessment and certification. All complaints from legal entities regarding the issued certificates should be directed to and handled by NCCA. Moreover, NCCA should collaborate with other national authorities or NCCAs, by the sharing of information on potential noncompliance of product or as per the with the SCS or the EU cybersecurity Act requirements. The role of NCCA is crucial and essential for certificates implying security assurance level High. In addition to this, the certificate issuance request is relayed to the NCCA from the CAB where an EU SCS requires an assurance level High.
I. PEER REVIEW

The last entity discussed for the EU Cybersecurity Certification Scheme is establishment of a peer review system between NCCAs. This is intended to attain mutual recognition of the complying SCSs and validate all other entities of the certification framework for compliance. The peer-review covers procedures for the compliance of a certified target with the certification requirements. The system should actively establish monitoring of CABs and verify the expertise of the staff of CABs who issue certificates for the security assurance High. It is also responsible for monitoring the manufacturers that are obligated to perform the conformity self-assessment.

Further Discussions: Besides the nine entities discussed above, the upcoming attributes are also relevant for certificates. The period of validity of a certificate is an important aspect defining the strength and flexibility of a certification scheme. The EU Cybersecurity Act, however does not specify limitations on the period of validity of a certificate. It remains flexible in stating that a certification scheme should include the maximum period of the validity of the certificate issued under the scheme, as long as the availability period of an EU statement of conformity is considered. Furthermore, the scheme should include a disclosure policy for certificates issued, withdrawn, expired or amended under a scheme. ENISA should make this information available in an electronic form until the expiry of a certificate. The scheme should also identify the conditions under which an update may have any potentially adverse impacts on the compliance such that the certified product requires re-certification or amendment in the scope of the certificate [38].

IV. EXISTING CYBERSECURITY CERTIFICATION SCHEMES

This section encompasses a discussion on the wide range of existing cybersecurity certification schemes (for organizations, products, systems, etc.). As the products are certified all across the globe with different certification schemes and governed by different jurisdictions, the comparison and assessment of the security levels of different IoT deployments is challenging [19]. Our study of the existing certification schemes and current initiatives towards IoT device certification serves as a starting point for identifying characteristics of an ideal IoT Device SCS for different classes of IoT devices. In this regard, surveys like [21] provide a comprehensive overview of the current cybersecurity certification schemes. The schemes are assessed against a set of challenges of IoT certification identified from current institutional and research studies. However, the focus of this survey is on risk assessment and testing options for IoT. Nevertheless, the challenges identified in this survey for IoT certification [21] have proved relevant in establishing the state-of-the-art of IoT certification.

Common Criteria (CC) is an international standard for certification of computer systems that require a high level of security [8], [24]. It has been the leading security standard for certification of operating systems, firewalls, etc [24]. The scheme specifies different Evaluation Assurance Levels (EAL). A protection Profile (PP) for a Target of Evaluation (TOE) is stated which identifies Security Assurance Requirements (SAR) and Security Functional Requirements (SFR). The Common Criteria have proven efficient in the last two decades in EU for the certification.
of integrated circuits and smartcards. Due to its contribution in the enhancement of the level of security of ICT devices and services, a Common Criteria based European candidate cybersecurity certification scheme is proposed for ICT in general [37] An optimal SCS approach for IoT devices should consider the dynamic nature of the IoT ecosystem and the networked environment in which the IoT device will operate. In the case of CC, the experience and the time needed to perform the evaluation is a major limitation even for TOEs that it is defined for. Additionally, the lack of flexibility in the scheme to handle changes in the certified product is also a limitation considering the dynamic nature of IoT devices, software updates and runtime states. New updates and changes to the configuration can invalidate the certification since the CC certifies a specific version of the product in specific configurations. This cost can be a problem in the case of an IoT device where regular patches and updates are crucial to handle new vulnerabilities discovered in an IoT device or a component. Hence, a quick certification procedure is necessary to assure that the security levels are up to date throughout the IoT device lifecycle. Furthermore, the certification approach should manage the needs of the IoT market which require cost-effectiveness especially by avoiding delays in product launch [20].

The baseline criteria, set by NIST for consumer-level IoT labelling is intended towards development of IoT labels, understandable by the consumers to make informed decisions. Hence the representation of the label and education material for consumers is recommended to be designed for non-expert consumers. The outlined baseline provides a mechanism to construct IoT labelling programs from existing standards and schemes and assert compliance using conformity assessment methods carried out by the scheme owner [14]. NIST has also produced several voluntary recommendations for IoT device manufacturers in its publication NISTIR 8259 [28], [29]. In recent years, UK has continuous recommendations for IoT device manufacturers in its publication ETSI TS 103 645 [39] containing the cybersecurity baseline for non-expert consumers. The Finnish Cybersecurity Label [16] is a national certification scheme. The Finnish Cybersecurity Labelling (E-IoT-SCS) was developed to comply with the EU cybersecurity certification framework. It focuses on the substantial and basic assurance levels of security as described in the EU Cybersecurity Act. The scheme was developed with a focus on smart card products aiming to provide a ground for low-risk products certification. It introduces the definition of a Security Profile similar to the CC [8], [35]. Figure 2 represents the Target of Evaluation (TOE) according to the Eurosmart scheme. According to the scheme, smart home devices include actuators or sensors are not usually targeted on the hardware level. Thus Restricted Operation Environments (ROE) functionalities adopt a small number of sophisticated attacks. The scheme points out that the vendor should apply security updates and secure configurations automatically without expecting the users to act. Security requirements defined in Chapter 11 such as tamper detection, tamper protection and hardware-based immutable root of trust are advanced and difficult to be followed by many of the IoT devices consumers. As vendors utilise ready-to-use hardware and standard software components, then combine them to form a working IoT device. Using off-the-shelf products limits the opportunities for vendors to contribute to such an evaluation and to fulfil the requirements [8]. The scheme presents a risk-based assessment methodology which makes it an admirable candidate for substantial and high levels of assurance. It should be noted that a basic assurance level that relies on self-assessment is not applicable in the scheme [8]. Finally, the period of validity of the certification issued is not identified by the scheme. However, it provides vulnerability management after certification issuance and provides rules for suspending and withdrawing a certificate [40].

B. FINNISH CYBERSECURITY LABEL

The Finnish Cybersecurity Label [16] is a national certification initiative set by the National Cyber Security Centre Finland (NCSC-FI) at Traficom information security. The label is a cybersecurity certificate and targets consumer devices and facilitates companies to get their product certified nationally. A certified product or service is proof that it meets the information security requirements set by the authority, i.e. NCSC-FI. The label is granted to a product or service...
after an inspection and evaluation of security requirements by NCSC-FI which is an approved body for this process. The requirements for compliance are derived from ETSI standard and the label is maintained annually through a rigorous review process.

C. CYBERSECURITY LABELLING SCHEME (CLS)
The Cyber Security Agency of Singapore (CSA) has launched the Cybersecurity Labelling Scheme (CLS) [15] for consumer smart devices. The efforts are targeting Internet of Things (IoT) security to improve cyber hygiene levels of the Singaporean cyberspace. The labelling identifies the devices according to their provisions assisting the user’s decisions in trusting devices. The Cybersecurity Labelling Scheme is recognized by the Finnish Cybersecurity Label [16] which is a step towards interoperability of labelling schemes. The scheme, however provides a basic level of assurance and security critical devices are left under the umbrella of generic schemes like Singapore Common Criteria Scheme (SCCS) [18] for IT products.

D. PSA CERTIFIED
PSA Certified [36] is an independent security evaluation scheme for the Platform Security Architecture (PSA) based IoT systems. The scope of this scheme is solely IoT products. It forms trust through a multi-level assurance evaluation for chips, including a security component ensuring Root-of-Trust (RoT) which offers trusted functionality to the platform [41]. PSA’s certification levels for devices is shown in Table 2. The security requirements of the scheme are derived from IoT threat models, security best practices and governments regulations.

For level 1 (Figure 3), IoT vendors check for critical security requirements through a security questionnaire. The questionnaire provides mappings for ETSI 303 645, NIST 8259v2 and Californian State Law SB-327 to assure that the products align with regulations [36]. Level 2 (Figure 4) is a fixed-time evaluation which makes the scheme cost-efficient. The document JSADEN001 [42] version 2.1 contains a lightweight Protection Profile (PP) that defines the Target of Evaluation (TOE), threats and security functions for level 1. According to the scheme, the certification is designed for IoT products that are deployed at scale. To meet level 2, there should be no remote attacks applied to a class of devices. Protecting against physical attacks on a single device is not required. Hence, the scheme does not consider the attacks that require physical access for the exploitation phase. Physical attacks in the identification phase of the attack, which results in scalable remote attacks are considered (such as exposure of a class key shared by all devices) [36]. It should be noted that only the RoT that is integrated into an IoT device should be provided by TOE. Figure 3 and 4 represent the scopes of PSA certified level 1 and level 2, respectively. Other components and functions are not covered by the PSA certification.

Although the security requirements evaluated in the scheme derived from IoT threat models, the scheme does not provide risk analysis and risk management during the life cycle of the evaluation nor after the certificate issuance [40]. Finally, the maximum validity of the certificate issued is not identified by the scheme, and the user should interpret the validity of the product. However, the digital certificate is available on the
PSA website for four years with the possibility for renewing or delta certification [36].

Pros and cons: The above in-depth study has assisted us in summarising the benefits and drawbacks of each certification scheme and standard. Eurosmart is a risk-based certification scheme, and it also provides vulnerability management after the certification issuance. The scheme adopts its assessment methods from the CC, and is by far the most relevant attempt towards a candidate scheme. Its security requirements are mapped to security standards and it has two assurance levels: basic and substantial. However, it does not support self-assessment. The Finnish Cybersecurity Label is a national certification initiative by the Finnish government and checks for compliance of products on the ETSI standard. It grants the label after assessment and supports annual maintenance. However, it does not support levels of certification and there is no mechanism in place for self-assessment of the products. The Singaporean Cybersecurity Labelling Scheme (CLS) reference the ETSI EN 303 645 standard and provides 4 rating levels to specify the status of security testing on consumer IoT devices. On the other hand it is not recommended for security-critical usecases requiring a higher level of assurance. PSA Certified is a certification scheme with two assurance levels and multiple available assessment methodologies. Its security requirements are mapped to security standards, but it is not a risk-based scheme. From this discussion, it becomes evident that none of the existing proposals/schemes fully encompass the EU Cybersecurity Act requirements.

V. ANALYSIS OF CYBERSECURITY CERTIFICATION SCHEMES FOR IoT

As already mentioned, the scope of this paper and a major contribution is establishing the key elements of an IoT Device SCS from existing literature and ENISA’s guidelines. In this section, we condense the IoT Device SCS requirements concluded from the previous section and highlight the relevance of these requirements to the IoT ecosystem.

The Subject-matter and scope of the certification scheme should be explicitly stated including the category of the IoT device (smarthome, automotive, etc.). In order deduce the level of assurance required by the intended users, a clear description of the purpose of the scheme is important. This specification then entails how the selected standards, evaluation methods and assurance levels correspond to the IoT device. The levels of security provided/assured by the scheme should map to the assurance levels specified by ENISA, where applicable. Since these levels are defined for all ICT products and services alike, IoT devices can be placed and their level of security assessed parallel to the other ICT products. The IoT Device SCS should include the evaluation criteria and methods to be used for assessment of the IoT category. These include the types of evaluations possible and how each evaluation parameter fulfills the objectives referred in Article 51 for IoT certification.

An indication of self-assessment of conformity being permitted under the scheme. The concept of self-assessment is emphasized in ENISA’s regulations for certification of non-critical devices. An IoT Device SCS should be able to offload the responsibility of assessment from the CAB to the device, to reduce the overhead on CABS, in trivial IoT usecases.

Specific or additional requirements to guarantee technical competence of CABS. An IoT Device SCS should explicitly state the additional technical capabilities that the CAB should possess, to enable it to assess the IoT category. Here ENISA also emphasizes the need for the availability of peer assessment mechanism for CABS to harmonize the entire operation.

Once IoT Device security certificates are issued, the next step in the lifecycle is continuous compliance. Hence rules for monitoring compliance of the IoT device in accordance with the requirements of the European cybersecurity certificates or the EU statements of conformity need to be specified by the scheme. This can also encompass exemplary usecases demonstrating continued compliance with the specified cybersecurity requirements. In addition to compliance, certificate issuance, maintenance and renewal, as well as preconditions for certificate extension, early withdrawal and modification in scope of certification should be addresses in an IoT Device SCS. This however, holds true for any EU certification scheme in the ICT category and is not specific to IoT.

The IoT infrastructure is relatively volatile compared to the ICT category in general due to the dynamic nature of IoT operation and software vulnerabilities. This necessitates tailored rules on detection of cybersecurity vulnerabilities in IoT. The IoT Device SCS should hence establish or define a mechanism to report and handle such vulnerabilities in the assessment and certification lifecycle.

The standards used for evaluation of the IoT device (national, European and international standards) should be referred by the scheme. This supports the interoperability of certificates, hence enabling the trust on IoT devices across borders. To strengthen the interoperability of security certificates, the content and the format of the European cybersecurity certificates and the EU statements of conformity should be decided by the scheme beforehand. Conditions for the mutual recognition of certification schemes across countries should be considered an important element in the IoT Device SCS since it provides an easy alternative to the complex process of re-certifying IoT devices under different jurisdictions.

The rules for retention of records and assessment results by CABS and the disclosure policy for European cybersecurity certificates should map to the lifespan of the IoT device and be simultaneously accepted across borders. Moreover, the period of the availability of the EU statement of conformity, technical documentation, and other relevant information to be provided by the manufacturer or provider of IoT device should also be specified. A viable duration for the availability of this information should be decided so that the
facts available are never outdated. The maximum period of validity of European cybersecurity certificates issued under the scheme may vary depending on the nature of the IoT device category. Some devices have a lifespan of mere months while others are rather long-lasting. Depending on the nature and scope of the IoT category, this period should be specified by the IoT Device SCS. Finally, the certification withdrawal and renewal approaches should be essentially lightweight, especially in case of IoT category where resources are limited.

In a nutshell, an IoT Device SCS should provide an approach to minimize the risk of attacks on components of the IoT infrastructure and should maintain the security level of the IoT device throughout the lifecycle as well as identify potential vulnerabilities. The EU cybersecurity certification framework facilitates the creation of risk-based certification schemes as a whole set of rules, cybersecurity standards, technical requirements, evaluation methods, product categories, support for self-assessment and assurance levels. We select features we consider are most important parameters from our gap analysis above and conduct a comparison of the studied features we consider are most important parameters from our study which provides enough reference materials to help different stakeholders with a starting point to select a suitable certification scheme for any category of IoT devices (smarthome, industrial, automotive, etc.). The template also consists of recommendations that satisfy each selected element. An IoT SCS should include the key elements described below:

A. TECHNICAL SPECIFICATION OF REQUIREMENTS (TSR)

Before we describe the proposed template in detail, we define the process of cybersecurity certification of an IoT device in the following steps. The actors involved in certification also correspond to the entities shown in Figure 1.

- **Step 1**: The manufacturer/vendor sends the relevant documentation and a sampling of the TOE to the CAB.
- **Step 2**: The CAB is the laboratory which performs the conformity assessment by evaluating the TOE against the security requirements identified by a PP and issues the certificate in the assurance levels Basic and Substantial. CAB can perform the assessment in the level assurance High upon approval from the NCCA.
- **Step 3**: The NCCA performs the conformity assessment by evaluating the TOE against security requirement identified by a PP and issues the certificate in the assurance level High. It also implements and supervises CABs. It authorizes CABs to perform designated tasks after requirement fulfilment as per the scheme.
- **Step 4**: The NAB accredits the CABs if they fulfill specific requirements set in the EU Cybersecurity Act.
- **Step 5**: Vendors and manufacturers can perform conformity self-assessment and issue the EU statement of conformity but only in case of security assurance Basic.
- **Step 6**: The manufacturer/provider should submit a copy of the EU statement of conformity to ENISA and the NCCA.

We identify and propose key elements of a potential EU IoT Device Security Certification Scheme (SCS) concluded from the systematic gap analysis of existing standards and certification schemes and in accordance with the EU Cybersecurity Act. This template can be used to instantiate a certification scheme for any category of IoT devices (smarthome, industrial, automotive, etc.). The template also consists of recommendations that satisfy each selected element. An IoT SCS should include the key elements described below:

VI. A TEMPLATE FOR EU IoT DEVICE SECURITY CERTIFICATION SCHEME (SCS)

1) SCOPE OF THE SCHEME

This proposed scheme is a high-level certification scheme and presents a template for the evaluation of IoT devices’ security properties based on the EU cybersecurity certification framework, described in the Cybersecurity Act. The certification scheme considers IoT devices of ranging capabilities. The template proposes that vendors/manufacturers can select different procedures to evaluate the IoT device. For example, if the manufacturer/vendor certifies the IoT using CC guidelines, the IoT Device SCS devised using this template would recognize and reuse the results of the evaluation and maintain cost-efficiency and compatibility. We have selected schemes like PSA Certified, CLS, E-IoT-SCS in our study which provides enough reference materials to help different stakeholders with a starting point to select a suitable evaluation scheme for their IoT usecase.

2) THE PURPOSE OF THE SCHEME

The purpose of the certification scheme is validating an IoT device’s compliance with specific requirements aiming at protecting confidentiality, integrity and availability of the data (stored or/and transmitted) used in the IoT device under the EU Cybersecurity Act.

3) PROTECTION PROFILE (PP)

When a manufacturer/vendor applies for the certification, the manufacturer/vendor can use a standard PP from CC or any selected evaluation method. The PP includes a list of security objectives which determine the security behaviour of the TOE in a specific environment and addresses the resistance level of the TOE against particular attack methods [8].

A. Khurshid et al.: EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme
4) SECURITY TARGET
The manufacturers can also construct a tailored Security Target (ST) for a TOE (i.e., the IoT Device). In case the manufacturer/vendor creates an ST suited for the IoT category, it should be validated by the IoT Device SCS owner. The ST must also be reviewed annually and while updating the certification to keep the threat landscape up to date.

5) TOE SECURITY OBJECTIVES
The security objectives of the IoT category consider CIA (confidentiality, integrity and availability) for every IoT category (such as smart camera, thermostat, smart TV etc.). In order to design specialized security objectives and security requirements for the ST, it is necessary to identify: common threats to the IoT category, common vulnerabilities that lead to these threats and risk-assessment of the identified threats.

Here, ENISA’s Baseline Security recommendations for IoT can be adapted to consider common threats related to the IoT infrastructure [44].

6) OPERATIONAL ENVIRONMENT
The operational environment where the IoT device is installed also requires consideration during certification. The PP document includes different generic types of the operational environment namely consumer, enterprise, critical etc. to assess the security risks and to provide different assurance levels.

7) SECURE DEVELOPMENT LIFECYCLE
The IEC 62443-4-1 standard [45] provides secure development lifecycle requirements specific to industrial automation and control systems. Although the standard is not specifically

![Figure 5](image-url)

**Figure 5.** Two-step process of analysing gaps in existing IoT certification schemes and standards and extracting the key elements of a potential EU IoT Device Security Certification Scheme (SCS). The regulation set out by ENISA, the Common Criteria, EUCC and IoT certification schemes and standards are an input to this process, and the 8 key elements depicted on the right side of the figure are the output.
targeting the IoT domain, it is relevant to consumer and industrial domains [46] and can be used as baseline for secure development lifecycle.

B. ASSURANCE LEVELS

The scheme targets the security assurance levels: Basic, Substantial and High following from their significance emphasized in the EU Cybersecurity Act.

- **Basic** security assurance level encompasses consumer IoT devices that require a minimum security level.
- **Substantial** security assurance level includes IoT devices with data/operations prone to privacy and confidentiality. However, specifying the exact level of security of an IoT device requires further evaluation.
- **High** security assurance level is required for IoT devices dealing with safety-critical operations.

The generic PP document, provided by E-IoT-SCS is relevant to consumer and industrial IoT domains, and can be mapped to Basic and Substantial assurance levels. Similarly, the lightweight PP for chip vendors provided by PSA Certified Level 2 can also be used as a reference for the Basic and Substantial assurance level [36]. The PP documents provided by CC are relevant to the assurance level High and can be used for an IoT Device SCS for security critical IoT devices.

C. RISK-BASED APPROACH

The Technical Specification of Requirements (TSR) discussed above should be identified through a risk-based approach. The security objectives and requirements of the PP should undergo a risk assessment process. This assessment further determines the potential threats to the PP/ST and the respective mitigation. We propose/suggest NISTIR 8228 [27] to conduct the risk-based assessment and identification of TSR. Guidelines such as ISO/IEC 27400:2022 [26] and a combination of them can also be used to the same effect. When conducting a risk assessment for Substantial and High assurance levels, it is mandatory to consider a number of inputs are including: potential threats on the IoT device, IoT software vulnerabilities and usecase-specific security objectives. The impact and the likelihood of the identified threats are calculated amounting to a numeric value for a each risk which allows efficient comparison of different scenarios. While several risk assessment methodologies exist, we propose the use of the Common Vulnerability Scoring System (CVSS) [47] for IoT, since it is not complex and has been used in the National Vulnerability Database (NVD). Other methodologies like the Common Weakness Scoring System (CWSS) [48] and OCTA VE [49] are also valid options. In addition to the above, the risk-assessment methodology provided by E-IoT-SCS can also be used.

Following up from the risk assessment, the list of security objectives covering the previously calculated risks can be generated. It should be noted that different security objectives can be generated for the same IoT device based on different operational environments. Therefore, we propose defining different security objectives for each usecase of the TOE. As a result, for every security requirement, there can be one or more security assurance activities (i.e., evaluation methods) to achieve the security objective.

D. EVALUATION METHODOLOGY

The evaluation methodology suited to a single usecase of a TOE is decided according to the calculated risk of identified threats. The evaluation methods can range from technical documentation review to penetration testing. Once an evaluation by the CAB or NCCA is passed, the evaluating body generates a label for the IoT device. The label is then published along with the certified device and the level of security assurance on a public website so users can make informed decisions about device selection and trust.

The European CyberSecurity Organisation (ECSO) proposes assessment options and evaluation methods that can be used to measure the compliance of this template [2]. The ENISA qualification system [8] is another relevant option proposed alongside the Cybersecurity Certification regulations to assess the merit of a certification scheme. The parameters of this qualification system are relevant to the scope of our proposed certification template. We choose the later methodology due to its quantitative nature of evaluation which we believe will provide a concrete standing of the IoT Device SCS. The following evaluation methods are enlisted by the ENISA Qualification system for each assurance level.

**Evaluation methods for Basic assurance level:**
- Technical documentation review.
- Onsite audit of security procedures.
- Functional security testing of IoT device and the software.
- Basic robustness testing using fuzzing for IoT software.
- Vulnerability analysis to check for known vulnerabilities in software and during the design and manufacturing process.
- Penetration testing against the identified and known attacks using methods based on international standards such as ISO/IEC 17825:2016 [25]. Pen-testing approach is chosen based on level of risk and as per the PP.

**Evaluation methods for Substantial assurance level:**
- Technical documentation review.
- Onsite audit of security procedures.
- Functional security testing of IoT device and the software.
- Basic robustness testing using fuzzing for IoT software.
- Vulnerability analysis to check for known vulnerabilities in software and during the design and manufacturing process.
- Penetration testing against the identified and known attacks using methods based on international standards such as ISO/IEC 17825:2016 [25]. Pen-testing approach is chosen based on level of risk and as per the PP.

**Evaluation methods for High assurance level:**
- Technical documentation review.
- Onsite audit of security procedures.
- Source code review.
- Functional security testing.
- Advanced robustness testing using fuzzing templates developed specifically for the particular IoT software.
- Vulnerability analysis.
Penetration testing against all possible known attacks. The attack potential is calculated for every attack scenario in the usecase; the methodology provided by CC can be used to accomplish this step of evaluation.

Self-assessment: The option of self-assessment is supported in our proposed template. This enables the IoT device to meet the mandatory security requirements by self-assessment and attain the basic assurance level without excessive evaluation overhead. We propose that in the IoT Device SCS, most essential security requirements are checked through a security questionnaire answered by the manufacturer/vendor. We recommend the questionnaire to be mapped to ETSI EN 303 64 [31]. Questionnaires by NISTIR 8259 [28], IoT security foundation [50] and PSA Certified Level 1 [36] can also be selected depending on the TOE. After the questionnaire is filled, has been double reviewed by different internal teams of the manufacturer/vendor and passed the evaluation, the manufacturer/vendor can issue the EU Statement of Conformity. A copy of this statement is to be submitted to the NCCA and to ENISA so it can recognised across the Union member states.

**E. CONFORMITY ASSESSMENT**

As per the requirement stated in the EU Cybersecurity Act, a document stating the requirements on CABs based on ISO/IEC 17065:2012 [33] is available. The conformity assessment process is conducted by the NCCA based on this document to ensure that CABs meet the requirements of ISO/IEC 17065:2012 or are accredited to the standard requirements by a NAB. The results of IoT evaluation and assessment originating from an accredited CAB are accepted.

**F. VULNERABILITY MANAGEMENT**

The manufacturer/vendor should support the end-users of the IoT device throughout the device lifecycle by technical and non-technical means. This can be achieved by providing a platform to report security vulnerabilities. It can include means for contacts such as web forms and phone numbers. The end-users and NCCA should also be notified about identified vulnerabilities as soon as possible. The NCCAs and CABs should monitor potential new vulnerabilities using platforms such as CSIRTs, CERT and security vulnerability databases. NCCA should assess the severity of the vulnerability that has been identified. This process can be done using E-IoT-SCS’s vulnerability management. The severity level of the vulnerability determines how the vulnerability should be handled and the NCCA informs the manufacturer/vendor to patch the vulnerability accordingly. The NCCA also notifies a CAB to conduct a risk assessment related to the vulnerability in a limited time that follows, to determine the impact on the TOE. Thus, the NCCA decides if the results of the assessment affect the validation of the certificate or not. NCCA should also map the vulnerability to the threats of the PP. We propose the following standards to be followed for vulnerability management: ISO/IEC 30111:2019 [34] and ISO/IEC 29147:2018 [32].

**G. MONITORING FOR COMPLIANCE**

The responsibility of ensuring a device is compliant after the issuing of the certification falls on the NCCA. This can be achieved through documentation review and onsite audit inspection of the vendor’s supply chain and by surveillance carried out by CABs. The NCCA can utilize existing metadata certificate services (or databases) that are publicly available to store information on the certified IoT devices. The stored information can include the scope of the certification, validity period and level of certification etc. The NCCA also conducts random evaluations of the CABs with reference samples validating the results obtained from the CABs. NCCA can also conduct round-robin tests for comparison of the CABs where audited CABs are more than five-per-cent every year. The audits assess technical knowledge and qualifications of the evaluators. It should this, the NCCA provides the CABs with working groups and technical experts capturing the state-of-the-art of security evaluation knowledge.

**H. CERTIFICATE MAINTENANCE AND SURVEILLANCE**

The manufacturer/vendor must notify the NCCA about any changes to the certified IoT device, which can affect the conformity. The NCCA then decides if further assessments or testing needed. The manufacturer/vendor is not allowed to deploy devices under certification until the NCCA has informed and permitted the manufacturer/vendor to proceed. These changes include changes to device requirements, changes in the certification scheme and discovered vulnerabilities. Patching and software updates may also affect the validity of the certification. If the manufacturer/vendor wishes to change the scope of the certification, it becomes necessary to re-apply to the CAB. The decision of continuity of an assurance level is carried out in a relatively short and fixed amount of time to allow even minor product changes to be evaluated. As proposed previously, a list of the certified IoT devices is publicly available via an online certificate service which is maintained by the NCCA. If the surveillance shows a breach in conformity, or if there is any violation of the certification parameters, the certification is suspended. The certificate can be re-instmted if corrective procedures are taken. Certification can also be withdrawn if surveillance shows breach in conformity and corrective procedures cannot be taken. Otherwise, the certification is considered valid by default until changes occur. However, the maximum validity period for certification can not be longer than five years.

**I. AN EXAMPLE OF INSTANTIATING A SCS**

In this section, we provide one example of an IoT Device SCS instantiated from the template scheme proposed in the previous section. The TOE here is a water meter device. Water meters are among the constrained class of IoT devices deployed in massive scale, operating on batteries for years.
TABLE 4. Example of instantiating an IoT Device SCS from the proposed template for a water meter TOE.

| Element                      | Description                                                                 |
|------------------------------|-----------------------------------------------------------------------------|
| TSR - Scope of Scheme        | The scheme identifies the certification procedure for water meters.         |
| TSR - Purpose of Scheme      | The scheme provides water meter manufacturers with guidelines for validating the compliance of the meter with respect to data confidentiality. |
| TSR - PP                     | The PP includes a set of security objectives for the TOE. For the sake of this example, we specify one security objective. |
| TSR - TOE Security Objective | Confidentiality of the sensor data captured by the water meter.             |
| TSR - Operational Environment| Water meters are data-collecting devices, often deployed as part of a huge networked infrastructure in offices, homes, farmlands, etc. |
| TSR - Security Target        | We tailor the ST according to the water meter use case and hence it should be validated by the manufacturer. The ST needs to be reviewed annually as well as before updating the certification. |
| TSR - Secure Deployment Lifecycle | We use the IEC 62443-4-1 standard as a baseline for secure development lifecycle. |

**Evaluation of the Proposed Scheme**

In this section, we present the evaluation of our proposed IoT Device SCS Template. We perform the evaluation of the template based on the ENISA Qualification System. We have stated previously in our template scheme (Section VI-D) why we chose this specific metric as our evaluation methodology.

**A. ENISA Qualification System**

ENISA presented a proposal for a qualification system for the security certification schemes [8] which aims at simplifying the comparison procedure between the certification schemes. The qualification system consists of a number of parameters for qualifying a certification scheme's quality and a scoring system. Table 5 presents an evaluation of the proposed IoT Device SCS Template using the ENISA qualification system parameters.

As shown in the table, the ENISA qualification system provides 29 parameters. It is discussed below in a point-wise fashion how proposed IoT Device SCS Template addresses these parameters. It should be noted, however, that the certification template is a high-level approach with potential recommendations and its instantiation (in Section VI-I) is a minimal example demonstrating how the template can be used. Hence, we do not provide the risk assessment, IoT evaluation, vulnerability scores and concrete device vulnerability management steps throughout the lifecycle in our study.

1) The scope of the target of the certification is a specific IoT category with a precise definition and description of its internal components.
2) While our scheme does not present specific Protection Profiles (PP) document for every IoT category, we suggest and present a guide on defining a PP.
3) The scheme recommends stating the operational environment in the IoT Device SCS.
4) A certification scheme formulated using our template can cover the IoT device components fully or partially. The template proposes to accept different certification procedures results.
5) This certification template is based on re-using existing certification schemes and security standards. The scheme provides reference materials for stakeholders to find more information about other existing schemes.
6) The scheme proposes defining all the security objectives of the TOE by using existing schemes.
7) We suggest process/es for identifying the security objectives of the TOE.
8) The scheme recommends covering all the security objectives that consider the different security attributes (CIA) for individual components of the TOE. These include the parts of the IoT hardware and software.
9) The scheme recommends to identify a different set of security objectives for different use cases of TOE.
10) We propose different risk-assessment procedures that can help the vendors and manufacturers to identify the security objectives.
| Components of Certification Scheme | No. | Qualification parameters                                                                 | Fulfillment |
|-----------------------------------|-----|------------------------------------------------------------------------------------------|-------------|
| Objective of the certification    | 1   | Accuracy level defining the scope of the target                                           | HIGH        |
|                                   | 2   | Use specific Security Profile/PP for each type of products                                | YES         |
|                                   | 3   | Operational environment consideration                                                     | YES         |
|                                   | 4   | Composition certification allowed                                                         | YES         |
|                                   | 5   | Other schemes evidence re-use allowed                                                    | YES         |
| Security objectives for the target| 6   | Definition level of the security objectives                                              | Not Covered |
|                                   | 7   | A process is in place for defining the security objectives of the target                 | YES         |
|                                   | 8   | Consider CIA for individual components used in targets                                   | YES         |
|                                   | 9   | Different security objectives are defined for different usecases of target                | YES         |
|                                   | 10  | Security objectives are defined through a risk assessment procedure                       | YES         |
| Evaluation areas covered by the TSR| 11  | Documentation review                                                                      | YES         |
|                                   | 12  | Audit of security procedures associated to the target                                     | YES         |
|                                   | 13  | Audit inspection level                                                                    | YES         |
|                                   | 14  | Security functional testing                                                               | YES         |
|                                   | 15  | Robustness testing                                                                       | YES         |
|                                   | 16  | Vulnerability analysis                                                                    | YES         |
|                                   | 17  | Penetration testing style                                                                 | Risk-based  |
|                                   | 18  | Measure resistance of products against different types of attacks                         | YES         |
|                                   | 19  | The attack potential is calculated for each attack method                                  | YES         |
| Methodology for requirements identification| 20  | Quality of identification methods                                                         | HIGH        |
| Process of the evaluation methodology| 21  | Objectivity of the evaluation methodology                                                 | HIGH        |
|                                   | 22  | Use evidence formalism                                                                   | Not Covered  |
|                                   | 23  | Produce comparable results                                                                | Not Covered  |
| Conformity Assessment |
| Market surveillance | 24  | Surveillance audits in certified products                                                 | HIGH        |
|                                   | 25  | Public records of certificate metadata                                                    | YES         |
| Laboratories surveillance | 26  | Random evaluations                                                                      | HIGH        |
|                                   | 27  | Round-Robin evaluations                                                                  | HIGH        |
|                                   | 28  | Procedures maintaining state-of-the-art shared knowledge in security                     | HIGH        |
|                                   | 29  | Audit of technical knowledge                                                             | HIGH        |

11) The evaluation methodology identified in the scheme includes documentation review that covers guidance documents and design plans.

12) The scheme suggests audit of the security in the design and manufacturing procedures, besides monitoring and maintenance of security procedures in the post deployment phase.

13) The audit of security procedures carried out through documentation review and onsite audit inspection of the vendors’ supply chain is proposed in the template.

14) The template states that functional testing of all security functions used in the device should be conducted is for evaluation assigned to the assurance levels *substantial* and *high*.

15) The template specifies basic stress test of security functions and operational features used in the device in evaluation methods assigned to the assurance level *substantial*. Advanced stress test of security functions and operational features of the device is to be included in the evaluation methods assigned to the assurance level *high*.

16) The scheme provides an in-depth discussion on continuous monitoring possibilities for known vulnerabilities throughout the device lifecycle.

17) The scheme covers penetration testing as an evaluation method for *High* assurance level, and recommends the pen-testing style to be risk-based per profile.

18) Penetration testing against a wide range of attacks using various tools and methods and based on international standards is suggested in the template.

19) The attacking potential is calculated for every attack scenario and our template provides suitable schemes that can be used for the calculation.

20) The methodology of identification of requirements is based on risk assessment procedures to assure that security objectives related to the each usecase of the TOE are met and the potential threats are mitigated by the selected security requirements.

21) Self-Assessment with double review by different internal teams and independent third-party assessment is addressed in the template scheme.

22) The template proposed is based on definitions used by existing schemes such as CC and does not specify formal and structured language for the specification of technical requirements. Hence this point is not addressed.

23) The evaluation procedures are independent of discretionary assessments and always produce repeatable but not comparable results. This proposed scheme is a high-level approach providing several documents and schemes to conduct evaluation but it does not include technical details of the evaluation methodology. Therefore, this point is not covered by the scheme.

24) We suggest surveillance audits based on well-known mechanisms.
In addition to the evaluation of the scheme, it is paramount to identify its salient features. The apparent benefit of the template is the uniformity it will establish in the European Union Internal Market. Since the proposed template addresses the requirements derived from a multitude of international standards and regulations, it encompasses the aggregate of IoT certification must-haves. In our proposed IoT Device SCS Template, we provide diverse options for fulfillment of each element, hence making the scheme flexible enough to be moulded as per specific IoT usecases. However, this flexibility renders the proposed template less concrete as it does not provide a tactile certification scheme for the IoT but rather, the methodical means to create an IoT Device SCS for different IoT categories.

VIII. CONCLUSION

IoT device security is a critical requirement with the development of IoT technology and advancement of IoT infrastructure. IoT device cybersecurity certification, assurance, and maintenance of the certification throughout the lifecycle of the device increases consumer and user-trust in these devices. The US executive order 14028 has tasked NIST with initiating and proposing IoT labelling schemes for device assurance starting from a reasonable baseline. The government of UK is ensuring the development of secure smart devices from the beginning as well as assurance during the device lifecycle. These collective efforts are catalogued under Secure by Design. The European Cybersecurity Act also entered into force and launched the European cybersecurity certification framework for Internet and Communications Technology (ICT) with the objective of decreasing the risk of fragmentation in the Single Market. However, the development of a cybersecurity certification scheme exclusively for IoT is still in preliminary stages due to the challenges arising from the dynamic nature of IoT ecosystem. New vulnerabilities, configuration changes, software updates, nature of data and operational environment also have an impact on product security and need to be taken into account while establishing a certification scheme.

In this paper, we have presented an overview of selected certification schemes. We analyzed international certification requirements and efforts by bodies across the globe. As a result, we identified and formulated key elements of a candidate cybersecurity certification scheme for IoT. The proposed template for IoT device Security Certification Scheme (SCS) can be used to instantiate certification schemes for different categories of IoT devices. We evaluated the merit of the proposed approach using the ENISA qualification system and found that it addresses the required criteria for an EU certification scheme. It should be noted here that the proposed IoT Device SCS is a template and does not include technical details like the specific choice of evaluation methods. However, the scheme is flexible and we suggest different options that can be adopted to fulfill the requirements. We also present an incentive instance of an IoT Device SCS using the proposed template for a water meter IoT device. Future work following this paper focuses on a more precise requirement identification relevant to the all security assurance levels of IoT device categories. We believe this study and template will assist ENISA in designing a potential IoT Device Security Certification Scheme that not only suits the existing IoT devices but will also be adaptive to emerging devices.

Future Directions: The potential future directions of this work are the identification and resolution of challenges around the technical aspects of IoT cybersecurity certification. These include remote attestation, risk assessment, security testing, certificate distribution and management processes, etc. Remote attestation is a fundamental building block to establish trust in software systems by providing/verifying the state of the hardware and software components of a system [51]. One of the challenges with the existing remote attestation mechanisms is in the alignment of assurance guarantees with the device profile and context of deployment of IoT devices. Considering the dynamic nature of IoT devices, it is equally challenging to maintain/update the level of assurance of the device based on the software’s current health. Furthermore, it is basal that the remote attestation results are backed by a hardware Root-of-Trust (RoT) on IoT devices. To this end, remote attestation schemes are being tailored to generate hardware or hybrid attestation proofs and hardware-based capabilities are being developed for constrained IoT devices [52], [53]. Another challenging aspect is automating the certification process to avoid cumbersome documentation, limit manual intervention while constantly producing comparable meaningful results. To establish a unified cybersecurity certification framework, these technical challenges also need to be addressed along with the policy/regulation aspects.

REFERENCES

[1] S. Vivek, D. Verma, and P. Krishnan, “Towards solving the IoT standards gap,” in Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI), Sep. 2018, pp. 1441–1447.
[2] ECSO. (2019). European Cyber Security Certification Assessment Options WG1 1 Standardisation, Certification, Labelling and Supply Chain Management. [Online]. Available: https://www.ecs-org.eu
[3] S. Soltan, P. Mittal, and H. V. Poor, “BlackIoT: IoT botnet of high wattage devices can disrupt the power grid,” in Proc. 27th USENIX Secur. Symp. (USENIX Security), 2018, pp. 15–32.

[4] N. A. Khan, A. Awang, and S. A. A. Karim, “Security in Internet of Things: A review,” IEEE Access, vol. 10, pp. 104649–104670, 2022.

[5] C. Kollas, G. Kambourakis, A. Stavrou, and J. Voas, “DDoS in the IoT: Mirage and other bottlenecks,” Computer, vol. 50, no. 7, pp. 80–84, 2017.

[6] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Burstein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, and M. Kallitsis, “Understanding the mirai botnet,” in Proc. 26th USENIX Secur. Symp. (USENIX Security), 2017, pp. 1093–1110.

[7] N. M. Karie, N. M. Sahri, W. Yang, C. Valil, and V. R. Kebande, “A review of security standards and frameworks for IoT-based smart environments,” IEEE Access, vol. 9, pp. 121975–121995, 2021.

[8] ENISA. (Feb. 2020). Standardisation in Support of the Cybersecurity Certification. [Online]. Available: https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa.

[9] A. Khurshid et al.: EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme

[10] The EU Cybersecurity Certificate Framework. Accessed: Dec. 14, 2022. [Online]. Available: https://www.enisa.europa.eu/topics/standards/certification

[11] EU Cybersecurity Certification Framework. Accessed: Dec. 14, 2022. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[12] M.S. Department for Digital, Culture. (2019). Secure by Design. [Available: https://www.gov.uk/government/collections/secure-by-design

[13] TRAFICOM. (2021). Grant Programme for Consumer IoT Assurance Schemes 2020/21

[14] S. N. Matheu, J. L. Hernández-Ramos, A. F. Skarmeta, and G. Baldini, “Understanding the Mirai botnet,” in USENIX Security

[15] S. N. Matheu-García, J. L. Hernández-Ramos, A. F. Skarmeta, and G. Baldini, “Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices,” Comput. Standards Interfaces, vol. 62, pp. 64–83, Feb. 2019.

[16] S. N. Matheu, J. L. Hernández-Ramos, and A. F. Skarmeta, “Toward a cybersecurity certification framework for the Internet of Things,” IEEE Security Privacy, vol. 17, no. 3, pp. 66–76, May/Jun. 2019.

[17] S. N. Matheu, J. L. Hernández-Ramos, A. F. Skarmeta, and G. Baldini, “A survey of cybersecurity certification for the Internet of Things,” ACM Comput. Surveys, vol. 53, no. 6, pp. 1–36, Nov. 2021.

[18] H. Badran, “IoT security and consumer trust," in Proc. 20th Annul. Int. Conf. Digit. Government Res., Jun. 2019, pp. 133–140.

[19] A. Cire, P. R. Sousa, J. S. Resende, and L. Antunes, “IoT security certifications: Challenges and potential approaches," Comput. Secur., vol. 116, May 2022, Art. no. 102669.

[20] CCRA. The Common Criteria. Accessed: Dec. 14, 2022. [Online]. Available: https://www.commoncriteriaportal.org/

[21] Information Technology, Security Techniques, Testing Methods for the Mitigation of Non-Invasive Attack Classes Against Cryptographic Modules, document ISO/IEC 17825:2016, 2016. [Online]. Available: https://www.iso.org/standard/60612.html

[22] Cybersecurity—IoT Security and Privacy—Guidelines, document ISO/IEC 27400:2022. 2022. [Online]. Available: https://www.iso.org/standard/44373.html

[23] K. Boeckl, M. Fagan, N. Lefkovitz, K. Megas, E. Nadeau, D. G. O’Rourke, B. Piccarreta, and K. Scarfon, “Considerations for managing cybersecurity and privacy risks,” NIST, Gaithersburg, MD, USA, Tech. Rep. Draft NISTIR 8228, 2018, pp. 1–40. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2019/NISTIR.8228.pdf, doi: 10.6028/ NISTIR.8228-draft2.pdf

[24] K. Scarfeno, M. Fagan, and K. N. Megas. (Jan. 2020). Draft (2nd) Nistir 8259 Recommendations for IoT Device 2 Manufacturers. NIST, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2020/NISTIR.8259-draft2.pdf

[25] M. Fagan, K. Megas, K. Scarfeno, and M. Smith, “Foundational cybersecurity activities for IoT device manufacturers,” Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 8259, 2020.

[26] “IoT device cybersecurity capability core baseline.” Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 8259A, May 2020.

[27] ETSI. (2020). Cyber; Cyber Security for Consumer Internet of Things: Baseline Requirements. [Online]. Available: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[28] Information Technology, Security Techniques, Vulnerability Disclosure, document ISO/IEC 29147:2018, 2018. [Online]. Available: https://www.iso.org/standard/72311.html

[29] Conformity Assessment, Requirements for Bodies Certifying Products, Processes and Services, document ISO/IEC 17065:2012, 2012. [Online]. Available: https://www.iso.org/standard/45658.html

[30] Information Technology, Security Techniques, Vulnerability Handling Processes, document ISO/IEC 30111:2019, 2019. [Online]. Available: https://www.iso.org/standard/69725.html

[31] Eurosmart. Eurosmart IoT Certification Scheme: Eurosmart: The Voice of the Digital Security Industry, Accessed: Dec. 14, 2022. [Online]. Available: https://www.eurosmart.com/eurosmart-iot-certification-scheme

[32] Psacertified. PSA Certified | Created to Improve the Security and Trust of Internet of Things Devices and Their Data. Accessed: Dec. 14, 2022. [Online]. Available: https://www.psacertified.org/

[33] ENISA. (2020). Cybersecurity Certification: Candidate EUC; Scheme. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-certification-euc-candidate-scheme

[34] Regulation (EU) 2019/881 of the European Parliament and of the Council, European Union, Brussels, Belgium, Apr. 2019.

[35] ETSI. (2019). Cyber; Cyber Security for Consumer Internet of Things. [Online]. Available: https://www.etsi.org/deliver/etsi_iso/306300_306399/306369/01.01.01_60/en_306369v010101p.pdf

[36] Eurosmart. (Feb. 2020). A Cartography of Security Certification Schemes/Standards for IoT: Eurosmart: The Voice of the digital security industry, Accessed: Dec. 14, 2022. [Online]. Available: https://www.eurosmart.com/a-cartography-of-security-certification-schemes-standards-for-iot

[37] Psacertified. Can We Insure Billions of Connected Devices? Accessed: Dec. 14, 2022. [Online]. Available: https://www.psacertified.org/blog/can-we-insure-billions-connected-devices/

[38] (2022). PSA Certified Level 1 Questionnaire Version 2.1. [Online]. Available: https://www.psacertified.org/app/uploads/2021/03/ISADEN001-PSA_Certified_Level_1-1_2_1_Updated_March_2021.pdf

[39] Common Criteria. Protection Profiles. Accessed: Dec. 14, 2022. [Online]. Available: https://www.commoncriteriaportal.org/ppps

[40] Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures, ENISA, Athens, Greece, 2017.

[41] IEC Webstore, document IEC 62443-4-1:2018, 2018. [Online]. Available: https://www.iesc.org/publications/iec62443-4-1-2018.

[42] IoTSF. IoT Security Assurance Framework. [Online]. Available: https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTsf-IoT-Security-Assurance-Framework-Release-3-0-Nov-2021-1.pdf
[51] G. Coker, J. Guttman, P. Loscocco, A. Herzog, J. Millen, B. O’Hanlon, J. Ramsdell, A. Segall, J. Sheehy, and B. Sniffen, “Principles of remote attestation,” *Int. J. Inf. Secur.*, vol. 10, no. 2, pp. 63–81, 2011.

[52] ARM Limited. (2018). *Trustzone Technology for Armv8-M Architecture Version 2.1*. [Online]. Available: https://developer.arm.com/documentation/100690/latest/

[53] TC Group. (2019). *Trusted Platform Module Library Part 1: Architecture*. [Online]. Available: https://trustedcomputinggroup.org/wp-content/uploads/TCG_TPM2_r1p59_Part1_Architecture_pub.pdf

ANUM KHURSHID received the B.S. degree in computer science and the Master of Science degree in computer science specializing cybersecurity from COMSATS University, Islamabad, in 2014 and 2017, respectively. She is currently pursuing the Industrial Ph.D. degree with the Cybersecurity Unit, RISE Research Institutes of Sweden, Stockholm, and Uppsala University. She is doing her Ph.D. thesis in hardware-assisted trusted execution environments focused on IoT security. Her research interests include software security, embedded systems security, the IoT security, and certification and assurance.

REEM ALSAAIDI received the master’s degree in information security from the Department of Computer and Systems Sciences, Stockholm University, Stockholm, Sweden. She is currently a Security Generalist with BCSS Security Engineering, Ericsson. She has interned at the Cybersecurity Unit, RISE Research Institutes of Sweden. Her research interests include cybersecurity, computer forensics, and privacy.

MUDASSAR ASLAM received the B.S. degree in computer science, in 2002, the master’s degree in security from the KTH, Sweden, in 2009, and the Ph.D. degree from Mälardalen University, Sweden, co-hosted by RISE (formerly SICS), Sweden, in 2014. Previously, he was a Senior Researcher with the Cybersecurity Unit, RISE, where this work was carried out. He is currently an Assistant Professor with the NUCES-FAST, Islamabad, Pakistan. His research interests include the IoT, and edge and cloud security with expertise in platform security mechanisms provided by TEEs. His research, during Ph.D., was recognized with the Best Paper Award in SIN 2013 Conference.

SHAHID RAZA (Senior Member, IEEE) received the Master of Science degree in cybersecurity from the KTH, Sweden, in 2009, and the Industrial Ph.D. degree from Mälardalen University, in 2013. He is currently the Director of the Cybersecurity Unit, RISE Research Institutes of Sweden, and an Associate Professor with Uppsala University. He is also supervising four Ph.D. students (including Anum Khurshid) as the main supervisor. His work on IoT security is published in prestigious journals and conferences and, only in last two years, he has received over 1700 citations on his IoT security papers. His research interests include security and privacy in the IoT.

***