IoT Security Certifications: Challenges and Potential Approaches

André Cirne[a], Patrícia R. Sousa[a], João S. Resende[a], Luís Antunes[a]

[a]*CRACS-University of Porto*

Abstract

The Internet of Things (IoT) has changed how we interact with the world around us. Many devices are moving from offline to online mode, connecting between them and the Internet, offering more functionality to users. Despite the increase in the quality of life for users provided by IoT devices, it is also necessary to establish trust in the privacy and security of end-users. With this level of connectivity, the amount of data exchanged between devices also increases, inducing malicious activities.

One of the main problems is the lack of regulation in the IoT industry, especially between different manufacturers. There are no formal security rules, and manufacturers may not install security mechanisms. Therefore, it is necessary to promote the adoption of security measures. One way to do this is by using IoT devices and systems certification.

In recent years, IoT certifications have emerged. Meanwhile, the European Union has passed the Cyber Security Act to unify and regulate security certifications in member states. Our work collects the requirements that different IoT environments and application scenarios impose on certifications and discusses the current certifications' status according to those requirements. Besides, we also explored how EU measures apply to IoT and, where applicable, how certifications implement them, highlighting future research challenges.

Keywords: IoT, Certifications, Security, Trust

1. Introduction

Internet of Things (IoT) is a buzzword from the 21st century, and there is no consensus on its definition. Depending on the provided services, purposes, and architecture, the definition differs [1].

There are also different definitions from a variety of organizations, such as the Institute of Electrical and Electronics Engineers (IEEE) [2], National Institute of Standards and Technology (NIST) [3] and European Telecommunications Standards Institute (ETSI) [4]. Nevertheless, IoT is often considered a concept of interconnecting objects that gather information from the environment, interact with the physical world, and leverage the Internet connection to reach a common goal [5].

Nowadays, the number of IoT devices is continuously increasing. These systems are taking responsibilities in different domains and becoming increasingly essential for their operation. As a result of the intense adoption of IoT devices, new security concerns arise. The demand for more inexpensive systems produces heterogeneity between devices and a generalized lack of standards [6]. Aligned with the neglect of most manufacturers to implement network protocols with security in mind, the heterogeneity between different components emerges as a gateway for attackers to compromise the infrastructure.

The architecture of an IoT system is composed of

Email addresses: andre.cirne@fc.up.pt (André Cirne), patricia.sousa@fc.up.pt (Patrícia R. Sousa), jresende@fc.up.pt (João S. Resende), lfa@fc.up.pt (Luís Antunes)

sensors, actuators, communication channels, external utilities, and decision triggers [3]. The sensors and actuators are devoted to gathering and aggregating information. These devices often have limited resources, so it becomes more challenging to apply standard security measures the same way we apply to a full-size computer. [7].

IoT systems have dynamic and temporary communication channels between devices, leading to a preference for wireless communications [8]. However, this introduces new attacks, such as interference and information tampering [7]. Also, as the choice of protocols only considers network requirements, such as power consumption, bandwidth requirements, and interoperability [9], these protocols generally do not offer effective security mechanisms, resulting in serious security threats [10].

In addition to the architecture of these IoT systems, their context also influences their security, namely the environment where the system operates, the costs that a security breach or privacy violation can induce, the physical location of each system's element, and its topology at a specific instant of time [11]. This context establishes the necessary security requirements for a system [12].

With the emergence of new attacks and vulnerabilities, automated monitoring, testing, and mitigation tools are essential to address the risks arising from such threats or potential manufacturing or configuration failures. Thus, device manufacturers should promote automated solutions that guarantee device security, management, and secure deployment [13].

However, most manufacturers are not creating security and privacy solutions by design, leading to a lack of security measures on IoT devices. A solution for this issue can be government grants, awards, or enforcement through laws and regulations [14].

Phillip A. Laplante et al. [15] present the hypothesis of improving IoT security through certifications. They emphasize three possible directions that an IoT certification can take: certification of products, in which we certify a device or a system; certification of entities that create IoT systems, as it happens with licensed electricians and other professionals; and finally, certification of production processes for these systems.

The certification of IoT systems is an urgent need, as it is the most effective solution to improve their security mechanisms [15]. Their role is to support implementing different security requirements and increase the buyers' confidence in these systems. Some certifications are already on the market, and the academic community is still working on new ones.

To follow this trend and as a way to standardize new certifications that may arise, the European Union (EU) established the EU Cyber Security Certification Framework (ECSCF) [1] that defines a format and methodology to be used by certifications in all member states. The Cybersecurity Act, a legislation that aims to strengthen European capabilities in terms of cybersecurity, reinforces this scheme [17].

In brief, security measures depend on the devices' heterogeneity, low resources, and dynamic context [18]. Also, the developers and manufacturers are not applying security and privacy by design. Securing development guidelines is a fundamental building block for IoT security, and certifications help advance security by design in the IoT ecosystem.

Over the last years, some IoT certifications have emerged. In this direction, this paper focuses on analyzing IoT security certifications' current state, exploring their integration and adaptation for different IoT environments. In addition to that, we also point out some open research challenges and discuss potential solutions.

In brief, our work aims to answer the following research questions:

- **RQ1:** What are the requirements that IoT environments expect from certifications?
- **RQ2:** What are the special requirements that different IoT application scenarios impose on certifications?
- **RQ3:** Are current certifications able to meet the requirements imposed by IoT?

[1] ECSCF [16] is a meta-scheme for standardization, certification, labeling, and supply chain management. Thus, this is not a certification but a structure that new certification schemes should follow.

- **RQ4:** Is ECSCF ready to integrate with the current certifications?

This paper is divided into the following sections: Section 2 describes some past works that focus on certifications and frameworks addressing IoT security. In Section 3, we explain the definition of security certification introduced by the ECSCF. Section 4 discusses the different requirements that IoT and its application domains impose. Section 5 evaluates the level of alignment of the ECSCF according to the IoT requirements. Section 6 describes existent IoT certifications. Then, it is discussed the implementation of IoT certifications requirements in the studied certifications in Section 7. Finally, Section 8 proposes some future research directions based on our findings, and Section 9 provides the conclusions of our research.

2. Related Work

The certification of IoT systems is considered a significant challenge due to the growing number of devices in our daily lives. Several IoT certifications have emerged in recent years. It is essential to compare each one and ensure that they address the IoT requirements.

Badran [19] provides an overview of the different security frameworks and certifications applied to IoT devices and adopted by each country. Beyond that, this research compares different options used to express the buyer's certification results, labeling the product to indicate that it meets a certain security level. *Badran*'s work evaluates multiple frameworks and certifications but focuses on the different techniques to express the certification result to consumers. Thus, the author does not check if it is suitable for IoT devices. For example, some certifications addressed are based on the Common Criteria certification [20], which is unsuitable for IoT devices [21]. Alternatively, our approach asserts whether or not a certification is appropriate for an IoT environment.

Privitera and Li [22, 23] evaluate the effectiveness of commercial IoT certifications against the perception of IT professionals and consumers about security threats of IoT devices. The authors plan to survey these two communities to identify their perception of IoT security requirements and compare them with the purpose of the existing certifications. However, this is an ongoing project, and currently, there are no conclusions. This work intends to compare the consumers' perceptions and IT communities with the security checks implemented by certifications, unlike ours, which compares the certifications' security checks with the requirements pointed out by the scientific research.

In 2020, *Sara N. Matheu et al.* [24] made an overview of cybersecurity certifications to facilitate the definition of a structure that fits in emerging scenarios, such as the IoT paradigm. However, this work focuses on examining general certifications rather than IoT-focused certifications', which is our focus.

Contrarily to these works, our paper analyses the IoT certifications and explores the integration and adaptation to different IoT application scenarios. As far as we know, this is the first work that addresses these issues.

3. Security Certifications according to ECSCF

Security certification is an assessment to determine whether certain assumptions are correctly implemented, operating as intended, and producing the desired outcome to meet security requirements [25].

These certifications are designed by the scheme owner [2], who should keep them up to date according to the needs of the industry, and are carried out by Conformity Assessment Body (CAB)s, who are expected to conduct applicable conformity assessments and generate an evaluation report to grant the certification.

In this section, we will introduce the different characteristics of security certifications. Beyond that, we will also explain the requirements and structure imposed by the ECSCF on security certifications.

[2] According to the ECSCF nomenclature. The scheme owner is the institution responsible for the certification development [26]

3.1. Certification characteristics

There are three fundamental characteristics in any security certification: a context, a target, and an audience (Fig. 1). These attributes help define which use cases can use a specific certification.

This set of attributes was inspired by the ECSCF, which is the European Union Agency for Cybersecurity (ENISA) classification system for security certifications [26], and by the characteristics of the *EUROSMART* certification [27].

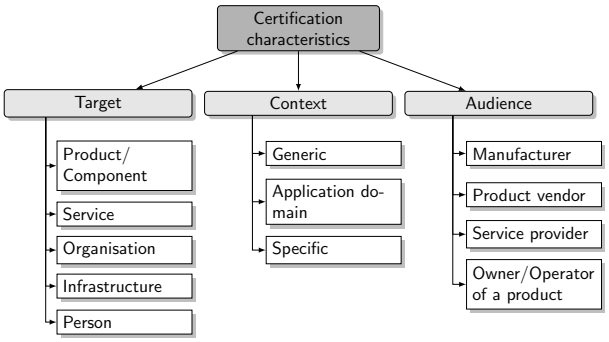

Figure 1: Certification characteristics

The *target* characteristic focuses on what the certification is trying to evaluate. For example, it can be an evaluation of a unique product or component (for example, an intelligent bulb), a service (for instance, an assessment of a complete system that includes a smart bulb, an IoT gateway, and a Web API), or an organization [28].

The *context* is the type of environment used during the certification procedure, which can vary from a general use case, where only the generic characteristics of that environment are known, or a specific application scenario, such as smart cities. The effectiveness of certification varies depending on the context, the scope assessed, the threats considered, and the assumptions made. A more precise context definition will result in a more detailed list of security requirements, resulting in a more secure device [11].

The certification *target* and *context* will affect the *target audience*. The *audience* could be divided into two groups: sponsors and consumers. The sponsor is the organization that finances the target's certification, and the consumer is the entity for which the certification intends to prove it is compliant with the security requirements. The main actors are the manufacturer, product vendor, service provider, and device owner in both groups [28].

This wide range of characteristics causes great diversity among certifications, and this heterogeneous scenario is what the Cybersecurity Act wants to regulate and unify.

3.2. European guidelines for certification scheme

With the Cybersecurity Act, the European Union (EU) intends to create an ECSCF that defines a structure and methodology to harmonize cybersecurity evaluations across the EU.

To achieve this goal, the ENISA and European Cyber Security Organisation (ECSO) have published several recommendations.

ECSO created the ECSCF, which is a framework that tries to solve issues identified by its industry partners. ECSO realized that, despite assessing the security of products, services, and systems with excellent results, existing schemes are not agile and require a lengthy certification process. Therefore, the ECSCF intends to be a base block for building lightweight certifications that combine existent security certifications taking advantage of their strengths.

To support the ECSCF, ENISA created documents to clarify the Cybersecurity Act implementation [26] and a list of existing certifications grouped by application domain [29].

Every three years, the European Commission defines a work program with the priorities for future European cybersecurity certification schemes. Then, the ENISA must prepare candidate schemes or review existing ones to answer the European Commission's expectations. These schemes must follow the ECSCF structure [30].

The following subsections will summarize the significant ECSCF guidelines that certifications must satisfy.

3.2.1. Scheme owner responsibility

The owner of a cybersecurity certification is responsible for keeping the certification updated according to the industry's needs. To do this, it must

maintain a working relationship with relevant stakeholders [26].

Besides, the owner must set up a structure for the operation and management of the scheme, including mechanisms to ensure transparency and trust. These methods should deal with vulnerabilities discovered after the certification was issued and ensure that everyone involved in the certification process has the required technical skills and competencies to certify a target [30].

3.2.2. Core components

Article 54 of the Cybersecurity Act [30] lists the recommended components for EU cybersecurity certification candidates. From this list, we highlight three central elements, considered mandatory, to meet the organization proposed by the ECSCF.

Technical Specification of Security Requirements
The document contains a collection of requirements describing the desired security features that must be implemented and covered by the certification scheme.

Assessment Methodology
The document defines the validation procedures to assess the target against the technical security requirements, including documentation review, test procedures, and the level of automation taken. It should also indicate the expected results of the assessment, such as a report or score.

Conformity Assessment Specification
The document describes all the policies and processes that govern the certification scheme, covering the certification scheme's scope, the surveillance of certified products, and laboratories responsible for the evaluation.

Without these components, it is impossible to meet the structure proposed by ECSCF. The Cyber Security Act also states that these elements should be reused based on existing standards when applicable and whenever possible.

3.2.3. Indicators of Confidence and Security

Depending on the importance of what we are evaluating, the confidence and level of security required will vary. Security certifications offer different evaluation levels to answer this need. These levels are called assurance levels and dictate the level of access and the amount of information required to evaluate a target. The higher the assurance level, the more secure the device is due to a complete analysis.

The ECSCF introduces a structure for assurance levels divided into two groups: the base group, in which a black-box type evaluation is carried out; and the advanced group, in which the target underwent an in-depth assessment where the context of the product is included.

When designing a security certification, the scheme owner must adapt this structure according to its use case and choose an evaluation methodology suitable for each assurance level [16].

3.2.4. Common language

One of the goals of the ECSCF is to reuse existing parts, such as standards or other certifications, as much as possible. A standard structure across different certification schemes is necessary to combine them. This section will describe the designs introduced by the ECSCF to facilitate the combination of various schemes.

The ECSCF sets three structures to ease the utilization of different components in the same certification: the Generalised Protection Profile (GPP), the Generalised Security Target (GST), and the European Cyber Security Certificate (ECSC).

GPP defines a security problem from a previous risk assessment and target's security goals. It must also describe the features that need to be implemented to meet the security goals and the assurance levels used to evaluate the device. The notion of GPP was borrowed from the Common Criteria [20]. A group of experts creates each GPP due to the need for deep technical knowledge in the target's application domain and threat landscape.

Based on the GPP, a GST is generated for the certification target. GST expands the GPP with the certification sponsor's specific security requirements.

The certification results must be in a unified format - the ECSC. It must include a label with the assurance level and a way to obtain detailed information, such as a QR-code or NFC-tag pointing for the ECSC detailed report. This report must contain the main attributes of the evaluation, such as the name of the product, the GPP used, the certification scope, and the results of the evaluation process.

This organization allows different certifications to share the same components and have the same certification procedure [26].

4. IoT landscape

IoT environments have unique characteristics, so security certifications must adapt to these characteristics to accurately assess this type of system. Besides, specific requirements for each application domain are needed when certifying a system for a particular use case.

There are some distinct categorizations of IoT application scenarios in the literature. *Atzori et al.* [8] divide the IoT applications into four domains: transportation, healthcare, smart environments, and personal domain. *Gubbi et al.* [5] also categorize the applications in four domains. However, they differ from the previous ones, dividing the domains into personal/home, enterprise, utility, and mobile. *P.P. Ray* [31] presents another possible classification with environments divided into nine different domains: RFIDs, service-oriented architectures, wireless sensor networks, supply chain management and industry, healthcare, smart societies, cloud service and management, social computing, and security.

Considering an IoT security certification, the categorization needs to group different environments with similar security requirements to maximize the effectiveness of security measures applied to each application domain. So, *Atzori et al.*'s approach is restrictive because it does not differentiate environments with distinctive security requirements. For instance, smart homes and industrial plants are in the same category, while, in terms of privacy concerns, the former demands more privacy requirements than the later. *P.P. Ray*'s categorization scheme is very detailed compared to the others but focuses on technologies rather than security requirements. Thus, during our research, we will focus on *Gubbi et al.* categorization scheme as it can group different applications with similar security requirements. This scheme was designed based on the environment's scale: individual, community, and national, as they tend to have the equivalent security and privacy needs.

Therefore, the categories that we will utilize during this work are: personal and home domain, enterprise domain, utility domain, and mobile domain.

In this section, we will enumerate the different requirements imposed by IoT on certifications, both at a general level and for the specific needs of each IoT application domain.

4.1. General requirements

From the literature available on the security requirements of IoT devices and systems, we have collected a list of resources that, ideally, a security certification in IoT needs to meet, namely security assessment, privacy impact assessment, pattern reuse, short time certification, attention to laws and regulations and update policy.

4.1.1. Security assessment

A security assessment is a process of determining how effectively a subject meets its security objectives [32].

Different security assessments can evaluate different parts of the IoT system, namely risk analysis, vulnerability assessments, penetration testing, audits, code analysis, and fuzzing.

Risk assessment is a way to identify threats and assess their likelihood of happening [33]. This analysis will more accurately represent the system's risks depending on the context. Each security certification must have a risk assessment to better express the target's specific security requirements. Without it, the assessment will not adapt to the context of the device [34, 35].

Vulnerability assessment is essential to minimize the problem of security vulnerabilities on IoT devices. This analysis aims to identify known vulnerabilities in a system [32]. The IoT environment

has the advantage of being a lightweight process that can be automated. However, it only looks for known vulnerabilities. Therefore, when a certification only applies a vulnerability assessment, it cannot discover unknown vulnerabilities.

Penetration testing is a technical assessment that simulates the behaviour of an attacker. This assessment differs from a vulnerability assessment because, in addition to looking for known vulnerabilities, it discovers new ones and puts them into practice to evaluate their actual impact. For IoT environments, this analysis should be improved using automated tests to increase coverage while decreasing the execution time [36].

Audit is an assessment that compares an existing system configuration to a standard. The audit may include other assessments, such as vulnerability assessments or penetration tests. This type of assessment is commonly used for the application of security guidelines.

Code analysis is a technical assessment where a security specialist analyzes the source code to find unknown vulnerabilities in software. This process can be partially automatized and, depending on the methodology used, can include dynamic software analysis or only static code analysis [37, 38].

Fuzzing is an assessment where we test different device interfaces against test data generated automatically by combining random data and generation rules. The main objective of this test is to discover unknown software vulnerabilities. Despite being an automatic technique, this is an intrusive procedure that could cause the device to crash [38].

The risk assessment is a mandatory analysis for a security certification, without which the context of the system will not be considered. Vulnerability assessment is essential in reducing IoT vulnerabilities. However, it has a limited scope when applied alone, assessing only known vulnerabilities. The penetration test is a robust assessment, and because of that, it is a long process and tends to be manual. The efficiency of an audit will always depend on the chosen standard. Code analysis and fuzzing are the most intrusive security assessments, requiring access to device source code. Moreover, in the case of fuzzing, tests cannot be done in a production environment due to a possible service disruption.

It is up to the certification to choose the type of security assessment that best suits its needs. Certifications should use multiple assessment types and more intrusive ones to achieve a higher assurance level.

4.1.2. Privacy Impact Assessment

Currently, IoT certifications cannot be limited to security assessments and must also have a Privacy Impact Analysis (PIA). PIA analyzes how information is handled to determine the risks of processing the personal data and assess safeguards to mitigate potential privacy risks [39].

Due to the proximity to human activities, mainly in healthcare and smart home systems, these systems can be a single point of failure for the environment's privacy. The privacy requirements are different depending on the system we are considering. Nevertheless, basic privacy requirements must be guaranteed [34].

4.1.3. Standard re-utilization

By itself, the IoT world is a source of heterogeneity, with many different devices, protocols, and a lack of standards in general. Therefore, to reduce the heterogeneity level in IoT, the certification coverage should incorporate solid points of different standards to increase confidence and respect for a new certification by inheriting part of it from the reused standard [40].

4.1.4. Certification time

The duration of the certification process is often a factor in the non-certification of a product. Long certification processes increase production time, costs and make the product financially unprofitable [14]. Therefore, long certification processes must be avoided.

4.1.5. Laws and regulations context

Ideally, certification must include different laws and regulations that a given system must fulfil. These

obligations vary depending on where the system is installed, which requires a modular certification. The laws and regulations must be inserted in the certification to promote it. For example, suppose the security certification evaluates compliance with applicable laws and regulations. In that case, the certification owner will know that he will not be subject to possible fines, thereby encouraging its use.

4.1.6. Update policy

One of the problems with IoT systems is the lack of security updates. When a researcher discovers a vulnerability on a device, it is likely never to be fixed, even if it is publicly known [41]. Therefore, the certification authority needs to be aware of this situation and encourage the manufacturer to support their devices longer. If the certification authority does not implement an updated policy, security vulnerabilities can be found on a certified device, discrediting the certification.

4.1.7. IoT context aware

As we mentioned earlier, an IoT system is influenced by its context. The context can be defined with variables that vary over time, basically collecting information about the physical world. Changes are detected based on this information, and adaptations are made according to new conditions.

This dynamic context is why many traditional security methodologies fail because classic security assessments are carried out periodically. As IoT systems change quickly, the likelihood of a new device emerging between periodic assessments will be high. The security assessment will not predict and consider possible changes that may occur before the next periodic assessment [11]. Thus, the effectiveness of certification can be compromised. Any security certification for IoT needs to be aware of this evolution in the system's context and assess the risks arising from this dynamism.

4.1.8. Access to Guidelines

In addition to all the requirements we collected from the literature, we also propose a new requirement called *access to guidelines* that should not exclude the possibility of systems that are not officially certified but are in compliance with the certification. It is preferable that access to the certification guidelines is free and that only the certification process has costs. That way, it is possible to minimize the problem of cheap IoT products that are not profitable to go through the certification process.

4.1.9. Summary

The requirements mentioned throughout this section are the requirements imposed by the IoT environment on security certifications and answer to the **RQ1**. Any certification that appraises IoT systems or devices must follow these requirements.

4.2. Specific requirements

The application domain of an IoT system affects the importance given to each of the requirements mentioned before and could also introduce new ones specific to that field. It is necessary to detail the crucial aspects to effectively assess a specific domain target and select the most appropriate certification for each domain.

This section will list only the essential requirements, with particular importance for each application domain. Additionally to the prerequisites already mentioned (subsection 4.1), others will be introduced in this section according to the following domains.

4.2.1. Personal and home domain

The personal and home domain represents the IoT systems used at an individual or household scale, including smart home systems and healthcare systems. Nowadays, practically all household appliances or devices at home are connected to the Internet and have automation features.

In addition to this, people use more devices such as fitness trackers. Although these devices may not always be categorized as health devices in the strictest (and most regulatory) sense of the word, devices can collect users' health data that must, undoubtedly, be protected.

The focus of these systems is always the personal environment. The critical requirement for this domain is a data-driven security assessment, as it

presents the highest risk of endangering users' privacy [42, 43, 44].

For this domain, the cost of certification is an essential concern. Given that context-specific certifications are expensive and owners in a small-environments are unwilling to pay for this type of service, these certifications should be supported by manufacturers [44].

Certifications of healthcare devices must cover privacy requirements and specific regulations (for instance, the Health Insurance Portability and Accountability Act regulation [45]). However, it is also necessary to ensure that critical devices (at the hospital, for example) are fault-tolerant as failure could put a patient's life at risk [46].

4.2.2. Enterprise domain

The enterprise domain includes IoT systems within a work environment. Usually, these systems provide monitoring capabilities and process automation, allowing owners to reduce their costs [47]. Examples of these domain environments are enterprises, industrial and agriculture facilities.

Similar to the personal and home domain, the certification cost will be essential for this domain. The budget for an IoT certification in an enterprise domain will not be as low as the home domain but will not be the main focus. Depending on the IoT system's importance for the company's primary revenue, it is advisable to evaluate the system in a specific application domain. [48]. The enterprise domain could benefit from a specific evaluation context. However, this has inherent costs, which could make the certification unviable.

Furthermore, this application domain typically uses particular technologies for automation and security needs. Examples of these technologies are SCADA systems [49] or gateways that enable the connection of legacy systems with the Internet, with specific security risks compared to other technologies. Certifications should consider domain-specific standards that define how to maintain the system security [50]. Standards like the ISO/IEC 62443 [51] or NIST SP 800-82 [52] specify special considerations for risk assessment to this type of system and the measures that need to be put in place to mitigate its risks.

In this field, another unique security requirement is the need for knowledge protection and anti-piracy protection [53]. This requirement is not new for the industry; however, it is necessary to adapt it to this new attack surface. These technologies enable new insights about production lines and processes, which can also infer product designs [53].

To sum up, certifications for this use case need to have an *application domain* context type, to be able to take into account the specifics of the technologies, and have measures to protect intellectual property.

4.2.3. Utility domain

The utility domain focuses on applying IoT technologies in a wide area. All types of smart meters, smart grids, and smart cities are included in this domain. Typically, these applications are intended to optimize services, so the average consumers of these technologies are electricity, water, communications companies, or public institutions.

As this domain has much critical infrastructure for countries, it is the main target of state-sponsored threat actors [54]. Therefore, security assessment should be as complete as possible to minimize the risks of an attack.

Also, certifications for this domain should ensure that these systems are fault-tolerant, as essential services, such as water and electricity, depending on them [55]. Further, fault-tolerance should include self-repair mechanisms to recover from failure, malfunction, or a compromised state [56]. Even though this is a requirement for system design, security certifications must ensure its implementation due to its benefits for this application domain.

In addition to all this, the utility domain shares many legacy technologies with the enterprise domain [49]. Namely, SCADA systems are widespread in critical infrastructure [57]. Thus, certifications should have a specific context evaluation to include these risks.

In essence, a certification for the utility domain must evaluate the device with the highest assurance level possible, including a specific evaluation context

and procedure that includes risk analysis, vulnerability assessment, penetration testing, and audit. Finally, the certification must guarantee that the system has fault-tolerance capabilities to ensure system reliability.

4.2.4. Mobile domain

The mobile domain has a continuous creation and destruction of communication channels and a constant movement of devices. Examples of this domain are smart transportation, smart logistics, and autonomous vehicles. Certification in this domain needs to be prepared for systems continually changing [58], which means that the risks of the system will also evolve.

While smart transportation and logistics do not have other unique characteristics that stand out from the general IoT requirements, autonomous vehicles have. Without the proper security measures, autonomous vehicles could endanger lives because a security breach could give the attacker complete control of a car [59].

Autonomous vehicles can be seen in two ways. At the macroscopic level, we have multiple vehicles communicating with each other and with the road infrastructure. On the other hand, at the microscopic level, each car is a system by itself, with multiple components from different vendors communicating. Each one of these views has its security and safety problems [60].

Therefore, we will not find a unique certification to solve these problems. The security and safety problem in autonomous vehicles is multi-disciplinary. So, any certification needs to appraise multiple domains, including hardware reliability, software validation, security testing, human-computer interaction, and policymaking [61, 62].

The dynamic environment problem could be minimized using the combination of different certifications, even for the autonomous vehicle sub-domain. This process is called certification composition. By dividing the systems into smaller systems that are certified separately, the whole system is certified using the security guarantees of the smaller parts. Herewith, we can appraise their security requirements more quickly and, at the same time, adapt to the dynamic environment because we do not need to certify the whole system when a new device appears, but only the parts that changed [63].

Therefore, from the certification standpoint, this problem should be approached using a composition of different certifications, with multiple certifications that certify small pieces of the system and then together certify the system as a whole.

4.2.5. Summary

Throughout this section, we answer **RQ2** by describing the special requirements imposed by each IoT application scenario, namely *Personal and Home Domain*, *Enterprise Domain*, *Utility Domain* and *Mobile Domain*. Table 1 presents an overview of these requirements and their applicability to each application domain.

Domain	**Important Requirements**
Personal	• Privacy concerns • Sponsored by product vendor • Fault tolerance - Healthcare sub domain • Healthcare devices regulations - Healthcare sub domain
Enterprise	• Enterprise domain aware • Ensure intellectual property protection
Utility	• Highest assurance level • Ensure fault tolerance
Mobile	• Adapt to dynamic environment

Table 1: Requirements for each application domain

5. ECSCF and the IoT

This section will analyze how the ECSCF relates to the IoT requirements that we defined in the previous sections and if the ECSCF limits their implementation.

ECSCF does not try to meet the requirements of a specific area but creates a framework that mitigates common problems in security certifications.

Some of the requirements mentioned in Subsection 4.1, such as reuse of standards, update policy, cost of certification, and time of certification, are already present in ECSCF. The ECSCF includes these requirements because they are not specific problems of IoT environments. However, they are a general issue of security certifications, which means that adapting an IoT certification to meet the ECSCF requirements is simpler because IoT shares some requirements with ECSCF.

The concern about reusing existing parts is present throughout the ECSCF. This framework tries to unify security certifications, so it also wants to reduce heterogeneity in security certifications, which also affects IoT. Therefore, the "re-utilization of standards" is also ensured by the ECSCF as it motivates the use of existent certifications.

In Subsection 4.1, we stated that IoT systems lack security updates, and this is one of the problems that must be minimized with security certifications. Thus, we concluded that security certifications for IoT must enforce updated policies. ECSCF shares this concern and creates mechanisms at the certification level to monitor certified systems, ensuring that certified systems' security vulnerabilities are mitigated and do not discredit the certification.

We also described the problem with cheap IoT products that are not profitable for certification. This problem is minimized by the ECSCF with different assurance levels and allowing self-assessment in the lowest assurance level. With that, even the cheapest devices can be certified at a reduced cost.

Finally, we mentioned that certifications for IoT often impact the production time of the device, sometimes by making the product unprofitable. In order to solve this problem, ECSCF tries to use different assurance levels. A device must choose the assurance level that best fits its use case, thinking that lower assurance certifications will have fewer security guarantees and a negligible impact on the certification time.

In brief, even though the ECSCF is a generic approach, some problems affect any security certification. Both ECSCF and IoT literature share concerns about reusing existing parts, having an updated policy, reducing the certification time, and the monetary impact that a certification process produces on the production costs. Thus, the legislative vision is not far from the IoT reality.

6. Security certifications

Certifications for IoT systems and devices are beginning to emerge. This section will describe eight certifications focused on IoT. Academic researchers designed two of these certifications, namely DSPSMA [64] and ARMOUR certification [65]. The industry created the other six, namely ICSAlabs certification [66], UL-2900 [67], BSI Kitemark for Internet of Things devices [68], IoTAA Security and Privacy Trustmark [69], Eurosmart IoT Security Certification [70], and ioXt [71].

6.1. DSPSMA

Dynamic Security and Privacy Seal Model Analysis (DSPSMA) [64] is a certification scheme that combines a real-time monitoring system and the existing certification model, where an audit is performed at a specific point in time. This certification is materialized in a dynamic seal applied to the system that can be updated over time. This seal is called Dynamic Security and Privacy Seal (DSPS). Currently, this certification does not have implementation yet.

Due to the attempt to combine a standard certification and a monitoring system, the DSPSMA is structured in two phases: the *initial certification phase* and the *monitoring phase*.

Although the possibility of adapting to other normative environments is mentioned in the initial certification phase, the system is assessed according to the European Union's normative environment, such as General Data Protection Regulation(GDPR) and e-privacy directives. Different technical standards and recommendations are also assessed. For instance, the ISO/IEC Information Security Management Systems standards will assure that security, privacy, and risk analysis will be performed on the system. Applying different standards in the same certification process minimizes the possibility of blind spots by using each standard's strengths to cover their limitations. Auditors and technical experts will be responsible for

conducting this part of the certification due to the required diversity of standards and regulations.

In the *monitoring phase*, the certified system will be continuously monitored. If this process detects a potential privacy or security breach, the systems' owner and the DSPSMA organization is notified. The notification triggers an evaluation process by the customer for the system and an obligation to report these results to the DSPS organization. Depending on the severity of the breach, a system re-certification may be required. This mechanism guarantees the validity of the certification over time.

The monitoring part of this certification fulfills different functions, depending on the different types of users. DSPS acts as a user-friendly tool for checking the certified system's overall status for a generic end-user. Advanced users, such as system owners and administrators, will have more advanced tools to view and analyze problems. DSPS organization will serve as a surveillance mechanism to monitor the certified system, dynamically update the certification, and as probes to detect new threats from the IoT world.

Finally, an interesting point of this architecture is applying a blockchain as a solution for log storage. The blockchain maintains the historical records of each certification and guarantees the authenticity and integrity of the data.

The existing standards support this certification. However, a crucial point is missing because it fails to provide quick unified guidance for the audition phase. This problem is recognized and identified in the technical certification report as future work. Also, this certification uses general security standards, such as ISO 27001, which may not be prepared for specific requirements of IoT environments [11].

6.2. ARMOUR certification

The European Union's ARMOUR project aims to address security and trust issues in the IoT, providing automated and simplified testing, benchmark, and certification processes for many devices. One of the project results is the proposal for a cybersecurity certification (ARMOUR Certification) [65].

This certification's design follows the main guidelines of ECSO, including ECSCF, but it also includes some additional components to accommodate the dynamic context where IoT devices are deployed.

This certification is divided into an initial security risk assessment and a continuous security testing phase. These two phases are based on the main European Telecommunications Standards Institute guidelines for risk-based safety assessment and test methodologies (ETSI EG 203 251) [72].

Initially, a context is established, where the goal is to understand the device's business and regulatory environment. A risk analysis is then performed, identifying the different vulnerabilities that can affect the subject. These vulnerabilities must have an associated test procedure. Finally, the device is configured to be tested and monitored continuously over time.

The tests are repeated in two situations: when a new vulnerability is found or when a new firmware update is released. If a new vulnerability is found, the tests are repeated after adding a test that assesses whether a particular device is vulnerable or not. Thus, the certification is updated when the device is unsafe, but the manufacturer has the opportunity to resolve it and recover the initial certification result.

One of the fundamental characteristics of this certification scheme is the labelling system, through which the result of the certification is transmitted to users. A QR code tag is attached to each device containing a link to a page. This page displays the updated certification status of the device. It can also contain the certification result for more specific contexts, such as when a device is used in a domestic environment [21].

This certification process ensures that a device is not vulnerable to known threats. However, it has no process for discovering unknown vulnerabilities specific to the scanned device, and IoT vulnerability databases are missing, limiting the efficiency of this certification. Finally, there is no analysis aimed at user privacy. Standard approaches tend to bind to GDPR requirements only if appropriate for the device and not as a general rule.

6.3. ICSA Labs certification

ICSA Labs is an independent company that provides product certification and testing to end-users

and business entities. ICSA Labs offers certification focused on IoT devices, among other certifications.

The certification is based on its IoT Security Testing Framework - a lightweight security guideline for IoT devices. This framework defines several security requirements grouped into seven domains, more precisely, encryption, communications, authentication, physical security, platform security, and alerting. In the case of encryption requirements, it is also important to note that they require a device to comply with the NIST and FIPS recommendations [66]. So, a device is certified if it meets these different security framework requirements [73].

When the certification is carried out, the device cannot be affected by any known vulnerability. However, it has no mechanisms to enforce security updates after the certification is issued, and it does not have an expiration date. Therefore, it is possible to have a device certified and affected by a vulnerability.

6.4. CAP

Cybersecurity Assurance Program (CAP) [74] is a security certification developed by Underwriters Laboratories (UL) [75]. This certification aims to test the security vulnerabilities and weaknesses in embedded devices and systems.

The certification assessment procedure is based on the UL-2900 [67], a proprietary group of standards developed by Underwriters Laboratories (UL) [75] for the safety of network-connectable products and systems.

This family of standards comprises three different groups: general requirements, industry requirements, and general process requirements. The industry requirements group defines guidelines for a specific application domain. For example, UL 2900-2-1 details the basic principles used in healthcare devices for healthcare products.

Furthermore, one of the standards of this family has already been recognized as the national cybersecurity standard for connectable components of healthcare and wellness systems by the American National Standards Institute [76].

In terms of the certification process, it is divided into different phases. Initially, documentation is gathered about its production process and functional requirements. After that, the product moves to the risk control and management phase, assessing different risks. A product safety assessment is then carried out, confirming whether the necessary measures have been taken to minimize previously identified threats. The product is checked for known vulnerabilities, and penetration tests are made. Besides this, high assurance targets must have fuzzing tests. Finally, the certification authority issues a certification and a report with different tests, assumptions, and results [77].

The certification process can take several months, and the certification insurance is valid for a year. During this period, every vulnerability found needs to be patched in a reasonable time frame [78]. Also, the vendor must inform the UL of any software change in the device.

CAP certification offers a high level of assurance. However, it presents some disadvantages compared to other certifications. As it is a proprietary certification, there was no open discussion about its procedure, causing distrust among cybersecurity certifications [78].

6.5. BSI Kitemark for Internet of Things devices

The British Standards Institution (BSI) is the UK's national standardization organization. It provides testing and certification services for several products, including IoT devices.

When it comes to IoT, it has a certification for IoT devices that offers three levels of guarantee: *Residential* (for residential environments), *Commercial* (for commercial environments), and *Advanced* (for high-risk residential and commercial environments).

The certification will include ISO 9001 compliance tests, vulnerability testing, and penetration testing. The penetration test is designed to adapt to the attack's complexity according to the level of assurance. For example, at the *Residential* level, the techniques used to test the target will be less complicated than those used to test at the *Advanced* level because devices in the Residential level typically face less complex attacks, and the certification budget during the development of these devices is reduced.

The device is also tested against the requirements of the ETSI technical specification for consumer IoT security (ETSI TS 103 645) [68].

BSI regularly monitors certified devices, repeating security tests to ensure that the devices remain secure. It is also important to mention that ETSI TS 103 645 enforces device measures to ensure user data privacy, regardless of the regulatory context. These measures follow the GDPR [79].

6.6. IoTAA Security and Privacy Trustmark

The IoT Alliance Australia (IoTAA) [69] is an Australian organization of different IoT companies and individuals to promote good IoT security practices.

One of their plans is to create an IoT certification for devices. Currently, the certification is not formulated yet. However, its guidelines are available under the name "IoTAA Security Guideline".

These guidelines consist of thirty mandatory requirements and seven recommendations. Manufacturers can choose not to follow these conditions if it is not suitable or to adapt the mandatory specifications concerning the field of application. The requirements address IoT devices' security and privacy needs aligning with Australia's Privacy Principles, an Australian regulation that guarantees privacy protection.

These guidelines have the particularity of enumerating network protocols and advising on the appropriate configurations to guarantee the device's security [80]. This forces IoTAA to constantly follow changes in these protocols and update the guidelines accordingly. If this process fails, it can compromise its credibility. Typically, other certifications delegate this type of recommendation to other specific guidelines. For instance, delegating the recommended TLS configuration to the National Institute of Standards and Technology (NIST) guidelines [81]. This way, the certification ensures the best recommendation possible by following the guidelines of a specialized organization for the field in question.

6.7. Eurosmart IoT Security Certification

The Eurosmart IoT Security Certification Scheme (e-IoT-SCS) is based on the ECSCF requirements. It focuses on IoT devices and evaluates them with *Basic* or *Substantial* assurance levels (Subsection 3.2.3).

This certification is designed to be sponsored by the IoT product vendor and answer to an IoT service provider or device owner's necessities in terms of the target audience. Because of these design options, the evaluation procedure is dependent on privileged access to the device [27].

This certification scheme has Security Profiles for each type of IoT product, which defines the security requirements and assurance activities for each specific security problem. The Security Profile considers the asset's sensitivity and the environment it operates, allowing it to scale the necessary security controls following the identified risks. It also tries to cover the entire attack surface from physical attacks to cloud infrastructure attacks [82]. The evaluation procedure is also driven by a risk approach and includes a vulnerability assessment and a testing phase to demonstrate if the device implements the necessary security features. This could include a penetration test and fuzzing, depending on the assurance level [83].

The e-IoT-SCS includes a phase of surveillance after the certification is issued. In this phase, the CABs involved in the certification process need to frequently re-inspect product samples. The Security Profile defines the frequency of these activities. Moreover, the CABs must monitor EU CSIRT sources for security alerts impacting the evaluated product [82].

Its security profile includes a wide range of stakeholders, including the device owner and a possible security operator/administrator, which may or may not have the necessary skills depending on the type of environment [84]. This type of premise is vital for IoT environments because, in some cases, like smart homes, the user can be a non-expert and expect a simple setup process. On the other hand, competent security operators could respond to threats in an environment like a smart city.

This certification accepts self-assessment in the supply-chain evaluation and checks that security goals and assumptions are correct.

6.8. ioXt security certification

ioXT is a security certification by the ioXt Alliance. The ioXt Alliance is a group of technology and industry companies that have established a security standard and certification for IoT devices. It is essen-

tial to highlight that companies like Google, Arm, and Tuya are working together on this initiative, and there are already a considerable amount of certified devices [71].

The ioXt security standard is based on eight principles: the device needs to have unique credentials; its interfaces must be properly secure; its communications and updates must use standard cryptography algorithms and protocols; it must receive regular security updates; the update mechanism must be secure; its default configuration must be secure; the manufacturer must have a vulnerability reporting program implemented, and be transparent regarding the period the device will be supported. Further detail can be found in the ioXt Security Pledge [85].

At its core, the ioXt certification has profiles and compliance tests. The ioXt Alliance develops profiles that contain three components: the type of device that can be certified under the profile, threat analysis, and a selection of tests required for certification, which are selected from the ioXt Alliance Compliance Test Case Library [85]. These profiles are not focused on the application domain but instead on the type of device. For instance, there is a profile for residential cameras and another for smart speakers.

Furthermore, depending on the number of requirements met, the device will obtain an assurance level on each principle mentioned earlier [86, 87].

The certification process is divided into multiple steps [71]. First, the manufacturer needs to register for the certification program. Then, the manufacturer should decide if he wants to self-certify or delegate to an authorized lab testing [85]. After choosing a profile and executing the necessary tests, the results and product information are submitted to the ioXt Alliance, which reviews the application and emits a certificate. The manufacturer adds a label to the product package indicating the certification result and a link for the detailed report [88].

After a device is certified, the relationship between the manufacturer and the ioXt Alliance does not end. The manufacturer is obligated to communicate any firmware change. On the other hand, the ioXt needs to inform the manufacturer of any IoT regulatory updates. Furthermore, any security researcher can dispute the certification result.

This certification has two peculiar characteristics. Firstly, it has a specific profile for mobile applications [89], which is out of scope for most IoT certifications. Secondly, it implements a bug bounty program for researchers who discover security vulnerabilities on certified devices to endorse third-party reviews [90].

7. Discussion

This section will analyze and compare the certifications we mentioned in Section 6, according to the requirements introduced in Section 4. In this analysis, we used all the public information about each certification, including security standards, certification documentation, and certified device reports.

Three tables will follow our analysis to make it easier to compare the certifications described in Section 6. Table 2 has the characteristics of each certification, Table 3 includes the different security assessments employed by each certification, and finally, Table 4 describes the fulfillment of the requirements that we defined in Section 4.1.

7.1. Reflection on certifications

Subsection 3.1 mentioned that certifications have three fundamental characteristics: context type, scope, and audience (divided into sponsor and target). Table 2 exhibits the characteristics of the certifications mentioned throughout this work.

Most certifications are carried out concerning an application domain or general context, probably because they are often performed during production, making it impossible to define a precise context for the system. For this reason, the DSPSMA is the only one with a specific context, as the target is certified when it is already deployed and not during production time.

Most certifications are sponsored by the product supplier and target the User/Consumer. The purpose of these certifications is to build trust among consumers of IoT devices.

DSPSMA is the only certification that sees the system owner as sponsor and target of the certification.

	Context type	**Scope**	**Sponsor**	**Target**
DSPSMA	Specific	System	System owner	System owner
ARMOUR	General	Device	Product Vendor	User
ICSAlabs	General	Device	Product Vendor	User
CAP	Application domain	Device & system	Product Vendor	User
BSI Kitemark	Application domain	Device	Product Vendor	User
IoTAA	Application domain	System	*Unknown*	*Unknown*
e-IoT-SCS	Application domain	Device	Product Vendor	User
ioXt	Application domain	Device	Product Vendor	User

Table 2: Certification characteristics

This certification targets critical IoT systems that require security evaluations to deploy IoT devices in a specific environment.

The sponsor and the certification target influence the certification scope. Certifications sponsored by a product vendor will evaluate devices, while certification sponsored by the end-users will target a complete IoT system.

Throughout the Subsection 4.1, we identified the requirements for an IoT certification. Table 3 lists the different security assessments applied to the subject during the certification process, and Table 4 summarizes how certifications implement the remaining requirements.

ICSAlabs, IoTAA, and ioXt certifications use a list of security requirements created especially for the certification, and in addition to that, they require a vulnerability assessment. BSI kitemark also applies a list of security requirements, but this list is a European technical specification. The BSI kitemark also conducts a vulnerability assessment and penetration testing as part of the audit. DSPMA employs a risk assessment and vulnerability assessment in its audit. ARMOUR certification does a risk assessment to find the device's right assurance level and a vulnerability assessment. ioXt executes a risk, vulnerability assessment, and code analysis if requested by the vendor. e-IoT-SCS performs a risk assessment, vulnerability assessment, penetration testing, and fuzzing test, depending on the assurance level. CAP is the most complete security assessment, performing all the security assessments we considered.

All certifications implement vulnerability assessments. On the other hand, code analysis and fuzzing are the less common assessments. This difference can be justified because code analysis and fuzzing tests are very intrusive methods, requiring access to privileged information such as the product's source code. Therefore, only vendors sponsor this type of high assurance certification.

We can also notice the discrepancy between the certifications that use vulnerability assessment and penetration testing. Every certification performs a vulnerability assessment, but only three certifications feature penetration testing. This assessment is often used because it is possible to automate it, making the certification process lighter than one with penetration testing [91].

As this analysis looks only for known vulnerabilities, relying only on a vulnerability assessment can put the device's security at risk. If the device has customized software that has never been analyzed, this method will not find them even if it has vulnerabilities. Penetration testing is one of the ways to discover unknown vulnerabilities. However, it has the disadvantage of being a manual process [91, 92].

The number of tests and whether they are manual are the main factors for the duration of the certification process [93]. Certifications attempt to overcome this problem with different assurance levels, including additional testing on higher assurance levels.

Subsection 4.1 mentioned the importance of a PIA,

	Risk assessment	Vulnerability assessment	Penetration testing	Audit	Code analysis	Fuzzing
DSPSMA	Yes	Yes	No	Yes	No	No
ARMOUR	Yes	Yes	No	No	No	No
ICSAlabs	No	Yes	No	Yes	No	No
CAP	Yes	Yes	Yes	Yes	Yes	Yes
BSI Kitemark	No	Yes	Yes	Yes	No	No
IoTAA	No	Yes	No	Yes	No	No
e-IoT-SCS	Yes	Yes	Yes	Yes	No	Yes
ioXt	Yes	Yes	No	Yes	Yes	No

Table 3: Security assessment comparison

which was a requirement to improve user data privacy concerns, even when this is not mandatory by regulation. Therefore, we only considered those that perform a PIA independently of the regulatory context. By this principle, the DPSMA, BSI Kitemark, IoTAA, e-IoT-SCS, and ioXt have PIAs. The others have no privacy concerns or only have them when required by regulation. This lack of PIAs may be due to these certifications trying to assess the certification target automatically. PIAs are done manually by interviewing the manufacturers or making questionnaires, which would imply a delay in the certification process [94]. Nevertheless, ioXt overcomes this problem by performing the PIA at the profile level, which is reused by multiple devices.

Generally, access to guidelines is free, except for the CAP. DPSMA has a free certification guideline but refers to paid standards, such as ISO 27001.

Most certifications include the assessment of applicable laws and regulations. The only one that does not do this is the ICSAlabs certification. BSI Kitemark exclusively includes the GDPR.

We could identify two approaches to address the IoT update issue. One is the constant monitoring of the subject after the certification phase, i.e., if the certification authority detects a vulnerability, it will automatically update the certification report (DSPSMA, ARMOUR, BSI Kitemark, and e-IoT-SCS). The other solution is creating a vulnerability report program, including public disclosure and vulnerability patching (BSI Kitemark, IoTAA, and ioXt). BSI Kitemark is the only certification that enforces these two types of control. ioXt goes a step forward and rewards researchers who find vulnerabilities in certified devices.

The requirement of awareness regarding the dynamic context in which the system is inserted is only applicable to the DSPSMA. Unfortunately, this certification does not consider the constant change of the system's environment. IoT technologies' dynamic environment is a known characteristic of IoT and is pointed out as one of the open research opportunities.

7.2. Reflection on domains

This section will analyze how the different certifications collected throughout this work are adapted for each application domain. From this analysis, we select those that best fit the domain requirements (Table 1) and describe their advantages and disadvantages.

Personal and home domain
Certifications for personal and domestic domains need to have two fundamental characteristics: guaranteeing user privacy and not having an associated cost for the end-user. To guarantee the privacy of the user, it could be, for example, performing a PIA. In terms of cost, it requires a certification focused on a general domain/application context and sponsored by the product supplier.

	PIA	Standard re-utilisation	Access to guidelines	Laws and regulations	Update Policy	IoT context aware
DSPSMA	Yes	ISO 27001 ISO 29190 ISO 15408 NIST SP 800-122	Free	Depends on the country	Constant monitoring for threats	-
ARMOUR	No	ETSI EG 203 251 ISO 15408 ECSCF	Free	Depends on the country	Constant monitoring for threats	*N.A.*
ICSA Labs	No	ICSA Labs Security Testing Framework	Free	-	-	*N.A.*
CAP	No	UL-2900 Standard	Payed	Depends on the country	Vulnerability report program and patch enforcement	*N.A.*
BSI Kitemark	Yes	ETSI TS 103 645 ISO 9001	Free	-	Vulnerability report program and regular surveillance	*N.A.*
IoTAA	Yes	IoTAA Internet of Things Security Guideline	Free	Australian laws	Vulnerability report program	*N.A.*
e-IoT-SCS	Yes	ECSCF	Free	Depends on the country	Active surveillance	*N.A.*
ioXt	Yes	ioXt pledge	Free	Depends on the country	Bug bounty program	*N.A.*

Table 4: Certification requirements

Three certifications fulfill these characteristics (Table 5): the e-IoT-SCS, the ioXt and the BSI Kitemark. All certifications aim to certify devices in an application domain, charging the manufacturer with certification costs. The certification results are expressed as a label in each device to inform the buyer/owner how secure the device is.

In terms of privacy issues, e-IoT-SCS, ioXt, and BSI Kitemark have well-established requirements to ensure its users' privacy. e-IOT-SCS requires that device development comply with the "privacy by design" principle and establish multiple requirements to achieve it. In addition to this, e-IOT-SCS also demands a PIA for any device that wants to be certified [84]. The BSI Kitemark demands that the user data is protected, including the user's consent, transparency about the collected data, and how it should be stored [79]. The ioXt follows this approach and sets specific privacy requirements according to the device type.

The significant difference between the BSI Kitemark and e-IoT-SCS is that e-IoT-SCS has an

	Privacy concern	Sponsored by product vendor
DSPSMA	Yes	No
ARMOUR	No	Yes
ICSAlabs	No	Yes
CAP	No	Yes
BSI Kitemark	Yes	Yes
IoTAA	Yes	-
e-IoT-SCS	Yes	Yes
ioXt	Yes	Yes

Table 5: Analysis of the requirement fulfillment for personal and home domain

evaluation based on risk analysis, which is not part of the BSI Kitemark assessment procedure (Table 3). On the other hand, the ioXt does not have penetration testing but has a lightweight system to include a PIA in the device evaluation. Moreover, the ioXt has a considerable amount of home devices already certified [71]. Finally, an advantage of e-IOT-SCS, when compared with the others, is that it is compliant with ECSCF.

Due to its regulations and possible effects of a failure, the healthcare devices subdomain needs a certification based on health regulations. Accordingly, CAP certification is indicated for this domain because, in addition to offering every type of security assessment (Table 3), it can also evaluate a device according to a security standard created to assess healthcare devices (UL 2900-2-1) [95].

Enterprise domain

The enterprise domain requires a certification capable of appraising the specific requirements of this application domain. So, the certification needs to be aware of the application domain or the system context. The certification sponsor must choose between these two contexts according to the importance of the IoT system for the company's primary revenue. Suppose the system is critical to the company. In that case, the evaluation should be specific to the system context to have the most accurate threat model possible and mitigate the maximum number of risks. It is up to the certification sponsor to find the correct evaluation context. Nevertheless, as we stated before, its context must be an application domain at the minimum.

The other essential requirement for this domain is to protect any copyright technology accessible by the IoT system.

	Enterprise domain aware	Anti-piracy protection
DSPSMA	Yes	No
ARMOUR	No	No
ICSAlabs	No	No
CAP	Yes	No
BSI Kitemark	Yes	No
IoTAA	Yes	-
e-IoT-SCS	Yes	No
ioXt	No	No

Table 6: Analysis of the requirement fulfillment for enterprise domain

From the certifications that we revised before (Table 6), there are only three that are not capable of including enterprise domain-specific security requirements.

e-IoT-SCS supports different application domains by including specific security risks in the risk assessment made for each device.

BSI Kitemark also has a risk assessment, but in addition to this process, it has two levels of assurance that can be used for this domain, commercial and enhanced. These two assurance levels were created to appraise the necessities of products used in enterprise environments depending on their value. With the increase of the assurance level, the product is submitted to a more extended evaluation period [96].

IoTAA chooses a different approach for this problem, delegating to a list of frameworks and standards from other organizations the measures that need to be followed for this domain. For instance, it defines that all recommendations of the Industrial Internet Consortium must be followed [97].

As IoTAA, CAP has included this application domain in its guidelines. However, it does not delegate measures to other entities. It has its security standard for this domain, the UL2900-2-2, with the

requirements necessary to evaluate industrial control systems.

DSPSMA was the only certification that we analyzed that evaluates a system according to a specific context type. It can create the most precise risk evaluation of an environment of this type because it assesses the real risks of the installed system.

There is a diversity of security certifications aware of the unique characteristics and technologies used in the enterprise domain. However, when we analyzed the anti-piracy protection requirement, we could not find any certification that directly appraises this matter. There are some general notions of maintaining asset confidentiality, but it is up to the company to identify the intellectual property as an asset to be protected.

Therefore, even with the condition described before, we were able to identify some certifications that partially meet the domain's requirements. From these certifications, the suitable one will depend on the assurance level required and if it is necessary to evaluate the device in place or if the application domain context is enough. Despite that, we only have two options for a high assurance level, the DSPSMA or the CAP.

Utility domain

The utility domain requires high assurance certifications because it is a preferred target for attackers. Beyond that, certifications for this domain need to ensure the existence of fault tolerance.

	High assurance level	**Ensure fault tolerance**	**Ensure resilience**
DSPSMA	Yes	Yes	No
ARMOUR	No	No	No
ICSAlabs	No	No	No
CAP	Yes	Yes	No
BSI Kitemark	Yes	No	No
IoTAA	No	Yes	No
e-IoT-SCS	No	No	No
ioXt	No	No	No

Table 7: Analysis of the requirement fulfillment for utility domain

Despite presenting some limitations, two certifications analyzed in Table 7 are suitable for this domain - DSPSMA and CAP.

DSPSMA is the certification that evaluates a system applied to a specific domain, so it is a high assurance certification. Moreover, during the audit phase, as this certification uses the ISO 27001 standard, it ensures that the system is fault-tolerant, an essential feature for critical environments [98]. Besides, this certification can support the system's owner by monitoring their assets.

CAP certification is also a high assurance evaluation. However, this certification evaluates the device or system against application domain risks and not specifically the deployment environment, limiting the risk analysis's effectiveness due to unknown risks.

Nevertheless, they both mention fault tolerance but they do not specify any measure to appraise resilience or self-repair capabilities. Despite being the only one that develop this feature, IoTAA can not be used for this application as it does not provide a high assurance evaluation.

Mobile domain

The mobility domain imposes that certifications need to be adapted to dynamic environments.

We did not find any certification created to evaluate a dynamic environment. As we stated in subsection 4.2.4, the best option for this domain is to use a composition of different certifications.

7.3. Overall IoT requirement fulfillment

The certifications analyzed implement most of the general requirements that we proposed. However, when we analyzed the existent certifications regarding the requirements established by each application domain, we noticed that there are some cases that do not have a certification that meets all of their needs.

Thus, to answer **RQ3**, IoT certifications meet most of the general IoT requirements but do not meet the specific application domain requirements.

Current limitations of IoT certifications are discussed in more detail in Section 8.

7.4. ECSCF and existent certifications

Only two of the reviewed certifications are compliant with the ECSCF, the ARMOUR certification, and e-IoT-SCS.

Naturally, certifications that do not target the European market will not be interested in implementing the ECSCF. Despite that, four certifications target the European market, and only two are compliant.

e-IoT-SCS is the most recent certification and is compliant with the ECSCF. ARMOUR certification was being developed when ECSCF was published and implemented the ECSCF. DSPSMA is not compliant with the ECSCF because it was released before the ECSCF. BSI Kitemark is the only certification released after the ECSCF that is not compliant. However, this certification was launched just six months after the release of ECSCF, so probably this is why it does not follow their recommendations.

This section has the answer to **RQ4**. We can see that new certifications are trying to be compliant with ECSCF. DSPSMA and BSI Kitemark are not compliant with ECSCF, probably because they were released around the same time as ECSCF, and, to be compliant, they would need to be redesigned.

8. Future research directions for certifications

Throughout this research, we analyzed the existing certifications and identified some areas that are not sufficiently developed to meet the requirements imposed by IoT. Therefore, there are still open research opportunities in this field.

Security certifications that assess risks regarding user privacy are increasingly common. However, half of the certifications assessed here consider only the privacy of the subject when legally required and not as a general rule. Therefore, certifications must encourage privacy by design on their subjects, regardless of the regulatory context. Another area that needs to be developed in this field is automating PIAs so that this type of evaluation is more easily integrated with automatic assessments.

Currently, there is a notable lack of attention to IoT systems that have a dynamic context in security certifications. Most of the certifications evaluate only the devices and not the entire system. Therefore, there is a need for a new certification that focuses better on IoT systems with a specific context to assess the IoT dynamic context. Even existent certifications that evaluate systems do not consider the dynamic context. There is already technology that can be used to shorten this gap. For instance, a certification can use conflict detection to analyze how safely we can connect devices from different vendors by detecting possible race conditions and deadlocks. There is already research that applies conflict detection to IoT. In addition to detecting this type of security problem, they can also prevent it through policies [99, 100]. Thus, it is necessary to start importing this feature to IoT certifications to improve the way heterogeneous systems are evaluated.

Another missing point is that most security certifications evaluate devices based only on security checklists and vulnerability scans, sufficient to know if a specific measure is implemented. However, this procedure fails to check for unknown software vulnerabilities, making it imperative to find a way to test for unknown threats without compromising the certification duration.

We can also detect a trend that certifications are aimed at manufacturers and not entirely at users. The certifications we analyzed (except DSPSMA) see the user as a pure consumer of the final report and not as the certification process's initiator. Most certifications are requested by the manufacturer, probably due to the costs involved. DSPSMA is user-focused but too heavy for small environments. There is still no light certification for small system owners who need assurance that their IoT system is secure.

In terms of academic research, multiple researchers point out the need for mechanisms that enable the self-repair of devices when they have malfunctioned or have been compromised [56]. The appearance of trusted platform modules in regular processors, such as ARM TrustZone [101] or Intel SGX [102], allowed the creation of new systems that can be resilient even in adverse situations. These systems can recover and minimize the amount of information exposed when they are compromised [103, 104, 105]. Thus, the technology has already developed capabilities, and the need for these systems exists. Regardless, no certifi-

cations are promoting the use of these technologies.

9. Conclusion

The evolution of IoT technology and connected devices can significantly improve business and automation, both personally and professionally. However, all systems connected to the Internet can be vulnerable to cyber-attacks. Buyers are buying more of these devices, but trust is still a problem between them and the manufacturers. Often, it is not transparent for the customers what is being done with the device's data and security. Also, manufacturers need to have standard security measures for all devices. For this, it is necessary at least that there is a guarantee that the devices comply with security requirements. Standards provide a common set of reference points to enable users to evaluate whether a device or system has processes, procedures, and other controls in place that meet a minimum of security requirements. The production of these devices needs to follow standards to produce compliant machines. With certifications, customers can guarantee that a company follows the security recommendations.

This paper focus on IoT certifications and their adequacy to the requirements imposed by an IoT environment. As the focus is the IoT, we present and suggest different requirements imposed by IoT on certifications, mainly general and specific requirements for each IoT application domain that we evaluate. With this, we answer both **RQ1** and **RQ2**.

We understood that security certifications are not separated from the requirements imposed by the IoT environment, and emerging certifications aimed at the European market are following European regulations. However, some IoT requirements have not yet been implemented by all certifications, which is the answer to **RQ3**.

By answering **RQ4**, we conclude that, although the BSI Kitemark and DSPSMA are not ECSCF compliant, newer certifications are trying to comply with the ECSCF. We consider that both certifications are not yet compliant because they were released simultaneously as the ECSCF. Now, to be compatible, they would need to be redesigned.

Finally, we also identify some fields in this area that have not yet been developed enough and require further research from the academic community. There is a lack of certifications analyzing IoT systems. The existing ones do not focus on the IoT dynamic context or only evaluate the device according to a generic context. Beyond that, some technologies, available in other fields, are not yet being used by the current certifications, as well as improve the IoT requirements qualification.

Acknowledgment

The work of André Cirne was supported by Fundação para a Ciência e Tecnologia (FCT), Portugal - 2021.08587.BD. The work of Patrícia R. Sousa was supported by the Project "City Catalyst – Catalisador para cidades sustentáveis", ref. POCI-01-0247-FEDER-046112, financed by Fundo Europeu de Desenvolvimento Regional (FEDER),through COMPETE 2020 and Portugal 2020. The work of João S. Resende was supported by the EU H2020-SU-ICT-03-2018 Project No. 830929 CyberSec4Europe (cybersec4europe.eu).

References

[1] R. Minerva, A. Biru, D. Rotondi, Towards a definition of the internet of things (iot), IEEE Internet Initiative 1 (2015) 1–86.

[2] O. Logvinov, B. Kraemer, C. Adams, J. Heiles, G. Stuebing, M. Nielsen, B. Mancuso, Standard for an architectural framework for the internet of things (iot) ieee p2413 (2016).

[3] J. Voas, Networks of 'things', NIST Special Publication 800 (183) (2016) 800–183.

[4] T. ETSI, 102 689 v1. 1.1,", Machine-to-Machine communications (M2M) (2010) 1–34.

[5] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (iot): A vision, architectural elements, and future directions, Future generation computer systems 29 (7) (2013) 1645–1660.

[6] S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim, S. R. Chaudhry, Iot architecture challenges and issues: Lack of standardization, in: 2016 Future Technologies Conference (FTC), IEEE, 2016, pp. 731–738.

[7] M. Nawir, A. Amir, N. Yaakob, O. B. Lynn, Internet of things (iot): Taxonomy of security attacks, in: 2016 3rd International Conference on Electronic Design (ICED), IEEE, 2016, pp. 321–326.

[8] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Computer networks 54 (15) (2010) 2787–2805.

[9] S. S. I. Samuel, A review of connectivity challenges in iot-smart home, in: 2016 3rd MEC International conference on big data and smart city (ICBDSC), IEEE, 2016, pp. 1–4.

[10] S. Deshmukh, S. Sonavane, Security protocols for internet of things: A survey, in: 2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2), IEEE, 2017, pp. 71–74.

[11] J. R. Nurse, S. Creese, D. De Roure, Security risk assessment in internet of things systems, IT Professional 19 (5) (2017) 20–26.

[12] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, S. Shieh, Iot security: ongoing challenges and research opportunities, in: 2014 IEEE 7th international conference on service-oriented computing and applications, IEEE, 2014, pp. 230–234.

[13] J. Hernández-Ramos, J. Martinez, V. Savarino, M. Angelini, V. Napolitano, A. Skarmeta, G. Baldini, Security and privacy in internet of things-enabled smart cities: Challenges and future directions, IEEE Security and Privacy Magazine PP. doi:10.1109/MSEC.2020.3012353.

[14] C. W. Axelrod, Enforcing security, safety and privacy for the internet of things, in: 2015 Long Island Systems, Applications and Technology, IEEE, 2015, pp. 1–6.

[15] J. Voas, P. A. Laplante, Iot's certification quagmire, Computer 51 (4) (2018) 86–89.

[16] European cyber security certification - a meta-scheme approach v1.0 (Dec 2017).
URL https://www.ecs-org.eu/documents/publications/5a3112ec2c891.pdf

[17] Legroju, The eu cybersecurity act (Jun 2019).
URL https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

[18] S.-R. Oh, Y.-G. Kim, Security requirements analysis for the iot, in: 2017 International Conference on Platform Technology and Service (PlatCon), IEEE, 2017, pp. 1–6.

[19] H. Badran, Iot security and consumer trust, in: Proceedings of the 20th Annual International Conference on Digital Government Research, dg.o 2019, ACM, New York, NY, USA, 2019, pp. 133–140. doi:10.1145/3325112.3325234.
URL http://doi.acm.org/10.1145/3325112.3325234

[20] ISO/IEC, Iso/iec 15408-1: Information technology — security techniques — evaluation criteria for it security, Tech. rep. (Dec 2009).

[21] S. N. Matheu-García, J. L. Hernández-Ramos, A. F. Skarmeta, G. Baldini, Risk-based automated assessment and testing for the cybersecurity certification and labelling of iot devices, Computer Standards & Interfaces 62 (2019) 64–83.

[22] D. Privitera, L. Li, Can iot devices be trusted? an exploratory study.

[23] D. A. Privitera, L. Li, Are certified iot devices trustworthy? a preliminary investigation.

[24] S. N. Matheu, J. L. Hernández-Ramos, A. F. Skarmeta, G. Baldini, A survey of cybersecurity certification for the internet of things, ACM

Computing Surveys (CSUR) 53 (6) (2020) 1–36.

[25] R. S. Ross, S. W. Katzke, L. A. Johnson, Minimum security requirements for federal information and information systems, Tech. rep. (2006).

[26] S. Górniak, R. Atoui, J. Fernandez, J.-P. Quemard, M. Schaffer, Standardisation in support of the cybersecurity certification, https://bit.ly/3jjwfr5, accessed: 2020-06-16 (Dec 2019).

[27] R. Atoui, Iot device certification scheme (jun 2019).
URL https://www.eurosmart.com/wp-content/uploads/2019/06/e-IoT-SCS-Eurosmart_IoT_Device_Certification_v1.0_RELEASE.pdf

[28] E. C. S. Organisation, Overview of existing cybersecurity standards and certification schemesv2, Tech. rep., https://www.ecs-org.eu/documents/uploads/updated-sota.pdf (Dec 2017).

[29] I. Barreira, H. Dettmer, M. Masi, L. O. Echevarria, A. Sfakianakis, Standards supporting certification, accessed: 2020-06-13 (Dec 2019).
URL https://bit.ly/3b1Rf2G

[30] Council of European Union, Regulation (eu) 2019/881 of the european parliament and of the council of 17 april 2019 (2019).

[31] P. P. Ray, A survey on internet of things architectures, Journal of King Saud University-Computer and Information Sciences 30 (3) (2018) 291–319.

[32] K. Scarfone, M. Souppaya, A. Cody, A. Orebaugh, Technical guide to information security testing and assessment, NIST Special Publication 800 (115) (2008) 2–25.

[33] G. Purdy, Iso 31000: 2009—setting a new standard for risk management, Risk Analysis: An International Journal 30 (6) (2010) 881–886.

[34] A. Jacobsson, M. Boldt, B. Carlsson, A risk analysis of a smart home automation system, Future Generation Computer Systems 56 (2016) 719–733.

[35] Y. Klochkov, S. Odinokov, E. Klochkova, M. Ostapenko, A. Volgina, Development of certification model, in: 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), IEEE, 2016, pp. 120–122.

[36] C.-K. Chen, Z.-K. Zhang, S.-H. Lee, S. Shieh, Penetration testing in the iot age, Computer 51 (4) (2018) 82–85.

[37] M. A. Howard, A process for performing security code reviews, IEEE Security & privacy 4 (4) (2006) 74–79.

[38] J. Li, B. Zhao, C. Zhang, Fuzzing: a survey, Cybersecurity 1 (1) (2018) 1–13.

[39] O. Memo, M-03-22, OMB Guidance for Implementing the Privacy Provisions of.

[40] E. C. S. Organisation, European cyber security certification, Tech. rep. (Dec 2017).
URL https://www.ecs-org.eu/documents/publications/5a3112ec2c891.pdf

[41] H. Lin, N. Bergmann, Iot privacy and security challenges for smart home environments, Information 7 (3) (2016) 44.

[42] A. Jacobsson, P. Davidsson, Towards a model of privacy and security for smart homes, in: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), IEEE, 2015, pp. 727–732.

[43] P. Gope, T. Hwang, Bsn-care: A secure iot-based modern healthcare system using body sensor network, IEEE Sensors Journal 16 (5) (2015) 1368–1376.

[44] C. Lévy-Bencheton, E. Darra, G. Tétu, G. Dufay, M. Alattar, Security and resilience of smart home environments: Good practices and recommendations, Publications Office of the European Union, 2015.

[45] A. Act, Health insurance portability and accountability act of 1996, Public law 104 (1996) 191.

[46] S. T. U. Shah, H. Yar, I. Khan, M. Ikram, H. Khan, Internet of things-based healthcare: Recent advances and challenges, in: Applications of Intelligent Technologies in Healthcare, Springer, 2019, pp. 153–162.

[47] A. Khan, K. Turowski, A survey of current challenges in manufacturing industry and preparation for industry 4.0, in: Proceedings of the First International Scientific Conference "Intelligent Information Technologies for Industry"(IITI'16), Springer, 2016, pp. 15–26.

[48] A. Malatras, C. Skouloudi, A. Koukounas, Industry 4.0 cybersecurity: Challenges & recommendations, European Union Agency for Cybersecurity 20.

[49] G. Falco, C. Caldera, H. Shrobe, Iiot cybersecurity risk modeling for scada systems, IEEE Internet of Things Journal 5 (6) (2018) 4486–4495.

[50] H. Flatt, S. Schriegel, J. Jasperneite, H. Trsek, H. Adamczyk, Analysis of the cyber-security of industry 4.0 technologies based on rami 4.0 and identification of requirements, in: 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), IEEE, 2016, pp. 1–4.

[51] B. Leander, A. Čaušević, H. Hansson, Applicability of the iec 62443 standard in industry 4.0/iiot, in: Proceedings of the 14th International Conference on Availability, Reliability and Security, 2019, pp. 1–8.

[52] K. Stouffer, J. Falco, K. Scarfone, Guide to industrial control systems (ics) security, NIST special publication 800 (82) (2011) 16–16.

[53] M. M. Alani, M. Alloghani, Security challenges in the industry 4.0 era, in: Industry 4.0 and engineering for a sustainable future, Springer, 2019, pp. 117–136.

[54] S. J. Shackelford, M. Sulmeyer, A. N. C. Deckard, B. Buchanan, B. Micic, From russia with love: Understanding the russian cyber threat to us critical infrastructure and what to do about it, Neb. L. Rev. 96 (2017) 320.

[55] A. Bartoli, J. Hernández-Serrano, M. Soriano, M. Dohler, A. Kountouris, D. Barthel, Security and privacy in your smart city, in: Proceedings of the Barcelona smart cities congress, Vol. 292, 2011, pp. 1–6.

[56] E. ENISA, Baseline security recommendations for iot in the context of critical information infrastructures (2017).

[57] D. Pliatsios, P. Sarigiannidis, T. Lagkas, A. G. Sarigiannidis, A survey on scada systems: secure protocols, incidents, threats and tactics, IEEE Communications Surveys & Tutorials 22 (3) (2020) 1942–1976.

[58] M. A. Elsadig, Y. A. Fadlalla, Vanets security issues and challenges: A survey, Indian Journal of Science and Technology 9 (28) (2016) 1–8.

[59] J. Cui, L. S. Liew, G. Sabaliauskaite, F. Zhou, A review on safety failures, security attacks, and available countermeasures for autonomous vehicles, Ad Hoc Networks 90 (2019) 101823.

[60] A. Chattopadhyay, K.-Y. Lam, Security of autonomous vehicle as a cyber-physical system, in: 2017 7th International Symposium on Embedded Computing and System Design (ISED), IEEE, 2017, pp. 1–6.

[61] P. Koopman, M. Wagner, Autonomous vehicle safety: An interdisciplinary challenge, IEEE Intelligent Transportation Systems Magazine 9 (1) (2017) 90–96.

[62] E. ENISA, Enisa good practices for security of smart cars (2019).

[63] E. C. S. Organisation, European cyber security certification - product certification composition, Tech. rep., https://www.ecs-org.eu/documents/

publications/5a3112ec2c891.pdf (Dec 2017).

[64] A. Q. Rodriguez, B. B. AS, M. Menon, S. Ziegler, A. M. P. H. AS, E. K. DG, S. Bianchi, Dynamic security and privacy seal model analysis.

[65] S. N. Matheu, J. L. Hernandez-Ramos, A. F. Skarmeta, Toward a cybersecurity certification framework for the internet of things, IEEE Security & Privacy 17 (3) (2019) 66–76.

[66] I. Labs, Internet of things (iot) security testing framework, Tech. rep., ICSA Labs (Octo 2016).
URL https://www.icsalabs.com/sites/default/files/body_images/ICSALABS_IoT_reqts_framework_v2.0_161026.pdf

[67] News: Announcing ul 2900 outlines, https://ulstandards.ul.com/downloads/news-announcing-ul-2900-outlines/, acessed: 27 November 2019.

[68] Testing and certification for iot connected devices, accessed: 2020-05-16.
URL https://www.bsigroup.com/en-GB/industries-and-sectors/Internet-of-Things/IoT-Assurance-Services/

[69] Internet of things alliance australia (iotaa), accessed: 2019-11-5 (2016).
URL https://www.iot.org.au/

[70] EUROSMART, Eurosmart iot certification scheme: Eurosmart: The voice of the digital security industry, https://www.eurosmart.com/eurosmart-iot-certification-scheme/, accessed: 2020-05-10.

[71] The global standard for iot security, accessed: 2022-01-06.
URL https://www.ioxtalliance.org/

[72] ETSI EG 203 251, Methods for Testing & Specification Risk-based Security Assessment and Testing Methodologies v1.1.1, 2016.

[73] Iot security & privacy, https://www.icsalabs.com/technology-program/iot-testing, accessed: 2020-06-10 (Nov 2015).

[74] UL, Standards supporting certification, accessed: 2021-03-07.
URL https://www.ul.com/resources/ul-cybersecurity-assurance-program-ul-cap

[75] U. Laboratories, About: Underwriters laboratories, https://ul.org/about, accessed: 2020-05-03.

[76] Food and drug administration modernization act of 1997: Modifications to the list of recognized standards, recognition list number: 049, https://bit.ly/3lq4YVz, accessed: 2020-06-23 (Jun 2018).

[77] J. Heyl, Overview of ul 2900, accessed: 2019-11-16 (Octo 2017).
URL https://cybersecuritysummit.org/wp-content/uploads/2017/10/4.00-Justin-Heyl.pdf

[78] J. Porup, Standards supporting certification, accessed: 2021-03-07 (Apr 2016).
URL https://bit.ly/3fkGOLO

[79] Cyber Security for Consumer Internet of Things, 2019.
URL https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

[80] W. . Security, N. R. of the IoTAA, Internet of things security guideline v1.2 (nov 2017).

[81] K. McKay, D. Cooper, Guidelines for the selection, configuration, and use of transport layer security (tls) implementations, Tech. rep., National Institute of Standards and Technology (2017).

[82] EUSOSMART, [tr-e-iot-scs-part-1] process & policy v1.2, Tech. rep., EUSOSMART (oct 2019).

[83] EUSOSMART, [tr-e-iot-scs-part-3] evaluation methodology v1.2, Tech. rep., EUSOSMART (oct 2019).

[84] EUSOSMART, [e-iot-scs-part-2] gpp v1.2, Tech. rep., EUSOSMART (oct 2019).

[85] ioXt, ioxt pledge, Tech. rep., ioXt Alliance, accessed: 2022-01-06 (2020).
URL https://static1.squarespace.com/static/5c6dbac1f8135a29c7fbb621/t/5fb43a05bda7c3689ea5bd32/1605646853608/ioXtPledgeBook_Secure.pdf

[86] ioxt 2020 base profile, accessed: 2022-01-06.
URL https://static1.squarespace.com/static/5c6dbac1f8135a29c7fbb621/t/5ede6a88e6a927219ee86bb2/1591634577949/ioXt_2020_Base_Profile_1.00_C-03-29-01.pdf

[87] Pixel 4/4xl and pixel 4a ioxt audit, accessed: 2022-01-06.
URL https://research.nccgroup.com/wp-content/uploads/2020/08/NCC_Group_Google_GOOG065C_Report_2020-08-13_v2.0.pdf

[88] Challenges and practical approaches to consumer software labeling, accessed: 2022-01-06.
URL https://www.nist.gov/system/files/documents/2021/09/03/IoXT-Challenges%20and%20Practical%20Approaches%20to%20Consumer%20Software%20Labeling.pdf

[89] ioxt 2020 mobile application profile, accessed: 2022-01-06.
URL https://static1.squarespace.com/static/5c6dbac1f8135a29c7fbb621/t/604aa3fa668a8e3b50630433/1615504379349/Mobile_Application_Profile.pdf

[90] ioxt researcher rewards version 2.1, accessed: 2022-01-06.
URL https://static1.squarespace.com/static/5c6dbac1f8135a29c7fbb621/t/608098330e7180252fe0f685/1619040308593/researcher-rewards.pdf

[91] J. N. Goel, B. Mehtre, Vulnerability assessment & penetration testing as a cyber defence technology, Procedia Computer Science 57 (2015) 710–715.

[92] K. Xynos, I. Sutherland, H. Read, E. Everitt, A. J. Blyth, Penetration testing and vulnerability assessments: A professional approach.

[93] S. P. Kaluvuri, M. Bezzi, Y. Roudier, A quantitative analysis of common criteria certification practice, in: International Conference on Trust, Privacy and Security in Digital Business, Springer, 2014, pp. 132–143.

[94] J. Zibuschka, Analysis of automation potentials in privacy impact assessment processes, in: Computer Security, Springer, 2019, pp. 279–286.

[95] A. Wirth, S. L. Grimes, Medical device cybersecurity—at the convergence of ce and it, in: Clinical Engineering Handbook, Elsevier, 2020, pp. 253–258.

[96] The bsi kitemark for the internet of things, https://www.bsigroup.com/globalassets/localfiles/en-ae/iot/km-iot-factsheet-web.pdf, accessed: 2020-05-16.

[97] I. I. Consortium, Industrial internet of things: Volume g4 security framework, Tech. rep. (2016).

[98] Information technology – Security techniques – Information security management systems – Requirements, Standard, International Organization for Standardization, Geneva, CH (Mar. 2013).

[99] R. Liu, Z. Wang, L. Garcia, M. Srivastava, Remediot: Remedial actions for internet-of-things conflicts, in: Proceedings of the 6th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation, 2019, pp. 101–110.

[100] Z. B. Celik, G. Tan, P. D. McDaniel, Iotguard: Dynamic enforcement of security and safety policy in commodity iot., in: NDSS, 2019.

[101] S. Pinto, N. Santos, Demystifying arm trustzone: A comprehensive survey, ACM Computing Surveys (CSUR) 51 (6) (2019) 1–36.

[102] V. Costan, S. Devadas, Intel sgx explained., IACR Cryptol. ePrint Arch. 2016 (86) (2016) 1–118.

[103] R. Liu, M. Srivastava, Virtsense: Virtualize sensing through arm trustzone on internet-of-things, in: Proceedings of the 3rd Workshop on System Software for Trusted Execution, 2018, pp. 2–7.

[104] A. Dave, N. Banerjee, C. Patel, Care: Lightweight attack resilient secure boot architecturewith onboard recovery for risc-v based soc, arXiv preprint arXiv:2101.06300.

[105] G. Amit, A. Shabtai, Y. Elovici, A self-healing mechanism for internet of things devices, IEEE Security & Privacy.