# Current challenges in certification schemes for consumer IoT security

Bachelor Thesis

by

Felix Körner


Potsdam University
Institute for Computer Science
Operating Systems and Distributed Systems

Supervisor(s):
Prof. Dr. Bettina Schnor
Dr. Samim Ahmadi

Potsdam, November 20, 2022

**Körner, Felix**
felix.koerner@uni-potsdam.de
Current challenges in certification schemes for consumer IoT security
Bachelor Thesis, Institute for Computer Science
Potsdam University, November 2022

# Selbständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig angefertigt, nicht anderweitig zu Prüfungszwecken vorgelegt und keine anderen als die angegebenen Hilfsmittel verwendet habe. Sämtliche wissentlich verwendeten Textausschnitte, Zitate oder Inhalte anderer Verfasser wurden ausdrücklich als solche gekennzeichnet.

Potsdam, November 20, 2022

_____

Felix Körner

**Abstract**

In contrast to computers according to their classical definition, the cybersecurity of consumer IoT devices is often forgotten. Consumer IoT devices are primarily used by people who have limited understanding of cybersecurity. For this reason, it is incumbent upon the manufacturer to set up their consumer IoT device securely. Implementing such measures is costly and often not done voluntarily by manufacturers. However, manufacturers are preparing for upcoming cybersecurity regulations and are interested in providing the consumer certainty that their consumer IoT are secure. For such reasons, manufacturers send their devices to certification bodies, where the consumer IoT devices get certified.
This thesis provides an overview of the current challenges in certifying consumer IoT devices. The ETSI EN 303 645 provided baseline security provisions to ensure product security for consumer IoT devices. Together with its accompanying assessment specification document ETSI TS 103 701 it provides a foundation of such a consumer IoT security certification. This thesis evaluates two different consumer IoT devices based on the ETSI EN 303 645 and TS 103 701. Furthermore, interviews were conducted with certification bodies that provide consumer IoT security certification. The two consumer IoT devices tested in this thesis failed the assessment after the ETSI TS 103 701. Consumer IoT certification is still in its infancy and needs to mature. However, the standard ETSI EN 303 645 is a good start.

Deutsche Zusammenfassung:
Im Gegensatz zu Computern gemäß ihrer klassischen Definition wird die Cybersicherheit von Consumer-IoT-Geräten oft vergessen. Consumer-IoT-Geräte werden in erster Linie von Menschen genutzt, die nur ein begrenztes Verständnis von Cybersicherheit haben. Aus diesem Grund obliegt es dem Hersteller, sein Consumer-IoT-Gerät sicher einzurichten. Die Umsetzung solcher Maßnahmen ist kostspielig und wird von den Herstellern oft nicht freiwillig durchgeführt. Die Hersteller bereiten sich jedoch auf bevorstehende Cybersicherheitsvorschriften vor und sind daran interessiert, den Verbrauchern die Gewissheit zu geben, dass ihre IoT-Geräte sicher sind. Aus diesem Grund senden die Hersteller ihre Geräte an Zertifizierungsstellen, die die Consumer-IoT-Geräte zertifizieren lassen.
Diese Arbeit gibt einen Überblick über die aktuellen Herausforderungen bei der Zertifizierung von Consumer-IoT-Geräten. Die ETSI EN 303 645 bietet grundlegende Sicherheitsvorschriften, um die Produktsicherheit für Consumer-IoT-Geräte zu gewährleisten. Zusammen mit der zugehörigen Testspezifikation ETSI TS 103 701 bietet sie eine Grundlage für eine solche Sicherheitszertifizierung. In dieser Arbeit werden zwei verschiedene Consumer-IoT-Geräte auf Basis der ETSI EN 303 645 und TS 103 701 evaluiert. Außerdem wurden Interviews mit Zertifizierungsstellen geführt, die Sicherheitszertifizierungen anbieten. Die beiden Consumer-IoT-Geräte, die in dieser Arbeit getestet wurden, haben die Bewertung nach ETSI TS 103 701 nicht bestanden. Die IoT-Zertifizierung für Verbraucher steckt noch in den Kinderschuhen und muss noch reifen. Die Norm ETSI EN 303 645 ist jedoch ein guter Anfang.

# Contents

# 1 Introduction

In recent years, the number of Internet of Things (IoT) devices has grown rapidly. In 2017, Gartner predicted that 20 billion devices will be connected to the Internet by 2020 [Gar17]. These devices are used in many places, such as in smart home or Industry 4.0 environments. Nowadays, heating thermostats, door locks, light switches, lamps and climate sensors are connected to the internet. This internet connection helps sensors to work in an interoperable environment to communicate with each other. However, interoperability as well as the connection, e.g. in meshed networks, leads to a large attack surface resulting in many cyber threats. For example, a popular cyber attack is based on the Mirai botnet. The Mirai botnet was used in 2016 to carry out a Distributed Denial of Service (DDoS) attack [Clo22]. At the time of the attack the security of many IoT devices was weak due to the use of default credentials. This could have been easily prevented by using secure passwords.

One reason for the lack of security is the general absence of regulations for IoT devices. Currently, only the safety of IoT devices is regulated (see e.g. RoHS, EMC, LVD). This situation applies specifically to Consumer IoT (CIoT) devices. CIoT devices are often devices with low processing power, such as sensors, which can be connected to the internet (either directly or indirectly). CIoT devices are mostly used by people who have limited understanding and awareness of cybersecurity. They lack the knowledge to identify whether an IoT device is secure and therefore do not take corresponding measures to use the device in a secure way, e.g. by not using default passwords. If manufacturers would have to develop devices securely, consumers do not have to worry much about security. Regulations are necessary to achieve this. In Europe, these regulations come from the European Union (EU).
The EU is working on solutions to protect the cybersecurity of CIoT devices by developing regulations such as the delegated regulation to activate the cybersecurity-related articles of the radio equipment directive [Com21].

One standard from the European standards organization European Telecommunications Standard Institute (ETSI) is ETSI EN 303 645 [ETSa]. The ETSI EN 303 645 [ETSa] has a corresponding assessment specification, namely the ETSI TS 103 701 [ETSb]. This technical specification was used in this work to evaluate two CIoT devices. These standards, in turn, form the basis for cybersecurity labels for CIoT devices and are used by certification bodies. With labels, it is possible to aide consumers to choose more secure CIoT devices. But all of this is still in its infancy and as of today there are no well established standards. This thesis will highlight the current challenges of cybersecurity certification for CIoT devices. It will also answer the question if the ETSI EN 303 645 [ETSa] can help achieve better security.

This thesis is divided into four chapters. The second chapter provides all the knowledge needed to understand the following chapters. The definition for IoT devices in standardization is presented

and the difference between Industrial IoT (IIoT) and CIoT is explained. To put the type of assessment in context, different classes of penetration tests are presented in section 2.2. One of the CIoT devices tested uses Zigbee, which is also explained. Afterwards the current situation of certification is highlighted and an overview of the current certification labels is given. In addition, the certification process for a CIoT device is explained in general. In preparation for the evaluation of the two CIoT devices, the used standard ETSI EN 303 645 [ETSa] is summarized. At the time of writing, there is no comparable standard to ETSI EN 303 645 [ETSa]. For this reason, ETSI EN 303 645 [ETSa] is compared to the German Bundesamt für Sicherheit in der Informationstechnik (BSI) requirements for CIoT devices.
The third chapter describes the tools to evaluate the two CIoT devices.
In fourth chapter, the actual evaluation of the two devices is performed. Due to this thesis's nature, three interviews were conducted to give the reader the perspective of a test lab. After evaluating the two CIoT devices against the ETSI TS 103 701 [ETSb], weaknesses in the standards were identified. These weaknesses are summarized. The chapter ends with a section on the current challenges of CIoT security certification.
The concluding chapter summarizes all the findings on the topic of this thesis. In addition, the question about the importance of the ETSI EN 303 645 [ETSa] is answered. Finally, an outlook on the future of CIoT certification is given.

# 2 Theoretical foundations

## 2.1 Definition Internet of Things

Before Internet of Things (IoT) can be talked about, the term must be defined. The International Telecommunication Union (ITU) divides the aspects of how the internet can be accessed in three dimensions. The first dimension is the time. At any time it is possible to access the internet. The second dimension is place. From any location on the earth you can reach the internet in theory. In practice, it is not feasible to provide enough satellites, but it would be possible to connect every place on the earth. The new revolution of IoT came with the third dimension, which is a thing. IoT means that the internet will not only consist of humans but also of things which can communicate with each other. For example, a rain sensor can communicate with the electrical motor control unit of a window, which needs to be closed if it rains. This example shows an important concept of IoT, which is called Machine to Machine (M2M) communication. This means that no human is involved in the information exchange between two machines.
As the name implies each IoT device needs to be connected to the internet. This can be found in the definition for IoT devices from the Institute of Electrical and Electronics Engineers (IEEE): "A network of items-each embedded with sensors-which are connected to the Internet." (IEEE: Report, Internet of Things, March 2014). The connection to the internet can be also achieved by the usage of a gateway. For example, a non-IP based network (e.g. Zigbee) can be used to establish a link between a sensor and a gateway. The gateway is then connected to a router, which is then connected to the internet.
An IoT device needs to be part of a network. A device which is working as an isolated instance and does not have the capability to communicate with another device, will not be classified as an IoT device.
The last point an IoT device must comply, is the connection towards the real world. In most cases, that is a sensing capability or control of a motor.
IoT devices can be classified according to their use cases. There exist two different use cases Industrial IoT (IIoT) and Consumer IoT (CIoT). IIoT describes IoT devices which are used in industrial environments such as in production industry (e.g. label printer in a logistics center). An IIoT device must be reliable, because a malfunction can lead to the stagnation of the whole production. It is also important that an IIoT device can be integrated with existing systems. In addition, IIoT devices have to run for a long time without any downtime.
In contrast to that, there are CIoT devices. Their setup must be easy and manageable for a consumer whithout a computer science degree. The main goal of CIoT devices is to improve the life quality of their users and save them time. For example, with the help of a smart thermostat the user can save money by only heating up an area, when it is needed. The user only has to setup the rules for that once. After that the thermostat will follow these rules and no interaction from the user is needed. European Telecommunications Standard Institute (ETSI) defines CIoT as:
"[...] network-connected (and network-connectable) device that has relationships to associated

services and are used by the consumer typically in the home or as electronic wearables
NOTE 1: Consumer IoT devices are commonly also used in business contexts. These devices remain classified as consumer IoT devices.
NOTE 2: Consumer IoT devices are often available for the consumer to purchase in retail environments. Consumer IoT devices can also be commissioned and/or installed professionally." [ETSa].

## 2.2 Penetration testing methods

It is important to clearly classify the tests done in this thesis. Tests performed as part of this thesis incorporate elements of a penetration test. Because of this the following section explains the classes of penetration tests, which can be performed.
According to [Pos] penetration tests are classified on the basis of the knowledge and access granted to the tester at the start of the assessment. The class with no additional knowledge about the target system is called **black-box testing**. This class simulates a normal attacker, which has no inside information. This kind of testing only assesses the outside facing services. Inside services are not explicitly checked and vulnerabilities of them are therefor often missed.
The opposite of black-box testing is **white-box testing**. In this case the tester gets all information about the target system from the client. The tester has the challenge to find the relevant information for the target system. The tester can be given user accounts and accounts with elevated privileges. The tester might also have the opportunity to talk to a developer of the software used by the target system. The tester gets all the knowledge he needs to test the system's security from every position in the network. This means that also internal vulnerabilities can be found.
One big disadvantage of white-box testing is the huge amount of time which is needed for the assessment. The third method tries to combine the strengths of white-box and black-box testing and is called **gray-box testing**. The tester is presented with a selection of the information about the target system. This means the information is filtered by the client or not available. It implies that the client chooses the focus of the assessment. This type of testing is used to simulate an attacker who has long-term access to the system.
In this thesis, only black-box testing is performed, because it was impossible to cooperate with the Supplier Organization (SO) of each product. Black-box testing also simulates the position of an importer, who typically has no further knowledge of the Device Under Test (DUT). This gives the opportunity to check if an importer could certify an IoT device without the help of the SO.

## 2.3 Zigbee

Zigbee is a wireless network which operates like Wi-Fi on the 2.4 GHz band, but is based on the standard IEEE 802.15.4. Wi-Fi and Zigbee cannot be mixed. Zigbee is not based on IP addresses. Instead, it uses 16 bit network addresses, which are assigned by the coordinator.
There are three different device classes in a Zigbee network. The first class is the coordinator, which is used to create and manage the network. The coordinator also can route between different networks. Only one coordinator per Zigbee network can exist. The second device class are routers. They route packets in the Zigbee network. The third class are Zigbee end devices. They are not part of the routing and need to have a selection of the features only, which are specified in

the Zigbee standard.

The Zigbee protocol provides two security measures. To protect the integrity of the packets, the message integrity code (MIC) is used. The MIC can have three different lengths 4, 8 or 16 octets. The confidentiality of the packets is protected by encryption. On the contrary to the integrity protection the encryption has always the length of 128 bit and uses Advanced Encryption Standard (AES). The Zigbee protocol supports multiple security levels, which can be found in the Zigbee standard [za17]. The available levels are listed in table 2.1. Security level 0x00 does not use either security measures and should only be used in development. The levels 0x01 to 0x03 only offer integrity protection and no encryption. In contrast to that Security level 0x04 only offers encryption. Level 0x05 and greater offer encryption and integrity protection. The Zigbee standard sets the default security level to 0x05 (refer to Table 4-2 NIB Security Attributes).

| Security Level Identifier | Security Level Sub-Field | Security Attributes | Data Encryption | Frame Integrity (length M of MIC, in Number of Octets) |
|---|---|---|---|---|
| 0x00 | ’000’ | None | OFF | NO (M = 0) |
| 0x01 | ’001’ | MIC-32 | OFF | YES (M=4) |
| 0x02 | ’010’ | MIC-64 | OFF | YES (M=8) |
| 0x03 | ’011’ | MIC-128 | OFF | YES (M=16) |
| 0x04 | ’100’ | ENC | ON | NO (M=0) |
| 0x05 | ’101’ | ENC-MIC-32 | ON | YES (M=4) |
| 0x06 | ’110’ | ENC-MIC-64 | ON | YES (M=8) |
| 0x07 | ’111’ | ENC-MIC-128 | ON | YES (M-16) |

**Table 2.1:** Table 4-30 Security Levels Available to the NWK, and APS Layers [za17]

## 2.4 Certification schemes for consumer IoT security

This section is divided into two subsections. The first subsection gives an overview over the current available cybersecurity certification labels for CIoT devices. The second subsection analyses the process, which is needed for a certification of a CIoT device.

### 2.4.1 State-of-the-art certification schemes in consumer IoT security

This section gives an overview of the available certification labels for CIoT device security. Table 2.2 shows the certification labels, which could be discovered. This thesis is based in Germany. A leading German organization practicing IoT Cybersecurity certification is the Technischer Überwachungsverein (TÜV). It can be found in the first line of the table. The TÜV-Verband has developed the Cybersecurity Certified (CSC) label, which is based on the standard ETSI EN 303 645 [ETSa]. The CSC can be done in three depth levels. The first level is called "Basic". It does not include any provisions which are based on the ETSI EN 303 645 [ETSa]. It just uses an internal requirements catalog. The second level, called "Substantial" and requires all the mandatory provisions of the mentioned standard. The third level is called "High". It is also based on the standard

BSI TR-03173 [BSI22b], which is the application of the standard ETSI EN 303 645 [ETSa] from the Bundesamt für Sicherheit in der Informationstechnik (BSI). Interviews with "TÜV Nord" and "TÜV SÜD" can be found in section 4.1.
Another label is the “IoT Security Assured” of the IASME consortium. IASME has been a partner of the British government since 2020. This label is also based on the standard ETSI EN 303 645 [ETSa] and offers three levels. Unlike the CSC label, this label is mapped to the IoTSF Security Compliance Framework.
CTIA Certification develops standards in the mobile wireless industry. They offer a label after their own standards. Like the other labels, it provides three depth levels. The test plan from CTIA provides a mapping to the standard ETSI EN 303 645 [ETSa].
The organization PSA Certified provides the label "PSA Certified Level 1" which can be mapped to the mandatory provisions of the standard ETSI EN 303 645 [ETSa]. This shows that also non-European organizations recognize the standard ETSI EN 303 645 [ETSa] from ETSI.
The label IoT Security Trust Mark tries to comply with as many standards as possible.
Eurosmart is an association consisting of technical experts in digital security. The members include, among others, FIDO alliance and SOG-IS. Eurosmart certifies with the E-IoT-SCS, which offers 2 assurance levels. The certification focuses on the substantial security assurance level as defined by the Cybersecurity Act. Traficom is the Finnish transport and communications agency. The agency offers the Cybersecurity label. The label only has one assurance level. The BSI has developed the IT-Sicherheitskennzeichen, which is awarded among other things for CIoT security. The BSI has added its own standard TR-03173 to map not clearly stated provisions of the standard ETSI EN 303 645 [ETSa] to their own best practices. In contrast to the other labels, the IT-Sicherheitskennzeichen is only a plausibility check and not a certification. This was decided by the German legislator.
SGS is a worldwide active association with a great network of laboratories. The SGS offers the label IoT-Security Checked, which has 4 assurances levels.
GlobalPlatform is an association of global players like ARM or Samsung. They offer the Security Evaluation Standard for IoT Platforms (SESIP) label, which has 5 assurance levels.
The BSIGroup should not be confused with the German BSI. BSIGroup offers the label "bsi. Internet of Things Devices Kitemark". The label is available in 3 assurance levels.
The ioXt alliance wants to offer the next global standard for IoT security. The alliance offers the label ioXt.
The Cyber Security Agency of Singapore (CSA) has developed its own CIoT security label, which offers 4 assurance levels. Level 3 and 4 are compatible with the requirements of Traficom.
VDE is an association for electrical, electronic and information technologies. The head quarter is based in Germany. The association offers a label "Smart Home", which is available in 4 assurance levels.
Norges Elektriske Materiellkontroll (Nemko) was founded in Norway in 1933 for mandatory safety testing and national approval of electrical equipment. Nemko has the “Nemko cyber secure mark” label in its portfolio. The mark provides only one assurance level.
Bureau Veritas is a consumer and technology product testing, inspection or audit and certification body. They issue the label "BV IoT certification", which offers 5 assurance levels.

| Organization | ETSI EN 303 645 | ETSI TS 103 701 | NIST IR 8259 | IEC 60335-1 | California State Law SB-327 | BSI TR-03173 | Own Standard | number of levels | Certificate was Issued | Own Certificate | Sources |
|---|---|---|---|---|---|---|---|---|---|---|---|
| TÜV Süd | ✓ | | ✓ | ✓ | | ✓ | | 3 | ✓ | CyberSecurity Certified | Source |
| TÜV Nord | ✓ | | ✓ | ✓ | | ✓ | | 3 | | CyberSecurity Certified | Source |
| IASME Consortium | ✓ | | | | | | | 3 | ✓ | IoT Security Assured | Source |
| CTIA Certification | | | | | | | ✓ | 3 | ✓ | IoT Cybersecurity Certification | Source |
| ARM Holdings | ✓ | | ✓ | | ✓ | | | 3 | ✓ | psa certified | Source |
| IoT Security Trust Mark | ✓ | ✓ | ✓ | | | | | 1 | ✓ | IoT Trustmark Certified | Source |
| Eurosmart | ✓ | | | | | | | 2 | | E-IoT-SCS | Source |
| Traficom | ✓ | | | | | | | 1 | ✓ | Cybersecurity | Source |
| BSI | ✓ | ✓ | | | | ✓ | | 1 | | BSI IT-Sicherheitskennzeichen | Source |
| SGS | ✓ | | ✓ | | ✓ | | | 4 | | IoT-Security Checked | Source |
| BSIgroup | ✓ | | | | | | | 3 | ✓ | bsi. Internet of Things Devices Kitemark | Source |
| ioxtalliance | ✓ | | | | | | | 1 | ✓ | ioXt | Source |
| CSA Singapore | ✓ | | | | | | | 5 | ✓ | Cybersecurity | Source |
| VDE | ✓ | | | | | | | 4 | | VDE | Source |
| Nemko | ✓ | | | | | | | 1 | | | Source |
| Bureau Veritas | ✓ | | | | | | | 5 | | | Source |

**Table 2.2:** Overview of the available cybersecurity CIoT labels. (State 08/2022)

Many certification schemes are based on the standard ETSI EN 303 645 [ETSa]. This helps the standard to reach great adoption. But there are also alternatives on the market like the label from CTIA Certification. Most of the labels offer three assurance levels. Not all databases with certified products are publicly available. It was not possible to inquire from all certifications, whether they have already been issued. Another problem is that many of the certifications do not clearly state which standards they are based on. Due to the research presented in this section, it can be said that CIoT security certification systems are implemented differently depending on the owner.

### 2.4.2 Consumer IoT certification process

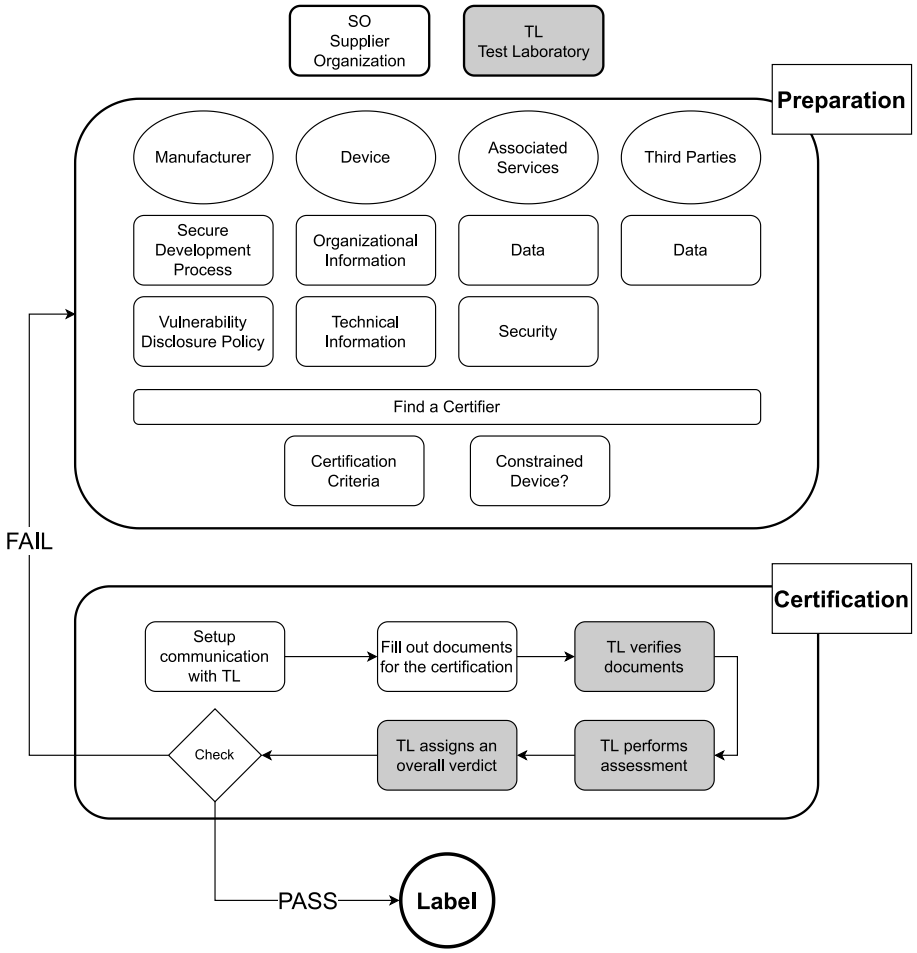


**Figure 2.1:** CIoT certification process

This section covers the certification process for a CIoT device. The certification process (see Figure 2.1) starts with the preparation of the certification by the Test Laboratory (TL). This step ensures that the certification can proceed as cost-effectively as possible. Four components have emerged in the preparation phase.
The first component is the manufacturer itself. It is only possible to develop a secure device if

there is a secure development process in place [Bai12]. This means not that over time a process has developed and is followed to the liking of the employees. It means that the manufacturer has implemented a standard, which builds the base for the development process of an CIoT device. The manufacturer also must set up a vulnerability disclosure policy [STA21]. In the case of a vulnerability, preset procedures need to be in place to fix security problems in an ordered and timely manner.
The second component is the device. It is important that the device is correctly documented [Fow99]. With the existence of good technical documentation, the certification process is much faster. It is recommended to write down organizational aspects. The SO has to select a person in the supplier organization, who will be the public contact for the certification.
The third component of the preparation are associated services. Many products rely on cloud services in the background. To achieve security best practices, communication with these services must be confidential at least. Some certifications also assess the associated services. It is advised to document, which data is sent to these services.
The last component is third parties. To increase revenue of the device, data is often shared with third parties [OPL+19]. It is recommended to document which data is given to whom for what purpose [Sha20].
After the baseline for the device is achieved. The supplier organization has to decide on a certification label. To give the greatest trust to the customer, this label should serve three points. It should be done by a third party, such that an independent assessment from the SO is proven. Second, the label should not only include a one-time assessment. There should be a reassessment every year. And last, the label should include an assessment of the associated services.
After the decision, the SO can check if there is the possibility to classify his device as constrained. In the standard ETSI EN 303 645 [ETSa] a constrained device is defined as a: “device which has physical limitations in either the ability to process data, the ability to communicate data, the ability to store data or the ability to interact with the user, due to restrictions that arise from its intended use”. If a device is constrained, it may have to meet fewer requirements. The SO also has to go through all the certification criteria and check if the device can pass them all. That concludes the preparation phase.

The first step in the certification phase is to set up communication with the TL. The contact person has to cover additional technical questions from the TL and can help to achieve an efficient certification.
After that, all documents required for the certification have to be filled out. At this point, if everything goes to plan, the work of the SO should end. The next three and last steps are performed by the TL, which is marked in Figure 2.1 with a gray background. Only these three steps are performed by the TL. All other steps are performed by the SO. The TL starts the certification by verifying the filled-out documents from the SO. Commonly, pieces of information are missing here. The SO should be prepared for inquiries. Now TL has all the information to start the assessment of the device. In the last steps, the TL assigns an overall verdict for the device. If the verdict is **FAIL** the preparation phase starts again. If the verdict is **PASS** the DUT gets assigned the label. This concludes the certification of the device.
After the certification, it might be interesting for the SO to speak with their marketing department about the certification. The trust of the customer in the DUT can be increased by publishing a selection of the certification documents.

## 2.5 European Standardization in consumer IoT security

**Figure 2.2:** CE label [Uni22]

In this section European standardization in CIoT cybersecurity will be introduced. In 2014 the Radio Equipment Directive (RED) was released by the European commission. The RED includes article 3.3 d-f. Article 3.3 d intends to protect the network there devices are installed. This means that newly installed devices need to be secure, to prevent an attacker from using the new device as an entry point for an attack. The above-mentioned articles will become active in 2024 by a delegated act passed by the European commission. As a result, Harmonized European Standards (HENs) are needed to apply RED article 3.3 d-f on a European scale. HENs are needed for self-certification. Only with self-certification, which is realized with declaration of conformity documents by the manufacturer themselves, a European wide adoption is possible. Every product placed on the European market must have a CE label Figure 2.2. If the product uses radio technology, it also must pass the RED. In conclusion, this means every product using radio technology must be secure. To define a secure product the standard TS 103 645 was created by the European standards organization (ESO) ETSI which was renamed to the standard ETSI EN 303 645 [ETSa] "Cyber Security for Consumer IoT: Baseline Requirements". ETSI consists of over 900 members from over 60 countries and 5 continents. ETSI supports the European regulations and legislation by contributing to HENs.

### 2.5.1 ETSI EN 303 645

ETSI EN 303 645 [ETSa] addresses cybersecurity of CIoT devices. It seeks to communicate best practices for the security of consumer devices connected to the Internet. It focuses on the development and manufacturing aspects by showing how to develop a product securely. The standard is organized into provisions that are outcome-based to provide organizations with the greatest flexibility in implementing security solutions. It provides only basic security and excludes attacks that are planned in detail or require physical access over a long time. The provisions are divided into three broad groups. The first group is called “Reporting implementation.” Its purpose is to verify that justification is provided for each provision that cannot be applied to the DUT. The next group, “Cybersecurity provisions for consumer IoT” is for verifying that the DUT is cyber secure. The final group, “Privacy Provisions for consumer IoT” provides good preparation for compliance with the General Data Protection Regulation (GDPR).
The standard includes a pro forma document that can be used to explain which provisions are supported by the DUT. This document is the Implementation conformance statement (ICS). The document is structured in tabular form (see Table 2.3).

| Clause number and title | | | |
|---|---|---|---|
| Provision | Status | Support | Detail |
| 4 Reporting implementation | | | |
| 4-1 | M | | |
| 5.1 No universal default passwords | | | |
| 5.1-1 | M C (1) | | |

**Table 2.3:** Section of Table A.1: Implementation of provisions for consumer IoT security

In the first column are listed the provisions. The provisions are all provided with statuses indicating the level of commitment. There are four levels of commitment.

- **M** the provision is a mandatory requirement
- **R** the provision is a recommendation
- **M C** the provision is a mandatory requirement and conditional
- **R C** the provision is a recommendation and conditional

If the level is a conditional one, it has one or more conditions associated with it in the form of numbers. It should be noted that the last version of the standard ETSI EN 303 645 [ETSa] is older than the technical specification ETSI TS 103 701 [ETSb]. For this reason, more conditions can be found in ETSI TS 103 701 [ETSb]. Because of that the ICS from ETSI TS 103 701 [ETSb] was used. The corresponding conditions can be found in section 4.2. At the moment only provisions with **M** and **M C** are relevant. This does not mean that the recommended and recommended conditional provisions are not relevant. The ETSI EN 303 645 [ETSa] [ETSa] also states that later provision which have the commitment level recommended at the moment could become mandatory. This was done to first just focus on the most important provisions and not overwhelm the SOs. The third column of the ICS named "Support" tells if the provision is found to be applicable for the DUT or not. There are three options to state the support.

- **Y** supported by the implementation
- **N** not supported by the implementation
- **N/A** the provision is not applicable (allowed only if a provision is conditional as indicated in the status column and if it has been determined that the condition does not apply for the product in question)

Accompanying this standard is the ETSI TS 103 701 [ETSb] a technical specification which gives guidance on how to assess the DUT.

### 2.5.2 ETSI TS 103 701

In companion to the ETSI EN 303 645 [ETSa] the ETSI TS 103 701 [ETSb] supplies the concrete test methodology for the provisions. This is done by providing test cases and assessment criteria

for each provision. The specification is addressed to first, second and third party-assessment. This means that the testing can be done as a self-assessment or by an independent testing organization. Due to the wide variety of IoT devices no specific tools or step-by-step instructions are given for the test cases. The technical specification provides a structured way to represent the relevant technical and organizational information. This can be realized with the help of tables. These tables are referred to as Implementation eXtra Information for Testing (IXIT)s. The first IXIT is called "1-AuthMech: Authentication Mechanisms" and lists all authentication mechanisms which are used by the DUT. An example of IXIT 1-AuthMech can be seen in Table 2.4.
After completion of the ICS, table "Table B.1: Required IXIT entries per provision" shows which IXITs are required. After all preparations are finished the testing can start. Every provision group from the ETSI EN 303 645 [ETSa] corresponds to a test scenario (TSO). For example, the provision group "5.1 No universal default passwords" is mapped to "TSO 5.1: No universal default passwords". Every provision is then mapped to a test group. An example for that would be provision 5.1-1 corresponds to test group 5.1-1. Each test group consists out of three parts: test group objective (example: 5.1-1-0), test case conceptual (example 5.1-1.1) and test case functional (example 5.1-1-2). The test cases are also composed of three parts. The first part is the test purpose. It describes the purpose of the current test. For example, the purpose of test case 5.1-1-1 is to assess the password-based authentication mechanisms. It is followed by the test units. The test case 5.1-1-1 only includes one test unit. The test unit (a) demands that the TL check that passwords are generated securely and unique per device. The last part of a test case is the verdict. In the case of 5.1-1-1 it states that a verdict of passed is assigned if all generated passwords are unique per device. Otherwise, the verdict fail is assigned.

| ID | Description | Authentication Factor | Password Generation Mechanism | Security Guarantees | Cryptographic Details | Brute Force Prevention |
|---|---|---|---|---|---|---|
| AuthMech-1 | A user can login over HTTPS at port 443 to gain access to the web frontend. (A user can request a login over HTTP at port 80 but is forwarded automatically to HTTPS on port 443.) The authentication on the login page is to be completed before any payload data over HTTPS is exchanged. No payload is readable without logging in first. The web server authenticates the given credentials against the login information stored in its SQLite database and grants access to the requested resources. The mechanism is used for user-to-machine authentication. The mechanism is directly addressable from a network interface. | Username and password (pre-installed and used in initialize state). | The username is fixed "admin". The password is generated randomly and is unique per device. The password has a length of 16 and consists of upper case chars, lower case chars and numbers. The password is generated by use of /dev/urandom on a UNIX configuration system during manufacturing phase. | The username and password are transmitted over an HTTPS channel, so the DUT ensures confidentiality and integrity during the transfer. | Authentication is performed via a form-based HTML interface by an internal PHP script in combination with an SQLite database. Integrity and confidentiality of the password transfer to the DUT is realized over TLS 1.2. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCM-SHA384. | After 3 invalid login attempts the login interface is inaccessible for 5 minutes. |

**Table 2.4:** Table C.1: Sample IXIT 1-AuthMech (Authentication Mechanisms) [ETSb]

### 2.5.3 All steps of the certification process according to ETSI TS 103 701

Figure 2.3 shows the certification process according to ETSI TS 103 701 [ETSb]. The process is divided into two phases. The first phase is the preparation phase. To certify a CIoT device, the company must follow a secure development process. Looking at the characteristics of the CIoT device, it is possible to get a good overview of whether all the provisions of the ETSI EN 303 645 [ETSa] can be met. If this is the case, the company must find a certifier. In Germany, this could be the TÜV.
The second phase starts with the selection of a contact person for the certification. The next step is to create all the pro forma documents for the DUT. This includes three documents that can be found in ETSI TS 103 701 [ETSb]. The first document is the "A.2 Identification of the DUT pro forma" from ETSI TS 103 701 [ETSb]. This document defines which device is being tested. The second document is the "A.3 Implementation conformance statement (ICS) pro forma". At the end of this document, the conditions are listed. Each condition must be answered yes or no. A rationale for the answer must also be provided. The conditions are numbered, which is important for the next step. The ICS must be filled in. This is described in subsection 2.5.1. The third document, IXIT, must also be filled out, as described in subsection 2.5.2. Now everything is ready for certification by the TL.
The TL reviews the ICS and performs the actual assessment. At the end of the assessment, the TL gives an overall verdict for the examinee. If the verdict is **FAIL** the preparation phase starts again. If the verdict is **PASS** the DUT is a label asigned.

## 2.6 Interplay between ETSI EN 303 645 and national recommendations

The German BSI has a very good international reputation in the CIoT cybersecurity community. The BSI issues its own label IT security mark for CIoT devices. The standard ETSI EN 303 645 [ETSa] has a generic character. This is important to ensure that the standard can still be applied with the technical innovations made in the future. To achieve that the standard relies on best practices. These best practices are often not defined in the standard. There are concrete examples offered in the accompanying technical report TR 103 621. The problem here is that these are only examples and not mandatory requirements. To solve this problem the BSI has developed its own standard, the BSI TR-03173 [BSI22b].
The BSI TR-03173 [BSI22b] is divided into 4 amendments. The first amendment deals with best practice cryptography. The provisions concerned are:

- Provision 5.1-3: User Authentication
- Provision 5.3-7: Secure Update
- Provision 5.5-1, 5.5-6, 5.5-7, 5.8-1 and 5.8-2: Secure Communication

The provisions concerned all relate to cryptography. ETSI EN 303 645 [ETSa] offers several options here. BSI restricts itself to the SOGIS-ACM catalogs [Gro20] and BSI TR-02102 [BSI22a] "Cryptographic procedures: Recommendations and Key Lengths".
The first amendment contains 3 notes. The purpose of the first note is to take away the fear of the

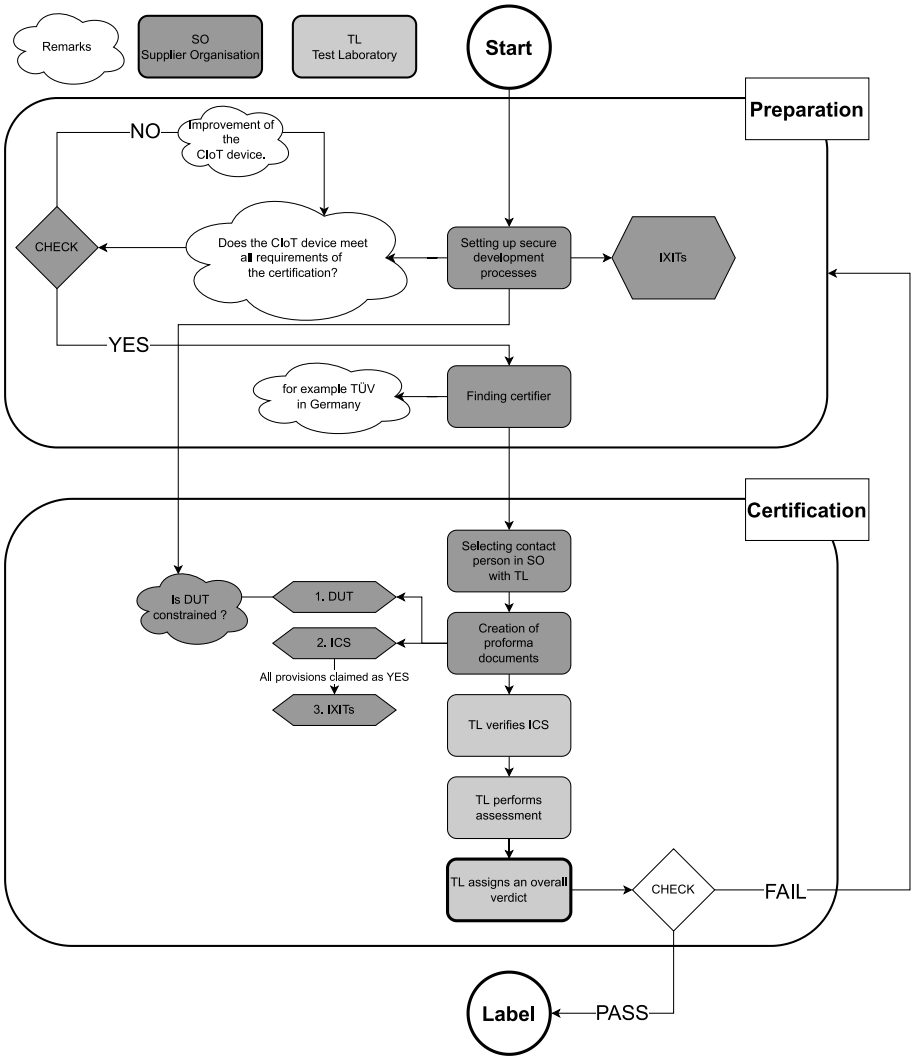


**Figure 2.3:** CIoT certification process according to ETSI TS 103 701 [ETSb]

SOGIS-ACM. The SOGIS-ACM is used in connection with cryptography products that require a high encryption standard. This is not required for the ETSI EN 303 645 [ETSa]. The BSI therefore indicates that the standard contains cryptographic requirements and recommendations for use cases above the level basic.

The second note merely informs the reader that it is possible to use cryptographic algorithms that are not included in either of the two catalogs. However, proof must then be provided that the cryptography used is considered best practice cryptography.
The third comment simply states that this does not change the test according to ETSI TS 103 701 [ETSb]. It merely specifies the term "reference catalog".
The first appendix concludes with a non-exhaustive list of primitives and communication protocols that should be considered vulnerable. At the time of writing, these were:

- SSL, TLS 1.0, TLS 1.1 for the use cases of communication with associated web services
- WEP for the use cases of Wi-Fi communication

The second amendment concerns usability. The provisions affected are:

- Provision 5.1-4: Changing authentication value
- Provision 5.3-3: Simple application of updates
- Provision 5.3-13: Publication of support period
- Provision 5.3-14: Publication of support period and replacement support for constraint devices
- Provision 5.8-3: Documentation of external sensing capabilities
- Provision 5.11-1: Erasing user data
- Provision 5.11-2: Removing personal data from associated service
- Provision 6.1-2: Obtaining the processing of personal data

The ETSI TS 103 701 [ETSb] includes the "user with limited technical knowledge" model in appendix D.3. This model is to be used for the provisions listed above. This solves the problem with the imprecise wording of these provisions.
The third amendment covers secure storage. The provision affected is:

- Provision 5.4-1: Secure storage of sensitive security parameters

The ETSI TS 103 701 [ETSb] contains in Annex D.2 the "baseline attacker model". This model shall be used to verify whether a security guarantee is suitable for a protection mechanism. The model describes the capabilities of an attacker.

The fourth extension includes additional applications. An IoT device can have the ability to install applications from first- or third-party vendors. BSI states that pre-installed applications should be considered part of the DUT. This excludes applications that are only prepared (for example, a link to the store), are disabled by default, or are installed by the user after initialization. These excluded applications are not exempt from the following provisions.
BSI adds comments to these provisions for clarification:

- Provision 5.4-1: Secure storage of sensitive security parameters
  Consider the interaction of the application with the DUT concerning “Security Guarantees” and “Protection Schemes ”(see ETSI TS 103 701 [ETSb]).
- Provision 5.13-1: Data Input Validation
  Consider the interface between the application and the DUT as API

As can be seen in BSI TR-03173 [BSI22b], the BSI has accepted the ETSI EN 303 645 [ETSa], which is tested according to ETSI TS 103 701 [ETSb]. Only a few mappings to its own documents were necessary to prepare the standard for its own label IT-Sicherheitskennzeichen.

# 3 Methodology

## 3.1 Structure of the interviews

This section explains the method of the interviews. Due to time constraints, the interviews were conducted in a digital context. Each interview had the duration of one hour. The first 5 minutes were used to warm up and provide insight into the thesis. As part of this thesis, two Consumer IoT (CIoT) devices were evaluated according to the standard ETSI TS 103 701 [ETSb]. Since not all information about the tested devices was available, three interviews were conducted to present the situation of a Test Laboratory (TL) without the limitations of this thesis. Normally, when evaluating devices according to the ETSI TS 103 701 [ETSb], the Supplier Organization (SO) is present and accessible for any question about the device. This was not the case for the assessments performed in this thesis.
This situation led to two questions. The first question is "What are the experiences and processes in dealing with IXIT documents?". During the assessment it was not possible to collect all the information needed to complete the IXITs. This question attempts to capture the situation that all the required information were available.
The second question, "What problems were encountered during the testing of the devices?" also attempts to represent the situation where all information is available.
Since all interviewees offer certification labels, this should also be included in the interviews with the following question: "Which Cybersecurity label for CIoT devices is offered by the organization?".
During testing, the problem of imprecise wording became apparent. The question: "How is imprecise wording in the ETSI EN 303 645 [ETSa] standard dealt with?", captures how the TL deals with this.
The ETSI EN 303 645 [ETSa] uses the wording "best practice cryptography". With the question: "Which standards are used to achieve "best practice cryptography"?", the TLs interpretation of this phrase is recorded.
To give the respondent room for information not covered by the interview the question: "What are the challenges in CIoT certification?" was introduced. It is an open question trying to get more answers on the topic of CIoT certification

## 3.2 Methods of testing

This section will explain how the technical aspects of the test were performed.

### 3.2.1 Test setup

In this thesis two devices were tested to the standard ETSI TS 103 701 [ETSb]. The devices will be referenced with CIoT-1 and CIoT-2. To test these devices it was necessary to setups two different

network infrastructure owing to the fact that they use different network technologies.

#### CIoT-1

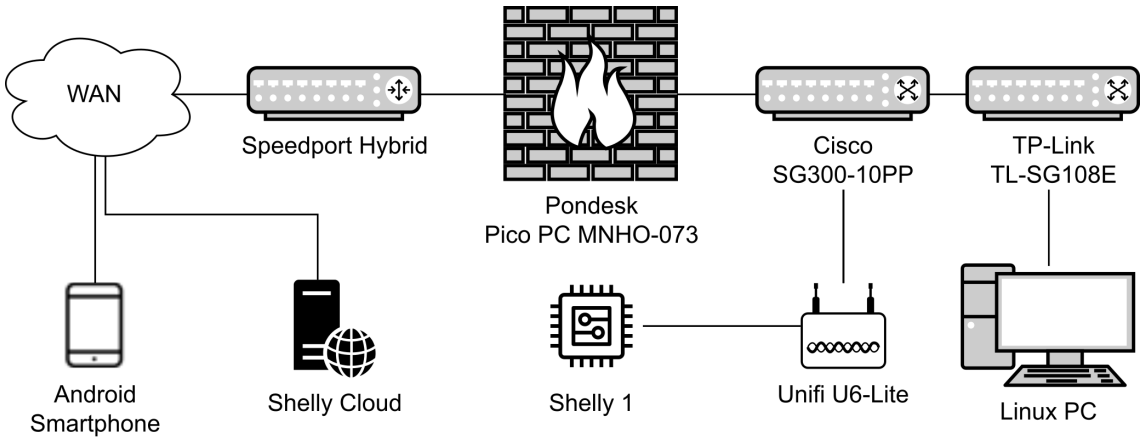


**Figure 3.1:** Setup to evaluate the Shelly CIoT (CIoT-1) device according to ETSI TS 103 701 [ETSb]

The first device tested is produced by the manufacturer Allterco Robotics LTD under the brand Shelly. The device uses 2.4 GHz Wi-Fi to connect to a network. For the test setup the Wi-Fi access point U6-Lite from Unifi was used. To test the cloud functionalities an Android smartphone was used. The smartphone was connected to mobile data only at the moment of testing, to create an entry point outside the local area network. The local area network includes all devices behind the Speedport Hybrid. Interaction with the device was possible over an API, a web interface or MQTT.

#### CIoT-2

The second device tested is produced by the manufacturer Lumi United Technology Co., Ltd under the brand Aqara. The device uses Zigbee to connect to a network. In this test setup the Zigbee network was provided by a smart home system called Home Assistant [Ass22a]. Home Assistant (OS Version: OS 8.4, Core: 2022.8.4, deployed as Docker container) provides integrations for extension. One of these integrations is "Zigbee Home Automation" [Ass22b], which adds the functionality of a Zigbee co-ordinator to Home Assistant. For the hardware site of the co-ordinator a C2652 USB device was used. The C2652 comes with a Zigbee compatible antenna used to create the test network.

### 3.2.2 Network scan

```
1 sudo nmap -Pn -sU -p- <ip address> // UDP scan
2 sudo nmap -Pn     -p- <ip address> // TCP-SYN scan
```

**Listing 3.1:** Nmap commands

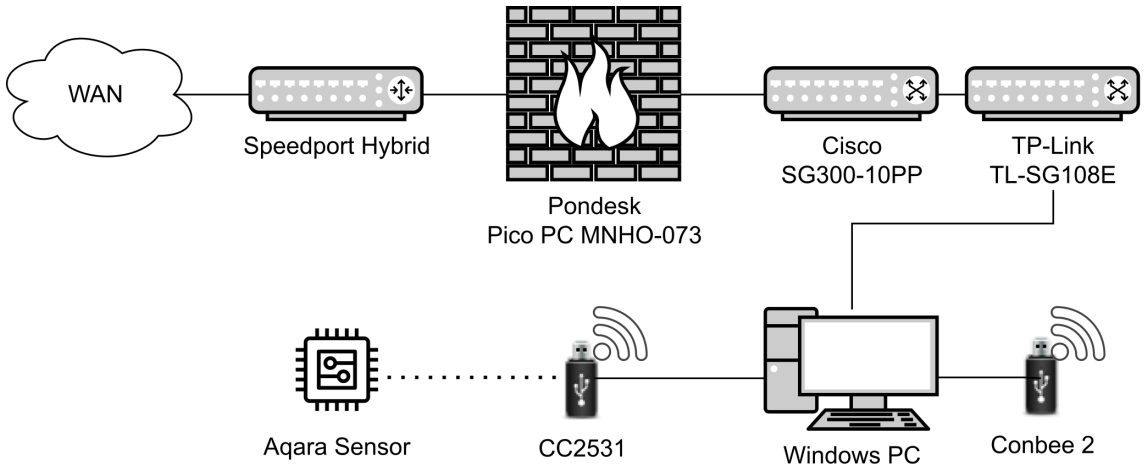


**Figure 3.2:** Setup to evaluate the Aqara CIoT (CIoT-2) device according to ETSI TS 103 701 [ETSb]

For port scans the tool Nmap was used. A port scan is done to see which services are exposed to the network. Every exposed service can be an entry point for an attacker. With a port scan the tester can verify that no unnecessary services are exposed. Nmap offers different scan types. The first scan which is performed is a SYN scan. A SYN scan is a special TCP scan. For this scan, Nmap creates a SYN packet, which is the first packet that is send to establish a TCP connection. This scan type is more efficient than a normal TCP scan, because a connection is never formed. Nmap only analyzes the response of the target on the SYN packet. Not all services use TCP. To also discover services using UDP, a UDP scan is performed after the SYN scan. In the default mode Nmap only scans the well-known ports (port numbers from 0 to 1023). The flag `-p-` is used to scan all possible ports. Both scans (see Listing 3.1) should run quickly and are easy thus to integrate into a test routine.

### 3.2.3 Network capture

The standard ETSI EN 303 645 [ETSa] requires that all data in transport has to be encrypted. To verify the encryption claims of the manufacturer the network traffic of the Device Under Test (DUT) needs to be captured. This will now be explained for the two test setups.

The first connection point of the device was the Unifi U6-Lite Wi-Fi access point, as shown in Figure 3.1. It was possible to connect to the access point from the Linux PC using the SSH protocol. The tool tcpdump is installed on the access point. tcpdump could be used to directly capture network traffic on the device. SSH was then used to run tcpdump on the access point. The output from tcpdump could then be forwarded to Wireshark running on the Linux PC. Wireshark visualizes the recorded traffic. This allowed a thorough examination of each network packet. Wireshark also provides several tools for analyzing recorded data. The command used on the Linux PC is shown in Listing 3.2.

```
1 Wireshark -k \
2   -i <(sshpass -p <password of root>    \
3   ssh -oHostKeyAlgorithms=+ssh-dss      \
4   root@<ip address of the access point> \
5   -p 22 tcpdump -i any -U -w - not port 22)
```

**Listing 3.2:** Capture command

To record the traffic in the Zigbee network, a second antenna was needed. The Conbee2 USB adapter (can be seen in figure 3.2) was chosen for that task. Conbee2 was connected via USB to the Windows PC. To use the Conbee2 as a capture device, special firmware needed to be flashed on it. This can be done with the ZShark software [de22]. The ZShark software also provides the connection between Wireshark and Conbee2. This allowed for an easy analysis of the captured network traffic.

# 4 Results

## 4.1 Interviews: Getting a consumer IoT device certified today

At the time of writing, Consumer IoT (CIoT) certification is still a fairly new topic. The relevant European harmonized standards are not yet ready. CIoT certification providers need to develop certification programs based on the most promising standards. Overall, everything is constantly changing, and vendors need to adapt. An overview of current CIoT security labels can be found in Table 2.2. Three interviews were conducted to capture the current situation from the perspective of an Test Laboratory (TL).

### 4.1.1 TÜV Nord

The interview was conducted by e-mail in German on the 6th of July 2022. The interview partner is Gerald Krebs. He oversees the department Business Security & Privacy at TÜV Informationstechnik GmbH, which is part of TÜV NORD GROUP.

#### How is imprecise wording in the ETSI EN 303 645 standard dealt with? Which standards are used to achieve "best practice cryptography"?

TÜV IT decides how to deal with inaccurate formulations on a case-by-case basis. In doing so, it relies on common sense. An example of this is the wording "An update must be easy for the user to apply" from provision 5.3-3, which is answered by the interviewee with: "We are flexible here and it must be obvious that the mechanism is simple". This is based on experience from the Industrial IoT (IIoT) domain, pentest colleagues, or the Common Criteria domain. If no concrete cryptographic algorithms are specified, TÜV IT uses the cryptographic guidelines of the BSI.

#### What are the experiences and processes in dealing with IXIT documents?

TÜV IT does not use the ETSI TS 103 701 [ETSb] at the time of the survey. This means that the Implementation eXtra Information for Testing (IXIT)s are not used. This is due to the fact that manufacturers are already overwhelmed with following a standard for secure product development. Compliance with a standard for secure product development, such as IEC62443-4-1, is the basis for TÜV Nord's certification seal. The interviewee gives four examples of the state of manufacturers:

- The manufacturer uses best practices based on his own experience. In most cases, these best practices are applied after development. Penetration testing is an example of this.
- The manufacturer has implemented in parts a secure product development process. However, the process is not defined in a formal document or incompletely documented.

- The manufacturer has decided on a process according to a standard and works according to this standard.

To classify these statements, only the last statement is sufficient for certification according to the CyberSecurity Certified label.

#### Which cybersecurity label for consumer IoT devices is offered by TÜV Nord?

TÜV Nord offers the CyberSecurity Certified label. This can be obtained in three different security levels, namely "Basic", "Substantial" and "High". At the time of the interview, the label had not yet been issued to a product.

#### Which problems have arisen as a result of testing the devices?

No devices have been tested yet.

#### What are the challenges in consumer IoT certification?

The interviewee points out that the biggest problem right now is the maturity of manufacturers.

### 4.1.2 TÜV SÜD

The interview was conducted via video call and the interviewee was Roland Fiat. He is working for TÜV SÜD as Senior Cybersecurity Engineer in ICS & CIoT. The interviewee has been working in the field of CIoT for about 3 years. Before that, he was working in the operational technology (OT) space. IIoT devices are used in OT. IIoT is the counterpart of CIoT.

**How is imprecise wording in the ETSI EN 303 645 standard dealt with?** TÜV SÜD deals with inaccurate formulations on a case-by-case basis. It uses discussion groups within the organization and with external partners such as the German BSI or ETSI directly to make a judgment. When a provision is in question. Decisions are made based on a risk analysis. For example, TÜV SÜD evaluates a temperature sensor that only transmits temperature data and uses vulnerable cryptography. This then poses no threat due to the lack of risk potential. The respondents refer to test case 5.5.1.1 from ETSI TS 103 701 [ETSb].

**Which standards are used to achieve "best practice cryptography"?** The respondent noted that SOGIS-ACM is used, which is mentioned in the ETSI TS. Also, the TR-02102 is used.

**What are the experiences and processes dealing with IXIT documents?** The TÜV SÜD has made the experience that the creation of IXITs by the manufacturer is quite complex and difficult. In practice, that means manufacturers often need up to 6 versions until the IXIT documents are filled out satisfyingly. The Interviewee points out, that the manufacturers are not just left with the IXIT documents. TÜV SÜD has developed an intelligent Excel sheet, which consists of yes/no questions drop down lists their possible. Also, before the certification process starts, the manufacturer is given a workshop about how to deal with the IXIT documents. In the opinion of the

interviewee, the IXIT document should not be so extensive and be reduced to non-technical questions. The interviewee points out that the standard ETSI EN 303 645 [ETSa] would have a greater adoption, if the IXIT documents were less complicated and complex.

**Which Cybersecurity label for consumer IoT devices is offered by the TÜV SÜD?** In addition to an ETSI EN 303 645 [ETSa] certification mark, TÜV SÜD issues the certification label CyberSecurity Certified. Which was developed by the TÜV Verband. TÜV SÜD also offers the CSA CLS certification (levels 1 - 4), as well as an AoC (attestation of conformity) for NIST IR 8259.

**What problems were encountered during the testing of the devices?** When testing the devices, the respondent encountered several problems, two of which are described as follows: TÜV SÜD bases its evaluation of the devices first on the ETSI EN 303 645 [ETSa] and then on the ETSI TS 103 701 [ETSb]. This can lead to contradictions. An example of this is test case 5.6.3.1 Test unit c and the corresponding provision 5.6-3.
Test case 5.6.3.1: Test unit c from ETSI TS 103 701 [ETSb]: "For each physical interface in IXIT 15-Intf that does not require permanent exposure according to "Description", the TL shall check whether the interface is disabled according to "Status" for all periods in which the use of the interface is not required."
Provision 5.6-3 from ETSI TS 103 701 [ETSb]:
"Device hardware should not unnecessarily expose physical interfaces to attack. Physical interfaces can be used by an attacker to compromise firmware or memory on a device. "Unnecessarily" refers to the manufacturer's assessment of the benefits of an open interface, used for user functionality or for debugging purposes"
In this example, the DUT has an interface that is only required for maintenance purposes. This interface is activated in the initialized state but is hidden under the housing of the device. After the test unit, the DUT would FAIL the evaluation because the interface is enabled but not needed permanently. Considering the model of an attacker (see table "D.2.3 Characterization of the attacker" from ETSI TS 103 701 [ETSb]), the interface is hidden under the housing of the device, so that an attacker cannot easily reach it, and the test would PASS.

The respondent got noted by a SO that the sample IXIT 10-SecParam does contradict its own requirements. The SecParam-2 has the type critical, which means that after test case 5.4.3.1 test unit b it is not allowed to be used during operation. The description of SecParam-2 states that the parameter is used to decrypt firmware update packages. The sample DUT would FAIL the test unit. Test case 5.4.3.1: Test unit: b from ETSI TS 103 701 [ETSb]:
"The TL shall assess whether for all critical security parameters in IXIT 10-SecParam, which are hard coded in device software source code according to "Description", the corresponding "Provisioning Mechanism" ensures that it is not used during the operation of the DUT."
Table C.10: Sample IXIT 10-SecParam (Security Parameters) from ETSI TS 103 701 [ETSb]:

- SecParam-2
  - Description: AES key for decrypting critical firmware update packages (prior to verifying with SecParam-1). The key is not a hard-coded identity. The key is hard-coded

in device software source code.

- Provisioning Mechanisms: The key is hard-coded in the firmware and is modified only through a verified firmware update package.

**What are the challenges in consumer IoT certification?** The respondent sees the greatest challenge in the acceptance of CIoT certification by manufacturers. Certification on the basis of voluntariness is not enough. The RED will be updated in 2024. However, this will only make a subset of the ETSI EN 303 645 [ETSa] requirements mandatory. In addition, the RED only applies to CIoT devices that use wireless technology.
The interviewee also sees a major problem in the fragmentation of standardization. A single international standard would be optimal. The interviewee also noted that this is a difficult goal to achieve.

### 4.1.3 Bundesamt für Sicherheit in der Informationstechnik

The interview was conducted via video call with two experts from the BSI. The BSI is a German government agency for cybersecurity standards. Among other things, the BSI collaborated on SOGIS-ACM [Gro20], the only European standard for cryptography.

**How is imprecise wording in the EN 303 645 standard dealt with?** The respondents note that in general a certification/labelling scheme can deal with imprecise wording.

**Which standards are used to achieve "best practice cryptography"?** The respondents note that ETSI TS 103 701 [ETSb] describes a framework for dealing with "best practice cryptography" and the option for the scheme owner to concretize how to apply the phrase. In the case of the German security label ("IT-Sicherheitskennzeichen") BSI-TR 03173 builds up on this approach.

**What are the experiences and processes in dealing with IXIT documents?** TÜV SÜD has made the experience that the preparation of the IXIT TÜV SÜD by the manufacturer is quite time-consuming and difficult. In practice, this means that manufacturers often need up to 6 versions until the IXIT documents are satisfactorily completed. The interviewee points out that manufacturers are not only left alone with the IXIT documents. TÜV SÜD has developed an intelligent Excel spreadsheet consisting of yes/no questions with drop-down lists possible. In addition, the manufacturer receives a workshop on how to handle the IXIT documents before the certification process begins. According to the interviewee, the IXIT document should not be so extensive and should be limited to non-technical questions. The interviewee points out that the standard ETSI EN 303 645 [ETSa] would find greater acceptance if the IXIT documents were less complicated and complex.

**Which Cybersecurity label for consumer IoT devices is offered by the BSI?** The respondents note that the BSI offers the "IT-Sicherheitskennzeichen" for certain CIoT Products. It requires among other things a manufacturers declaration referring to a conformance assessment based on ETSI TS 103 701 followed by a plausibility check by the BSI.

**What problems were encountered during the testing of the devices?** The respondents consider provision 5.13 to be problematic concerning an assessment. The goal of this provision is to protect from all data input at relevant exposed interfaces of the device under test. This is typically done by looking at different layers of each interface under consideration. While the idea behind this provision is desirable, it is too costly and complex to assess under a strict interpretation.
Another issue is to practically verify that the device is sending only the data specified in the IXIT. This might not be easily possible via eavesdropping if encryption is implemented correctly.

**What are the challenges in consumer IoT certification?** The respondents noted that a major challenge with CIoT labelling/certification is the comparability of the various labels. The standards community has also noted this problem. The PWI (Preliminary Work Item) ISO 27404 attempts to provide a part of the solution via a subordinate metric for comparing labels. The approach is based on Singapore's "TR 91: Universal cybersecurity labelling framework for consumer IoT" standard and has a high potential but is still at an early stage of discussion.

## 4.2 Assessing devices based on ETSI EN 303 645 & TS 103 701

This section will cover the testing of two CIoT devices after the standard ETSI EN 303 645 [ETSa] and ETSI TS 103 701 [ETSb]. To represent the current situation, only mandatory and mandatory conditional provisions were taken into account. The Assessments were performed without any contact to the SO. This shows the view of an importer who wants to bring a product to the European Union (EU) market.

### 4.2.1 Assessment of CIoT-1 (smart relay)

The Device Under Test (DUT) is a smart relay which can be used in many applications. The standard application is to integrate normal light switches into a smart home system. The DUT is manufactured by the company Shelly. The company offers a cloud platform to easily give their users remote access to their products.
In the first step, the conditions of the Implementation conformance statement (ICS) from the ETSI TS 103 701 [ETSb] were applied to the CIoT-1. All conditions and their justification can be found in subsection B.1.1.

All conditions are numbered. These numbers indicate which conditions from the ICS must be applied to assess the DUT. In the case of CIoT-1 the following conditions (see Table 2.3) applied: 1, 5, 7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 27, 28.
Due to these conditions only, the following provisions must be met to ensure cyber security according to ETSI EN 303 645 [ETSa]: 4-1, 5.1-1, 5.1-3, 5.1-4, 5.1-5, 5.2-1, 5.3-2, 5.3-3, 5.3-7, 5.3-8, 5.3-10, 5.3-13, 5.3-16, 5.4-1, 5.4-3, 5.4-4, 5.5-1, 5.5-5, 5.6-1, 5.6-2, 5.6-4, 5.13-1, 6-1, 6-2, 6-3.
Table B.1: Required IXIT entries per provision from ETSI TS 103 701 [ETSb] shows which IXIT entries were needed for the assessment.
After establishing which IXITs were required for CIoT-1, the IXITs could be filled out. The IXITs

can be found in subsection B.1.2.

At this point the preparation for the assessment of CIoT-1 was completed. The Assessment of CIoT-1 can be found in subsection B.1.3.

#### Final verdict CIoT-1

The DUT got the final verdict **FAIL** according to ETSI TS 103 701 [ETSb]. This was not only due to the lack of information from the Supplier Organization (SO). The DUT simply did not yet met some requirements. The SO would have to fix the following points:

- **Encryption** The DUT needs to use encryption for the communication over Intf-1. This would guarantee confidentiality and integrity for the authentication of the web interface.
- **Debug Interface** Intf-2 is a debug interface, which does not need to be enabled at the initialized state of the DUT.
- **Vulnerability disclosure policy** The DUT is missing a vulnerability disclosure policy, which is important to quickly inform the SO about vulnerabilities of the DUT.
- **Brute Force Prevention** The DUT is missing a mechanism which protects against brute force attacks.
- **Support Period** The SO has to publish a support period for the DUT.
- **Initialized State** The DUT is completely unprotected in the initialized state. It also does not guide the user into enabling a restriction for the web interface. To pass the assessment, the DUT needs to have a unique password in the initialized state, if condition 17 applies. Condition 17 applies for all devices, which support changing the password over a network interface.
- **Missing Documentation** The SO needs to supply documentation for the update mechanism and input validation. The update policy of the SO is also needed. Without the documentation an assessment is not possible.

The last point showed that it was not possible to assess a device with user input and an update mechanism without the SO.

### 4.2.2 Assessment of CIoT-2 (weather sensor)

The DUT is a Zigbee climate sensor. It can measure temperature, air pressure and humidity. It is sold by Xiaomi but produced by Lumi United Technology Co., Ltd under the Brand Aqara. The intended use of the DUT is with an Aqara Hub. Only the DUT was tested, and the hub was ignored. The DUT is constrained in many aspects. This has the consequence that less provisions of the ETSI EN 303 645 [ETSa] applied.
In the next step, the conditions of the ICS from the ETSI TS 103 701 [ETSb] were applied to the CIoT-2. All conditions and their justification can be found in subsection B.2.1.

To fill out the conditions the security of the DUT needed to be analyzed. To achieve that the traffic of the device was captured. The DUT uses Zigbee. The Zigbee protocol offers different security levels as described in section 2.3. It was not possible to find the security level sub-field in the captured network traffic of CIoT-2 (see 3.2.1). However, it is possible to see the network key of the Zigbee network in the Wireshark record in line 18 of Listing 4.1. For this reason, it can be said that CIoT-2 used security level 0x05 for all communication. This resulted in a critical safety parameter being transferred and stored on the device. The transfer is done by a secure key exchange mechanism to protect confidentiality.

```
1  Frame 21: 127 bytes on wire (1016 bits), 127 bytes captured
       (1016 bits)
2  IEEE 802.15.4 Data, Dst: 0x0000, Src: 0xf121
3  ZigBee Network Layer Data, Dst: 0x0000, Src: 0xf121
4      Frame Control Field: 0x0248, Frame Type: Data, Discover
           Route: Enable, Security Data
5          .... .... ..00 10.. = Protocol Version: 2
6          .... ..1. .... .... = Security: True
7      Destination: 0x0000
8      Source: 0xf121
9      Radius: 30
10     Sequence Number: 155
11     [Extended Source: Jennic_00:07:d3:c2:e3 (00:15:8d:00:07:d3:
           c2:e3)]
12     ZigBee Security Header
13         Security Control Field: 0x28, Key Id: Network Key,
               Extended Nonce
14         Frame Counter: 5
15         Extended Source: Jennic_00:07:d3:c2:e3 (00:15:8d:00:07:
               d3:c2:e3)
16         Key Sequence Number: 0
17         Message Integrity Code: 9762a0fd
18         [Key: f540a6f66978d5354cf2af5b94458df1]
19         [Key Label: ZHA]
```

**Listing 4.1:** Zigbee capture: Network layer

All conditions are numbered. These numbers indicate which conditions from the ICS must be applied to assess the DUT. In the case of CIoT-2 the following conditions applied: 3, 4, 14, 16, 18, 19, 23, 27.
Due to these conditions only the following provisions have to be met to ensure cyber security according to ETSI EN 303 645 [ETSa]: 4-1, 5.2-1, 5.3-13, 5.4-1, 5.4-3, 5.5-1, 5.5-7, 5.6-1, 5.6-2, 5.8-3, 5.13-1.
The table B.1: Required IXIT entries per provision from ETSI TS 103 701 shows, which IXIT entries were needed for the assessment.
After establishing which IXITs were require for CIoT-1. The IXITs could be filled out. The IXITs can be found in subsection B.2.2.

At this point the preparation for the assessment of CIoT-2 was completed. The Assessment of CIoT- 1 can be found in subsection B.2.3.

#### Final verdict CIoT-2

The DUT got the final verdict **FAIL** according to ETSI TS 103 701 [ETSb]. This was not only due to the lack of information from the SO. The DUT simply did not yet met some requirements. The SO would have to fix the following points:

- **Support Period** The SO has to publish a support period for the DUT.
- **Disclosed Information** The DUT does not need to disclose any version information. This information could be useful to a malicious acter.
- **Missing Documentation** The SO needs to supply documentation for the input validation. Without the documentation an assessment is not possible.

The last point showed that it was not possible to assess a device with input possibilities without the SO.

## 4.3 Problems of ETSI EN 303 645 & TS 103 701

This section will expose the weaknesses of the standard ETSI EN 303 645 [ETSa].
For most people, the ETSI EN 303 645 [ETSa] has only one corresponding document, the ETSI TS 103 701 [ETSb]. The problem is that there is a third document, the ETSI TR 103 621 [ETSc] which is not referenced in either the ETSI EN 303 645 [ETSa] or the ETSI TS 103 701 [ETSb]. The third document contains concrete examples such as cryptographic ciphers or algorithms that are considered “best practices cryptography”.
Many provisions (Provision: 5.1-3, 5.3-7, 5.5-1, 5.8-1) use the term "best practice cryptography". When working with standards, best practices must be applied to ensure longevity. The ETSI TR 103 621 [ETSc] gives concrete examples of these best practices. The SOGIS-ACM [Gro20] is also listed as a reference for verified cryptography. It may be problematic to incorporate new developments in cryptography because these documents cannot be changed quickly. There is no mechanism for rapid security bulletins.

Another problem was found in provisions: 5.1-4, 5.3-3, 5.11-1, 5.11-2, which use the word “simple”. In all of these provisions, “simple” describes the usability of the user interface. The phrase simple is not clear enough. Is enabling developer settings in Android easy or hard? For someone who has done it before, it is quite easy, but the first time it takes a while to get it done. A metric like the number of clicks it takes to reach an action from the home screen would be better. This action would be for provision 5.11-1 to delete all user data from the device. This would also prevent manufacturers from hiding such options deep in their settings menus. In the case of Provision 5.3-3, this goes even further. As currently written, provision 5.3-4, which requires automatic updates, is not mandatory. This means that the manufacturer is allowed to implement updates with the help of an external USB stick. It would be good to add something to provision 5.3-3 to prevent such behavior, or to make provision 5.3-4 mandatory.
Another problematic formulation was the use of imprecise time periods. This is found in provisions 5.2-2 “acted on in a timely manner” and 5.3-8 “be timely”. It is understandable that in some cases it may take quite a long time to fix a bug in the system, but not setting an upper limit is not an option. This can lead to unnecessary delays or even blockage on the part of the supplier organization.
This problem can also occur with update management, which is covered in Provisions 5.3-1 “securely updatable” and 5.3-2 “update mechanism for the secure installation of updates”. Neither provision clearly defines what securely updatable or secure installation means. The same is true for provisions 5.5-8 “secure management processes” and 5.6-9 “secure development processes.”
In many cases Internet of Things (IoT) devices are used with a gateway. The ETSI EN 303 645 [ETSa] does not check for any interactions between DUTs and gateways. One example for such an interaction can be found under the resiliency against outages. To secure availability, it must always be tested if the DUT can establish automatic an connection to the gateway if it or the DUT suffers a power failure. It cannot be expected of an end user to reconnect the DUT to the gateway or initiate a new pairing process for the DUT. This is especially true when looking at CIoT devices installed by a different party than the user.

## 4.4 Elaboration of current challenges of consumer IoT security certification

All sections of this thesis have worked towards this section. A wide variety of perspectives have been explored. The first challenge for CIoT security certification is the rapid change of the topic. In order to make an impact across the board in the CIoT landscape, legislators must be involved. Unfortunately, this means going through many instances to be able to define requirements in the end. However, the CIoT landscape is a very new area that is still in flux. In addition, the topic is strongly influenced by technological progress. Furthermore, it is not only security experts who want to push through their goals in standardization organizations. Manufacturers are also trying to bring in their interests. This can cause drafts to be delayed. One example is the cryptography catalog SOGIS-ACM [Gro20], on which ETSI EN 303 645 [ETSa] is based. The catalog was last updated in 2020.
Based on ETSI EN 303 645 [ETSa], many safety labels have emerged. An overview can be found in Table 2.2. The overview shows that the labels are not readily comparable because, although they meet the requirements required by ETSI EN 303 645 [ETSa] at a certain level of security, this level may vary. The ISO 27404 standard, which borrows heavily from Singapore's TR 91: Cybersecurity labeling for consumer IoT, attempts to address this issue by creating a standardized label. Until 2024, there is no mandatory requirement for manufacturers to certify their CIoT devices for cybersecurity. This means that until that time, cybersecurity labeling is primarily for the consumer. Cybersecurity is a complex issue for the end consumer. This makes it all the more important that the labels are consistent and easy to understand. Otherwise, a situation similar to buying fish in the supermarket will arise. When you go to the supermarket, for example, you are overwhelmed by a multitude of labels. Few consumers can still see through and distinguish which labels make sense. In this example, which fish can be bought with a clear conscience.
During the evaluation of two CIoT devices and during interviews with TL, the following problems emerged. First, the IXITs under ETSI EN 303 645 [ETSa] are overly complex and present an obstacle to certification for some manufacturers. For example, certification is often performed by a product owner who has too little technical knowledge. This leads to less adoption of the standard ETSI EN 303 645 [ETSa] than would be possible. Test certifications have already been carried out without IXITs, with very good results. Only some organizational issues are missing to complete the certification. This is made possible by providing the TL with the firmware of the CIoT device.
The next problem is posed by provision 5.13 of the ETSI EN 303 645 [ETSa]. This provision is intended to verify that each input of the CIoT device is protected. In practice, this means that a gray-box pentest must be performed on the CIoT device. This requires a large amount of time, which is usually not available. The manufacturer does not have to make the firmware of the CIoT device available, which means that the TL can only find weak points in the input validation by fuzzing.
Another problem with the standard is encryption. How can the device be accessed if encryption is used securely by the CIoT device? For example, to verify that only documented data is sent back to the manufacturer. To make this happen, all traffic from the CIoT device must be recorded and decrypted. But how is this possible if the encryption cannot be cracked? The ETSI EN 303 645 [ETSa] standard does not require the manufacturer to provide a method for decrypting the device's traffic. It must be ensured that the method can only be used during testing.

At the current state there are many challenges that still need to be resolved.

# 5 Conclusion

In the following, all findings of this thesis will be summarized. Currently, it is difficult to compare CIoT cybersecurity labels because they are not standardized.This shows a major problem that Consumer IoT (CIoT) labels currently have. The ISO 27404 standard, which borrows heavily from Singapore's "TR 91: Cybersecurity labeling for consumer IoT," attempts to solve this problem by creating a standardized label.
To obtain a cybersecurity label, the device must go through a certification process. This process can be divided into two phases. In the first phase, the manufacturer prepares everything for the second phase, the actual assessment. The first phase is especially important to ensure a fast and efficient certification. The manufacturer can reduce his work by checking if his device can be classified as constrained. This can be a great relief if testing the device after the ETSI EN 303 645 [ETSa].
Currently, there is no standard for CIoT security comparable to ETSI EN 303 645 [ETSa]. For this reason, a comparison was made with the requirements of the Bundesamt für Sicherheit in der Informationstechnik (BSI). The ETSI EN 303 645 [ETSa] relies on best practices to be highly compatible and up to date. The problem with this is that best practices are not precisely defined by the ETSI EN 303 645 [ETSa]. The BSI has its own best practices. The standard BSI TR-03173 [BSI22b] aligns the best practices from the BSI with those from the ETSI EN 303 645 [ETSa]. Beyond that, the BSI has not imposed any additional requirements.
During this thesis three interviews were conducted in section 4.1. The interview partners were Technischer Überwachungsverein (TÜV) Nord, TÜV SÜD and the BSI. It was interesting to note here that the BSI has only a regulatory interest in certification and the other two interviewees also have a financial interest. This was most evident in the question, "What are the experiences and processes in dealing with IXIT documents?". The two TÜVs state that the IXIT are too complicated and are only an unnecessary burden. In contrast, the experts from the BSI clarified the importance of this effort. They argue that by creating the IXIT, the manufacturer is forced to look deeper into his device.
Two CIoT devices were tested after the ETSI TS 103 701 [ETSb]. Both devices failed the evaluation. This was not only due to the fact that not all information about the devices was available from the manufacturers. A support period was missing for both devices. The assessments showed that it is not possible for an importer to certify devices without the Supplier Organization (SO).
While working with the ETSI EN 303 645 [ETSa], some flaws were discovered. The greatest strength is also the greatest weakness of this standard. The standard attempts to be as versatile as possible, drawing on best practices. It may be problematic to incorporate as well new developments in cryptography because these documents (ETSI TR 103 621 [ETSc], SOGIS-ACM [Gro20]) cannot be changed quickly. There is no mechanism for rapid security bulletins. The standard uses the wording "simple" and "timely", which is not precisely defined. This does not pose a problem if the standard is used by a third-party Test Laboratory (TL). However, if this standard is used as a basis for self-certification, this poses a problem. The ETSI EN 303 645 [ETSa]

completely ignores the fact that many CIoT devices use a gateway. There are no provisions which check the synergies between the Device Under Test (DUT) and the gateway. During the interviews it was discovered that the sample IXITs of the ETSI TS 103 701 [ETSb] contain errors. These errors can confuse SOs.

In the following, an overview of the current development and future trends in CIoT certification schemes will be given. The European Union (EU) agency ENISA is developing the EUCC scheme (EU Common Criteria), EU5G (EU 5G Networks) and EUCS (EU Cloud Services) after the Cybersecurity Certification Framework. A scheme for IoT devices is also under discussion.
Security Evaluation Standard for IoT Platforms (SESIP) has developed a standard for IoT device security [NXP20]. The standard offers 5 different assurance levels. It also covers the life cycle of the IoT device, which is divided into 4 phases. The first phase is called "Vendor Provisioning". At this stage, the device is assigned credentials. In the second phase named "User Provisioning" the device is for the first time in the hands of the end user. This includes the initial deployment and personalization. At this point the user chooses his own credentials. The third phase is the "Normal Usage", which can include an owner transfer. The last phase is the update phase. The standard is optimized to test IoT-specific building blocks. Different assurance levels can be applied for the same device. For example, there is a higher assurance level appropriate for the co-processor, which is handling the security of the device, than for the rest components. SESIP could be relevant in the future as especially for connected IoT devices with lots of hardware components, every single chip could be "SESIP certified". If every component as well as the operating system and crypto library is "SESIP certified", what SESIP aims to do, then the whole IoT device already provides a high level of security.
The problem of not comparable cybersecurity labels is focused by the standard ISO 27404, which is strongly influenced by Singapore's standard TR 91:2021 Cybersecurity labeling for consumer IoT.
Another approach in the standardization community is trying to reuse the existing standard IEC 62443-4-2, which is used to certify Industrial IoT (IIoT) devices, for CIoT devices.
Recently the standard Matter for CIoT devices was launched. The standard wants to ensure interoperability between all CIoT devices. Device of manufacturer A should function with device from manufacturer B if both support the Matter standard. Matter also requires a special initialization process, which involves a unique per device setup code. This can lead to greater baseline security. About 300 companies are currently working on the Matter standard in the Connectivity Standards Alliance. This could lead to certifications based on Matter.
Articles 3.3 d-f of the Radio Equipment Directive (RED) will enter into force in 2024 through a delegated act adopted by the European Commission. As a result, a subset of the ETSI EN 303 645 [ETSa] requirements will be required of all CIoT devices that use wireless technology.

# List of Figures

# List of Tables

# A Abbreviations

**ETSI** European Telecommunications Standard Institute

**DUT** Device Under Test

**ICS** Implementation conformance statement

**IXIT** Implementation eXtra Information for Testing

**SO** Supplier Organization

**TL** Test Laboratory

**ESO** European standards organization

**HENs** Harmonized European Standards

**EU** European Union

**RED** Radio Equipment Directive

**GDPR** General Data Protection Regulation

**TÜV** Technischer Überwachungsverein

**CSC** Cybersecurity Certified

**BSI** Bundesamt für Sicherheit in der Informationstechnik

**ITU** International Telecommunication Union

**IEEE** Institute of Electrical and Electronics Engineers

**DDoS** Distributed Denial of Service

**AES** Advanced Encryption Standard

**M2M** Machine to Machine

**IoT** Internet of Things

**CIoT** Consumer IoT

**IIoT** Industrial IoT

**SESIP** Security Evaluation Standard for IoT Platforms

# B Assessments

## B.1 CIoT-1

### B.1.1 Conditions

This section contains the conditions and their justifications for CIoT-1 according to ETSI TS 103 701 [ETSb].

1. Condition: passwords are used
   Justification: The access to the web interface can be secured with a password.
   Status: **Yes**

2. Condition: pre-installed unique per device passwords are used
   Justification: All passwords are user-defined.
   Status: **No**

3. Condition: software components are not updateable
   Justification: All software components of the device are updateable.
   Status: **No**

4. Condition: the device is constrained
   Justification: The device is not constrained.
   Status: **No**

5. Condition: the device is not constrained
   Justification: The device uses mains power and has an ESP8266, which is suitable for the use case.
   Status: **Yes**

6. Condition: telemetry data being collected
   Justification: No telemetry data is collected.
   Status: **No**

7. Condition: personal data is processed on the basis of consumers' consent
   Justification: In the initialized state the device does not process any personal data. To use the cloud functionality of the device a user account is required. By registering for the user account, personal data is processed.
   Status: **Yes**

8. Condition: the device allowing user authentication
   Justification: It is possible to enable user authentication for the web interface of the device.
   Status: **Yes**

9. Condition: the device supports automatic updates and/or update notifications
   Justification: The device is manually updatable and shows update notification in the app and web interface.
   Status: **Yes**

10. Condition: a hard-coded unique per device identity is used for security purposes
    Justification: The only parameter, which is used for security purposes, is username and password for the web interface. These parameters are user-defined.
    Status: **No**

11. Condition: updates are delivered over a network interface
    Justification: Updates are delivered over the Wi-Fi interface.
    Status: **Yes**

12. Condition: an update mechanism is implemented
    Justification: The device can be updated.
    Status: **Yes**

13. Condition: a debug interface is physically accessible
    Justification: The device has a serial interface, which can be used to flash firmware or for debugging.
    Status: **Yes**

14. Condition: sensitive security parameters are stored persistently
    Justification: For the user authentication username and password need to be saved.
    Status: **Yes**

15. Condition: critical security parameters used for integrity and authenticity checks of software updates in device software or for protection of communication with associated services in device software exist
    Justification: With the available means, it was not possible to clearly determine whether critical security parameters were used for verification. To define a status, the TL relied on the analysis of the DUT's traffic. A certificate was transmitted when the update was sent. This leads to the assumption that only public keys are available on the device.
    Status: **No**

16. Condition: access to device functionality via a network interface in the initialized state is possible
    Justification: The device creates an ad hoc Wi-Fi access point for the initial configuration.
    Status: **Yes**

17. Condition: device functionality that allows security-relevant changes in configuration via a network interface exists
    Justification: The device can be controlled over the web interface. This is the only way to perform security relevant changes over a network interface.
    Status: **Yes**

18. Condition: critical security parameters are transmitted
    Justification: Username and password are transmitted for the user authentication of the web interface.
    Status: **Yes**

19. Condition: critical security parameters are transmitted via remotely accessible network interfaces
    Justification: User authentication is only accessible in the LAN.
    Status: **No**

20. Condition: critical security parameters relating to the device exist
    Justification: Password and username are chosen by the user for the web interface.
    Status: **No**

21. Condition: personal data is transmitted between a device and a service
    Justification: If the cloud functionality is enabled, only usage data is transmitted. This was verified by capturing the network traffic of the DUT.
    Status: **No**

22. Condition: sensitive personal data is transmitted between a device and a service
    Justification: If the cloud functionality is enabled, only usage data is transmitted. This was verified by capturing the network traffic of the DUT.
    Status: **No**

23. Condition: external sensing capabilities exist
    Justification: The device does not have external sensing capabilities.
    Status: **No**

24. Condition: user data is stored on the device
    Justification: User data is not stored on the device.
    Status: **No**

25. Condition: personal data is stored on associated services
    Justification: If cloud functionality is enabled, only usage data is stored on associated services.
    Status: **No**

26. Condition: personal data is stored
    Justification: If cloud functionality is enabled, only usage data is stored.
    Status: **No**

27. Condition: data input via user interfaces or transferred via APIs or between networks in services and devices is supported
    Justification: The device has an App, web interface and an API.
    Status: **Yes**

28. Condition: personal data is processed
    Justification: If the cloud functionality is enabled, personal data is processed during the

registration.
Status: **Yes**

### B.1.2 IXIT documents

This section shows the Implementation eXtra Information for Testing (IXIT) documents for Consumer IoT (CIoT)-1.

- IXIT 1-AuthMech: Authentication Mechanisms
  - ID: AuthMech-1
    - Description: The authentication mechanism restricts the access to the web interface of the Device Under Test (DUT). The mechanism is used for user-to-machine authentication. The mechanism is directly addressable from a network interface. The mechanism uses ComMech-1.
    - Authentication Factor: Username and password (set by user when "Restrict Login" (authentication) is enabled)
    - Password Generation Mechanism: N/A (Authentication mechanism is password set by the user)
    - Security Guarantees: The mechanisms attest that the authenticated entity has a valid password.
    - Cryptographic Details: None
    - Brute Force Prevention: None
- IXIT 2-UserInfo: User Information
  - Documentation of Change Mechanisms: The way to change the authentication values is documented for the user in the user manual.
  - Model Designation: The model designation "Shelly 1 v3" is provided to the user on the top of the DUT's case in plain text.
  - Support Period: Missing
  - Publication of Support Period: Missing
  - Publication of Vulnerability Disclosure Policy: Missing
  - Documentation of Personal Data: The information about processing personal data is documented for the user on the website [1].
- IXIT 4-Conf: Confirmations
  - Confirmation of Update Procedures: Not possible to determine without the SO.
- IXIT 6-SoftComp: Software Components
  - ID: SoftComp-1
    - Description: Firmware is based on "Mongoose OS" [Ltd].

[1] https://my.shelly.cloud/privacy_policy.html

    * Update Mechanism: Firmware can be updated according to UpdMech-1.

- IXIT 7-UpdMech: Update Mechanisms
  - ID: UpdMech-1
    * Description: User-initiated firmware update over web interface. The DUT downloads the firmware from `http://shelly-42-eu.shelly.cloud/firmware/SHSW-1.zip` during the update process. There is an update check mechanism, which is not known in detail. The firmware seems to be protected by a certificate.
    * Security Guarantees: The mechanism seems to provide authenticity and integrity protection for the firmware file. It was not possible to verify this.
    * Cryptographic Details: It could not be determined which certificate in detail is used for integrity protection. While capturing the network traffic of the DUT, a certificate was found.
    * Initiation and Interaction: Checks for new updates are performed automatically by the DUT. If a new update is available, it can be installed over the web interface or mobile app. The user needs to initiate an update over the settings menu.

- IXIT 8-UpdProc: Update Procedures
  - ID: UpdProc-1
    * Description: This cannot be answered without the SO.
    * Time Frame: This cannot be answered without the SO.

- IXIT 10-SecParam: Security Parameters
  - ID: SecParam-1
    * Description: Username and password combination for authentication against the web interface. The combination has no hard-coded identity and is not hard-coded in device software source code.
    * Type: critical
    * Security Guarantees: The combination is not accessible by an attacker so that its confidentiality is ensured.
    * Protection Scheme: An attacker needs access to the file system to change the password.
    * Provisioning Mechanism: Username and password are chosen by the user, then authentication is enabled in the web interface.
    * Generation Mechanism: N/A (SecParam-1 is not used for integrity and authenticity checks of software updates or for protection of communication with associated services)

- IXIT 11-ComMech: Communication Mechanisms
  - ID: ComMech-1

        - Description: The DUT offers a connection for its web interface. This connection is based on IP/TCP/HTTP.
        - Security Guarantees: None
        - Cryptographic Details: None

- IXIT 13-SoftServ: Software Services
  - ID: SoftServ-1
    - Description: Software service is provided over the web interface using HTTP. The service is accessible over the network. The service is accessible in the initialized state.
    - Status: Enabled
    - Justification: The service is necessary to provide the user with the possibility to configure the DUT.
    - Allows Configuration: Yes. The user can access all settings of the device over the web interface.
    - Authentication Mechanism: AuthMech-1

- IXIT 15-Intf: Interfaces
  - ID: Intf-1
    - Description: WLAN interface to connect the user's wireless environment.
    - Type: Network, physical, logical
    - Status: Enabled
    - Disclosed Information: This interface discloses firmware version. This information is security-relevant because it can give an attacker a hint to which CVEs the DUT is vulnerable.
    - Debug Interface: N/A (The interface is not a physical interface)
    - Protection: N/A (The interface is not a physical interface)
  - ID: Intf-2
    - Diescription: The serial interface allows the user to flash the device with alternative software.
    - Type: Physical, logical
    - Status: Enabled
    - Disclosed Information: The serial interface discloses diagnosis information. This information is security-relevant because it can give an attacker complete access to the DUT's software.
    - Debug Interface: Yes, this interface is just used for debugging purposes.
    - Protection: None

- IXIT 21-PersData: Personal Data

- Processing Activities:
  - providing the Services and their functionalities to the User
  - responding to Users' inquires or requests
  - sending information about the Services (such as direct marketing, maintenance or security information)
  - processing and deliveries of purchase orders
  - improvement of the Services and personalized User experience
  - sending a limited number of offers for additional products and services that may be of interest for the User
  - permitting subcontractors to perform Service related activities, provided they are under an obligation of confidentiality and do not use the information for their own benefit without the prior explicit consent of the User
  - complying with applicable law or legal process
  - investigating suspected fraud, harassment, danger to persons or property or other violations of any law, rule or regulation, or the terms or policies for the Services or such of Controller's/Processor's business partners with which the User has committed to comply
  - transfer of information in connection with the sale or merger or change of control of the Controller/Processor or the division responsible for the services with which the Personal Data is associated
  - sharing non-personal or de-identified information with any number of parties, including analytics companies, technology providers and other business partners; or combine it with data from other sources outside of the use of the Services, such as data obtained from Wi-Fi access points
- ID: PersData-1
  - Description: name
  - Obtaining Consent: The user needs to confirm the general terms and conditions prior to registering for the cloud service of the Supplier Organization (SO).
  - Withdrawing Consent: The user has to delete his cloud account.
- ID: PersData-2
  - Description: e-mail adress
  - Obtaining Consent: The user needs to confirm the general terms and conditions prior to registering for the cloud service of the SO.
  - Withdrawing Consent: The user has to delete his cloud account.
- ID: PersData-3
  - Description: MSISDN (mobile number)
  - Obtaining Consent: The user needs to confirm the general terms and conditions prior to registering for the cloud service of the SO.

    * Processing Activities: Refer to PersData-1 “Processing Activities”
    * Withdrawing Consent: The user has to delete his cloud account.

- IXIT 27-UserIntf: User Interfaces
  - ID: UserIntf-1
    * Description: The user can enter configuration data on the web interface accessible on port 80.
  - ID: UserIntf-2
    * Description: The user can enter configuration data on the cloud interface accessible at `my.shelly.cloud`.
  - ID: UserIntf-3
    * Description: The user can enter configuration data on the mobile app, which uses the shelly cloud. The mobile also supports non-cloud usage in the LAN.

- IXIT 28-ExtAPI: External APIs
  - ID: ExtAPI-1
    * Description: Common HTTP API `https://shelly-api-docs.shelly.cloud/gen1/#common-http-api`
  - ID: ExtAPI-2
    * Description: MQTT `https://shelly-api-docs.shelly.cloud/gen1/#mqtt-support`
  - ID: ExtAPI-3
    * Description: CoInternet of Things (IoT) Protocol `https://shelly-api-docs.shelly.cloud/gen1/#coiot-protocol`

- IXIT 29-InpVal: Data Input Validation
  - ID: InpVal-1
    * Description: The user can input a custom name for the DUT in the web interface or the mobile application. Validation is missing: → `<script>alert(1)</script>`
  - **Note**: The DUT has multiple input fields which are not documented here. It can only be guessed what input validations are in place. For a precise analysis, the source code of the device is needed.

### B.1.3 Assessment

This section contains the test cases, organized by provision, against which the CIoT-1 is evaluated. To represent the current situation only mandatory and mandatory conditional provisions are taken into account.

**Provision 4-1** This assessment was conducted as part of this thesis. This means for the assessment, that SO and TL are the same person.

- Test case 4-1-1 (conceptual)
  a) The TL has verified that a justification was given for every recommendation considered not applicable for the DUT. **PASS**
  b) The TL has verified that a justification was given for every recommendation considered to applicable for the DUT. **PASS**
- Verdict: **PASS**

#### Provision 5.1-1

- Test case 5.1-1-1 (conceptual)
  a) The password AuthMech-1 is defined by the user. **PASS**
- Test case 5.1-1-2 (functional)
  a) The TL could not find other authentication mechanisms. **PASS**
- Verdict: **PASS**

#### Provision 5.1-3

- Test case 5.1-3-1 (conceptual)
  a) The DUT has only one authentication mechanism, which is AuthMech-1. AuthMech-1 does not provide integrity and authenticity. This is also not handled by the corresponding communication mechanism ComMech-1. **FAIL**
  b) The TL has assessed that the mechanism according to "Description" is appropriate to achieve the "Security Guarantees". Because there are no security guarantees. **PASS**
  c) No cryptography is used. **PASS**
  d) No cryptography is used. **PASS**
- Test case 5.1-3-2 (functional)
  a) No cryptography is used. **PASS**
- Verdict: **FAIL**

#### Provision 5.1-4

- Test case 5.1-4-1 (conceptual)
  a) The TL has assessed that the change mechanism documented in "Documentation of Change Mechanism" in IXIT 2-UserInfo is considered to be understandable for a user with limited technical knowledge. **PASS**
- Test case 5.1-4-2 (functional)

a) The TL has performed a change of authentication values for AuthMech-1. **PASS**

b) The TL has verified that a) was successful. **PASS**

- Verdict: **PASS**

#### Provision 5.1-5

- Test case 5.1-5-1 (conceptual)
  a) The TL could not identify a brute force protection in the IXIT 1-AuthMech. **FAIL**
- Test case 5.1-5-2 (functional)
  a) The TL has assessed that no further network-based authentication mechanisms exist, that are not listed in IXIT 1-AuthMech. **PASS**
  b) The TL could brute force every network-based authentication mechanism described in IXIT 1-AuthMech. **FAIL**
- Verdict: **FAIL**

#### Provision 5.2-1

- Test case 5.2-1-1 (conceptual)
  a) The publication of the vulnerability disclosure policy is not available. **FAIL**
- Test case 5.2-1-2 (functional)
  a) The DUT does not have a corresponding vulnerability disclosure policy. **FAIL**
  b) Refer to a). **FAIL**
- Verdict: **FAIL**

#### Provision 5.3-2

- Test case 5.3-2-1 (conceptual)
  a) The UpdMech-1 offers security features. It was impossible to determine them in detail, due to the nature of this thesis. The updates are downloaded over HTTP, which means it could be intercepted and modified. The TL could not verify if there are mechanisms in place to protect the integrity. **INCONCLUSIVE**
- Test case 5.3-2-2 (functional)
  a) An MITM is possibile for UpdMech-1 because of the usage of HTTP. But it could be that were is a certificate in place to prevent this. It is not clear which root certificates are used by the DUT. **INCONCLUSIVE**
  b) Due to the time constraints of this assessment this was not possible. **INCONCLUSIVE**
- Verdict: **INCONCLUSIVE**

#### Provision 5.3-3

- Test case 5.3-3-1 (conceptual)
  a) The DUT has only the software component SoftComp-1. SoftComp-1 uses UpdMech-1, which is easy to apply for a user. **PASS**
- Verdict: **PASS**

#### Provision 5.3-7

- Test case 5.3-7-1 (conceptual)
  a) The TL was not abile to determine if the UpdMech-1 provides an integrity and authenticity check. This is because the source code of the DUT was not available and questioning the SO was not possible. **INCONCLUSIVE**
  b) In theory the UpdMech-1 can achieve all security goals. **INCONCLUSIVE**
  c) The TL was not able to determine which cryptography was used. With the available resources as described in test case a was it not possible to understand, which cryptography was used by the SO. **INCONCLUSIVE**
  d) Refer to c). **INCONCLUSIVE**
- Verdict: **INCONCLUSIVE**

#### Provision 5.3-8

- Test case 5.3-8-1 (conceptual)
  a) This cannot be assessed without the SO. **INCONCLUSIVE**
  b) This cannot be assessed without the SO. **INCONCLUSIVE**
- Verdict: **INCONCLUSIVE**

#### Provision 5.3-10

- Test case 5.3-10-1 (conceptual)/(functional)
  a) Apply Test case 5.3-9-1 units a and b.
    * Test case 5.3-9-1 (conceptual)
      a) The TL could not determine if cryptography is used to verify the authenticity of the software. This is due to the missing resources for this assessment (refer to test case 5.3-7-1 test unit c). **INCONCLUSIVE**
      b) The TL could not determine if cryptography is used to verify the integrity of the software. This is due to the missing resources for this assessment (refer to test case 5.3-7-1 test unit c).**INCONCLUSIVE**

  b) The TL could not determine if UpdMech-1 relies on a valid trust relationship. **INCONCLUSIVE**
  c) The TL could not find a not documented update mechanisms. **PASS**
- Verdict: **INCONCLUSIVE**

#### Provision 5.3-13

- Test case 5.3-13-1 (conceptual)
  a) The DUT does not have a public support period. **FAIL**
- Test case 5.3-13-2 (functional)
  a) The DUT does not have a public support period. **FAIL**
  b) Refer to a). **FAIL**
  c) Refer to a). **FAIL**
- Verdict: **FAIL**

#### Provision 5.3-16

- Test case 5.3-16-1 (conceptual)
  a) TL has verified, that the model designation can be obtained in a clearly recognizable way. **PASS**
- Test case 5.3-16-2 (functional)
  a) The TL has verified, that the model designation can be obtained in the described way of recognition in "Model Designation" in IXIT 2-UserInfo. **PASS**
  b) The TL has verified that the model designation is available in simple text and corresponds with the expected model designation described in "Model Designation" in IXIT 2-UserInfo. **PASS**
- Verdict: **PASS**

#### Provision 5.4-1

- Test case 5.4-1-1 (conceptual)
  a) The DUT has only one security parameter. The TL has verified, that the declared "Type" of SecParam-1 is consistent with the "Description". The SecParam-1 is used for authentication and needs to be confidential. This means that SecParam-1 needs to be of type critical. This is the case. **PASS**
  b) The TL has verified, that the "Security Guarantees" of SecParam-1 are enough to achieve integrity and confidentiality protection. **PASS**
  c) The TL has verified, that the "Protection Scheme" of SecParam-1 can provide the claimed "Security Guarantees". **PASS**
  d) The TL could not find security parameters, which are not documented. **PASS**
- Test case 5.4-1-2 (functional)
  a) The TL has verified, that the "Protection Scheme" for SecParam-1 is implemented. **PASS**
- Verdict: **PASS**

#### Provision 5.4-3

- Test case 5.4-3-1 (conceptual)
  a) The DUT does not use security parameters, which are hard-coded in the device software source code. **PASS**
  b) Refer to a). **PASS**
- Test case 5.4-3-2 (functional)
  a) The DUT does not use security parameters, which are hard-coded in the device software source code. **PASS**
- Verdict: **PASS**

#### Provision 5.4-4

- Test case 5.4-4-1 (conceptual)
  a) The DUT has only one security parameter. The TL has verified that SecParam-1 is not used for updates or encryption of communication. **PASS**
  b) SecParam-1 is chosen by the user. The parameter is not generated. **PASS**
- Verdict: **PASS**

#### Provision 5.5-1

- Test case 5.5-1-1 (conceptual)
  a) The DUT has only one communication mechanism. ComMech-1 is used to access the web interface of the DUT. The web interface can be protected with SecParam-1. The confidentiality of SecParam-1 is not provided by ComMech-1. **FAIL**
  b) Refer to a). **FAIL**
  c) ComMech-1 does not use cryptography. **PASS**
  d) Refer to c). **PASS**
- Test case 5.5-1-2 (functional)
  a) The DUT has only one communication mechanism. ComMech-1 does not use cryptography. **PASS**
- Verdict: **FAIL**

#### Provision 5.5-5

- Test case 5.5-5-1 (conceptual)
  a) Test case 5.5-4-1 is applied to SoftServ-1.
    a) AuthMech-1 is referenced as authentication mechanism for SoftServ-1. **PASS**

b) AuthMech-1 only gives authorization if valid credentials are used. **PASS**

c) AuthMech-1 does not use cryptography. AuthMech-1 can be compromised by a man-in-the-middle attack. **FAIL**

d) AuthMech-1 does grant and denies access with the adequate access rights. **PASS**

- Test case 5.5-5-2 (functional)
  a) Test case 5.5-4-2 is applied for SoftServ-1.
    a) The DUT can be accessed by every user in the initialized state. AuthMech-1 needs to be enabled by the user. **FAIL**
    b) Refer to a). **FAIL**
    c) The TL has verified that AuthMech-1 is implemented as documented. **PASS**
- Verdict: **FAIL**

#### Provision 5.6-1

- Test case 5.6-1-1 (conceptual)
  a) The DUT has two interfaces:
    * Intf-1: The interface is needed to operate the device. **PASS**
    * Intf-2: The interface is only used by advanced users. It does not need to be enabled in the initialized state. **FAIL**
- Test case 5.6-1-2 (functional)
  a) The DUT has two interfaces. Both interfaces are enabled as documented. **PASS**
  b) The TL has verified that all interfaces of the DUT are documented. **PASS**
- Verdict: **FAIL**

#### Provision 5.6-2

- Test case 5.6-2-1
  a) The DUT has two interfaces. All disclosed information by both interfaces is labeled by the SO as security-relevant. **PASS**
  b) Intf-2 does not need to be enabled in the initialized state of the DUT. For this reason, the disclosed information could be completely avoided in Intf-2. **FAIL**
- Test case 5.6-2-2
  a) All disclosed information is documented. **PASS**
- Verdict: **FAIL**

#### Provision 5.6-4

- Test case 5.6-4-1 (conceptual)
  a) Intf-2 is labeled as debug interface. The interface does not have a software mechanism to disable it. **FAIL**
  b) Intf-2 is required for flashing alternative software. **PASS**
  c) Intf-2 is not disabled by default. **FAIL**
- Test case 5.6-4-2 (functional)
  a) Intf-2 is enabled as documented. **FAIL**
  b) Only Intf-2 can be used for debugging purposes. **PASS**
- Verdict: **FAIL**

#### Provision 5.13-1

- Test case 5.13-1-1 (conceptual)
  a) Due to the nature of this thesis, the TL could not perfom an assessment. **INCONCLUSIVE**
  b) Refer to a). **INCONCLUSIVE**
- Test case 5.13-1-2 (functional)
  a) Due to the nature of this thesis, the TL could not perform an assessment. **INCONCLUSIVE**
  b) The TL has verified, that all user interfaces of the DUT are described in IXIT 27-UserInf. **PASS**
  c) The TL has verified that all remotely accessible APIs of the DUT are described in IXIT 28-ExtAPI. **PASS**

  i
- Verdict: **INCONCLUSIVE**

#### Provision 6-1

- Test case 6-1-1 (conceptual)
  a) The TL has verified that “Documentation of Personal Data” can be obtained in a suitable way for the consumer. **PASS**
- Test case 6-1-1 (functional)
  a) The TL has verified that the provided information about processing personal data is consistent to the description in “Documentation of Personal Data” in IXIT 2-UserInfo. **PASS**
  b) The TL has verified the obtained information about processing personal data accessing the “Documentation of Personal Data” in IXIT 2-UserInfo match their description in “Processing Activities” in IXIT 21-PersData. This was done be analyzing the network traffic of the DUT. **PASS**

c) The TL has verified that it is understandable described for the user, what personal data is processed. **PASS**

d) The TL has verified that it is understandable described for the user, how and by whom personal data is used. **PASS**

- Verdict: **PASS**

#### Provision 6-2

- Test case 6-2-1 (conceptual)
  a) The TL has verified that for PersData-1, PersData-2 and PersData-3 the consent of the user is given freely, obvious and explicitly. **PASS**
- Test case 6-2-2 (functional)
  a) The TL has verified that for PersData-1, PersData-2 and PersData-3 the consent of the user is obtained as described in the IXIT 21-PersData. **PASS**
- Verdict: **PASS**

#### Provision 6-3

- Test case 6-3-1 (conceptual)
  a) The TL has verified that for PersData-1, PersData-2 and PersData-3 the described way in IXIT 21-PersData is possible at any time. **PASS**
- Test case 6-3-2 (functional)
  a) The TL has verified that for PersData-1, PersData-2 and PersData-3 the consent can be withdrawn as described in IXIT 21-PersData. **PASS**
- Verdict: **PASS**

## B.2 CIoT-2

### B.2.1 Conditions

This section contains the conditions and their justifications for CIoT-2.

1. Condition: passwords are used
   Justification: The device does not use any passwords
   Status: **No**
2. Condition: pre-installed unique per device passwords are used
   Justification: The device does not use any passwords
   Status: **No**

3. Condition: software components are not updateable
   Justification: Zigbee2MQTT does not show an update option. This does not prove that no update mechanisms are implemented. It was not possible with the information given to find an update mechanism. During a web research the TL could not find information about an update mechanism.
   Status: **Yes**
4. Condition: the device is constrained
   Justification: The device is limited in its storage capacity. Assuming no update mechanism is implemented.
   Status: **Yes**
5. Condition: the device is not constrained
   Justification: The DUT is constrained.
   Status: **No**
6. Condition: telemetry data being collected
   Justification: While analyzing the traffic of the device, no telemetry data could be identified.
   Status: **No**
7. Condition: personal data is processed on the basis of consumers' consent
   Justification: There is no way of inputting personal data into the device.
   Status: **No**
8. Condition: the device allowing user authentication
   Justification: The device does not have user authentication.
   Status: **No**
9. Condition: the device supports automatic updates and/or update notifications
   Justification: The device has no update mechanism.
   Status: **No**
10. Condition: a hard-coded unique per device identity is used for security purposes
    Justification: The device does not use a hard-coded unique per device identity for security purposes.
    Status: **No**
11. Condition: updates are delivered over a network interface
    Justification: The device has no update mechanism.
    Status: **No**
12. Condition: an update mechanism is implemented
    Justification: The device has not update mechanism.
    Status: **No**
13. Condition: a debug interface is physically accessible
    Justification: The device is covered with a plastic casing. During the tests, it was not possible to break open this casing. Considering these circumstances, no physically accessible debug interface was found.
    Status: **No**
14. Condition: sensitive security parameters are stored persistently
    Justification: The device is connected via ZigBee. Zigbee uses several keys for encryption.

These keys need to be stored on the device.
Status: **Yes**

15. Condition: critical security parameters used for integrity and authenticity checks of software updates in device software or for protection of communication with associated services in device software exist
Justification: The device does not have an update mechanism. The device does not communicate with associated services.
Status: **No**
16. Condition: access to device functionality via a network interface in the initialized state is possible
Justification: The device is connected via Zigbee, which is accessible in the initialized state.
Status: **Yes**
17. Condition: device functionality that allows security-relevant changes in configuration via a network interface exists
Justification: The device is connected via Zigbee. The sensor of the device can be calibrated over Zigbee. This can be security relevant if the recorded sensor data is used for smart home automations. One example would be opening and closing windows. In a smart home context, it is unlikely that the sensor is used in such a context.
Status: **No**
18. Condition: critical security parameters are transmitted
Justification: The device is connected via Zigbee. Keys need to be exchanged for the encryption of Zigbee transfer.
Status: **Yes**
19. Condition: critical security parameters are transmitted via remotely accessible network interfaces
Justification: The Zigbee network key is transmitted.
Status: **Yes**
20. Condition: critical security parameters relating to the device exist
Justification: The device is connected via Zigbee. Zigbee devices can come with an installation code. The usage of an installation code requires out-of-band communication with the trust center. This is not the case at the initialization of this device.
Status: **No**
21. Condition: personal data is transmitted between a device and a service
Justification: The device is only connected via Zigbee. This means that the device cannot communicate with a service.
Status: **No**
22. Condition: sensitive personal data is transmitted between a device and a service
Justification: The device is only connected via Zigbee. This means that the device cannot communicate with a service.
Status: **No**
23. Condition: external sensing capabilities exist
Justification: The device has the capabilities to sense temperature, humidity and air pressure.

Status: **Yes**

24. Condition: user data is stored on the device
    Justification: The device only stores sensing data.
    Status: **No**
25. Condition: personal data is stored on associated services
    Justification: The device cannot communicate with associated services.
    Status: **No**
26. Condition: personal data is stored
    Justification: It is not possible to enter user data in the device.
    Status: **No**
27. Condition: data input via user interfaces or transferred via APIs or between networks in services and devices is supported
    Justification: The device can be calibrated over Zigbee.
    Status: **Yes**
28. Condition: personal data is processed
    Justification: The device only processes sensing data.
    Status: **No**

### B.2.2 IXIT documents

This section contains the IXIT documents of CIoT-2.

- IXIT 2-UserInfo: User Information
  - Documentation of Sensors: DUT has a temperature, air pressure and a humidity sensor.
  - Publication of Vulnerability Disclosure Policy: The DUT is manufactured by Lumi Technology Co., Ltd but sold by Xiaomi. The manufacturer does not have a vulnerability disclosure policy. The seller provides a program on the website [2]. This website is not given in the manual. It was found by a google.de search.
  - Support Period: Missing
  - Publication of Support Period: Missing
  - Model Designation: The Model designation is printed in clear text on the bottom auf the device.
- IXIT 10-SecParam: Security Parameters
  - ID: SecParam-1
    - Description: Zigbee network key is used to encrypt all traffic in the zigbee network. The key is used on the Zigbee network layer (NWK).
    - Type: critical
    - Security Guarantees: The key is not accessible by an attacker so that its confidentiality is ensured.

[2] https://trust.mi.com/misrc/response

        * Protection Scheme: The key is obtained via secure key exchange procedure. An attacker needs access to the file system of the DUT to gain access to the key.
        * Provisioning Mechanism: The parameter is assigned by the Zigbee coordinator during adoption.
        * Communication Mechanisms: ComMech-1

- IXIT 11-ComMech: Communication Mechanisms
  - ID: ComMech-1
    * Description: Zigbee is used for wireless connection.
    * Security Guarantees: Zigbee has several security features.
    * Cryptographic Details: Zigbee encryption uses 128-bit AES.

- IXIT 15-Intf: Interfaces
  - ID: Intf-1
    * Description: Zigbee
    * Type: Network, physical, logical
    * Status: enabled
    * Discilosed Information: The Zigbee interface discloses the firmware version and hardware version of the DUT. The DUT also discloses several information about the Zigbee components used. This information is security-relevant because it can give an attacker a hint to which CVEs the DUT is vulnerable. This information is only accessible if the attacker controls the connected Zigbee coordinator.

    i

- IXIT 22-ExtSens: External Sensor
  - ID: ExtSens-1
    * Description: temperature sensor: -20° – +50°C, ±0.3°C (-4° –122°F ±0.54°F)
  - ID: ExtSens-2
    * Description: humidity sensor: 0 – 100% relative humidity, ±3%
  - ID: ExtSens-3
    * Description: air pressure sensor: 30 kPa – 110 kPa, ±0.12 kPa

- IXIT 27-UserIntf: User Interfaces
  - ID: UserIntf-1
    * Description: The user can enter configuration data as a command over Zigbee.

- IXIT 28-ExtAPI: External APIs
  - The DUT has no external API.

- IXIT 29-InpVal: Data Input Validation
  - The TL could not find any input validation.

### B.2.3 Assessment

This section contains the test cases, organized by provision, against which the CIoT-2 is evaluated. To represent the current situation only mandatory and mandatory conditional provisions are taken into account.

**Provision 4-1** This assessment was conducted as a part of this thesis. This means that SO and TL are the same person.

- Test case 4-1-1 (conceptual)
  a) The TL has verified that a justification was given for every recommendation considered not applicable for the DUT. **PASS**
  b) The TL has verified that a justification was given for every recommendation considered applicable for the DUT. **PASS**
- Verdict: **PASS**

#### Provision 5.2-1

- Test case 5.2.1.1
  a) Xiaomi provides a website, which is publicly available for anybody. **PASS**
- Test case 5.2.1.2
  a) The TL has verified that the website is publicly available. **PASS**
  b) The TL has verified that the policy contains:
    * contact information: security@xiaomi.com **PASS**
    * information on timelines: Xiaomi will respond within 48 hours. The actual vulnerability response time can vary. **PASS**
- Verdict: **PASS**

#### Provision 5.3-13

- Test case 5.3-13-1 (conceptual)
  a) The publication of support period in IXIT 2-UserInfo is missing. **FAIL**
- Test case 5.3-13-2 (functional)
  a) The publication of support period in IXIT 2-UserInfo is missing. **FAIL**
  b) Refer to a) **FAIL**
  c) Refer to a) **FAIL**
- Verdict: **FAIL**

#### Provison 5.3-16

- Test case 5.3-16-1 (conceptual)
  a) The TL has verified that the model designation can be obtained as described in IXIT 2-UserInfo “Model Designation”. **PASS**
- Test case 5.3-16-2 (functional)
  a) The TL has verified that the model designation is written in clear text on the bottom of the device. **PASS**
  b) The TL has verified that the model designation is written in simple text. **PASS**
- Verdict: **PASS**

#### Provision 5.4-1

- Test case 5.4-1-1 (conceptual)
  a) iThe TL has verified that the “Type” of SecParam-1 is consistent with the description. **PASS**
  b) The SecParam-1 is acqired with a secure key exchange procedure. This procedure guarantees confidentiality and integrity. It is not clear if SecParam-1 is protected by input validation. **FAIL**
  c) Refer to b) **FAIL**
- Test case 5.4-1-2 (functional)
  a) It was not possible to verify that an input validation is in place. **FAIL**
- Verdict: **FAIL**

#### Provision 5.4-3

- Test case 5.4-3-1 (conceptual)
  a) SecParam-1 is the only parameter. It is not hard-coded in the software. **PASS**
  b) Refer to a) **PASS**
- Test case 5.4-3-2 (functional)
  a) No parameter is hard-coded in the device software. **PASS**
- Verdict: **PASS**

#### Provision 5.5-1

- Test case 5.5-1-1 (conceptual)
  a) Zigbee can guarantee confidentiality by encryption. It also can guarantee integrity by the use of checksums. **PASS**
  b) Refer to a) **PASS**
  c) AES 128-bit is used by ComMech-1 and can be found in SOGIS Agreed Cryptographic Mechanisms [Gro20]. **PASS**
  d) There is no knowledge about a vulnerability of AES 128-bit. **PASS**
- Test case 5.5-1-2 (functional)
  a) ComMech-1 was captured and analyzed. All traffic captured was encrypted with a network key. The encryption AES 128-bit was used for that. **PASS**

#### Provision 5.5-7

- Test case 5.5-7-1 (conceptual)
  a) Test case 5.5-1-1 is applied to ComMech-1.
    a) ComMech-1: Zigbee can guarantee confidentiality by encryption. It also can guarantee integrity by the use of checksums. **PASS**
    b) ComMech-1: Refer to a) **PASS**
    c) AES 128-bit is used by ComMech-1 and can be found in SOGIS Agreed Cryptographic Mechanisms [**?**]. **PASS**
    d) There is no knowledge about a vulnerability of AES 128-bit. **PASS**
- Test case 5.5-7-2 (functional)
  a) Test case 5.5-1-2 is applied to ComMech-1.
    a) ComMech-1 was captured and analyzed. All traffic captured was encrypted with a network key. The encryption AES 128-bit was used for that. **PASS**
- Verdict: **PASS**

#### Provision 5.6-1

- Test case 5.6-1-1 (conceptual)
  a) The DUT only has the interface Intf-1, which is needed. **PASS**
- Test case 5.6-1-2 (functional)
  a) Intf-1 is enabled as declared. **PASS**
  b) The TL could not find a non-declared interfaces. **PASS**
- Verdict: **PASS**

#### Provision 5.6-2

- Test case 5.6-2-1 (conceptual)
  a) All disclosed information is indicated as security relevant. **PASS**
  b) The DUT has no update mechanism. Because of that there is no reason to disclose the firmware version. **FAIL**
- Test case 5.6-2-2 (functional)
  a) Only the declared information of the IXIT 15-Intf can be found in the authenticated state. **PASS**
- Verdict: **FAIL**

#### Provision 5.8-3

- Test case 5.8-3-1 (functionalu)
  a) The DUT is advertised with its 3 documented external sensing capabilities. The external sensing capabilities can also be found in the manual. **PASS**
  b) The external sensing capabilities are understandable for a user with limited technical knowledge. **PASS**
  c) The TL has verified that all sensing capabilities of the DUT are documented. **PASS**
- Verdict: **PASS**

#### Provision 5.13-1

- Test case 5.13-1-1 (conceptual)
  a) The TL has verified that all input methods are documented in the IXITs. **PASS**
  b) The DUT has no input validation methods. **PASS**
- Test case 5.13-1-2 (functional)
  a) The DUT has no input validation methods. **FAIL**
  b) The TL has verified that all user interfaces of the DUT are described in IXIT 27-UserIntf. **PASS**
  c) The DUT has no API. **PASS**
- Verdict: **FAIL**

# C Capture files

For the sake of the environment, no capture files are appended. However, all capture files are available in a GitHub repository. The access to that repository is available from the author of this thesis.

# Bibliography


[Ass22a] Home Assistant. Website of home assistant. https://www.home-assistant.io/, 2022. Visited last on: 11.11.2022.

[Ass22b] Home Asssistant. Zigbee home automation integration. https://www.home-assistant.io/integrations/zha/, 2022. Visited last on: 11.11.2022.

[Bai12] Eric Baize. Developing secure products in the age of advanced persistent threats. *IEEE Security & Privacy*, 10(3):88–92, 2012.

[BSI22a] BSI. Bsi tr-02102 kryptographische verfahren: Empfehlungen und schlüssellängen. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html, 2022. Visited last on: 12.11.2022.

[BSI22b] BSI. Bsi tr-03173: Amendments for conformance assessments based on etsi en 303 645/ts 103 701. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03173/TR-03173.pdf?__blob=publicationFile&v=5, 2022. Visited last on: 12.11.2022.

[Clo22] Cloudflare. Was ist mirai? https://www.cloudflare.com/de-de/learning/ddos/glossary/mirai-botnet/, 2022. Visited last on: 10.11.2022.

[Com21] European Commission. Commission delegated regulation (eu) of 29.10.2021 supplementing directive 2014/53/eu of the european parliament and of the council with regard to the application of the essential requirements referred to in article 3(3), points (d), (e) and (f), of that directive. https://single-market-economy.ec.europa.eu/system/files/2021-10/C_2021_7672_F1_COMMISSION_DELEGATED_REGULATION_EN_V10_P1_1428769.PDF, 2021. Visited last on: 12.11.2022.

[de22] dresden elektronik. Zshark: Software to capture zigbee traffic with conbee2. https://phoscon.de/en/conbee/software#zshark, 2022. Visited last on: 11.11.2022.

[ETSa] ETSI. Cyber security for consumer internet of things: Baseline requirements. Available from: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf.

[ETSb] ETSI. Cyber security for consumer internet of things: Conformance assessment of baseline requirements. Available from: https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf.

[ETSc] ETSI. Guide to cyber security for consumer internet of things. Available from: https://www.etsi.org/deliver/etsi_tr/103600_103699/103621/01.01.01_60/tr_103621v010101p.pdf.

[Fow99] K. Fowler. Documentation-do or die! *IEEE Instrumentation & Measurement Magazine*, 2(2):53–56, 1999.

[Gar17] Gartner. Leading the iot. https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf, 2017. Visited last on: 10.11.2022.

[Gro20] SOG-IS Crypto Working Group. Sog-is crypto evaluation scheme, agreed cryptographic mechanisms. https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf, 2020. Visited last on: 12.11.2022.

[Ltd] Cesanta Software Ltd. Mongoose os. Available from: https://mongoose-os.com/.

[NXP20] NXP. Sesip delivers cost-effective security evaluation for iot. https://www.nxp.com/docs/en/brochure/SESIP-BROCHURE.pdf, 2020. Visited last on: 11.11.2022.

[OPL+19] Hyeontaek Oh, Sangdon Park, Gyu Myoung Lee, Hwanjo Heo, and Jun Kyun Choi. Personal data trading scheme for data brokers in iot data marketplaces. *IEEE Access*, 7:40120–40132, 2019.

[Pos] Howard Poston. What are black box, grey box, and white box penetration testing? [Updated 2020]. Available from: https://resources.infosecinstitute.com/topic/what-are-black-box-grey-box-and-white-box-penetration-testing/.

[Sha20] Sanjay Sharma. *GDPR's Scope of Application*, pages 45–57. 2020.

[STA21] Yuan Stevens, Stephanie Tran, and Ryan Atkinson. See something, say something? coordinating the disclosure of security vulnerabilities in canada's infrastructure. In *2021 IEEE International Symposium on Technology and Society (ISTAS)*, pages 1–5, 2021.

[Uni22] European Union. Ce label. https://europa.eu/youreurope/business/product-requirements/labels-markings/ce-marking/index_de.htm, 2022. Visited last on: 11.11.2022.

[za17] zigbee alliance. zigbee specification revision 22 1.0. https://csa-iot.org/developer-resource/specifications-download-request/, 2017. Visited last on: 11.11.2022.