Secura

A BUREAU VERITAS COMPANY

CONSUMER IOT STANDARDS AND CERTIFICATION

What are the best options for your products?

SECURA

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)88 888 3100
E info@secura.com
W secura.com

Follow us on

1. Consumer IoT Products & Threats Landscape

The current rise of the Internet of Things (IoT) ecosystem is something that cannot be denied. For example, smart building elements, vehicles connected to a smart transport infrastructure, or gadgets that can be controlled remotely through mobile applications and cloud are only a few examples of the current state. Moreover, the rate at which IoT is expanding is currently accelerating. Based on recent reports, it is expected that 5.8 billion IoT endpoints will be in use by the end of 2020, only in automotive and enterprise environments[1].

Whenever the term IoT is mentioned, the thoughts are initially running towards smart consumer gadgets. In fact, this paradigm, even though slightly outdated, is still correct for a large extend. Based on reports, the market of consumer IoT products is projected to reach 153.8 Billion $ by 2026[2]. However, together with the increase in connected products volume and functionality, the cybersecurity risks associated with these products are strongly increasing as well. Due to the volume of this market, as well as its connectivity to other high-risk environments, this becomes a serious issue.

The IoT is truly a holistic concept, resulted by the fact that the world becomes more and more connected. The combination of "smart" devices, mobile or web applications used to interact with them and cloud services allowing them connect with each other lead to the development of overlapped IoT ecosystems.

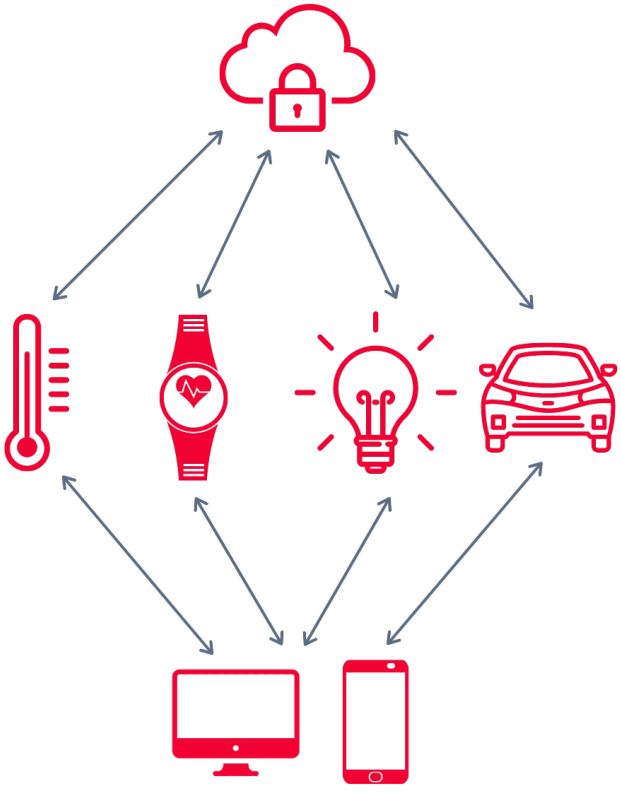


Table of Contents

[1] https://informationmatters.net/internet-of-things-statistics/
[2] https://www.verifiedmarketresearch.com/product/consumer-iot-market/

This also allows for a better understanding of how security threats can affect the domain of consumer IoT products. We know that the security of a general system, network and ultimately, home, is as strong as the weakest link involved. The multitude of "smart" consumer gadgets that increasingly populate our homes opens up multiple potential doors towards personal sensitive data.

In most of the cases, the actual component or gadget that has an embedded vulnerability is not the actual target of an attacker. Imagine for example a smart surveillance camera that is used in a home environment. The camera is connected to the home router, therefore to the trusted network. All the other smart appliances and devices which are found in the home are directly connected to the same network.

In case an attacked can exploit a vulnerability embedded in the mentioned camera and get access to the main home network, then it would be theoretically possible to access the other devices or information shared on the network. And if a camera itself does not sound like a critical component in case of a security attack, then how about the connected smart door locks, the in-home alarm system, the connected personal medical devices or the smart fire-detection system? If we see things in this perspective, we can start observing that an apparent "inoffensive" gadget can actually be much more concerning than initially thought.

With these aspects in mind, in the last years there was an intense focus on developing efficient standards aimed at addressing the security of consumer IoT products. Together with the standards, also options for certification schemes were developed.

2. Reference Standards & Certification Schemes for Consumer IoT

Starting from the premise that consumer IoT products need to start having a strong focus on their security capabilities and functionalities, in the last years we have seen a wide range of standards, frameworks and best practice documents published on this matter. What started as a promising approach to make security more concrete in such products, quickly transformed into a rather confusing aspect for manufacturers: If there are so many available publications providing guidance and security requirements for IoT products, which one is the best and which one should be followed?

To briefly summarize, at this moment we have in place an extensive list of publications which manufacturers can consider in order to approach security into their connected products. Without the purpose of making this an exhaustive list, relevant examples include the **IoT Security Foundation Framework, IEC 62443, OWASP IoT requirements, GSMA IoT requirements, UL 2900 family, ENISA Best Practices for connected products**, or the **ETSI EN 303 645**. The list can of course become much more extensive if we consider additional publications that are not issued by smaller security organizations, and furthermore if we consider other local requirements which are published for specific countries and regions.

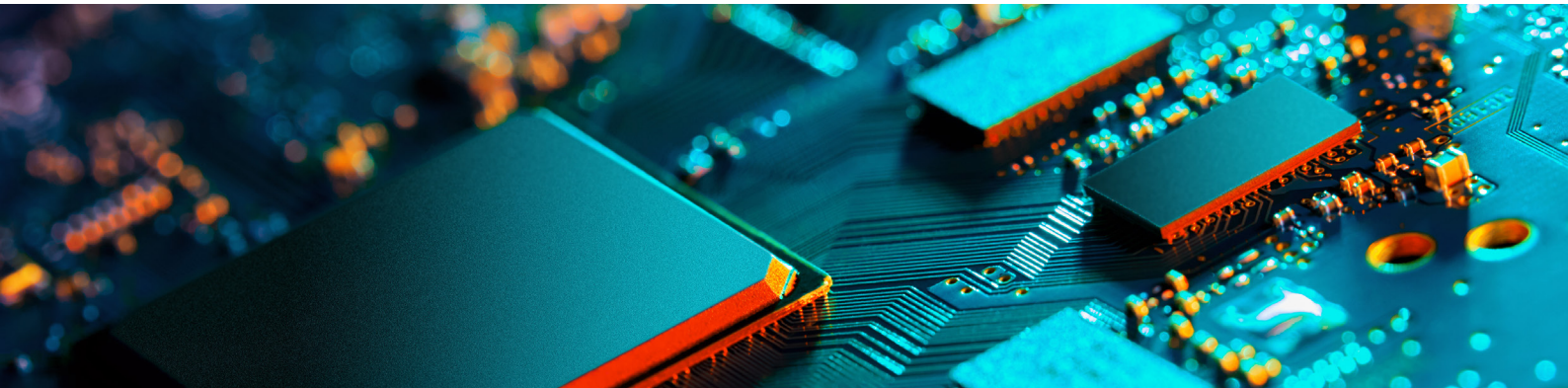
The **ETSI EN 303 645** standard was published with the main idea to provide a clearer view on consumer IoT products real-life risks and vulnerabilities, and create a feasible testing and evaluation approach. With this standard quickly obtaining more and more attention, starting from the EU level, many manufacturers have started to get interest into its security requirements. Furthermore, ETSI is also working on publishing a methodology for performing validation testing in line with the requirements of the ETSI EN 303 645, which will be documented in the ETSI TS 103 701 publication.

Besides the topic of issuing relevant standards, there is of course the discussion on certification options for smart devices. Here the concerns can be even stronger, as a good certification program for consumer IoT needs to have in place several aspects, such as:

- Clear requirements and testing methodology
- Smooth assessment and certification process, resulting in a limited effort approach
- High international visibility and recognition of the resulting certificate

Furthermore, there is the topic of creating a certification program that can successfully address the various layers of a consumer device, and also the supply chain interaction behind its development. Having these constraints in mind, there are currently several certification options that are possible options for manufacturers. **Common Criteria** certification is arguably the most recognized certification program for IT products, with its results recognized in many countries across multiple continents. To provide some alternatives to Common Criteria, the recent years have seen the development of other, consumer focused certification schemes, such as SESIP (focused on the IC components and platforms used for IoT), IoT Security Foundation label, or the public and private certification schemes operating based on the ETSI EN 303 645 standard.

In this multitude of available standards and certification options, it is critical for manufacturers to get the best decision regarding the specific standard or certification in which they will invest their efforts. With the aim of providing more clarity on the topic, the rest of this document will focus on two specific programs, the Common Criteria international security certification and the ETSI EN 303 645 based certification.



3. Focus on Common Criteria

3.1. What is Common Criteria?

The **Common Criteria for Information Technology Security Evaluation**, shortly referred to as Common Criteria or CC, is an **international standard for independent security evaluation and certification of IT products** implemented as hardware, firmware or software.

Common Criteria consists of three main parts plus the recommended methodology to perform evaluations:

- **Part 1:** Introduction and general model, April 2017, version 3.1, revision 5;
- **Part 2:** Security functional components, April 2017, version 3.1, revision 5;
- **Part 3:** Security assurance components, April 2017, version 3.1, revision 5;
- **Common Methodology for Information Technology Security Evaluation** (further referred to as CEM), April 2017, version 3.1, revision 5.

Several stakeholders are involved in a CC evaluation, as follows:

- **Sponsor of the evaluation**. The party that plans to certify a product (could be either a developer of the product or a third party).
- **National certification scheme.** National CC scheme, providing own set of tailored rules for evaluation and certification of IT products, based on the CC standard.
- **IT Security Evaluation Facility (ITSEF).** Accredited and licensed lab specialized in performing CC evaluations for a particular class of IT products.

Under Common Criteria, it is possible to evaluate and certify a broad range of products, including:

- Smart cards and ICs
- Software and application products
- Operating systems
- Antivirus and network protection software
- Network equipment
- Embedded devices such as IoT, printers, automotive components, medical devices, etc.

A Common Criteria evaluation can be conducted based on seven increasing assurance levels, each of the levels coming with more stringent requirements that need to be fulfilled by the product, as well as the evaluation methodology. A resulting Common Criteria certificate is mutually recognized in a wide range of countries, spread across the EU, Asia, North America, Australia or UK. Given its history, tradition and large number of issued certificates, Common Criteria is one of the most recognized certification methodologies across the world.

3.2. How to Test & Certify based on Common Criteria?

Common Criteria introduces **seven different levels of evaluation (EAL1 to EAL7)** depending on the level of assurance in the security of the evaluated product. According to CC, higher assurance results from the application of greater evaluation effort. The increasing level of effort is based upon:

- **Depth of Evaluation** - the effort is greater because it is deployed to a finer level of design and implementation detail;
- **Coverage of Evaluation** – the effort is greater because more evaluation requirements are in scope
- **Rigor of Evaluation** - the effort is greater because it is applied in a more structured, formal manner.

The assurance increases with every level and the "default" levels in a CC evaluation are identified in the following way:
EAL1 – functionally tested;
EAL2 – structurally tested;
EAL3 – methodically tested and checked;
EAL4 – methodically designed, tested and reviewed;
EAL5 – semi-formally designed and tested;
EAL6 – semi-formally verified design and tested;
EAL7 – formally verified design and tested.

Selecting the desired evaluation level is based on the preference of the manufacturer. Typically, embedded products including consumer IoT devices are suited for a lower level evaluation (e.g. EAL 1 to EAL 3). This is due to the less critical security risks that are directly applicable to these devices, compared for example with products like ICs or e-passports, which are typically better suited for higher evaluation levels.

The evaluation activities include a combination of several elements, such as:

- Evaluation of the product's Security Target (the overview of the product's security scope and capabilities)
- Design review of the products and overview of its interfaces and architecture
- Review of the product's guidance requirements
- Review of the product's development life cycle processes
- Validation and penetration testing of the product's security capabilities.

The conducted assessment activities are documented in several deliverables that are shared with the certification scheme. Once these deliverables are agreed by the scheme, a final certificate is issued and published on the Common Criteria portal.

4. Focus on ETSI EN 303 645

4.1. What is ETSI EN 303 645?

The **ETSI EN 303 645 norm** is currently one of the **main standards for the assessment and validation of IoT products**, with a special focus and relevance on the side of consumer IoT. Originally inspired by the UK IoT Code of Practice for security, the ETSI EN 303 645 grew up to an EU recognized framework, therefore being a very good reference for upcoming EU level certification schemes for consumer IoT products.

The ETSI EN 303 645 norm is designed to provide an efficient, baseline assessment methodology for the evaluation of IoT products and solutions. **Aspects of this methodology include:**

- Password security
- Secure software updates
- Security of interfaces and data communications
- Product's availability
- Completeness and correctness of user guidance
- Vulnerability disclosure procedures and patch management
- Product logging
- Protection of personal data
- Validation of data inputs

4.2. How to Test and Certify Based on ETSI EN 303 645?

The standard itself aims to provide a baseline of security requirements, therefore, as expected, the testing depth is medium. General security evaluation knowledge related to hardware, software and protocols security are sufficient in order to go through the requirements. The difficulty comes however from interpreting some requirements which are made "flexible" on purpose. For example, the requirement "The product shall have an update mechanism for the secure installation of updates" requires first of all consensus on what is meant by "secure installation", especially in sense of what is good enough and what is not good enough.

There are multiple other instances of such requirements where common interpretation is needed in order to reach a testing verdict. In order to help in creating a common base for evaluation and testing, ETSI is currently working on a separate document, ETSI TS 103 701, aimed at providing an evaluation methodology based on the ETSI EN 303 645 standard.

From a certification point of view, there are already some options that manufacturers can have in place in order to obtain a compliance label based on the ETSI IoT standard. The existing certification schemes are at the same time quite new, given the fact that the standard itself has been formally published in 2020. Examples of national initiatives include the **Finland TRAFICOM certification scheme**, as well as the **Singapore Cybersecurity Label Scheme (CLS)**, both operating based on the requirements of the ETSI standard. From a private point of view, some Certification Body companies have developed their own programs focused on providing compliance labels, and example in such case being the Bureau Veritas certification program based on ETSI EN 303 645.

Given the fact that certification options based on ETSI EN 303 645 are relatively new, the number of already certified products is smaller than compared with other "classic" approached such as Common Criteria. However, given the quick market adoption of the standard, combined with the smooth and limited effort approach that some of these schemes are adopting, it is expected that such labels will become much more common in the next years.

5. What is the Best Option for your Product?

As it was highlighted above in this document, currently manufacturers of consumer IoT products have several options in place in order to allow for certification of their products. Some specific case studies have been presented for the Common Criteria and ETSI EN 303 645 certification schemes.

In the end, which one of these options is the best for manufacturers to take, and based on which can this decision be taken? While the final answer will depend strongly on certain aspects that are manufacturer related, the table on the next page aims to summarize the characteristics of these schemes against several selected aspects.

Characteristic	Common Criteria Certification	ETSI EN 303 645 Certification
International recognition	**Common Criteria is widely known**, being mutually recognized in multiple countries spread across the world.	Certification schemes based on ETSI EN 202 645 are relatively new, therefore the international recognition of these certificates is slowly emerging. That being said, manufacturers are free to promote or display the certificate on their products.
Value of certificate	**A Common Criteria certificate is mutually recognized in multiple countries,** all over the world. Many times, large institutions or asset owner organizations will ask for a CC certificate in order to sign a partnership with a device manufacturer. Finally, having a CC certificate can represent a strong differentiator against competitors.	While the international recognition of these schemes is gradually increasing, the value of the certificate is already quite good. **ETSI EN 202 645 is already a well known standard in the domain of consumer IoT.** A certificate or label based on this standard will therefore be an important confirmation of the product's capabilities.
Flexibility of the process	Common Criteria **is a very carefully defined evaluation process**. All the evaluation activities are documented, and a project cannot deviate from them. The relation between the stakeholders is clear and strict.	Certification approaches based on ETSI EN 202 645 often **allow for interpretation of requirements**. While a product that does not fulfill a large part of the requirements will likely not obtain a certificate, there is currently room for alignment, such that manufacturers can defend the design decisions that they adopted for their products.

Required effort 	The effort depends per the level of evaluation, and **will progressively increase among the seven possible levels in Common Criteria**. As a rought indication, 40 – 60 person days can be expected for a Level 2 evaluation, which is a well suited level for consumer IoT devices.	Certification schemes based on ETSI EN 202 645 were designed to be market accessible. Therefore, **the expected effort can be generally considered lower than for example a Common Criteria evaluation.** A rough indication can be around 20-25 person days, which depends strongly on the type and complexity of the product.
Required involvement from the manufacturer 	In a CC evaluation, **the manufacturer holds an important role**. The manufacturer is responsible for drafting the evaluation evidence, in a particular format required by the CC scheme. A site-audit can be part of the evaluation process as well.	These schemes have been developed in order to provide **a smooth process, minimizing where possible the involvement of the manufacturer.** Often there is a clear checklist of documents that need to be provided by the manufacturer in the beginning, such that the rest of the evaluation process can be performed as much as possible by the laboratory without further support.
Project Duration 	Typically, **Common Criteria projects do not result in quick verdicts.** Of course, the duration strongly depends on the evaluation level. As an indication, a duration of 3-4 months can be considered relevant for an evaluation based on Level 2[3].	**The duration of the project, including the drafting of the final report and issuing of the certificate is minimized**, the whole process being possible to be finalized within 1 month.
Specific Value for Consumer IoT Products 	Common Criteria is a highly recognized evaluation and certification scheme. Therefore, the value of such certificate will be of importance, including in the domain of consumer IoT products. Besides offering possibilities for governmental or large asset owners access, a CC certificate **can be an important differentiator against the competitors.**	A certification based on ETSI EN 202 645 could be an important milestone for a manufacturer of consumer IoT products. While not as internationally recognized as a Common Criteria certificate, such a certificate will represent an **appreciated label particularly among users and integrators of consumer equipment.**

[3] *This indication is given considering an evaluation performed under the Dutch Common Criteria scheme, NSCIB.*

6. Conclusion

This document aimed to describe the existing standards and certification options applicable for the domain of consumer IoT products. Luckily, we do not lack in terms of available standards. In fact, this can even be considered to be an element that sometimes provides confusion among the manufacturers: which standard or certification scheme would be the best one to follow.

Common Criteria has traditionally been the main international certification program for IT products, applicable therefore also for consumer IoT devices. On the other hand, the ETSI EN 303 645 standard came with an approach that aims to make the evaluation of these devices smoother, and with less involvement from the manufacturer. That could in particular be useful for small-scale IoT manufacturers, due to the less stringent evaluation methodology and less extensive required effort.

Both Common Criteria and ETSI EN 303 645 can result in valuable certificates. While Common Criteria will provide direct international recognition, ETSI EN 303 645 certification is a label that will attract the attention especially among users and integrators of consumer IoT products.

Would you like more guidance on which option might be the best for your product, or more information about consumer IoT standards and certification? If yes, feel free to contact Secura's experts for more help.

About Secura

Secura is your independent cybersecurity expert. Secura provides insights to protect valuable assets and data. We make cybersecurity tangible and measurable in the field of IT, OT and IoT. With security advice, testing, training and certification services, Secura approaches cybersecurity holistically and covers all aspects from people, policies, organizational processes to networks, systems, applications and data.

For more information, please visit: **secura.com.**

Keep updated with the latest insights on digital security and subscribe to our periodical newsletter: secura.com/subscribe.

Follow us on

Contact us today at info@secura.com or visit secura.com for more information.

SUBSCRIBE

TO OUR NEWSLETTER

Secura

A BUREAU VERITAS COMPANY

BUREAU VERITAS

Shaping a World of Trust