EUROPEAN UNION AGENCY
FOR CYBERSECURITY

LABELLING CYBERSECURITY CERTIFICATION

Recommendations for Labelling
European Certification and Qualification

NOVEMBER 2021 V15.11.2021

ABOUT ENISA

REMINDER : IPR NOTICE !!! to be updated with new rules

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes[1] with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency collaborates with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure.

More information about ENISA and its work can be found here: www.enisa.europa.eu

CONTACT

To contact the authors please use ……@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS

Marie-Laure LULE, ENISA
Credit @ Jose RUIZ GUARDA, Thomas NIESSEN, Danilo D'ELIA, Yoann KASSIANIDES

ACKNOWLEDGEMENTS

Over the course of this study, we have received valuable input and feedback from 42 participants[2].

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN SHOULD BE PLACED HERE, DOI SHOULD BE PLACED HERE (IF APPLICABLE)

[1] ISO/IEC 17065:2012 for the meaning of ICT product, service and software
[2] CIRCABC platform see List of participants in Annex XX

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Cybersecurity Act (EU, 2019) aims to promote EU labelled certifications across the European Union in a more significant market. In this context, labelling is a new challenge, a window of opportunity for all cybersecurity stakeholders in Europe to show they care. However, beyond technical security measures, the adoption of a labelling strategy is raising many new legal, policy and operational challenges, broad and complex in scope, that needs to be investigated. The rapid rate of change in technology has outpaced the ability of the associated policy, legal, and regulatory structures to adapt, leaving no clear security framework to follow.

For these reasons, ENISA is clarifying in this report a set of recommendations in the field of Labelling Cybersecurity Certification. This report lays down the flow of work, the orientations and recommendations for the establishment and application of a future EU cybersecurity labelling policy as a requirement flexible enough to evolve smoothly and cope with the speed of innovation in the European cybersecurity market.

As a result of this work, after taking into consideration all the background research conducted, the views expressed by the experts interviewed, and the good practices and security measures identified, a series of recommendations has been developed.

LEGAL - In theory, each scheme may define its own appropriate labelling requirements. In reality, ENISA will favour the establishment of an overarching label (or family of labels) under the EU Cybersecurity Act. Therefore, it is the objective of the Labelling thematic group, and in particular its LEGAL subgroup, to provide for a framework to be employed by all existing or forthcoming cybersecurity certification schemes developed under the EU Cybersecurity Act. Moreover, existing European normative references have helped to frame our work activities all along this process. And, ISO standards and specifications have served as a common basis to elaborate ENISA labelling for cybersecurity certification. The use of ISO series will also contribute to improved market confidence, international recognition and consumer acceptance of third-party marks of conformity.

OBJECTIVES – during our activities, particular attention was drawn up to specific objectives e.g. operating better in the internal market and on national markets, or valuing a competitive advantage or reducing costs. Labelling can also facilitate market surveillance, or help promoting cybersecured trustworthy solutions concerning ICT products, ICT services and ICT processes. All the objectives referred to in this report have an equivalent value.

The future labelling implementation will serve them equally. In a first pilot-phase, our efforts will focus on:

- explaining the processes associated to certification and informing end users of certified solutions;
- encouraging certified solutions from providers;
- promoting European certification and related ecosystem e.g. certified solutions and also CABs including CBs and ITSEFs/auditors.
- In parallel, a similar effort will have to be deployed vis-à-vis the end users in close collaboration with ENISA communication structures.

All along the process, information will be dispatched on:

- the pertinence of a European framework via the certification platform;
- the promotion of certified based-solutions to allow a better information, visibility, comparison, choice;
- the support on competitive advantage and excellence along common grounds;
- the incentivisation of cybersecurity certified developers;
- the market surveillance conditions;
- the awareness campaign.

IMPLEMENTATION - The implementation eco-system will rely on a web-portal, a label generator, incentives and capacity-building projects to support the take-off. They will be elaborated between 2022>2025 along the lines described in this report. The analysis has taken into account different aspects such as the audience and the coverage of the label, or its various requirements e.g. logo mark, visible references, apps, webpage. The label has been designed to provide the information in different layers. The information to be provided in each layer will be incremental. It is highly recommended in terms of labelling to favour a gradual and flexible approach in line with the uptake speed and the attractiveness of the labelling cybersecurity certification. At this stage, the EU cybersecurity mark of conformity can take the following form:

- a label (level basic and general communication)
- a label with a distinct QR code
- a label with a QR code inserted (EUCC)
- a PIS[3]-type labelling or Information-only label[4]
- and/or a digitalized seal

AWARENESS – Building a solid European cybersecurity certification framework will involve a European based campaign to increase the visibility of newly certified solutions at European level. Labelling is aiming to match such objective of promoting awareness, reputation, excellence of the full spectrum of the solution certified when European customers will interact with EU certified solutions. The aim is that they will be fully aware of the existence and recognition of EU certified solutions. A communication campaign outlined in this report will be associated to the launch.

COMPLIANCE - Labelling aims at assisting market surveillance[5] authorities, i.e. national bodies and/or market-led organisations with a view to promoting innovation and competition as a key motivator to realign market incentives and enhance an optimal level of digital security. When continuing use of a certification mark is authorised for placement on a certified product, process or service (or its packaging, or information accompanying it be a bar-code or a QR-code type), surveillance shall be established and shall include periodic surveillance of marked products, services or software to ensure the on-going validity of the demonstration of fulfilment of the product requirement[6]. Compliance mechanisms associated with labelling are described in this report to support the certification eco-system in Europe. They will need additional consideration in due course.

****

In brief, this report lays down the flow of work, the orientations and recommendations for the establishment and application of a future EU Cybersecurity labelling policy as a requirement flexible enough to evolve smoothly and cope with the speed of innovation in the European cybersecurity market.

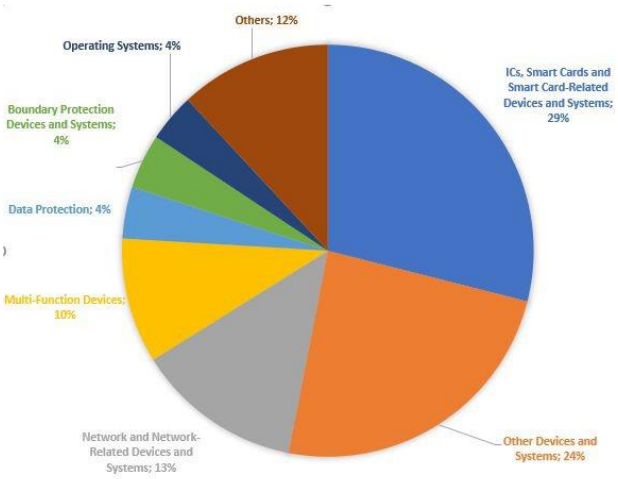
As a result of this work, after taking into consideration all the background research conducted, the views expressed by the experts interviewed, and the good practices and security measures identified, a series of recommendations has been developed under the following main chapters of this Report, namely:

- ❑ the harmonisation of the EU's labelling of cybersecurity certification;
- ❑ the validation of the labelling goals;
- ❑ the clarification of the labelling legal requirements;
- ❑ the implementation of the labelling ecosystem;
- ❑ the promotion of the labelling launch and its awareness campaign;
- ❑ the provision of the labelling compliance rules;
- ❑ the preparation of ENISA Labelling Workplan 2022>2025.

[3] PIS product Information Sheet see ENERG and XML. Here the "product" is not the product itself, but the certificate delivered. PIS in the view of the author is equivalent to the information dispatched in the QR code. 'Information-only label' as detailed in PETRAS 2018 Study refers to descriptive labels that communicate important information to consumers (such as the support period offered with a device) may provide proximate indicators of a device's security posture. The amount of information needs to be kept relatively simple and not too excessive as end-users have limited cognitive resources to expend during purchasing. Pictograms may be more successful than written information as they are more accessible to different demographics. However, research on the energy label has demonstrated that the accompanying information is often misunderstood and end-users often give more weight to certain types of information than others (e.g. energy efficiency over consumption) and this can lead to biased search behaviour. Furthermore, this type of label may be most suitable for voluntary uptake. see p12 in https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/949614/Rapid_evidence_assessment_IoT_security_oct_2018_V2.pdf
PIS questions also the issue of languages linguistic versions of the complete product/service/process information sheet in all official languages of the Union or only one…
[4] most suitable for voluntary uptake
[5] Reg No 765/2008 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008R0765
[6] ISO/IEC 17065 point 7.9.3 and 7.9.4 op cit

INTRODUCTION

CONTEXT - In a society where **digital ubiquity** is becoming predominant, each day we recognise the extraordinary opportunities that it has to offer. Cybersecurity is a growing opportunity with technical, social, and economic significance for every ICT related product, service and process available on the European market. It comprises a wide range of European Common Criteria based products, - EUCC -, such as smart cards and machine-readable passports, secured signature-based devices, tachographs. Are also included European Cloud based services such as EUCS based services or processes from cloud infrastructure services to office productivity applications[7], as well as interconnected products, services and/or processes, such as sensors, consumer products and everyday smart home objects, cars, and industrial and health components, tightly bound to cyber-physical systems. However, this transformation does not come without new threats that are constantly increasing in number, effectiveness and sophistication. Many security considerations are inherited from the use of networking technologies. Forthcoming ICT deployments depend on the robustness of all systems involved, whether they be the devices themselves, cloud backend and services, applications, maintenance and diagnostic tools, etc. For ENISA, as in its longstanding remit[8], addressing these challenges and ensuring security in cyberspace is of the utmost importance.

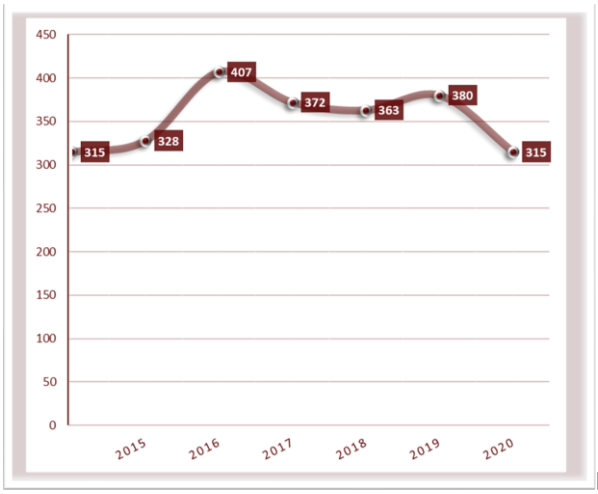


Top product categories (2021) source JTSEC 2021

At a time when these risks indiscriminately affect government authorities, businesses and individuals, it is crucial to be aware of the vital importance of putting in place appropriate solutions for securing information systems at the right level. While they there are many and diverse cybersecurity solutions available on the market, they are not equally effective and robust. Through European-based certification schemes, ENISA is proposing solutions to counter the impact that various threats may have on people's security, privacy and safety. The value of **European certification** is the degree of confidence and trust that is established by an impartial and competent demonstration of fulfilment of specified requirements by a third-party. Furthermore, certification schemes are usually only valid within a specific jurisdiction. A company would therefore have to undergo new certification processes for every new market it intends to target, which may incur significant additional costs associated with the proliferation of norms across countries and the risks of market fragmentation. These need to be addressed to ensure end user trust and confidence in the Internet, connected devices and related services, along with the labelling of cybersecurity certification.

[7] Étude cloud 2021 - Colt Technology Services https://www.colt.net/fr/go/cloud-research-report/?utm_term=&utm_campaign=Colt+-+FR+-+H2+Cloud+Display+2021&utm_source=adwords&utm_medium=ppc&hsa_acc=2612717853&hsa_cam=14128117394&hsa_grp=127114506884&hsa_ad=536956492944&hsa_src=d&hsa_tgt=&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gclid=EAIaIQobChMI8fzbkueZ9AIVjfDtCh2-CAKPEAEYASAAEgJ3V_D_BwE

[8] JRC Analysis and recommendations for a European certification and labelling framework for cybersecurity in Europe, 2017 https://data.consilium.europa.eu/doc/document/ST-12183-2017-ADD-9/en/pdf including data, case-studies.



Number of certifications in the last 5 years
source JTSEC 2021

The Cybersecurity Act (EU, 2019) aims to promote EU labelled certifications across the European Union in a more significant market. In this context, **labelling** is a new challenge, a window of opportunity for all cybersecurity stakeholders in Europe to show they care. However, beyond technical security measures, the adoption of a labelling strategy is raising many new legal, policy and operational challenges, broad and complex in scope, that need to be investigated. The rapid rate of change in technology has outpaced the ability of the associated policy, legal, and regulatory structures to adapt, leaving no clear security framework to follow. This has led most companies and manufacturers to take their own approach when designing cybersecurity labelling. This causes confusion.

For these reasons, ENISA is clarifying in this report a set of recommendations in the field of Labelling Cybersecurity Certification.

VALUE CHAIN – With labelling, all of the value-chain must have its say. Obviously, depending on the perspective of each value-chain stakeholder, labelling strategies will have to address a certain number of key-requirements.

For **companies**, the label is a way to communicate responsibility in an eye-catching manner and show that information security has been considered in the design of a product or service, e.g. traceability for the product's components, digital security policies, adherence to standards, etc. When dealing with certification, even more so at the European level, corporate responsibility becomes a competitive advantage on the European markets. Certification of an ICT product, service or software confers an element of differentiation, of distinction, and of excellence[9].

From the **end users**' perspective, the requirements for information on the security features of smart devices will become more stringent as cybersecurity gains importance and international standards and regulations develop. In many cases currently, transparent and reliable information on the key areas[10] of cybersecurity is hard to access and almost impossible to compare, even for an ICT expert. And when supply side actors provide such information,

[9] Akerlof, George A. (1970). "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism"
[10] OECD Digital Economy Papers, Enhancing the digital security of products. Feb.2021 p19 I Figure 3.2 provides an overview of six key areas where more transparency may be needed to reduce information asymmetries and enable customers to make more informed risk-based decisions:

- Product features for digital security, e.g. updatability and strong authentication.
- Processes and policies that are put in place by supply-side actors (e.g. EOL).
- The product's code: is the source-code open? Has it been scanned and tested by third-parties such as certification companies or governmental agencies?
- Traceability: is there is a list of code components? Is there enough clarity regarding the product's value chain? Where is the data stored and where does it transit?
- General trustworthiness: this area does not focus on the product itself, but rather on its broader ecosystem. What is the track-record of the organisation for managing digital security? Where are the servers, development teams and headquarters of the supply-side actors located? What is the impact of applicable domestic law (e.g. privacy, access to data, etc.)?
- Finally, third-party evaluation is key to increase transparency, and connects with the other five areas.

[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

it is difficult for customers to trust it, in the absence of appropriate market-based instruments such as certification[11], assessments of conformity, labels and ex post mechanisms. At present, individual consumers cannot distinguish the level of assurance between devices that offer security when making purchasing decisions. In fact, currently they have to research the security of the product themselves before making a decision. This involves evaluating technical information including its encryption standards, length of support, whether it ships with a default password etc.

From their side, **public authorities[12]** need to incentivise cybersecurity stakeholders to provide end users with clear and easily accessible information about a product, service, or source-code, in order to allow for comparability and informed choices. They also can play a leveraging role in pushing for EU cybersecurity-certified solutions in calls for tenders and public procurements. Since December 2021[13], at least five EU/OECD countries are considering launching, or have already launched, labelling schemes for the digital security of products: Austria, Germany, Finland, France and Spain.

STRENGTHS – A future EU cybersecurity label widely used, positively recognised, can provide greater visibility to offers of products, services and processes on European markets.

EU Cybersecurity labelling will be part of the Cybersecurity policy of the Community, which may aim at favouring the robustness of the EU Cybersecurity space by promoting those products, services and processes which have a high level of cybersecurity performance through the use of **EU labelling for cybersecurity certification**. To this effect, it will be appropriate to require that the criteria with which products, services and processes must comply in order to bear the EU label be based on the best cybersecurity performance achievable on the Community market. Those criteria should be simple to understand and to use, and should be based on scientific evidence, taking into consideration the latest technological developments. Those criteria should be market oriented and limited to the most significant threat impacts during the whole life cycle of the products, services and processes concerned.

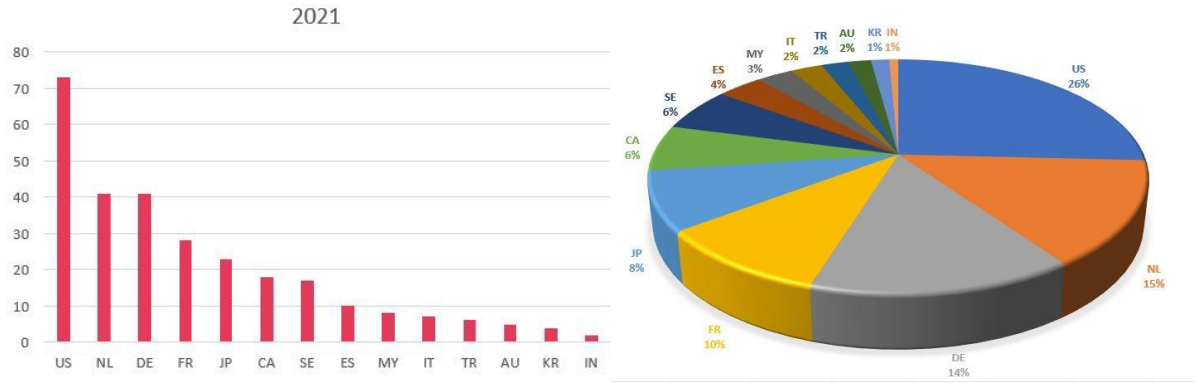
On one side of the cybersecurity chain, the cybersecurity label associated with the EU certificates will help **companies** to comply with current and future European requirements. This could be promoted with a community of supporters, thanks to regular events that would be scheduled each year, or public procurements requiring producers and contractors to meet high levels of digital security requirements for instance.

On the other side, **end users** need to be made more aware of the digital security risks associated with the product, or service they purchase with a view to empowering them to make informed choices. They should be able to assess whether products meet certain digital security criteria, such as adherence to industry best practices, length of commercial support, etc. Labels can be developed by or with the industry by taking into account appropriate and reliable information. In the absence of clear and simple information that allows for comparability, end users are often unable to leverage, for example, assessments of conformity based on ISO standards. Evaluation and certification processes evolve rapidly in the cybersecurity sector. This does not enable end users to apprehend these dynamics with confidence. With the support of certification and labelling, the certified brand's global recognition and the end users' empowerment remain stable.

[11] OECD Digital Economy Papers, Enhancing the digital security of products. Feb.2021 p41. The definition of certification varies across sectors and OECD countries. Certification can be defined as a mechanism to assess with more certainty, through evaluation by an independent third-party, whether products, processes or organisations meet a certain level of digital security. In that regard, some other experts consider that certification does not necessarily need to rely on an assessment of conformity. For instance, penetration testing may be used to certify that a product or an organisation meets a certain level of maturity regarding digital security, while not relying on technical standards. Alternatively, other experts consider that certification is one way of assessing conformity, along with other methods such as self-assessment. For this report, reference is made to Cybersecurity Act Articles ….
See also op cit JRC Analysis and recommendations for a European certification and labelling framework for cybersecurity in Europe, 2017
[12] In the United States, NIST is proceeding in 2021 to consultations with respect to labelling IoT following a report in 2018 suggested that the "government should convene industry, civil society, and government stakeholders in a multi-stakeholder process to explore requirements for a viable labelling approach", "so security-conscious consumers can make informed choices and create market incentives for secure-by-design product development" (DHS and DoC, 2018). More recently, another report recommended the creation of a "National Cybersecurity Certification and Labelling Authority, empowered to establish and manage a program on security certifications and labelling of ICT products" (Cyberspace Solarium Commission, 2020).
[13] OECD Digital Economy Papers, Enhancing the digital security of products. Feb.2021 p42.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

From a perspective of **fact & figures**, studies on the impact of nutrition labels in the EU communicated by the Commission have found that in 2018 they increased healthy product choices by 18%, indicating that they do empower consumers to choose healthier food. Other research on energy labelling in the EU demonstrated that consumers are willing to pay more for energy efficient products as rated by labelling schemes and that around 50% of European customers opt for Energy Labels as a key source of information to support decision making when purchasing (see Blythe and Johnson, 2018). Studies[14] also found, in the privacy field, that labelling enabled participants to find information more quickly and accurately than standard privacy policies. Labelling cybersecurity certification also has a positive effect on consumer behaviour. In Finland, almost 80% of consumers pay attention to information about security features when purchasing new digital products and would perceive a cybersecurity label as a positive factor when choosing a product according to Traficom, 2019.

Top Certifier schemes source JTSEC 2021
out of 286 products certified (09>2021)



Top three schemes account for 54% of the certification source JTSEC 2021

[14] McDonald AM, Reeder RW, Kelley PG, Cranor LF. A comparative study of online privacy policies and formats.

1. LABELLING CYBERSECURITY CERTIFICATION

1.1 INTRODUCTION TO ENISA THEMATIC GROUP ON LABELLING

BASED ON THE RELEVANT CHAPTERS OF THE CANDIDATE EUCC AND EUCS SCHEMES, AND EXISTING LABELS OF MEMBER STATES, IN 2021 ENISA HAS BEGAN ITS ACTIVITIES IN THE FIELD OF LABELLING, IN PARTICULAR SPECIFYING A FRAMEWORK LABEL WITH A VIEW TO IMPLEMENTING IT FROM 2022.

According to common practice and standards[15], the overall aim of certifying products, processes or services is to give confidence to all interested parties that a product, process or service fulfils specific requirements. The value of certification is the degree of confidence and trust that is established by an impartial and competent demonstration that the specified requirements of a third-party have been fulfilled.

Parties that have an interest in certification include but are not limited to:

a) the clients of the certification bodies;
b) the customers of the organisations whose products, processes or services are certified;
c) governmental authorities;
d) non-governmental organisations;
e) consumers and other members of the public.

Certification of products, processes or services in specific schemes[16] is a means of providing assurance that they comply with pre-defined specifications. With respect to our remit, as at the date of the publication of this report, we have been working with the two candidate schemes prepared by the ENISA Certification unit.

At this stage, the Candidate schemes[17] concerned are:

- European candidate cybersecurity certification scheme EUCC[18], which is based on common criteria;
- European Cybersecurity Certification Scheme for Cloud Services EUCS[19].

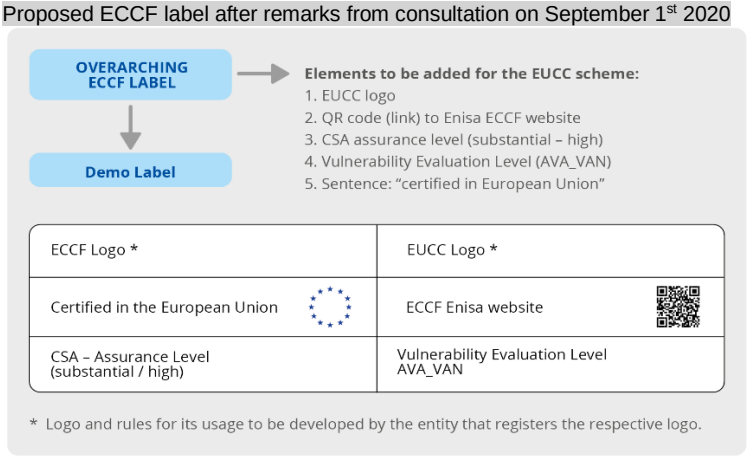
This Report has been prepared with a view to consolidating consistently its conclusions towards any forthcoming schemes, as well as – where provided – any specific or common label being developed in the future. It lays down the flow of work, the orientations and recommendations for the establishment and application of the EU Cybersecurity labelling as a requirement flexible enough to evolve smoothly and cope with the speed of innovation in the European cybersecurity market.

[15] ISO/IEC 17065 see Introduction IV ref to add
[16] Some product, process or service certification schemes may include initial testing or inspection and assessment of its suppliers' quality management systems, followed by surveillance that takes into account the quality management system and the testing or inspection of samples from the production and the open market. Other schemes rely on initial testing and surveillance testing, while still others comprise type testing only.
[17] Video updates schemes 29.06.2021 https://www.ssi.gouv.fr/actualite/lecosysteme-cyber-en-pleine-expansion/
[18] https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme
Following a request from the European Commission in accordance with Article 48.2 of the Cybersecurity Act (CSA), ENISA has set up an Ad Hoc Working Group to support the preparation of a candidate EU cybersecurity certification scheme as a successor to the existing schemes operating under the SOG-IS MRA. This has been named EUCC scheme (Common Criteria based European candidate cybersecurity certification scheme) and it looks into the certification of the cybersecurity of ICT products, based on the Common Criteria, the Common Methodology for Information Technology Security Evaluation, and corresponding standards, respectively, ISO/IEC 15408 and ISO/IEC 18045.
[19] https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme
Following a request from the European Commission in accordance with Article 48.2 of the Cybersecurity Act (CSA), ENISA has set up an Ad Hoc Working Group to work on the preparation of the candidate scheme on cloud services, as part of the European Cybersecurity Certification Framework. Draft version 12-2020
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

To this extent, this labelling work[20] will be merely a presentation and dissemination activity of practices that may affect the market, that is, would contribute towards a higher market homogenization and maturity. The focus is on the European Digital Single market. The certification market will benefit from the level of end user usability of certificates. In order to reach end users, it is necessary to support the market by means of the visual identity of a product, service or process that has been conformity assessed in the EU, according to a cybersecurity certification scheme. This approach would serve the need for market recognition across economic actors that are likely to consider such certified product or service. This requirement has been identified clearly in the first draft candidate cybersecurity certification scheme on Common Criteria (EU-CC) and it follows the provisions of article 55 of the CSA.

On 30 March 2021, the various stakeholders[21], - meaning NCCAs, NABs, CABs composed of CBs and ITSEFs, manufacturers or providers of ICT products -, agreed on the actions necessary to operate the EU-CC scheme. Among them, the establishment a Thematic Group on Labelling was listed. Its mandate was to investigate the operational aspects of labelling cybersecurity certification along the format hereafter.

Proposed ECCF label after remarks from consultation on September 1st 2020



This Labelling group is based on the ENISA work programme (SPD Activity 7: Supporting the European cybersecurity market and industry output O.7.3). This activity seeks to foster the cybersecurity market in the EU and the development of the cybersecurity industry, in particular small and medium-sized enterprises (SMEs) and start-ups, to reduce dependence on bodies outside the EU and to reinforce supply chains inside the EU. Actions to support this activity include compiling guidelines and good practices on cybersecurity requirements. The legal basis for this activity is Article 8 and Title III (cybersecurity certification framework) of the CSA. The objectives of Activity 7 are two-fold:

- Improve conditions for the functioning of the internal market
- Foster a robust European cybersecurity industry and market

Since the second semester of 2021, the rapporteur regularly informed the ECCG and the SCCG, as well as the EU-CC and the EU-CS Ad Hoc Working Groups. These bodies have regularly contributed with their inputs to this report (see timeline in 1.2.2 paragraph).

1.2 – ENISA THEMATIC GROUP ON LABELLING

REPRESENTATIVES FROM ENISA AD HOC WORKING AND EXTERNAL EXPERTS IN THE FIELDS OF CYBERSECURITY AND/OR LABELLING GATHERED THROUGHOUT THE SECOND SEMESTER OF 2021 TO DRAW UP THE CONCLUSIONS OF THIS REPORT.

[20] ENISA WP O.7.3 Based on the descriptions and requirements worked out in the EUCC paper, various processes for the creation/registration, publication and maintenance of individual certification schemes labels will be developed. These processes will cover the interaction of the certificate issuer, the certificate owner and certificate user, for the entire life cycle of the certificate. The work will produce process descriptions and necessary roles within the process execution, including legal aspects governing the participation/responsibilities of these roles.
[21] see Acronyms in Annex...

The **ENISA thematic group on labelling** aims at improving awareness of the cybersecurity efficiency, reliability and robustness of products, services and processes on the EU market. The proposed framework labelling needs to provide a clear, intuitive and durable indication of the requirements of cybersecurity schemes and other key features of products and services at the point of purchase when EU certified or certified in Europe.

1.2.1 Composition

More than 42 participants[22] registered for our labelling activities. With the collaboration of our five experts[23], various stakeholders from all sectors contributed their specific experiences in the field to our explorations. Additionally, our work was explained regularly in ENISA's consultative bodies, meaning SCCG and ECCG, whose members also contributed high quality inputs. This report reflects all these inputs with gratitude.

1.2.2 Deliverables

TG Labels management I Collection of benchmarking experiences with labels I TG Labels subgroups Expertise
Reports on the development of the specifications of a framework label with various options

- ❑ to be discussed with ENISA and designated statutory bodies (Single Programming Document of the Agency);
- ❑ to be validated by statutory bodies at the proposal or conceptual stage at the beginning of the project; and
- ❑ at the advance draft stage of the formation of this report.

Rq: Importantly validation feedback needs to be taken into account ahead of producing the final draft report.

Timeline of our work is available in ANNEX xxx

1.3 NOTIONS AND LEGAL REFERENCES

WHAT ARE WE TALKING ABOUT?

WHEN DEALING WITH LABELLING, IT IS ACKNOWLEDGED THAT A CERTAIN NUMBER OF DOCUMENTS ALREADY EXIST AND THESE CAN HELP TO BETTER ENVISAGE THE NOTION OF LABELLING.

1.3.1 European Normative References

A reference to 'marks or Labels' is mentioned but not defined per se in the **Cybersecurity Act:**[24]

> **Article 54.1. (CSA)** A European cybersecurity certification scheme shall include at least the following elements: (…) where the scheme provides for marks or labels, the **conditions** under which such marks or labels may be used.
> **Article 2 (20) (CSA)** '**technical specification**' means a document that prescribes the technical requirements to be met by, or procedures fo assessing conformity relating to, an ICT product, ICT service or ICT process.
> **Recital (40) (CSA)** ENISA should also strive to provide consumers with **relevant information** on applicable certification schemes, for example by providing **guidelines** and **recommendations**.

[22] see List of members of the Labelling TG available on CIRCABC (42) in Annex…

[23] See ANNEX xxx
[24] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification[24] and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) op.cit.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

With respect to ENISA certification schemes, the **EUCC** draft scheme and guidance includes labelling in accordance with marks and labels[25]. It refers specifically to:

1. A **specific** EUCC label and associated mark, established for the European Cybersecurity Certification Framework of this scheme.
2. The label is not a precondition for establishing certificates according to the EUCC. However **when in place**, it will affect the process of issuing certificates.
3. The **conditions** under which this label is to be used include the combination with a QR code provided by ENISA once a certificate is issued, the required information as defined under the EUCC, a mapping to the evaluation levels AVA_VANs for the EUCC and an indication of where the service is established if this is part of the requirements and assessment at a particular level for the EUCS.

Although in theory this rule would allow for each scheme to define individual specific conditions, it is the aim of the EU commission as well as ENISA to provide for an overarching label (or family of labels) under the EU Cybersecurity Act. Therefore, it is the objective of the Labelling thematic group, and in particular the LEGAL subgroup, to provide for a framework to be employed by all Cybersecurity schemes developed under the EU Cybersecurity Act.

Additionally, labels are considered as ''technical specifications'' in both **REGULATION[26] (EU) No 1025/2012** on standardisation and **DIRECTIVE[27] (EU) 2015/1535** laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.[28] Regulation 1025/2012 establishes rules, among others, with regard to the identification of ICT technical specifications eligible for referencing. Article 2.4 defines *technical specifications* as a document that prescribes the technical requirements to be fulfilled and that specifies certain elements, for example the characteristics a product should have and the requirements it should fulfil. Marking or labelling are listed as one of the areas that such requirements could cover. According to Article 2 (19) REG2017/1369 on Energy Labelling[29], 'label' means a graphic diagram.[30] In addition to the cybersecurity information of the products and/or the services referred to, the labels could also provide specific data about other relevant features of their use, such as the product's emissions or the energy consumption and the CE marking for instance.

Article 2 (4) **'technical specification'** means a document that prescribes technical requirements to be fulfilled by a product, process, service or system and which lays down one or more of the following: (a) the characteristics required of a product including levels of quality, performance, interoperability, environmental protection, health, safety or dimensions, and including the requirements applicable to the product as regards the name under which the product is sold, terminology, symbols, testing and test methods, packaging, marking or labelling and the procedure for assessing conformity to these requirements.

1.3.2 ADDITIONAL NORMATIVE REFERENCES

A label is considered as a ''**market-based-instrument**' in OECD references - ''Label and labelling schemes are market-based instruments (MBIs) for companies and consumers to strengthen trust and confidence and contribute to reinforcing a high level of mutual recognition and circulation of smart digital products and services across the EU in the framework either of self-regulation or co-regulation.''[31] Labels[32] can be displayed on the product's package, on the producer's website or on the customer's smartphone after scanning a product's identification such as a

[25] in Guidance T3 19.03.2021 EUCC, "10. MARKS AND LABELS"
[26] REGULATION (EU) No 1025/2012 of the European Parliament and the of the Council of 25 October 2012 on European standardisation https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012R1025
[27] DIRECTIVE (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services[27] (codification)
see also definitions Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.1998.204.01.0037.01.ENG&toc=OJ%3AL%3A1998%3A204%3ATOC
[28] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L1535
[29] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02017R1369-20210501

[30] More precisely According to Article 2 (19) REG2017/1369 on Energy Labelling, 'label' means a graphic diagram, either in printed or electronic form, including a closed scale using only letters from A to G, each letter representing a class and each class corresponding to energy savings, in seven different colours from dark green to red, in order to inform customers about energy efficiency and energy consumption; it includes rescaled labels and labels with fewer classes and colours in accordance with Article 11(10) and (11).
[31] EUROPA website - Commission Vademecum tool#18 on the choice of policy instruments and OECD
[32] OECD Digital Economy Papers, Enhancing the digital security of products. Feb.2021 p42.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

barcode or a QR code. Labelling models include information-only, e.g. list of ingredients, or seal of approval, traffic lights and graded schemes. They can be awarded by public authorities or industry-led organisations. Like conformity assessments, they can be voluntary or mandatory, and rely on self-assessment or certification, by a third-party. Some labelling schemes include certification as a criterion for awarding the label. The main difference between labels and assessments of conformity is the accessibility of the information provided: labels are developed in order to increase transparency for mainstream users.

A label is referred as a '**mark of conformity**' in the International Standards Organisation (ISO). ENISA usually refers explicitly to standards in its glossary.[33] In ISO series 17000>17030>17065, labels may take many forms and different uses. They can convey useful information about a product or indicate particular characteristics of a product such as its safety, quality, performance, reliability or impact on the environment. They are found on products, certificates and publications denoting conformity to the specified requirements of a product, management system, service, process, person or an organisation. They clarify their notion and their conditions of use.

Labels are defined as marks of conformity according to ISO 17000[34], 17030[35], 17065[36] etc…

- ISO/IEC 17000, *Conformity assessment — General vocabulary* [1)]
- ISO/IEC 17028, *Conformity assessment — Guidelines and examples of a certification scheme for services*
- ISO/IEC 17030, *Conformity assessment — General requirements for third-party marks of conformity*
- ISO/IEC 17032, *Conformity assessment — Guidelines and examples of a scheme for the certification of processes*
- ISO/IEC 17065, *Conformity assessment — Requirements for bodies certifying products, processes and services*
- ISO 28219:2017, *Packaging — Labelling and direct product marking with linear bar code and two-dimensional symbols*
- ISO/TS 18614:2020, *Packaging — Label material — Required information for ordering and specifying self-adhesive labels*

These normative references have helped us to frame our work activities throughout this process. ISO standards and specifications have served as a common basis to elaborate ENISA labelling for cybersecurity certification.

[33] Indispensable baseline security requirements for the procurement of secure ICT products and services — ENISA (europa.eu), December 2016
[34] The use of International Standard ISO 17030 should lead to improved market confidence, international recognition and consumer acceptance of third-party marks of conformity
[35] https://www.iso.org/obp/ui/#iso:std:iso-iec:17030:ed-1:v1:en
[36] See Introduction V - ISO/IEC17065 does not set requirements for schemes and how they are developed and is not intended to restrict the role or choice of scheme owners, however the requirements of schemes should not contradict or exclude any requirement of this international standard.

2. OBJECTIVES OF LABELLING

Labelling is based on market feedback and demands from various users and issuers of marks of conformity. ISO Series 17000 stresses that the prime objective of all marks of conformity is to gain the confidence of the market, including consumers, in products and other objects to which these marks have been applied. The overall objective of labelling is to improved market confidence, international recognition and consumer acceptance of marks of conformity.

LABELLING, WHAT FOR?

Label(s) and labelling features are market-based instruments for companies and consumers to strengthen their trust or confidence and Information or Awareness with a view to contributing and reinforcing a high level of mutual recognition and the circulation of cybersecurity-based digital products, services and solutions across the EU, via self-regulation, co-regulation or regulation.

Remember that the Cybersecurity Act[37] requests in its Recital 40 that ENISA should also strive to provide consumers with relevant information on applicable certification schemes, for example by providing guidelines and recommendations.

Labelling linked to certification provides a clear and simple indication of the state-of-the art with respect to cyber-security efficiency and robustness. Additionally, it can encompass other key features of products and services at the point of purchase. The labels could also provide specific data about other relevant features of use, such as the product's emissions and/or energy consumption and/or geographical origin.

At the occasion of their kick-off meeting, on 10 June 2021, Members of ENISA Labelling shared and contributed their relevant experiences on the OBJECTIVES of labelling. In particular, some emphasised at enhancing operations in the internal market and on national markets. Others contributed to improving the value of a competitive advantage, and/or reducing costs. Most of the members shared the view that labelling can also facilitate market surveillance or help in promoting cyber-secured trustworthy solutions concerning ICT products, ICT services and ICT processes. We will develop these ideas further through our work and in the coming pages.

[37] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (europa.eu) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN>
EU Awareness > ENISA should contribute to raising the public's awareness of cybersecurity risks, including through an EU-wide awareness-raising campaign by promoting education, and to providing guidance on good practices for individual users aimed at citizens, organisations and businesses. ENISA should also contribute to promoting best practices and solutions, including cyber-hygiene and cyber-literacy at the level of citizens, organisations and businesses by collecting and analysing publicly available information regarding significant incidents, and by compiling and publishing reports and guidance for citizens, organisations and businesses, to improve their overall level of preparedness and resilience. ENISA should also strive to provide consumers with relevant information on applicable certification schemes, for example by providing guidelines and recommendations. ENISA should furthermore organise, in line with the Digital Education Action Plan established in the Commission Communication of 17 January 2018 and in cooperation with the Member States and Union institutions, bodies, offices and agencies regular outreach and public education campaigns directed at end users, to promote safer online behaviour by individuals and digital literacy, to raise awareness of potential cyber threats, including online criminal activities such as phishing attacks, botnets, financial and banking fraud, data fraud incidents, and to promote basic multifactor authentication, patching, encryption, anonymisation and data protection advice.

[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Throughout our activities, members shared their experience in case-studies (use-cases), in particular with respect to the following non-exhaustive list of validated objectives:

- promoting information, awareness, excellence and marketing vis a vis the end-users;[38]
- operating in the internal market and the national markets;
- strengthening trust in the digital internal market and its competitiveness;
- adding value to a competitive advantage, a qualitative differentiation, a European based-labelling;
- incentivising developers to produce more secured and certified products and services;
- facilitating market surveillance and gaining confidence;
- increasing the transparency of cybersecurity assurance levels;
- comforting the EU cybersecurity certification eco-system;[39]
- securing trustworthy cybersecurity solutions;
- measuring EU-cyber resilience;
- promoting best practices and solutions, including cyber-hygiene and cyber-literacy;
- enabling consumers[40] to make conscious choices regarding the features and capabilities of certified products and to be assertive and savvy;[41]
- any additional objectives… robustness, empowerment.[42]

These objectives were validated at the plenary on 10 June 2021. However, due to time constraints for this Report, we have focused our attention to the following objectives:

- **Functioning of the internal market and national markets**
- **Valuing a competitive advantage, a market differentiation**
- **Incentivising access to labelled certification to developers**
- **Facilitating market surveillance and fair competition**
- **Promoting awareness, excellence and empowerment**

2.1 > FUNCTIONING OF THE INTERNAL MARKET AND NATIONAL MARKETS

The internal market comprises an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured. In this context, labels have to respond to a market need to avoid poor use of the label, or situations in which a label is unknown to the developers or the users in specific fields in which legal regulation is either difficult or where achieving it is premature.

For example, the CE marking brings two main benefits to businesses and consumers in the European Economic Area:

- Businesses know that products bearing the CE marking can be traded without restrictions.
- Consumers enjoy the same level of health, safety, and environmental protection.

In REGULATION (EC) No 765/2008 Art 2(20) **'CE marking'** shall mean a marking by which the manufacturer indicates that the product is in conformity with the applicable requirements set out in Community harmonisation legislation providing for its affixing.[43]

In fixing the label CE, manufacturers play a crucial role in ensuring that products in Europe are safe.
They are responsible for checking that their products meet EU safety, health, and environmental protection requirements.

[38] EUCC Candidate Scheme, v1.1.1., May 2021 Chapter 10 … make the certification easily recognizable as both the label and the associated mark may be printed on the package of the product, on technical documents and on leaflets used for marketing purposes
[39] EUCC Candidate Scheme, v1.1.1., May 2021 Chapter 10 … to highlight that the ICT product has been certified in the European Union and to provide immediate information regarding the certificate by making reference to the framework (ECCF), the evaluation scheme and the assurance level
[40] 'By means of transparent criteria, it enables consumers to make conscious choices regarding the features and capabilities of certified products' see (TG10) Report on Guidance regarding manufacturer/provider commitments applicable to the EUCC scheme, July 2021
[41] Interviews Chiara GIOVANNINI, ANEC on 2 June 2021 & Ursula PACHL and Frederico DA SILVA, BEUC on 26.05.2021
[42] "All stakeholders should understand digital security risk and how to manage it" (OECD, 2015[17]).
[43] Case-study CE marking Lessons learnt, presentation of Marta PABIAN, DG GROW 10.06.2021

It is the manufacturer's responsibility to carry out the assessment of conformity, set up the technical file, issue the EU declaration of conformity, and affix the CE marking to a product.

Only then, can a product be traded on the European Economic Area. CE marking also supports fair competition by holding all companies accountable to the same rules. With respect to cybersecurity labelling and certification, it remains a key-factor that European-based solutions are being certified, encouraged, promoted and used by a maximum number of end users.

In this context, it is recommended that we focus our labelling work on the pertinence of a European framework, while first encouraging certified based-solutions.

2.2 > VALUING A COMPETITIVE ADVANTAGE, A QUALITATIVE DIFFERENTIATION

In the context of a **GREEN EUROPE**, if companies want to market their products and services as 'green', the EU ECO-label and the ENERG-label are two options that bestow a competitive advantage.[44]

The **EU ECO-label**[45] has been recognized since 1992 across Europe and worldwide. Circa 78,000 references[46] and 1,892 licences may display the ECOLABEL[47] indicating their **environmental excellence** based on a voluntary scheme.[48] In another context,[49] the **ENERG-label**[50] indicates the **energy-efficiency**[51], for example, of every television and television monitor or screen to be sold in Europe. It is a market differentiator for energy efficiency. Over 600,000 models are registered in the system, among them **ICT products** such as: televisions, enterprise servers, computers, monitors, UPS devices, imaging equipment, game consoles.

[44] Six reasons for SMEs to support the ECO-label https://ec.europa.eu/environment/ecolabel/eu-ecolabel-for-businesses.html
[45] https://ec.europa.eu/environment/ecolabel/index_en.htm
[46] https://youtu.be/jjrheP-nqNc?list=PLIzqPSxpstTnv9Mpw66K5a6Iv0PFCWzy6
[47] https://ec.europa.eu/environment/ecolabel/index_en.htm
https://ec.europa.eu/environment/ecolabel/documents/label_you_can_trust.pdf
[48] Regulation (EC) No 66/2010 of and the Council of 25/11/2009 on the EU Ecolabel: "the scheme is intended to promote those products which have a high level of environmental performance through the use of the EU Ecolabel" (rec. 5)

- ✓ It is the official EU voluntary label for environmental excellence, guiding consumers and procurers towards sustainable goods and services
- ✓ It is based on the only EU-wide ISO 14024 Type 1 Ecolabel: reliable; multi-criteria; life-cycle approach; open-transparent-multi-stakeholder and science-based criteria setting; third party verified
- ✓ It is managed by the European Commission and the Competent Bodies
- ✓ the e-catalogue guarantees products with: ✓Best available energy efficiency classes; ✓Restricted use of hazardous substances; ✓Design for higher product durability, reparability and recycling; ✓At least 10% of post-consumer recycled plastics content; ✓Respect for social aspects.

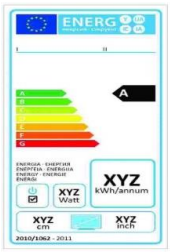
[49] Case-study presentation by Paolo TOSORATTI, DG GROW

50 ENERG-label > Regulation (EU) 2017/1369 of the European Parliament and of the Council of 4 July 2017 setting a framework for energy labelling: • Set the framework for labelling of energy related products • Delegated acts (Regulations) set requirements on specific products • Established the "product database" and its "portal" (one-stop-shop for ecodesign/labelling regulations) – (op.cit.)

REG2017/1369 on Energy Labelling https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02017R1369-20210501 Repealed Commission delegated Regulation (EU) No 1062/2010 of 28 September 2010 supplementing Directive 2010/30/EU of the European Parliament and of the Council with regard to energy labelling of televisions

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32010R1062

[51] The EU ENERG-label features in a diagram: the EU flag, the ENERG letters, countries, id of the supplier or company, the life-cycle e.g. for products placed on the market, a label on a scale from A (most efficient) to G (least efficient) is used, the television's model, the average annual on-mode energy consumption (also in Watts), screen dimension in inches and cm.



. The Energy labelling Objectives are threefold:

- **Information** > to facilitate scaling from A to G according to how much energy products consume;
- **Choice** > to help consumers save money by choosing products that consume less energy;
- **Advantage** > to encourage companies to design products that consume less energy.

In comparison, an EU cybersecurity label would provide, through certification, exigent guidelines for companies looking to increase awareness of the excellence of their solutions and guarantee the efficiency of their cybersecurity solutions through third party controls. Furthermore, many companies would turn to the criteria of the EU Cybersecurity label for guidance on cybersecurity best practices when developing their product and services lines.

Thus, EU cybersecurity labelling would also help to promote information, choice, advantage and excellence along common grounds, as indicated in the EU-CC scheme.

2.3 > INCENTIVISING ACCESS TO LABELLED CERTIFICATION FOR DEVELOPERS

In the cybersecurity area, companies face an extra burden of costs when dealing with certification and labelling. These additional costs will be passed on the final prices charged on the end users. For the third-party certification model, assessing conformity usually incurs significant costs for the manufacturers. There are both direct costs such as purchasing a service from a company authorised to certify and, indirect costs such as increased time-to-market.

In this respect, the EU common labelling may help in:

- ❑ reducing the costs of collecting information on 26 national provisions to allow companies to sell their products and services throughout the European Union;
- ❑ avoiding fragmentation and a lack of common interpretation with respect to clearly displaying information on how to comply, enforce and inform European end users;
- ❑ financially supporting certification fees and fees for the label submission of applications for labels.

Along the lines of the **EU ECO-label,**[52] this scheme is designed to be as low cost as possible. However, as the costs of running the scheme vary between competent bodies and from one product to another, fees may vary accordingly. The EU Ecolabel for Businesses[53] details the reasons to opt for it.

From the same perspective, a future EU Cybersecurity label may favour an equivalent approach:

1. On the **B2C level**, increased awareness about the benefits of cybersecurity certified products and services creates a favourable climate for the cybersecurity market as end users such as administrations, SMEs and consumers, are becoming increasingly mindful when purchasing these products and services.

2. Public procurers on the **B2G level**[54] are facing increasing pressure to work with manufacturers of products and services that bear cybersecurity labels in accordance with ISO standards in order to meet procurement requirements.

[52] Interview with Silvia FERRATINI on 18.05.2021, DG ENV on the Eco-label
https://ec.europa.eu/environment/ecolabel/index_en.htm

[53] https://ec.europa.eu/environment/ecolabel/eu-ecolabel-for-businesses.html

[54] An important impact can be also foreseen for national authorities as buyers of ICT products and services. The promotion of certification and labelling under the Framework, would allow national authorities to make more informed purchase decisions. They could e.g. decide to procure ICT solutions with a certain cybersecurity assurance and, thanks to the mutual recognition system, they would reap the full

[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

3. Within the **B2B level**, checking whether companies' products or services comply with the EU criteria for cybersecurity labelling will lead to optimised production processes and increased corporate profitability and reputation, so that compliant brands stand out from their competitors.

In this context, fees can be used as support mechanisms.[55] Reduced fees can also be rendered available for SMEs, micro-enterprises and companies from developing countries.[56] For instance, the application fee can be reduced by 20% for applicants registered under the Community certification scheme and/or audited under ISO standards. This reduction is subject to the condition that the applicant explicitly commits, in its cybersecurity policy, to ensuring full compliance of its certified products and/or services with the EU criteria for cybersecurity labelling throughout the period of validity of the certificate.

The Cyber Security Agency of Singapore (CSA) has launched the Cybersecurity Labelling Scheme[57] (CLS) for consumer smart devices. The CLS also aims to help manufacturers stand out from their competitors and be incentivised to develop more secure products. Currently, consumer smart devices are often designed to optimise functionality and cost. They also have a short time-to-market cycle, where there is less scope for cybersecurity to be incorporated into product design from the beginning. The issue of scalability of IoT and labelling incentives is also a challenge. With the number of connected devices expected to reach 20 billion in 2020, the third-party certification model may not be scalable to all smart products (Blythe and Johnson, 2018). Therefore, a specific labelling scheme will have to be adapted for these products and services. Certification would then be rather targeted at substantial or high-risk products and services. To encourage the adoption of the scheme, Singapore CSA has waived the application fees for the Cybersecurity Labelling Scheme for one year.[58] The Cyber Security Agency of Singapore also has a dedicated website page listing pre-approved cybersecurity solutions under the auspices of SMEsGoDigital.

Here, cybersecurity certification labelling becomes the entry-door to all types of incentives supporting the European cybersecurity market.

2.4 > FACILITATING MARKET SURVEILLANCE & FAIR COMPETITION

Labelling aims at assisting market surveillance[59] authorities, i.e. national bodies and/or market-led organisations with a view to promoting innovation and competition as a key motivator to realign market incentives and enhance an optimal level of digital security. When continuing use of a certification mark is authorised for placement on a certified product, process or service (or its packaging, or information accompanying it as a bar-code or a QR-code), surveillance shall be established and shall include periodic surveillance of marked products to ensure the validity of the mark is on-going and that product requirement[60] are being fulfilled.

2.4.1 Market surveillance and self-regulation

From the perspective of corporate responsibility, labelling is a simple way, for companies, to communicate commitment and show that information security has been considered in the design of a product or service.

benefits of unfettered competition and cross-border free trade across the Union. In https://data.consilium.europa.eu/doc/document/ST-12183-2017-ADD-9/en/pdf

[55] See table in ANNEX XXX

[56] The complete list of developing countries. Note that Hong Kong, Taiwan and Macau are not eligible for a fee reduction.

[57] https://www.csa.gov.sg/Programmes/psg-cybersecurity-solutions
It aims to improve the Internet of Things (IoT) security, raise overall cyber hygiene levels and better secure Singapore's cyberspace.

[58] Until October 2021

[59] Reg No 765/2008 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008R0765

[60] ISO/IEC 17065 point 7.9.3 and 7.9.4 op cit

[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

As such, PEGI is considered to be a successful and durable self-regulatory model of European mutual recognition in the field of content rating with respect to the protection of children in the gaming and film industries. The Pan-European Game Information PEGI-label[61] provides information on the age-suitability and content of video games and films. PEGI was developed by the Interactive Software Federation of Europe[62] (ISFE) and came into use in 2003, replacing many national age-rating systems with a single European system. It is recognised throughout Europe, and is used in 39 countries (2021).

The video games sector and the media content industries are evolving continuously, as the cybersecurity market. Therefore, PEGI needs to keep track on these developments to stay relevant. Under the support of the European Commission, PEGI rating system[63] has developed a surveillance mechanism regulating PEGIs day-to-day management, supervision and development. This Pan-European Game Information label is based on a Code of Conduct[64], a set of rules to which every publisher using the PEGI system is contractually committed. Drawing on wide experience, PEGI is steered by way of a number of boards and committees as envisaged in article 12 of the PEGI Code of Conduct**.** A complaint mechanism is also operated in a transparent way.

2.4.2 Market surveillance and co-regulation

French ANSSI cybersecurity visa – The **Visa de sécurité**[65] represents an umbrella brand[66] with regards to trustworthy cybersecurity solutions[67]. It combines both certification and qualification processes from the French

[61] https://pegi.info Interview on 12.05.2021 of BAENSCH Jürgen, ISFE and Case-study presentation by Dirk BOSMANS, PEGI
The PEGI system is handed to PEGI s.a., an independent, not-for-profit company with a social purpose established under Belgian law.
[62] https://en.wikipedia.org/wiki/Interactive_Software_Federation_of_Europe
[63] Age ratings are systems used to ensure that entertainment content, such as games, but also films, TV shows or mobile apps, is clearly labelled with a minimum age recommendation based on the content they have. This easy-to-read graphical age ratings system provides guidance to consumers, parents in particular, to help them decide whether or not to buy a particular product for a child. Content description[63] on its side details the main feature of a film, a video or a game.

[64] https://pegi.info/pegi-code-of-conduct
[65] Study-case Presentation on 10.06.2021 and 02.07.2021 by Marine GONINET and interview of Sylvain LEROY ANSSI
security-certification-of-products_security_visa_anssi.pdf
[66] No Trade Mark ™ No reference to ISO 17030
[67] Le directeur général de l'Anssi a par ailleurs fait état de la nécessité « vitale » d'utiliser la certification afin d'assurer la confiance dans les fournisseurs de services numériques. Et ce, non seulement concernant les produits de cybersécurité en tant que tels, mais également d'autres équipements, services et solutions très importants liés au cloud ainsi qu'à la 5G. « Il faut créer des schémas organisés par l'ENISA pour résoudre les vrais problèmes de sécurité et de confiance », a expliqué Guillaume Poupard. Non sans mettre le doigt là où ça fait mal : « la France plaide pour des offres avec un niveau de sécurité technique le plus élevé possible, mais il y a aussi une question juridique majeure de faire certifier des offres du niveau de sécurité le plus élevé soumises au Cloud ou Patriot Act et d'aller piocher
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

National Cybersecurity agency (ANSSI). While there are many and various cybersecurity solutions available on the market, they are not all equally effective and robust. This is why ANSSI, in its capacity as a national authority, and aware of the need for clarification about this market, is helping companies and government authorities to make a choice thanks to its security visas. They provide an easy way to identify solutions[68] that ANSSI considers the most reliable following a qualification or certification process. They are a guarantee of security for users and provide a significant competitive edge for product suppliers and the providers of security services.[69]

The Visas meet three compliance objectives:

- REGULATORY, to meet the French and/or European provisions that enforce the use of solutions guaranteeing a tried and tested level of robustness;
- CONTRACTUAL, to provide a solution for public or private contractors who require that the solutions they use have obtained an ANSSI security Visa;
- COMMERCIAL, to enable a product supplier or a service provider, as well as the final users of these solutions to stand out from the competition by guaranteeing a certain level of robustness.

The Spanish model with the **CCN[70]-labels** pursue the following objectives:

- guaranteeing that the products used by public authorities comply with the required security levels;
- promoting the development of ICT security and encryption products;
- assessing and accrediting the ability of a product to manage secure information via the evaluation and certification of ICT security products;
- updating a catalogue of ICT products in which a list of ICT security products is proposed and guaranteed by the CCN itself.

The growing popularity of smart devices and their continuous development create both new opportunities for consumers and new threats for information security. From its side, the Finnish model via the IoT **Traficom-label** pursues the following objectives:

dedans. Ce n'est pas de l'anti-américanisme mais il faut assumer le fait que pour les systèmes les plus critiques, seuls les droits européens doivent s'appliquer ». Senat Français, in Le Monde 06.05.2021
https://www.lemondeinformatique.fr/actualites/lire-la-cybersecurite-europeenne-prete-a-passer-a-l-echelle-82848.html

[68] You will find in the following pages a description of the ANSSI's qualification process.

Additionally, the list of qualified products and services may be found on the Agency's website.

[69] Le nombre de produits et services ayant obtenu un Visa de sécurité a augmenté de 21% entre 2019 et 2020, passant de 114 produits certifiés a 132 produits et services qualifiés. Rapport 2020 ANSSI 29.06.2021
Pour la certification : 87 certifications Critères Communs + 27 certifications de sécurité de premier niveau (la CSPN, alternative FR aux critères communs, en temps et charge contraints pour l'évaluation) = 114 certifications
Pour la qualification : 35 qualifications de produits + 97 qualifications de services = 132 qualifications
TOTAL : 246 (+ 21% par rapport à 2019 où on en avait délivré 204 au total)

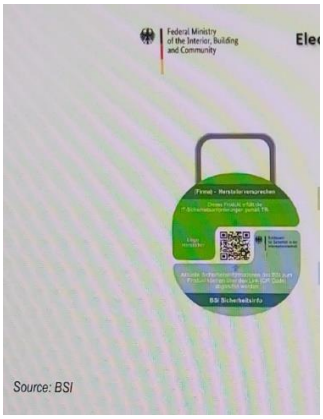
[70] https://oc.ccn.cni.es Case-Study Presentation on 2 July 2021

[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Tietoturva Cybersecurity Label Objectives of Traficom-label[71]

- making it easier for consumers to choose secure products and services;
- ensuring the security of smart devices and services by setting certain security requirements for them;
- improving public awareness of information security;
- supporting the competitiveness of companies investing in information security.

In Germany, the agency in charge of digital security (BSI) partnered with the industry to launch a voluntary labelling scheme, "IT Security", by the end of 2021. The labelling scheme is available for all IT products, even though the criteria used to award the labels are modified for each category of products such as routers, meters, etc.



Proposed IT label in Germany; Source[72]: BSI

In comparison with other labels, the IT security label is standardised, easily understandable by customers and up-to-date. The label takes the form of a QR code inserted in the product's package, which, upon scanning, presents two sets of information to the customer: the manufacturer's self-declaration and the BSI security information. The latter is intended to inform the consumer about security gaps or other IT characteristics relevant to security, while the manufacturer's declaration provides assurances that the product has certain IT security characteristics.

For the government, the objective of the label is to supplement existing statements by product manufacturers, which often lack visibility, relevance and comparability between products.

[71] https://tietoturvamerkki.fi/en/ Case-Study presentation on 2 July 2021
https://www.traficom.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label
In November 2019, the Finnish Transport and Communications Agency (Traficom) launched an "information security" label for IoT devices. The label is awarded to IoT products if they meet certain criteria for certification, based on the ETSI technical specification on Cyber Security for Consumer IoT (2019). The initiative resulted from a private-public partnership between the National Cyber Security Centre Finland (NCSC-FI) at Traficom and the following companies: Cozify Oy, DNA Plc and Polar Electro Oy. The label's website (Traficom, 2019) references the products that have been awarded the label and publishes information about the label. In addition, the website provides information to businesses on how they can apply for the label. The labelling scheme relies on several criteria, including certifications awarded to the product or the producer (e.g. STAR certification by the Cloud Security Alliance), support period, updatability, policies on the disclosure of vulnerabilities, encryption and privacy protection.
[72] Enhancing the Digital Security of Products: a policy discussion I OECD Digital Economy paper (op.cit)

AUSTRIA > more to come following meeting 07 October 2021 two colors and self regulation

https://www.cyber-trust.at/imprint/

2.5 > PROMOTING AWARENESS, EXCELLENCE AND BRANDING

Labels often have the objective of promoting awareness among dedicated communities. However, the proliferation of labels[73] may be counter-productive to both producers and customers. Therefore, our work has focused mainly on a framework labelling easy that is easy to use across different certification schemes. This part was organised with the support of the ECSO labelling and additional initiatives.[74]

CYBERSECURITY MADE IN EUROPE is an industry-driven marketing tool for a stronger and more competitive European cybersecurity market, designed to promote European cybersecurity companies and increase their visibility on the European and global markets. The lack of such a marketing tool in Europe inspired the European Cyber Security Organisation[75] (ECSO) to develop its trade-marked label.[76] The ECSO-label[77] "made in Europe" is based on ENISA's indispensable baseline security requirements[78] for the procurement of secure ICT products and services.

ECS-O label aims at identifying **European-based** manufacturers. The Label serves as a **market differentiator** based on geographic location. The Label raises **awareness** of the strategic value of cybersecurity companies originating in Europe and developing their businesses based on trusted European values. The Label increases **companies' visibility** among potential business partners, end-users and cybersecurity investors.

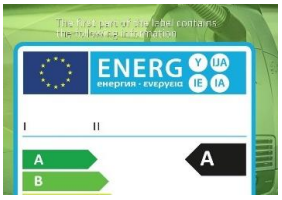
[73] see 106 bio-labels in Belgium site web Labelinfo.be
[74] see as well https://www.charteroftrust.com
[75] https://ecs-org.eu
[76] Case-Study Presentation by Danilo D'ELIA, ECSO on 10 June 2021
[77] https://ecs-org.eu/initiatives/cybersecurity-made-in-europe
[78] ENISA Indispensable baseline security requirements for the procurement of secure ICT products and services — ENISA (europa.eu), December 2016
see => https://www.ecs-org.eu/documents/uploads/label-conformity-declaration-enisa.docx

The **catalogue of STIC Products** (CPSTIC) offers a list of ICT Security products and services with proven security guarantees. In the meantime, the catalogue is identifying companies dealing in robust cybersecurity solutions. The CPSTIC is intended for public sector organisations or private entities that provide services to them and are under the scope of the National Security Scheme (ENS) or that manage classified information.

https://oc.ccn.cni.es/catalogo-productos-stic

As indicated, the Cyber Security Agency of Singapore (CSA) has launched the Cybersecurity Labelling Scheme (CLS) for consumer smart devices, as part of its efforts to improve Internet of Things (IoT) security, raise overall cyber hygiene levels and better secure Singapore's cyberspace. The Cyber Security Agency of Singapore website has a dedicated page listing pre-approved cybersecurity solutions under the auspices of SMEsGoDigital and referring to the names and contacts of the companies as such.
https://www.csa.gov.sg/Programmes/psg-cybersecurity-solutions

The French National Cybersecurity Agency (ANSSI), in its capacity as a national authority, is organising a ceremony to promote its Visa de sécurité for trustworthy cybersecurity solutions on a yearly basis. While there are many and various cybersecurity solutions available on the market, they are not all equally effective and robust. On 29 June 2021, more than 246 certified and qualified products and services were promoted on this particular occasion.https://www.ssi.gouv.fr/actualite/lecosysteme-cyber-en-pleine-expansion/



For its part, the EU **ENERG-label** has developed a promotional campaign to boost end users' awareness for a period of three years from 2019>2022 under the Belt[79] project. This campaign is totally funded by the Commission with an overall budget of circa €1,500,000.

****

With respect to our activities, we will capitalize on the knowledge collected on the various markets studied, while promoting the best use-cases in our model.

Concerning the future framework labelling, it may in particular allow the following specific objectives in a pilot-phase at first:

- explaining the processes associated with certification and informing end users of certified solutions;
- encouraging certified solutions from providers;
- promoting European certification and its related ecosystem, e.g. certified solutions and also CABs including CBs and ITSEFs/auditors.

In parallel, a similar effort will have to be deployed vis-à-vis the end users via ENISA ARET team and the Communication Unit.

In this context, it is recommended that we focus our labelling workplan on:

- **the pertinence of a European framework;**
- **the promotion of solutions based on certification to allow better information, visibility, comparison and choice;**
- **the support for competitive advantage and excellence in accordance with common grounds;**
- **the incentivisation of cybersecurity certified developers;**
- **the surveillance of market conditions;**
- **the awareness campaign.**

This concludes our chapter on the objectives assigned and validated by the participants on the occasion of their plenary on 10 June 2021.

[79] https://www.belt-project.eu/belt/tv
BOOST ENERGY LABEL TAKE UP | BELT Project | H2020 | CORDIS | European Commission (europa.eu)
https://cordis.europa.eu/project/id/847043
Project Information BELT Grant agreement ID: 847043 Start date 1 September 2019 > End date 28 February 2022
Funded under H2020-EU.3.3.7. and H2020-EU.3.3.1. Overall budget €1,499,98875 - EU contribution €1,499,98875
Coordinated by ALTROCONSUMO EDIZIONI SRL Italy

3. LEGAL TERMS AND REQUIREMENTS FOR LABELLING CYBERSECURITY CERTIFICATION

Thanks to the assistance of a very active LEGAL sub-group, led by Thomas NIESSEN, our labelling activities have explored the legal terms and requirements in which we need to deal in establishing a cybersecurity label.

CSA Article 54.1 provides that 'A European cybersecurity certification scheme shall include at least the following elements: i) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used.' The European Cybersecurity Certification Framework[80] may provide for a label and associated mark. When available, such a label shall be specifically implemented for this scheme, in order to allow its application on each certificate, certified ICT product and related documentation. A label and associated mark shall only be used when the certificate is awarded and until its expiration: failure to respect this condition shall be considered an irregularity.

Remember that the prime purpose of the **ISO 17030** international standard is to:

- enable a uniform approach to the use of marks of conformity;
- fill relevant gaps in existing ISO, IEC, ISO/IEC Standards and Guides;
- address potential problems arising from different uses of marks of conformity;
- provide a clear and rational basis for their use and
- set out general requirements.

For the purposes of this document, the terms and definitions given in the international standardisation[81] **ISO/IEC 17000 series**[82] apply.

As **'marks of conformity'** labels are protected mark[83] issued by a body performing third-party conformity assessment. These indicate that an object of conformity assessment such as product, process, person, system or body, conform with specified requirements. Marks of conformity can be product certification marks, quality management system certification marks etc.

The **ISO/IEC 17028:2019** describes the role of marks of conformity (labels) in the framework of a **scheme**:

> **6.7.2.1** The scheme can determine if a specific mark of conformity will be granted. If this is the case, the scheme should specify requirements for its use, ensuring that it is used only in conjunction with the certified service, e.g. on sales literature or promotional material.
>
> **6.7.2.2** The owner of a mark of conformity is responsible for protecting the mark legally against unauthorized use.
>
> **6.7.2.3** Marks of conformity and their use should be in accordance with ISO/IEC 17030

ISO/IEC 17030:2003[84] provides general references for marks of conformity, including definitions and specific requirements concerning their **conditions of issue and use**[85] as indicated in Article 54.1 (CSA) under Elements of European cybersecurity certification schemes ''**a** European cybersecurity certification **scheme shall** include at least

[80] EUCC candidate scheme, May 2021
[81] OECD Digital Economy Papers, Enhancing the digital security of products. Feb.2021 p43. If labels are not based on recognised public standards e.g. international ones, they may lack transparency and consistency regarding the criteria used to award the label.
[82] https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:en ie 17028, 17030
[83] a protected mark is a mark legally protected under intellectual and/or industrial property law against any unauthorized use.
[84] Currently under review see CEN/CENELEC
[85] Article 54 (CSA) Elements of European cybersecurity certification schemes 1. A European cybersecurity certification scheme shall include at least the following elements… (i) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used.

the following elements… (i) where the scheme provides for marks or labels, the **conditions** under which such **marks** or **labels** may be used.''

The **objective** of the work of this sub-group is to define the legal framework that must be respected in the issuing and during the lifecycle of the cybersecurity label. The label is in this context defined as a mark of conformity to the respective scheme under the EU Cybersecurity Act.

Since this forms the basis for the processes of issuing as well as for the processes of surveillance, and also has an impact on the processes of communication, the legal sub group has a transversal function throughout all detailed aspects of the Thematic Group on Labelling Cybersecurity Certification.

The work obviously has to take into account the general objectives of the Cybersecurity Label, i.e. to strengthen the trust and confidence in digital products, services, processes and solutions across the EU. It must also allow for the suppliers of such products to demonstrate their cybersecurity awareness and cybersecurity competence to their customers. These differentiated criteria may lead to an elevation of the general level of cybersecurity awareness and more secure products and services throughout all of Europe.

In the following sections the aspects to be taken into consideration are outlined.

3.1 OWNER OF A MARK OF CONFORMITY AND OBLIGATIONS

Ownership

The owner is the organisation that has the legal rights to a mark of conformity (ISO 17030 3.2). In the case of the EU Cybersecurity label this owner has to be defined. The owner subsequently should define a governance process for the label and all accompanying regulations. Since the owner is holding the intellectual property rights to the label, it is also his responsibility to protect the mark, e.g. by registering a trademark. At this point in time, a decision on the ownership of the label has not yet been taken. In addition, the ENISA Labels TG insists that the labelling scheme and its management be operated by the same entity. The owner of the label is generally synonymous with ownership of the Conformity Assessment Programme.

State-of-Play
Status 1: ENISA is not the owner of labels as at the date of this report
Status 2: the European Commission[86] through the European Union is managing and supervising various EU labelling schemes
Status 3: Cybersecurity National Agencies[87] are the owners of their respective cybersecurity labels
Status 4: a partnership of companies and consumers under the auspices of EU is the owner and supervisor of its labelling scheme; an example being the PEGI-label.[88]
Status 5: regarding stakeholder-based organisations such as, for example, the ECSO-label[89], ECSO remains the sole owner and supervisor of its own labelling scheme. It does not issue the label.

[86] The **CE marking** Reg No 765/2008 Art 1.4 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008R0765
The **ECO-label** was established in 1992 - Regulation (EC) No 66/2010 of and the Council of 25/11/2009 on the EU Ecolabel: *"The scheme is intended to promote those products which have a high level of environmental performance through the use of the EU Ecolabel" (rec. 5)* based on the only EU-wide ISO 14024 Type 1 Ecolabel (reliable; multi-criteria; life-cycle approach; open-transparent-multi-stakeholder and science-based criteria setting; third party verified). It is managed by the European Commission and the Competent Bodies.
The **ENERG-label** established by COMMISSION DELEGATED REGULATION (EU) No 1062/2010 of 28 September 2010 supplementing Directive 2010/30/EU of the European Parliament and of the Council with regard to the energy labelling of televisions https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32010R1062 Regulation (EU) 2017/1369 of the European Parliament and of the Council of 4 July 2017 setting a framework for energy labelling: • Set the framework for labelling of energy related products • Delegated acts (Regulations) set requirements on specific products • Established the "product database" and its "portal" (one-stop-shop for ecodesign labelling regulations)
[87] ANSSI, CCN, CSA-SGP, etc…
[88] **PEGI-label** based on Council Resolution on the protection of consumers, in particular young people, through the labelling of certain video games and computer games according to age groups, 1 March 2002 (OJ C 65, 14.3.2002, p. 2).
[89] https://ecs-org.eu ECSO does not accept applications from companies and does not issue the label. However, it remains the sole owner and supervisor of the Label scheme.

Label ownership and Scheme Supervision

The owner of a mark of conformity is naturally the scheme supervisor. This does not automatically mean that supervision of the scheme is managed by the owner of the mark of conformity. This task can be delegated. ECSO and PEGI remain the sole supervisors of their respective labelling schemes. Other EU labelling schemes are generally supervised by the Commission and the competent bodies directly. It could be an option that the European Commission is *es quality* the owner of a future cybersecurity label, but the manager of the labelling scheme would be ENISA and its certification team.

Obligations – when supervising the labelling scheme, the owner of the mark of conformity shall comply with the following obligations:

- ❑ **Labelling schemes rules** - the owner shall have rules governing the use of its mark of conformity. (17030)
- ❑ **Legal protection** - the owner is responsible for protecting the mark legally against unauthorized use see ISO17028>6.7.2.2. The owner of a mark of conformity shall be responsible for protecting the mark legally against unauthorized use' see ISO17030. The owner shall provide, on request, information that explains the meaning of the mark of conformity. The owner shall maintain and update a list of objects that have been granted the mark of conformity based on their assessment of conformity. This list shall be available on request. He shall maintain, update and make available on request, a description of the rights and obligations of licensees, and other restrictions or limitations on the use of the mark.
- ❑ **Licensing**[90] - When the owner or the issuer of the mark of conformity grants a license for the use of that mark by others, a binding agreement shall be made according to the rules governing the use of the mark of conformity.
- ❑ **Governance or Compliance** in particular, the licensing rules shall require the licensee to:
  - control the use of the mark of conformity;
  - take measures to minimize misunderstandings and lack of clarity regarding the mark of conformity that could lead to a reduction in its effectiveness;
  - have rules to ensure that the mark of conformity and any accompanying information are not misleading and take action against their use in a misleading way;
  - undertake all necessary investigations to monitor the ongoing compliance by the holder with both the product group criteria and the terms of use and provisions of this contract
  - take corrective actions in case of non-conformity and have measures to protect and monitor the use of the third-party mark of conformity;
  - take actions to resolve misuses of the third-party mark of conformity, including withdrawal of the mark or appropriate legal action;
  - keep a record of all complaints relating to the use of the mark of conformity and make these available to the owner/issuer.

Example: ECSO partnership agreement[91] with each qualified issuer includes requirements to:

- ❑ inform interested parties about the label and its application process within of maximum of two weeks;
- ❑ accept applications and verify their eligibility for acquiring and renewing the label;
- ❑ keep a record and provide annual reports of the applications received and labels issued;
- ❑ support ECSO in communicating and promoting the label within their networks;
- ❑ cover the financial costs relating to the issuance of the label;
- ❑ revoke the right to use the label in cases of misuse, untrue statements or loss of eligibility by the user (see compliance chapter).

Rights

In return, ECSO commits to:

- ❑ granting the right to issue the label to organisations interested in becoming qualified issuing partners;
- ❑ maintaining the registry of applications and the European companies that have been labelled and managing the registry in accordance with the European Union data privacy and protection rules;
- ❑ ensuring the communication and marketing of the label at the European level;
- ❑ supervising and protecting the label trademark and its image;
- ❑ providing expertise and communication support to qualified issuing partners.

[90] ISO/IEC TER 17032:2019 ANNEX E Example of the contents of a licensing agreement for the use of a certificate and mark of conformity
[91] https://www.ecs-org.eu/documents/uploads/label-brochure-for-potential-partners.pdf

Therefore, the ENISA Labelling TG recommends that management of the labelling scheme falls under its sole mandate in the future certification website under the supervision of the European Commission and the competent bodies.

For the sake of consistency and legal certainty,[92] **RECOMMENDATIONS WITH RESPECT TO OWNERSHIP** will require further considerations as follows:

At Commission level,

- **Additional discussions will have to take place on the issue of the ownership of a future European cybersecurity labelling scheme;**
- **The issues of governance and supervision of the eco-system will have to be addressed in the knowledge that governance bodies shall supervise the surveillance of their market by national authorities and the management of their website or database;**

At ENISA level,

- **In this respect, its certification schemes, should be privileged when dealing with the issue of ownership and supervision;**
- **In any case, through its European certification schemes and website in conformity with Article 50, ENISA shall remain the manager of the labelling scheme, and in particular when dealing with its dedicated page and, possibly, its label generator;**
- **In this framework, a common register or registry will have to be put in place and be updated regularly. For the section authorized, this database shall be publicly available on the website dedicated to the EU cybersecurity certification.**

3.2 ISSUER OF A MARK OF CONFORMITY AND OBLIGATIONS

Issuer
The issuer is the body that grants the right to use a mark of conformity (ISO17030). The issuer may not be the owner of the mark of conformity, and may be authorized to sub-licence other bodies. Who is eligible to issue the EU cybersecurity label has yet to be defined. In other certifications, it is common practice that the conformity assessment body (CAB) which has issued the certificate will also issue the label (and subsequently bear responsibilities regarding surveillance). But it is also possible that the label will be issued by a separate entity (e.g. ENISA or an NCCA) appointed by the owner of the label. In particular, in the case of a statement of conformity there is obviously no CAB involved. The decision in this matter has not yet been taken.

State-of-Play

Status 1: the ENISA certification schemes
Certification schemes are not issuing labels as at the date of this Report.
Note: ITSELF status?

Status 2: the European Commission
Through the respective management of its databases and its labels enabler or generator, the European Commission is issuing labels

see ENERG-label / EPREL
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02017R1369-20210501

see ECO-label database ECAT User manual.pdf (europa.eu) https://webgate.ec.europa.eu/ecat_admin/

The EU Ecolabel Catalogue administration information system (ECAT_Admin) is an online open tool put in place to manage EU Ecolabel licences and products/services, deployed since July 2020.

www.ec.europa.eu/ecat/docs/ECAT20User%20manual.pdf

[92] Intellectual property law in particular and licensing

Status 3: NCCA I CAB I ITself
As certified bodies, NCCA, CAB and ITSELF can issue their respective certificates or statements and/or collaborate with the EU labelling scheme to generate cybersecurity labels thanks to the certification database or the transparency registry managed by the ENISA ECCF website and supervised by the competent bodies, for instance.

Status 4: Trusted bodies
see ECSO list of qualified issuing partners[93]

Status 5: Companies directly
see CE marking
Manufacturers play a crucial role in ensuring that products placed on the extended single market of the European Economic Area (EEA) are safe. They are responsible for checking that their products meet EU safety, health, and environmental protection requirements. It is the manufacturer's responsibility to assess the conformity of their products, set up the technical file, issue the EU declaration of conformity, and affix the CE marking to a product as generated by the CE marking system.
See ITSELF cybersecurity level basic

Rights

- The competent body which has awarded the certificate number to a product or service or software shall notify the ENISA ECCF Registry thereof or the NCCA within a reasonable time in order for the system to generate the EU cybersecurity label;
- The issuer, i.e. the certification body to which an application is made shall charge fees. The financial incentive for the use of the EU cybersecurity label shall be conditional upon the fees having been paid in due time and the receipt of the certificate registration in the database;
- Aob…

Obligations

The issuer shall have rules governing the use by applicants of the mark of conformity (ISO17030>...), in particular:

- an application shall specify the full contact details of the applicant or operator, as well as the product group in question and shall contain a full description of the product, including the URL or the website, as well as all other information requested by the competent certification body and referred to future label and certificate number, including a correct display of the label on its product or service and website or webpage dedicated to the product or service;
- a contract with each operator covering the terms of use of the EU cybersecurity labelling, including provisions for the authorisation and withdrawal of the EU cybersecurity labelling shall be concluded. To that end a standard contract shall be used in accordance with the template in Annex XXX;
- the issuer shall provide, on request, information that explains the meaning of the mark of conformity;
- the issuer shall maintain and update a list of objects, that following assessment, have been granted the mark of conformity and, that list shall be available on request;
- the issuer of a mark of conformity shall maintain, update and make available, on request, a description of the rights and obligations of licensees and other restrictions or limitations on the use of the mark in accordance with the owner's rights and obligations.

For the sake of consistency and legal certainty[94], **RECOMMENDATIONS WITH RESPECT TO ISSUANCE** are as follows:

- ❑ **the labelling scheme will be based on certified cybersecurity solutions[95] through the respective European schemes;**
- ❑ **in this respect, under the supervision of certification schemes, qualified issuing partners or bodies will be granted a license[96] for the use of the mark or labels;**

[93] https://ecs-org.eu/initiatives/cybersecurity-made-in-europe
[94] Intellectual property law in particular and licensing
[95] On the matter of the "Terms of Use", the label is to be awarded to all goods distributed, consumed or used on the EU market on condition that the cybersecurity certificate has been obtained see (TG10) Report on Guidance regarding manufacturer/provider commitments applicable to the EUCC Scheme, July 2021
[96] See a binding agreement shall be made according to the rules governing the use of the mark of conformity (ISO17030).

- **vis-à-vis applicants for the award procedure of a certificate and label, economic operators shall submit an application to the competent issuing body, which will verify the binding requisites regarding the criteria of the label;**
- **providers of certified solutions will have to respect an established communication framework concerning their respective certificates or statements, i.e. what to say, how to apply the logo associated with the label etc.**

3.3 HOLDER OF A CERTIFICATE INCL. A MARK OF CONFORMITY, RIGHTS & OBLIGATIONS

Along with our Recommendations and in line with TG10 Report 5.1.6, manufacturers or providers will be strongly advised to commit to scrupulously respecting the rules[97] governing the use of the label established for the scheme, in their roles as holders of one or several certificates as follows:

Rights

1. The holder has the right to use the EU cybersecurity label for its certified products or services as described in the annexed product or service specifications;
2. The EU cybersecurity label may be used on the products or services for which the EU cybersecurity label has been awarded and on their associated promotional material;
3. The holder shall be responsible under this contract for the manner in which the EU cybersecurity label is used in relation to the certified product or service, especially in the context of advertising and commercial practices;
4. The EU cybersecurity label shall be used only in the forms stipulated;
5. The holder is entitled to respect the use of the label and its display;
6. The right to use the label is linked to the payment of an annual fee.

Obligations

7. Any operator who wishes to use the EU cybersecurity label shall apply to the competent body i.e. the issuer;
8. The operator shall use the EU cybersecurity label in connection with the products and services certified on the basis of a certificate or statement of conformity;
9. The operator shall comply with the EU cybersecurity label criteria applicable to the products and services concerned and for which the EU cybersecurity label has been awarded;
10. The operator may place the EU cybersecurity label on the product only after conclusion of the contract and registration in the database;
11. The operator shall also place the registration number on the product bearing the EU cybersecurity label;
12. The holder shall ensure that the product or service to be labelled complies throughout the duration of his contract with all the terms of use and provisions as set out at all times;
13. A new application to obtain a new certificate including a new label will be required when substantial modifications in the characteristics to the products or services have occurred (ISO 17065);
14. The holder shall not advertise or make any statement or use any label or logo in a way which is false or misleading or which results in confusion with, or calls into question the integrity of, the EU cybersecurity label;
15. The award of the EU cybersecurity label shall be without prejudice to other regulatory requirements of Community or national law applicable to the product.

[97] Examples
Code of Conduct > The PEGI Code of Conduct | Pegi Public Site
Eco-label > EUR-Lex - 32010R0066 - EN - EUR-Lex (europa.eu)

3.4 AWARD, CONDITIONS & TERMS OF USE

The scheme can determine whether a specific mark of conformity will be granted. If this is the case, the scheme should specify requirements for its use, ensuring that it is used only in conjunction with the certified service,[98] e.g. on sales literature or promotional material. (ISO17028>6.7.2.1) similar to how it is usually described in EC law[99]. Moreover, during 2021 relevant EU-CC working groups issued recommendations[100] with respect to certain aspects of labelling.

Recommendations from the LABELLING sub-group LEGAL underline that a label must be:

1. in conformity with **specified requirements** (ISO 17030, Section 3) and defined **rules** (ISO 17030, Section 4.2)
2. based on a valid **certificate** or **Statement of Conformity** according to the EU-CSA
3. **traceable** to the specified requirements (ISO 17030 Section 5.3)

On this basis, the Legal Sub-group has agreed upon the following set of principles for the Cybersecurity labelling detailed below in 3.4.1, 3.4.2 and 3.4.3.

3.4.1 The EU cybersecurity label is in conformity with **ISO 17030, Section 4.2**

The certification scheme will thus define the requirements necessary for obtaining a EU cybersecurity label. This also extends to the definition of the objects of assessment for conformity which corresponds to the subject matter mentioned in Article 54.1a of the EU Cybersecurity Act.

> As an example, the EU-CS candidate scheme states that any type of ICT service, provided: the ICT service implements one or more capabilities offered through cloud computing that are invoked using a defined interface [ISO17788], can be the object of an assessment of conformity.

The specified requirements for a label thus derive from the underlying certification scheme and correspond to the defined assurance levels of the scheme which may differ in scope, depth and rigour.

3.4.2 It is based on a **valid certificate or statement of conformity** according to the EU-CSA

The first consequence is that the label can only be issued upon successful completion of a certification process or the acceptance of a statement of conformity (according to Article 53 of the EU Cybersecurity Act).

According to TG10 22 Report on Marks & Labels, without prejudice to Chapter 10: Marks and Labels of the EUCC version 1.1.1, the European Cybersecurity Certification Framework will provide for a label and associated mark. A label and associated mark will be based on the ISO/IEC 17065 and shall only be used when the certificate is awarded and until its expiration. Failing to respect this condition shall be considered an irregularity.

[98] see LABELLING COMPLIANCE sub-group
[99] CE marking Art.30 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008R0765
[100] Regarding the Terms of Use of the labels and marks, the TG10 refers to the work done by TG3. On the matter of the "Terms of Use" of the label, the following elements, already covered by other European labelling schemes, should be addressed:

1. Aim of the labelling scheme: By means of transparent criteria, it enables consumers to make conscious choices regarding the features and capabilities of certified products.
2. Key points of the labelling framework:
   - The label is to be awarded to all goods distributed, consumed or used on the EU market on condition that the cybersecurity certificate has been obtained;
   - Using a label without the legal prerequisite is equivalent to a fraud.
3. Identification of competent bodies: European Commission; ENISA; NCCAs; CABs.
4. Procedure for award and use of labels: In order to be awarded with a label, economic operators shall submit an application to the competent body which, once the binding requisites regarding the label criteria have been verified, will issue the label. ??? instead will issue the certificate including the label.

EUCC > (TG10) Report on Guidance regarding Manufacturer or Provider Commitments applicable to the EUCC scheme, July 2021

The label and associated mark will:

- highlight the fact that the ICT product has been certified in the European Union (to check if EU certified is better) and will provide immediate information regarding the certificate by making reference to the framework, the evaluation scheme and the assurance level;
- make certification easily recognizable as both the label and the associated mark may be printed on the package of the product, on technical documents and on leaflets used for marketing purposes;
- provide a direct link (in the form of a QR code) to the ENISA ECCF website (as required by Article 50 of the CSA) - where all the information regarding the certificate is disclosed, including the current status of the certificate.

At this point in time, the existing candidate schemes (Common Criteria and Cloud Services) do NOT include statements of conformity as means for obtaining the "Basic" assurance levels, but nonetheless the label concept should be valid for potential upcoming schemes that allow for statements of conformity.

As a second consequence, the label "shares the fate" of the validity of the underlying certificate or statement of conformity. If a certificate is suspended or revoked or if the period of validity of the certificate has expired and no renewal has been initiated, the label shall not be applicable for the object of conformity any longer.

As a third consequence, the label may be used solely as a mark for the object of conformity. The label is awarded to an actual object of conformity specified by the underlying scheme and therefore may only be used for the purpose signifying this. It may not be used in a way that might suggest that an entire company has been labelled instead of particular products and/or services.

3.4.3 The EU cybersecurity label for an object of conformity assessment shall **be traceable** to the specified requirements (see ISO 17030 Section 5.3)

The label shall include a reference to the underlying certification scheme (or statement of conformity) and allow for verification of at least the assurance level and the validity for the object assessed as to its conformity.

Therefore, the inclusion of a unique identifier for each label issued must be foreseen. This also could be achieved by integrating a QR Code (or comparable Bar-Code) into the label which would provide an unambiguous reference to the certificate or statement of conformity of the service or product.

3.5 COMPLEMENTARY FEATURES IN LINE WITH ISO/IEC 17065

3.5.1 (CSA) Recital (74) & GDPR requirements

When related to
- Database
- Identification of companies
- …

The Cybersecurity Act furthermore refers to labels in Recital 74:

Recital 74

The provisions of this Regulation should be without prejudice to Union law providing specific rules on the certification of ICT products, ICT services and ICT processes. In particular, Regulation (EU) 2016/679 lays down provisions for the establishment of certification mechanisms and of data protection seals and marks, for the purpose of demonstrating the compliance of processing operations by controllers and processors with that Regulation. Such certification mechanisms and data protection seals and marks should allow data subjects to quickly assess the level of data protection of the relevant ICT products, ICT

services and ICT processes. This Regulation is without prejudice to the certification of data processing operations under Regulation (EU) 2016/679, including when such operations are embedded in ICT products, ICT services and ICT processes.

So, while it is made clear that the certification and also the use of marks of conformity and data protection seals according to the GDPR (Art. 42, 43) are beyond the scope of the regulation some mechanisms which are already defined as mandatory in the accreditation processes of certification schemes und Article 42 GDPR can serve as guidance in developing the corresponding mechanisms for the EU Cybersecurity labels.

This is especially valid since in both instances the basis for the accreditation is very similar.
Article 60 of the EU Cybersecurity Act states:

Article 60

Conformity assessment bodies

(1) The conformity assessment bodies shall be accredited by national accreditation bodies appointed pursuant to Regulation (EC) No 765/2008. Such accreditation shall be issued only where the conformity assessment body meets the requirements set out in the Annex to this Regulation.
(2)

Whereas Article 43 (1) of the GDPR defines:

Art. 43 GDPR

Certification bodies

(1) …Member States shall ensure that those certification bodies are accredited by one or both of the following:
(a) the supervisory authority which is competent pursuant to Article 55 or 56;
(b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council[1] in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

So, in both instances the ISO CASCO Toolbox (ISO - ISO/CASCO - Committee on conformity assessment) forms an essential framework for managing compliance and providing an objective and defensible means to implement public policy and enforce legislation.

See protection of DATA in ECCF webportal in ANNEX XXXXX or in future work

Should a compliance section of the database be established, it will have to be in accordance with the following criteria:

(a) protection from unintended use and the safeguarding of confidential information by way of strict security arrangements;
(b) access rights based on the need-to-know principle;
(c) processing of personal data in accordance with Regulation (EC) No 45/2001 and Directive 95/46/EC, as applicable;
(d) limitation of data access in scope to prevent copying larger data sets;
(e) traceability of data access for the supplier with regard to its technical documentation.

3.5.2 Data & Compliance

The data in the compliance section of the database shall be treated in accordance with Commission Decision[101] (EU, Euratom) 2015/443. In particular, the specific cybersecurity arrangements of Commission Decision[102] (EU, Euratom) 2017/46 (2) and its implementing rules shall apply. The confidentiality level shall reflect the consequential harm resulting from disclosure of the data to unauthorised persons.

[101] Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).
[102] Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission (OJ L 6, 11.1.2017, p. 40). 02017R1369 — EN — 01.05.2021 — 001.001 — 17

This document endorses the definition of data under ISO/IEC 2382-1, considering data as “a reinterpretable representation of information in a formalized manner, suitable for communication, interpretation or processing.” It is, thus, needed that “Data should not be treated as a four-letter word. The concept of data encompasses data of any form, nature or structure, that can be created, uploaded, inserted in, collected or derived from or with cloud services and/or cloud computing, including without limitation proprietary and non-proprietary data, confidential and non-confidential data, non-personal and personal data, as well as other human readable or machine-readable data”.

3.5.3 IPR Requirements

Usually, brand names are trademarked[103]. The label design can also be protected under trademark, such as in the case of PEGI. The 3, 7, 12, 16 and 18 age labels are protected under trademark[104] in Europe and India. Copycats[105] emerge in the cases of PEGI and the European ENERG labelling.

The label for cybersecurity certification may not fall under IP, perhaps its design. Often, another option is to standardize the format. In Germany, BSI label is standardized.

The ENISA ECCF website will have a copyright notice, as a fairly standard format. The aim is to have the information on the website distributed as widely as possible, so to actually encourage partners to adopt our messaging.

Depending on the circumstances, the nature and impact of failure to respect the rules, wrongful use, misuse or, abuse of the mark and or label may have other legal implications regarding the protection of IP rights, possible criminal allegations (e.g. fraud, deceit), market surveillance regulations related to consumer protection (e.g. misleading and or unlawful comparative advertising or distribution of products).

These legal implications are outside the scope of this EUCC scheme[106].

These final points conclude the legal section of our recommendations regarding labelling cybersecurity certification.

[103] ISFE example https://www.tmdn.org/tmview/#/tmview/detail/EM500000003008810
[104] PEGI https://www.tmdn.org/tmview/#/tmview/detail/EM500000008929581
[105] PEGI rating copycat https://en.wikipedia.org/wiki/General_Commission_for_Audiovisual_Media
[106] https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme

4. LABELLING IMPLEMENTATION

Thanks to the expertise of a very dynamic IMPLEMENTATION sub-group, led by Jose RUIZ-GUALDA, our labelling activities have explored the requirements it would be useful to focus on when establishing a cybersecurity label. As indicated earlier, with respect to labelling, the CSA article 54.1 provides that a European cybersecurity certification scheme shall include at least where the scheme provides for marks or labels, the **conditions** under which such marks or labels may be used.

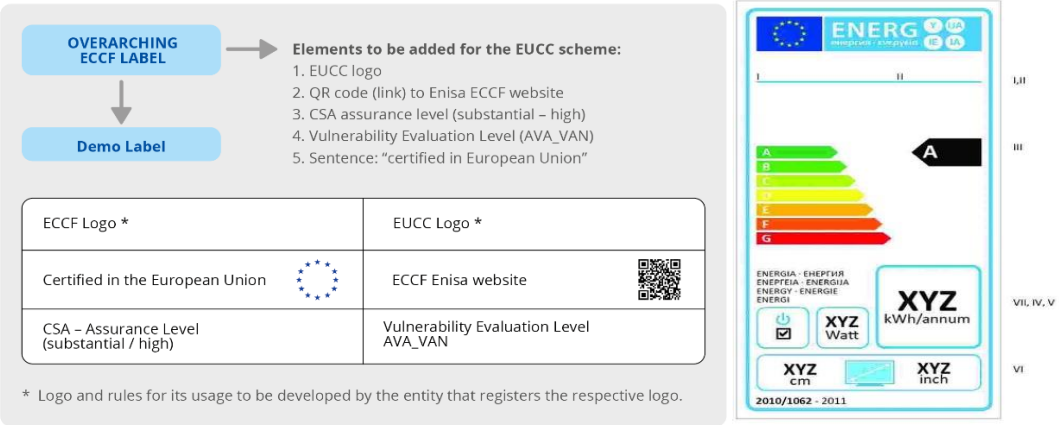
4.1 FROM EUCC CANDIDATE SCHEME TO FUTURE SCHEMES

The European Cybersecurity Certification Framework may provide for a label and associated mark. When available, such a label shall be specifically implemented for this scheme, in order to allow its application on each certificate, certified ICT product and related documentation.

4.1.1 Conditions under EUCC scheme[107]

A label and associated mark shall only be used when the certificate is awarded and until its expiration. To this end, a label and associated mark, established for the European Cybersecurity Certification Framework and specifically implemented for this scheme, will:

- highlight the fact that the ICT product has been certified in the European Union and provide immediate information regarding the certificate by making reference to the framework (ECCF), the evaluation scheme and the assurance level;
- make the certification easily recognizable as both the label and the associated mark may be printed on the package of the product, on technical documents and on leaflets used for marketing purposes;
- provide a direct link (in the form of a QR code (or a comparable code) to the ENISA ECCF website or webportal - as per Article 50 - where all the information regarding the certificate are disclosed, including the current status of the certificate;
- enable a logo of the ECCF/EUCC to be registered, regulated and protected by the entity in charge of the enforcement of the labelling framework;
- enable the creation of a QR code pointing to the web portal of ENISA and to the page where the effective status of the certificate of the product and the information regarding its lifecycle can be retrieved. The introduction of the QR code will imply, as defined by Chapter 20, Disclosure Policy for Certificates, a procedure for the release of the QR code;
- enable a CSA assurance level (with the introduction of a specific colour identifying each level) and related vulnerability evaluation to the AVA_VAN level;
- support the wording “Certified in the European Union” better EU certified?, together with the flag of the EU.



[107] https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme

Figure 1: The demo label to the EUCC scheme shows the basic information that the label associated with the scheme may contain. It is expected that a label will be associated with the European Cybersecurity Certification Framework, and will be specifically implemented for each scheme, including the EUCC scheme. CYBERSECURITY CERTIFICATION V1.1.1 | MAY 2021 36

4.1.2 Labelling Fundamental Requirements, Specification & Rationale

The requirements and specifications have been arrived at after a thorough analysis by experts. The analysis has taken into account different aspects such as the coverage of the label, the audience for the label or the requirements for accessibility. Below, the label requirements, specifications, and rationale are presented:

Category	Specification	Rationale
Audience	The audience for the label should take into account a wide range of end users from professionals to consumers. The label shall therefore be adaptable to for various audiences.	The label should be simple for consumers and allow access to detailed information for all end users.
Accessibility	It is a requirement that the various components e.g. QR code and colors of the label must take accessibility into account. W3C standard shall be used to develop websites https://www.w3.org/standards/	The label must be accessible for every kind of user regardless its defects on different devices such as phone, pad, laptop, etc.
Consistency	The label shall emphasize that EU certification is fostering the European market. Member States with no national labelling, as well as the EFTA countries implementing the CSA, should be encouraged to use the EU label as a priority.	National initiatives are outside the scope of the label. National requirements can be maintained by Member States. A transition period will be organised to deal with consistency of the eco-system. During this period, national labels, regardless of their goals (qualification, promotion, etc…), may co-exist with the label.
Coverage	All CSA schemes must be covered by labelling.	Article 54.1 states as follows *A European cybersecurity certification scheme shall include at least the following elements:* *i) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used."* Therefore, the CSA contemplates the use of labels for all schemes.
Eligibility	ICT certification (at different levels) or a statement of conformity under the CSA must be achieved before obtaining the label.	The label must allow end users to make an informed decision for acquisition or procurement. Therefore, the label aims to cover the full scope defined by the CSA. EUCC Candidate Scheme chapter 10, v1.1.1, May 2021 *When available, such a label shall be specifically implemented for this scheme, in order to allow its application on each certificate, certified ICT product and related documentation.* The label and associated mark shall only be used when the certificate is awarded or a statement of conformity is issued and only from then until its expiration.

Information display	Information shall be presented in a layered incremental approach. Static and dynamic information must be presented.	The goal of the label is to promote assessment of certification or conformity. Simplicity is important to engage end users. Information must be static if the label is going to be printed or displayed. Information should be dynamic to support the surveillance of the market and avoid revoked products, services or processes continuing to use the label.
Stability Durability Universality	The graphical representation of the framework label shall be stable over time to allow manufacturers to display it for their products, services or processes and for end users to get used to it so that it can be recognized quickly.	The label might be printed or displayed by applicants. The graphical representation of the label (e.g. logo) shall not be modifiable during the time[108] of its validity. For EUCC Candidate Scheme, v1.1.1 Chapter 10 *a label and associated mark shall only be used when the certificate is awarded and until its expiration.*

According to Blythe and Johnson, 2018 research[109], labelling schemes should insist on:

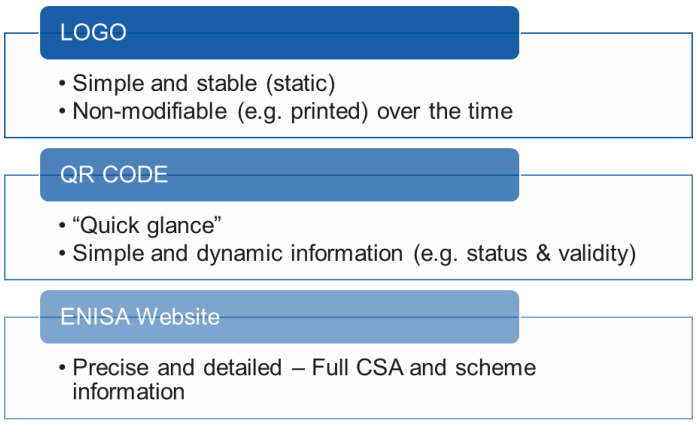
• **Simplicity**. In the EU, the introduction of A+ to A+++ in energy labels[110] has undermined the efficacy of the label as consumers did not perceive the difference between A+ to A+++ as the same as A to G. Similarly, traffic light nutrition labels have proven less effective than binary labels or scoring nutrition labels to drive better consumer choice.

• **Stability, Durability, Universality**. The more often consumers are exposed to a label, the more they understand it and the more likely they are to be positively influenced by the label. Unless the label is ubiquitous and mandatory on all products (e.g. nutrition scores), its absence is not considered by consumers as a sign of increased risk.

• **Comparability**: effective labels enable consumers to easily compare between products of the same category, and acknowledge various levels of maturity or conformity

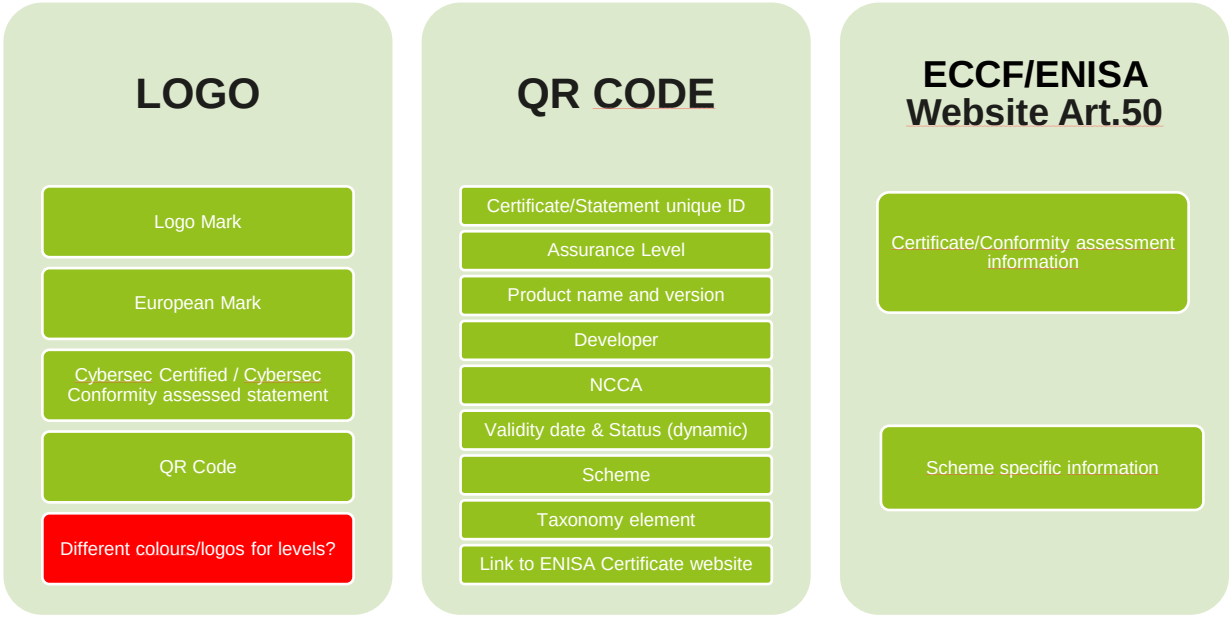
4.2 LABEL COMPONENTS & STRUCTURE

The label has been designed to provide the information in different layers. The information to be provided in each layer will be incremental. The following layers have been defined:



[108] It remains open to discussion whether the validity period and the level of assurance (B, S, H) may be present in the graphical representation of the label.
[109] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/949614/Rapid_evidence_assessment_IoT_security_oct_2018_V2.pdf
[110] Confirmed by Paolo TOSORATTI, DG GROW presentation on 10 June 2021

The following information must be included in each layer:



4.2.1 CYBERSECURITY LOGO MARK & VISIBLE REFERENCES

A non-exhaustive list of references is documented as follows:

- a logo providing visible and readable information at first glance or at fingertips
- a logo recognisable at first sight and not modifiable over the time (static information)
- a single viewable, downloadable and printable file of the cybersecurity label for each model
- a logo to be printed and used by a manufacturer for the promotion of certified products or services
- a logo centred around a symbolic image or icon related to cybersecurity
- a logo centred around a symbolic image, icon or flagship related to Europe[111]
- a differentiated logo depending on the CSA level[112] of insurance including with, for instance, the introduction of specific colours i.e. Gold, Silver, Copper or symbols e.g. asterisk (see password)
- a logo including the wording *Cybersecurity Certified* or *Cybersecurity Conformity Assessed* and/or a link to the ENISA ECCF website (URL, domain name tbc)
- a logo including a QR Code as a specific requirement of the EUCC candidate scheme

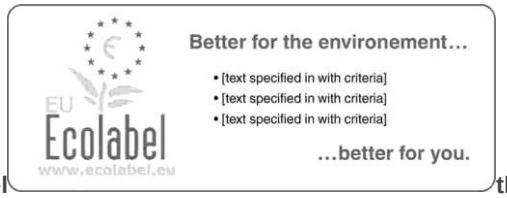
a logo centred around a symbolic image, icon or flagship related to Europe
like in the ENISA logo with a reference to
EU CYBERSECURITY AGENCY or CYBERSECURITYAGENCY.EU ?

[111] The use of the European Flag has been suggested as important if this fits with the official rules of the EU emblem: https://europa.eu/european-union/abouteuropa/legal_notices_en#emblem

[112] QR code linked information will specify the CSA Level concerned, the so-called **usability** by giving a clear and simple indication to the users of the provided level of trust.

Case-Study: Model of the ECO-label without QR code

the label



the optional label

registration number[113]

Case-Study: Models of National Cybersecurity labels without QR code

Case-Study: Model of Finnish logo IoT with QR code

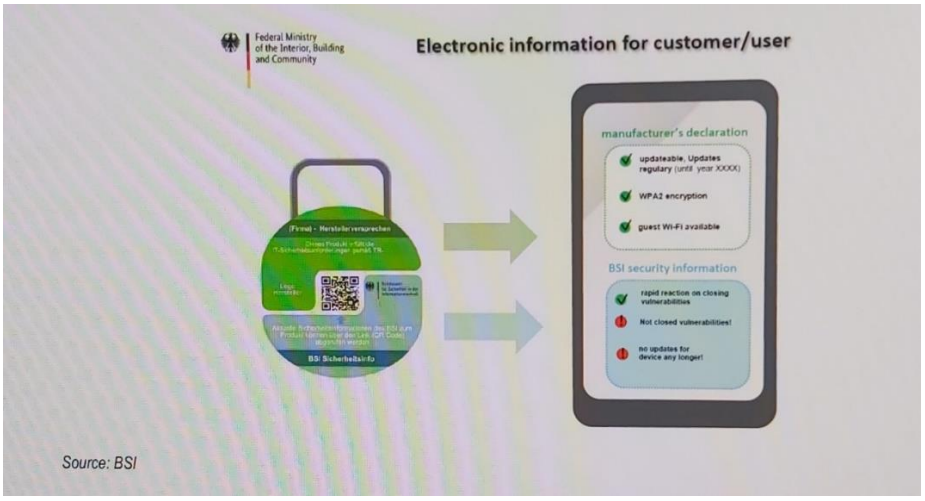
Case-Study: Model of German IT Security with QR code

In Germany, the voluntary labelling scheme[114] *IT Security* is available for all IT products, even though the criteria used to award the labels is adjusted for each category of products e.g. routers, meters and so on... The *IT security* label is standardised, easily understandable by customers and up-to-date.

The label takes the form of a QR code inserted in the product's package, which, upon scanning, presents two sets of information to the customer:

[113] Where **xxxx** refers to the country of registration, **yyy** refers to the product group and **zzzzz** refers to the number given by the competent body. The EU Ecolabel registration number shall also appear on the product. It shall take the following form: the label, the optional label with text box and the registration number shall be printed either in two colours (Pantone 347 green for the leaves and stem of the flower, the 'Є' symbol, the web address and the EU acronym and Pantone 279 for all other elements, text and borders), or in black on white, or in white on black.
[114] Case-Study Presentation by Matthias INTEMANN, BSI on 07 October 2021 available on CIRCABC

- the manufacturer's self-declaration to assure that the product has certain IT security characteristics, and
- the BSI security information to inform the end-user about security gaps or other security relevant IT characteristics.



ENHANCING THE DIGITAL SECURITY OF PRODUCTS: A POLICY DISCUSSION
OECD DIGITAL ECONOMY PAPERS | 45 Figure 4.4. Proposed IT label in Germany Source: BSI

At this stage, the EU Cybersecurity mark of conformity can take the following form:

- **a label with a distinct QR code**
- **a label with a QR code inserted**
- **a PIS[115]-type labelling or Information-only label[116]**
- **and/or a digitalized seal.**

It is highly recommended in terms of labelling to favour a gradual and flexible approach in line with the speed of uptake and the attractiveness of the labelling for cybersecurity certification.

4.2.2 QR CODE[117]

A non-exhaustive list for the dynamic QR code[118] information, usually known as PIS product Information Sheet and xml:

- QR code and logo can be displayed and printed together, in particular with the EUCC scheme
- QR code information has to be modifiable over the time, i.e. dynamic information e.g. such as status and validity
- QR code information is expected to be relevant and useful

[115] PIS product Information Sheet see ENERG and XML. Here the *product* is not the product itself, but the certificate delivered. PIS in the view of the author is equivalent to the information dispatched in the QR code. 'Information-only label' as detailed in PETRAS 2018 Study refers to descriptive labels that communicate important information to consumers (such as the support period offered with a device) and may provide proximate indicators of a device's security posture. The amount of information needs to be kept relatively simple and not too excessive as end-users have limited cognitive resources to expend during purchasing. Pictograms may be more successful than written information as they are more accessible to different demographics. However, research on the energy label has demonstrated that the accompanying information is often misunderstood and end-users often give more weight to certain types of information than others (e.g. energy efficiency over consumption) and this can lead to biased search behaviour. Furthermore, this type of label may be the most suitable for voluntary uptake. see p12 in
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/949614/Rapid_evidence_assessment_IoT_security_oct_2018_V2.pdf
PIS questions also the issue of languages linguistic versions of the complete product/service/process information sheet in all official languages of the Union or only one…
[116] most suitable for voluntary uptake
[117] EUCC Candidate Scheme, v1.1.1., May 2021 provide a direct link (in the form of a QR code) to the ENISA website (as per Article 50) - where all the information regarding the certificate are disclosed, including the current status of the certificate.
[118] https://www.sproutqr.com/blog/how-do-qr-codes-work
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

- QR code information will contain an URL link to ENISA ECCF Certification website[119]
- QR code information will contain the unique ID number of the certificate or statement including the scheme reference if needed on the website
- QR code information will specify the CSA Level concerned, and in particular the related vulnerability evaluation AVA_VAN level
- QR code information will contain the validity date of the certificate or statement of conformity within the 5 years validity limit
- QR code information will contain the NCCA/CAB identification where the certificate of assessment of conformity has been issued
- QR code information will contain the product or service name and version, including a website
- QR code information will contain the developer identification, including a website
- QR code information will contain the status of the certificate i.e. Valid, Revoked or Expired

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" version="0.1">

<xs:annotation>
  <xs:appinfo>
    Schema used for product/service/process certifications
    Created: 14.08.2021
    Last updated: 09.09.2021
    Version: 0.1
  </xs:appinfo>
</xs:annotation>

<xs:complexType name="ProductDetailsType">
  <xs:annotation>
    <xs:documentation>
    Information related to the certified ICT product and its manufacturer
    </xs:documentation>
    </xs:annotation>
  <xs:sequence>
```

This 2D code must be secured, and based on international standards in order to be easily and universally readable (even without an internet connection).

4.2.3 ENISA ECCF website or webportal

At this stage of our work, it remains to be clarified whether the certification webportal will operate as a transparent registry or a public portal only, or some elements of compliance and market surveillance will have to be included. For this reason, this subsection will only focus on the public aspect of a webportal. In this task, an architecture for the required IT-Infrastructure will be developed. Given the requirement for a web-based interface (esp. for the interaction with stakeholders), the task will deliver proposals for all relevant modules (such as workflow-engine, content management system, web-based labelling information display, etc.).

4.2.3.1 The architecture of the ENISA ECCF website will operate under the **following framework conditions:**

As shown in Figure 1 below, a public portal is a database management system that includes relevant public information on products or services available on the EU market. Relevant information pertaining to the cybersecurity labelling ecosystem is also published. This public information is cloned or updated on a regular basis from the public data provided.

[119] A dynamic QR code is a QR code with a short redirection URL encoded in it. The information communicated is not encoded in the QR code itself, like a static QR code or a barcode. https://www.scienceabc.com/innovation/whats-qr-code-how-its-different-from-barcode.html

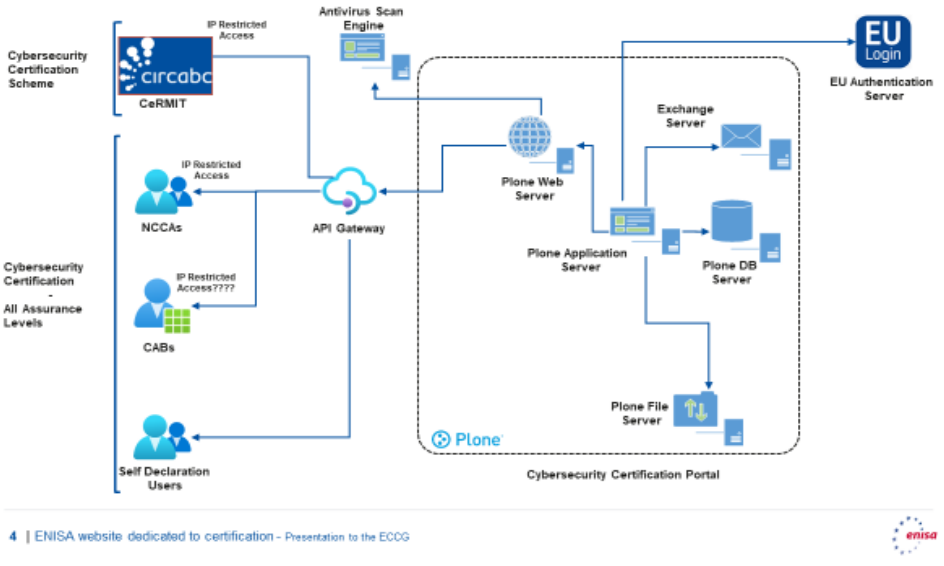


Figure 1 website

Under general transparency rules, suppliers, stakeholders, citizens, resellers, researchers and any interested visitor can freely access all public information stored in the public part of the portal, as well as suppliers, those interested in consulting legislation currently in force, related standards, guidelines, labelling events etc. regarding transparency[120], it has not been clarified yet at this stage whether the applicant shall have access and/or editing rights to the information entered in the database. In any case, a record of changes shall be kept, keeping track of the dates of any editing.

The database will:

- enable access to the mandatory specific parts of the technical documentation[121] that the issuer shall enter into the database including (a) a general description of the model, sufficient for it to be unequivocally and easily identified; (b) references to the harmonised standards applied or other measurement standards used; (c) specific precautions that shall be taken when the model is assembled, installed, maintained or tested; (d) the measured technical parameters of the model;

- be established in accordance with the following criteria: (a) minimising the administrative burden for the issuer and other database users; (b) user-friendliness and cost-effectiveness; and (c) automatic avoidance of redundant registration;

- provide the public with information about products and services placed on the market, their cybersecurity levels and information sheets[122] with up-to-date cybersecurity information.

The URL of the certification web portal will:

- be accessible directly or from the QR code and/or the label logo
- provide precise and detailed information of the product/service as requested by the Cyber Security Act (2019) for any product/service/process that has been certified or assessed for conformity

[120] See ANNEX XXXX list of information required
[121] ISO/IEC TER 17032:2019 ANNEX D Example of Information to be included in certification documentation of conformity and ANNEX F Example of Information to be included in a license for the use of certification documentation or mark of conformity
[122] OECD Digital Economy Papers, Enhancing the digital security of products. Feb.2021 p22

- formulate and implement confidentiality and cybersecurity requirements for the target IT system
- indicate any additional information requested by the scheme on its pages, including labelling
- specify a link to the certificate or statement of conformity information
- detail the information on the certificate or statement of conformity publicly available
- entail scheme-specific information including relevant information on the scheme that will allow professional users to understand the scope of the certification or assessment without reading the information on the certificate or statement of conformity (e.g. AVA_VAN in the EUCC scheme) since customers shall be able to easily identify the best assurance level for each group of products or services, allowing them to compare model characteristics and to choose the most robust products or services.
- allow a readable access of a cybersecurity catalogue of certified solutions for products, services or software via smartphones, as well as the labelling page
- respond to one or more of the following URL and domain name with vigilance[123]:
  - https://www.enisa.eu/certification
  - https://www.cybersecurityagency.eu
  - https://eucybersecurity.certified
  - https://www.cybersecuritycertified.eu
  - etc…

Usually, the Commission shall be empowered to specify, by means of implementing Acts or a framework implementing Act, the operational details of the product, service or process, after consultation with the ECCG and the SCCG.

4.2.3.2 The ENISA ECCF website will specifically have a dedicated **labelling page** explaining the labelling scheme[124] and containing the following information:

- Logo explanation > kesako: what, what, when, why, what for, who … how
- Useful documents: labelling strategy 2022-2025; users' manual for applicants, marketing guide, legal manual, a manual for competent bodies to be used in assessing the compliance of products and services with the relevant criteria, a manual for authorities that award public contracts which will provide guidance on the use of the EU cybersecurity labelling criteria. The Commission will provide templates translated into all official Community languages if necessary.
- Events
- Info contact helpdesk at URL link for cybersecurity certification
- Newsletter on the EU cybersecurity-label, interested? please register at: enisa.europa.eu/
- Link to page[125] how to apply for the cybersecurity labelling
- Labelling cybersecurity certification for consumers
- Labelling cybersecurity certification for businesses
- Objectives of labelling
- Incentives for developers
- FAQ[126]: More questions?
- Interested in engaging with us to promote the EU cybersecurity labelling[127]?
- QR code and URL can refer to the key-labelling information (PIS) page, and from this page additional links can be organised towards the certification schemes.
- An app to add to the settings or parameters of the devices

[123] What is a Look-alike Domain? | PhishLabs
[124] The ENERG-LABELLING SCHEME project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 847043 around €1.5million
[125] https://ec.europa.eu/environment/ecolabel/how-to-apply-for-eu-ecolabel.html
[126] Spain Organismo de Certificación - FAQ (cni.es) https://oc.ccn.cni.es/sobre-oc/faq
ECO-label https://ec.europa.eu/environment/ecolabel/documents.html
ENERG-label Frequently Asked Questions (belt-project.eu) https://www.belt-project.eu/faq

[127] https://ec.europa.eu/environment/ecolabel/faq.html

4.2.3.3 The ENISA ECCF website will welcome and manage **the automatic labelling generator:**

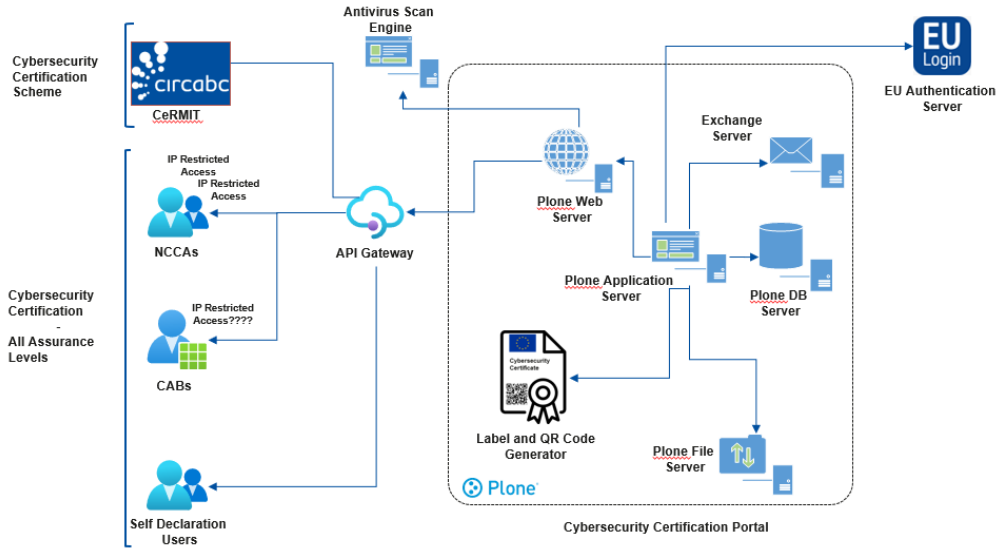


Figure 2 website Label generator

Label generation: By entering the data required, the issuer will proceed to the automatic generation of the cybersecurity label. The database will produce a label from the structured data entered. The file produced is a ZIP file containing the label (only one label) in various formats (JEPG, PDF, PNG, SVG) with a QR code inserted.

- ❑ Approval process: automatic process + automatically generated with the certification or statement of conformity
- ❑ Automatic label generator
- ❑ Label database publication
- ❑ Revocation
- ❑ Generation of information sheet[128] (PIS): the applicant can therefore download a version in any language for a preview of the automatically produced sheet.

NOTE: When possible, ITSELF operating at a basic level could also be given an option to upload a label independently created via the generator. It would have to be uploaded in just one format (PNG, PDF, SVG, JPEG, and TIFF) and with a limited size. ITSELF is responsible of the correctness of the label and its data.

4.2.3.4 Labelling fees

Catalogue
At some stage, companies will have to submit their application to a competent body.
The online registration of their certificate will be organised in the EU cybersecurity catalogue.
It will be initiated by the ENISA ECCF website and managed online in the registry.

[128] ideally, the structured data lets the system generate all language versions of the certificate or the statement and the Information sheet.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Annual Fees to be fixed?
Each applicant who has been awarded the EU cybersecurity labelling will be required to pay an annual fee (to be determined) for the use of the label. In the case of small and medium enterprises[129] and operators in developing countries, the maximum annual fee shall be no higher than a reasonable level. In the case of micro-SMEs the maximum annual fee shall be half of the previous fee. The period covered by the annual fee will begin with the date of the award of the certificate or statement to the applicant.

Fees Transparency[130]
Link to web page for cybersecurity labelling with exact fares or cost estimate for each competent body.
Special discounts for SMEs, micro-enterprises and applicants from developing economies will facilitate compliance.

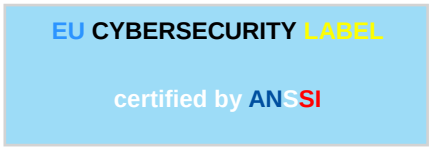
Application process
A step-by-step explanation of the application process will make every application as simple as possible.

4.3 FRAMEWORK LABELLING & COEXISTENCE OF NATIONAL[131] CYBERSECURITY LABELS

It is relevant to ensure that labelling schemes are proportionate and consistent across sectors and countries. It is acknowledged in our labelling workflow, that framework labels may be beneficial by ensuring the simplicity and universality of the labelling scheme – two key factors for its effectiveness –.

However, framework labelling may also be difficult to implement as digital security challenges and best practices may vary across sectors and between Member States, for which various specifications may be available.

From the ANSSI perspective, the establishment of an EU label would not prevent them from maintaining their national VISA, which could be based on the following:



During our discussions, participants recommended avoiding multiple labels for the sake of recognition and stability of labelling. There is a use-case in the field of durable labels or bio-labels. More than 106 durable labels exist on the Belgian market, e.g. FSC, NaturePlus, Cradle to Cradle and VinylPlus see Belgian website https://www.labelinfo.be .This situation often leads to increased confusion in the perception of end users.

[129] SMEs and micro-enterprises as defined by Commission Recommendation 2003/361/EC of 6 May 2003 (OJ L 124, 20.5.2003, p. 36)
[130] Example of ECO-label https://ec.europa.eu/environment/ecolabel/documents/eu-ecolabel_fees.pdf
[131] SOG-IS label was not brought on our table. It might be the case if needed in our future work. https://www.sogis.eu/uk/pp_en.html

At this stage, it is recommended that a gradual approach with respect to the following three dimensions be favoured:

- Members States with existing national labels who transition towards EU labelling
- Members States with no labelling and who are taking a direct jump into EU labelling
- Third countries

The label shall emphasize that EU certification is fostering the European market. Member States with no national labelling, as well as the EFTA countries implementing the CSA, should be encouraged to use the EU label as a priority.

Even though national initiatives are outside the scope of this labelling report, we have favoured a benchmarking methodology based on national experiences. It sounds logical that national requirements can be maintained by Member States. A transition period will be organised to deal with the consistency of the eco-system. During this period, national labels, regardless of their goals (qualification, promotion, etc…), may co-exist with the label.

It should be recommended that, in order to promote the smooth functioning of the internal market, as much transparency as possible should be ensured regarding national initiatives for the establishment of technical regulations[132]. In order to facilitate the marketing of products or services bearing cybersecurity labels at national levels and to limit additional work for companies, in particular SMEs, or to avoid confusing consumers, it is recommended that efforts to enhance coherence and promote harmonisation between cybersecurity certification labels should be encouraged.

[132] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02008R0765-20210716

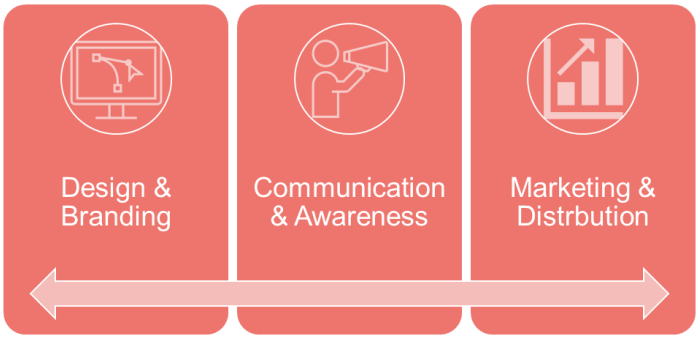
5. AWARENESS, EXCELLENCE & EMPOWERMENT

With the support of the Marketing sub-group, led dynamically by Danilo D'ELIA, the labelling activities have investigated the promotion of a cybersecurity label. Building a solid European cybersecurity certification framework (ECCF) will involve a European based campaign to increase the visibility of newly certified solutions at European level. The proposed concept and design of the framework label aims to match the objective of promoting the awareness, reputation and excellence of the full spectrum of the solution certified under the European cybersecurity certification framework. Without a pan-European approach to market the results of the cybersecurity scheme, the resources spent on technical working group(s) may not be effective in reaching end users and facilitating the adoption or promotion of certified solutions in the European market.

At some stage, it will become necessary to inform the public and to raise public awareness of the EU cybersecurity labelling by promoting information and education campaigns at local, national and Community levels. End users such as SMEs, administrations and consumers shall be aware of the value of the EU cybersecurity labelling in enabling them to make informed choices. These campaigns would also be necessary in order to make the scheme more attractive to applicants.

Concerning our methodology, with the feed-back from our labelling plenaries, the subgroup has collected and structured the information available from existing European, international and national cybersecurity labels and existing communication campaigns.

Proposed plan structured around three activity streams:



5.1 DESIGN AND BRANDING: SIMPLE AND CATCHY MESSAGES

The meetings with the group members have stressed the need for the elaboration of clear and simple messages for communication[133] purposes. The design of the logo and the elaboration of the branding messages should answer the following questions:

- What is the certification labelling about?

- What will potential end users purchase when acquiring "EU Certified" solutions?

- What are the values or specifications of "EU Certified" solutions?

[133] This point linked is linked closely with the outcome of the sub group on the operational implementation in Chapter 4

5.1.1 Principles

The following principles should be considered when elaborating the specification of the logo and the mission statement outlining the values of 'EU Certified" solutions to ensure that the European customers who intend to or who interact with certified solutions are aware of them.

- ❑ **(Pan) European** market: improve the European Union internal market so that the same label format is recognised across all European countries
- ❑ **Cybersecurity**: improve the cybersecurity of ICT solutions and raise the level of cyber hygiene or awareness across European society
- ❑ **EU Proof** of certified product and services: indicate clearly and easily that the digital solution has been evaluated in Europe according to or in compliance with appropriate EU cybersecurity standards and by an independent third-party evaluation. The general sales message is that the certified products, services or software have been found to fulfil a set of compelling criteria relating to cybersecurity.
- ❑ **Voluntary** based approach
- ❑ **Transparency and credibility**: provide greater transparency about security of ICT solutions so that end users will access more information to discern the level of security offered by ICT solutions available on the European market
- ❑ **Harmonisation, continuation and strengthening**: transition smoothly with existing labels.

However, in terms of branding and storytelling, some key references to the European context should be taken into consideration, in particular with:

- ❑ the objective of enhancing trust and cybersecurity in the EU Digital Single Market[134] and,
- ❑ the willingness of Europe to act - reference to the Cybersecurity Act (CSA)

5.1.2 Logo Design and Display

The following key elements on the design of the logo were discussed:

- **EU approach**: to underline *EU Certified - issued by XXX*[135]. Option to be positioned next to national label. In addition to the geographic perimeter, when discussing the opportunity to propose a mission statement or slogan of the label, the sub-group outlined that it was premature at this stage to include one.
- **Coloured graded format**: to allow consumers to compare the security of different devices or the type[136] of certification or qualification. The use[137] of colours and letters is a noticeable and accessible format and makes the information to consumers, directs their attention towards important information and is easy to interpret. Discussion at sub-group level has stressed the importance to go for a progressive approach. The idea is to start with only one colour in order to widely advertise and get the label known on the market. Then, in a second phase (2 years from the launch of the label) to adopt the coloured graded scheme.
- **Binary seal of approval:** to guide attention when consumers prefer simple labels. They are less effective in informing consumer choice. They can reduce cognitive burden but can also lead to dichotomous thinking[138].
- **Display and Design rules**: to foresee booklets or guidelines for the proper use of the label and chart logo
- **Marketing package**: to include the certificate or statement template to be issued by the owner of the label to the company

[134] see CHAPTER 2 Objectives
[135] For NLF when CE mark is used there is identification of CAB issued certificate via its identification number – it is much easier to identify them according to it instead of names that can be (intentionally) similar and therefore misleading. See EUROPA - European Commission - Growth - Regulatory policy - NANDO https://ec.europa.eu/growth/tools-databases/nando/
[136] see Austrian cybersecurity labelling
[137] see Waechter S, Sütterlin B, Siegrist M. Desired and undesired effects of energy labels - An eye-tracking study. PLoS One. 2015;10:1–26. This format has demonstrated efficacy in the energy and food labels and is more effective than binary or informational labels.
[138] For example, consumers may consider a device without a label to be insecure. This situation is likely to arise if the label scheme is not mandatory. Furthermore, logos are more vulnerable to halo effects, which in this context, may mean that consumers are led into a false sense of security when buying a device with a seal of approval or assume that it requires no intervention from them to keep it secure.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

In line with PEGI-label[139] advices, remember to keep in mind the basic rules for logo design:

- designed to be simple and universally understandable
- based on psychological assessment[140] and in accordance with existing standards
- specifically designed for interactive, non-linear media
- updated continuously
- linked to website or QR code to consult database

Alternatively, as raised by consumers' representatives[141] as well as by research by Blythe and Johnson in 2018, the following risks must be carefully addressed when designing labels:

- **Consumer inattention**: when exposed to too many labels, or to labels whose meaning is not clear, consumers are likely to fail to understand them or not take them into account in their purchasing decisions.
- **Lack of uptake by the industry**: if the labels are introduced in a voluntary framework, there is a risk that not enough companies adopt the label. If the label is not visible enough to end users, its impact will likely be limited.
- **Simplification of a complex issue**: while labels aim to facilitate consumers' understanding, they may also oversimplify an issue and disincentivise stakeholders from going beyond the label's requirements if a tiered approach is not used (risk of a race to the bottom). In addition, labels could be misunderstood by mainstream users as a guarantee of full digital security, even though they only signal that the product fulfils certain requirements for robustness.

Over times, labels can demonstrate somewhat limited efficacy. This is often due to poor design and implementation of updated versions of the label in end users' settings. This sustainability should be kept in mind when establishing the future cybersecurity labelling.

5.2 COMMUNICATION PLAN & AWARENESS CAMPAIGN

The need to have a targeted customer campaign (the WHO) so as to educate end users to favour certified solutions was addressed. A progressive approach can be encouraged to create durable brand recognition[142]. We envisage a long-term campaign (e.g. over 3 years) being elaborated on the model of the BELT project[143] with the objective of building an appetite for certified cybersecurity solutions (based on CSA) along these lines:

- Press campaign or roadshow: a list of European and national media including specialised blogs or journalists on technology and business, e.g. breakfast with journalists, distribution of kit, etc.
- Social media identity e.g. LinkedIn and Twitter accounts on the models of #EUCyberAct #EUCyberLabelling
- Link with the semestrial Presidency of the Council of the EU (2022-2025 plan): implementation review meeting
- Promotional video[144]
- Distribution channels or community of conformity Assessors or ambassadors
- Communication crisis strategy: to provide guidelines in the event of a crisis

[139] op.cit presentation 10.06.2021
[140] When making decisions, end-users use objective information and heuristic approach in which concepts, pictures, attributes and other types of information that are connected to an emotional affect influence their decision making. See PETRAS op cit.

[141] Interviews Chiara GIOVANNINI, ANEC on 2 June 2021 & Ursula PACHL and Frederico DA SILVA, BEUC on 26.05.2021
[142] Expert note on brand recognition: the endorsement of a label from a well-recognised entity at European level would facilitate the adoption of the label. While other EU label are pushed or driven by the regulatory power, the Certification Scheme is based on a voluntary approach. See IFSE initiative when launching PEGI labelling.

[143] BELT project link op cit p27
[144] ENERG video campaign https://youtu.be/odd-6N66aFE

Provider of cybersecurity: to be proud or to differentiate their products in the market and be incentivized to develop ICT solutions for more secure products. The framework labelling enables cybersecurity providers to demonstrate clearly that their products are already in line with the new market trends and enjoy a competitive advantage in satisfying the growing need for more secure digital solutions.

Pitch: key arguments for labelled products are as follows:
- strict cybersecurity criteria
- certification by independent bodies
- official EU scheme-based certificates in accordance with the EC laws and laws of EU Member States, and
- contribution to a sustainable and competitive digital economy (sustained by both producer and consumer).

Users of cybersecurity: in order to identify secure products and services, people need reliable information and indicators. In their search for orientation, they are often confused by the overabundance of independent, industry-specific, national and regional certificates, symbols and claims. Recommendation: to start with OESs, Critical Infrastructure Operators, Public Institutions… NIS2 sectors

Citizens: need protection or transparency on the security characteristics of products and services

5.3 MARKETING STRATEGY

5.3.1 The marketing campaign consists of the following tool-kit, including:

- Statement or boilerplate that contains basic information about labelling and "EU Certified" solutions. These statements on how the marketing plan is carried out will make or break the confidence of European clients.
- Marketing guide(s) for the label: to give some examples of best practices to effectively make the label visible in marketing material (websites, info posters, roll-up, logos in various languages, press releases)
- Marketing guide(s) should also include what the label is NOT? (e.g. privacy, safety, liability, geographic origin of the product)
- A leading by example network of ambassadors (national cybersecurity certification authorities, etc.)
- Ad hoc issuing ceremony: yearly?
- Ad-hoc session during the ENISA NIS Summer Schools
- Label roadshow: list of exhibitions or main events – need to negotiate ad-hoc partnership to promote the label (Mobile Congress, VivaTech, Les Assises Monaco, IT-SA, CyberSec Italy, etc).

5.3.2 The marketing campaign will gather a community of supporters and ambassadors

The framework label is a key-driver in creating a culture of trust across the EU - trust in the outcomes of schemes and EU-based certified solutions. Thus, a community of supportive stakeholders will have to be aggregated to the labelling strategy:

Step 1: Stakeholders identification

Step 2: Stakeholders engagement plan

Step 3: Multi-party MoU (using the MoU as a tool to mitigate risk)

The label can be an opportunity to develop a community of certified developers[145], who can benefit from specific information (newsletters, seminars…). Recently, the French Cybersecurity Agency ANSSI[146] gathered more than 200 editors and vendors of cybersecurity solutions to award its Visa de Securite and the label EBIOS.

The example of the UK Secured by Design scheme on building materials and products e.g. doors, locks and windows are built to a specified standard that is resistant to attack. This is currently a binary accreditation scheme that is intended to encourage housing developers (and others) to design out crime at the planning and building stage of development. Research suggests crime is less likely in and around housing that is constructed to SBD standards. As far as we are aware, the impact of the scheme on consumer choice is unknown, but industry membership[147] of the scheme – an alternate metric of the influence of the scheme - is substantial, with over 400 companies building products to SBD standards.

Another example is the PEGI gaming label[148], which was and remained an industry-led partnership of software manufacturers with the European Commission. It consisted originally of around 20 key-companies. As of 2021, PEGI is recognised in 32 countries.

The question as to how local NCCAs, CABs and ENISA are to be jointly associated will have to be determined. Based on the discussion with the Sub-group members, given the proximity of CABs and NCCAs to local ecosystems, these entities will have marketing role to play in order to promote the adoption of the certification scheme. Therefore, it was suggested to consider the development of a dedicated campaign for the CABs delivering the certificates (e.g. Affiliate CAB).

The Member States and their local administrations will also be key players in promoting and prioritizing the framework labelling as part of their national public procurement prerequisites.

On its side, for example, CCN Spain is editing a list of cybersecurity manufacturers to promote robust certified solutions, https://oc.ccn.cni.es/productos-certificados/productos-certificados/fabricante

Concretely,

- Leaflets should be created for the presentation of the certification schemes and activities, which have a longer time validity.
- The online catalogue should be designed as to be easily accessible and readable from mobiles.
- In terms of events, any big EU cybersecurity event (such as FIC in France) should provide an opportunity to advertise the label and to promote or celebrate new certificates.

[145] ANSSI interview 18.03.2021
[146] ANSSI 29.06.2021 webinar on the « Ecosystème cyber : les enjeux du passage à l'échelle » https://www.ssi.gouv.fr/actualite/lecosysteme-cyber-en-pleine-expansion/
[147] http://www.securedbydesign.com http://www.securedbydesign.com/members/ in Armitage R, Monchuk L. Sustaining the crime reduction impact of designing out crime: Re-evaluating the Secured by Design scheme 10 years on. Secur J. 2011;24:320–43. doi:10.1057/sj.2010.6. quoted by Blythe and Johnson 2018=
[148] Op cit p20 https://en.wikipedia.org/wiki/Interactive_Software_Federation_of_Europe
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

The draft budget[149] for this campaign will be presented in due time.

5.3.3 EC legal requirements

CE marking & Marketing rules
Reference to CE marking?

Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the **marketing** of products
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008R0765

In advertising its product, the applicant makes use of a selection of words and arguments that, even if not directly stating the product is certified, send a misleading message to the recipient as if the product is certified (case of Unfair commercial practice as for Directive 2005/29/EC concerning unfair business-to-consumer commercial practices). See also Compliance chapter and TG10 Final Draft Report on the Guidance for Manufacturers/Providers Commitments

ISO

- ISO 28219:2017, *Packaging — Labelling and direct product marking with linear bar code and two-dimensional symbols*
- ISO/TS 18614:2020, *Packaging — Label material — Required information for ordering and specifying self-adhesive labels*
- Etc.

EU cybersecurity labelling promotion and involvement of the Member States and the Commission

- Action Plan?
- Awareness actions?
- Website

> Model : **EU Ecolabel Promotion** EUR-Lex - 32010R0066 - EN - EUR-Lex (europa.eu)
>
> 1. Member States and the Commission shall, in cooperation with the EUEB, agree on a specific action plan to promote the use of the EU Ecolabel by:
>
> (a) awareness-raising actions and information and public education campaigns for consumers, producers, manufacturers, wholesalers, service providers, public purchasers, traders, retailers and the general public,
>
> (b) encouraging the uptake of the scheme, especially for SMEs,
>
> thus supporting the development of the scheme.
>
> 2. Promotion of the EU Ecolabel may be undertaken via the EU Ecolabel website providing basic information and promotional materials on the EU Ecolabel, and information on where to purchase EU Ecolabel products, in all Community languages.
>
> 3. Member States shall encourage the use of the 'Manual for authorities awarding public contracts', as specified in Annex I, Part A, point 5. For this purpose, Member States shall consider, for example, the setting of targets for the purchasing of products meeting the criteria specified in that Manual.

Therefore, the best way to make sure that European efforts in developing the certification scheme are being well spent is to develop a comprehensive awareness campaign and an effective marketing strategy to come up with a solid implementation plan of the framework labelling.

It is recommended in the 2022-2025 work plan to elaborate a RACI matrix to know who is having the tasks, roles and responsibilities, not only from the marketing operations but also from a broader management perspective (who will be the owner, who the promoter, who the supervisor….).

[149] Expert Note: Definition of the timeline and budget, the operational costs (time/manpower) + communication tools (link with specialised communication agencies) + leverage strategy on existing EC services (e.g. DG Grow, EDIHs, etc)

6. SURVEILLANCE AND COMPLIANCE

The objective of the work of this sub-group led by **Yoann KASSIANIDES** was to define the means that must be implemented, in parallel with attribution to the label, so that it is used in the conditions foreseen.

In accordance with the provisions of the European Cybersecurity Act, the national authorities are responsible for market surveillance and for punishing any misuse of the label. ISO 17065 [150]also makes reference to surveillance and compliance.

This is a key objective in the success of this label: indeed, this instrument aims to give users a clear and simple vision of the level of cybersecurity of a product or solution. Consequently, preventing this information from being distorted by an erroneous or misleading use of the label, whether voluntary or not, is a real challenge.

For this reason, it is very important to ensure, through several tools, that the conditions of use of the label are clearly disseminated and understood at the time of labelling (or obtaining the certificate). Secondly, it is also interesting to understand the conditions under which, and by whom, market surveillance can be conducted, in order to control the correct use of the label. Finally, it is also appropriate to provide for reporting mechanisms or feedback concerning possible incorrect use of the label.

6.1 COMPLIANCE WITH THE CONDITIONS OF USE OR VALIDITY CHECKS

In order to ensure that the conditions of use of this label are respected as far as possible, it is essential that they are well communicated to the holders of the label.

It is equally essential to provide the public with simple and effective means to verify the reality or validity of the label on a product or solution. Tools such as the 2D-code, in addition to their role in terms of supplementing information that cannot be included directly on the label, make it possible to verify very quickly that the label is indeed valid.

6.1.1 Communication of the conditions of use

The communication of the conditions of use of the label and the clear and precise indication of what may or may not be done with the label are essential to limit cases of inappropriate use.

These rules of use must be included in the general rule book of the label, but also, according to the experts of the sub-group, in a separate additional document intended to be easily transmitted to those, in the company, who will be in charge of the communication of the labelled product.

These documents must, as a minimum, indicate:

1. The general principles of the label:
   - the label is awarded to a product and a solution and not to the company as a whole;
   - the label is inseparable from a certification or self-assessment valid under the schemes rules; and
   - the label cannot be affixed if the certification or self-assessment is not attested, or is no longer valid.

2. The specific requirements for displaying the label:
   - Authorized use on digital and/or printed media,
   - Obligation to affix the label specifically to the product or solution (or directly related documents/packaging), without any confusion as to the scope of labelling (the product or solution).
   - Minimum size,

[150] ΕΛΟΤ EN ISO IEC 17065_2012-en_.pdf

Shape, colour, location allowed for displaying the label,
- Need to maintain the visibility and integrity of the label, in particular always ensuring the usability of the 2D verification code, etc.)

3. Sanctions for misuse of the label, and more specifically in the following cases:
   - displaying the label on a product whose certification or self-assessment is not valid or has been withdrawn;
   - display of the label leading to a misleading or overly broad interpretation of the real scope of the label (e.g. display leading to the belief that the whole company is labelled);
   - displaying the label in the absence of any certification or self-assessment.

6.1.2 Validity checks

In addition, the display of an element (2D Code) enabling the reality or validity of this label and the certification or self-assessment it underpins to be verified, is intended to function as a major deterrent to any actor who might consider deviant use of the label.

Indeed, the possibility of instant verification of the veracity of the claim made by the label is likely to make any attempt to display the label in a misleading way less attractive and, of course, less effective.

This is why the Compliance sub-group strongly recommends the presence of a 2D-Code, visible on the label.

This instrument serves multiple purposes:

- to have a dissuasive effect on potential counterfeiters,
- to allow verification of the existence and validity of the certification or self-assessment underlying the label at any time,
- to make available a great deal of additional information that the label does not allow to be shown in its entirety, in particular precise identification data of the labelled product or solution, information relating to the certification itself, type of certification, certifying authority, validity of the certificate, general information, etc.

In order to effectively meet each of the desired objectives, the 2D-Code must comply with the following criteria:

- **Security**: the question of the security and reliability of the data conveyed via the 2D code is crucial for the credibility of the label (which relates to... security certifications!). Therefore, it seems essential that special attention be paid to the choice of the label. The data carried by this 2D-Code must be electronically signed to avoid their falsification, denaturation, etc. Concerning their verification (reading of the 2D Code), the sub-group recommends that it should preferably be done through a free and trusty entry point and therefore a dedicated application rather than through means that do not offer sufficient guarantees in terms of security.

- **Usability**: the use of the verification tool must be simple and universal. Addressing the European market as a whole, the standard used to organize the data in the 2D Code must be an international standard (such as ISO/SEWIP 22376 currently being finalized). The system should also be multilingual by design. Finally, the possibility to access the 2D Code data, even offline, is also a potentially useful element (in this case, the verification reader must be regularly updated in order to check that the initial information, - i.e. validity of the certificate - is still true). The 2D Code (and the related database) should be able to store various types of data such as texts, images, serial number, product description, dynamic link to a dedicated website, etc.

- **Adaptability**: the verification system must be sufficiently adaptable to accommodate different use cases and in particular the market surveillance process foreseen by the European Cyber Act which involves several actors (ENISA, the European Commission, national authorities, CAB, national inspectors in charge of market surveillance, individual users). The system should allow for different levels of access to data depending on these categories.

- **Filling in or retention of the database linked to the labels issued:** under the European Cybersecurity Act, the national authorities are responsible for issuing and monitoring certifications or self-declarations. As regards the European label that accompanies these certifications or self-declarations, it seems appropriate that the final issuers of certifications (or registrations of self-declarations) should be able to issue, at the same time as the certificate, the accompanying label. However, considering the European dimension of the label and the unitary nature of the certification schemes under the responsibility of ENISA management, the idea of centralizing information on labels issued at European level should also be considered.

  Two options are possible for labelling certificates:

  - The final issuer of the certificate (CAB) is responsible for issuing the label and its 2D verification code according to the technical requirements provided by ENISA. In this case, the data concerning the validity and additional information are stored in a distributed manner by each issuer for all the certificates and labels it has issued. A copy of this information is then sent to the national authority and to ENISA.
  - The grantor of the certificate (CAB) is not entitled for the issuance of the label and its 2D verification code. In this case, this issuer will send the certificate and all necessary information to ENISA certification web portal in charge of generating the label associated to the certificate. This option seems more in line with the pan-European logic of the label.

6.2 MARKET COMPLIANCE

Once the label is issued and in circulation, it is important that a market surveillance system is used in order to control and, if necessary, sanction improper use of the label. This action contributes to strengthening the legitimacy and trust that users can place in the label.

The sub-group first tried to define the different cases of misuse. In a second step, it looked at which authorities were in charge of market surveillance and how they could enforce the different requirements related to the certification and the label. Finally, the need for a common tool so that anyone can report suspected misuse and the processes for dealing with such reports was discussed.

6.2.1 Expected cases of misuse of the label

The expected cases of misuse described by the sub-group are the following:

- Extending the scope of the label: the product has a valid certificate and label but the company uses the label in an extensive or misleading way.
- Unjustified use of the label:
  - the product does not meet the requirements for certification or self-assessment
  - the product is no longer certified (out of date)
  - the product has no certificate at all
  - the product displays a false or wrong label certificate
- QRishing[151]: Upon scanning a counterfeited or falsified code, users are directed to websites with counterfeited or falsified realistic-looking landing pages. A fake QR code also has the potential to connect to an unsecured Wi-Fi network or automatically navigate to a malicious link. Without neglecting that these types of codes may also direct users to websites where malware can be automatically downloaded.
- Apps upgrade or update are entry-door to malware: it will be paid attention to this issue

[151] See ENISA Threats Landscape 2021

6.2.2 Authorities in charge of the market surveillance

Extract of the European Cybersecurity Act

Article 58.7 National cybersecurity certification authorities shall:

(a) ***supervise and enforce rules included in European cybersecurity certification schemes*** *pursuant to point (j) of Article 54(1)* ***for the monitoring of the compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates that have been issued in their respective territories, in cooperation with other relevant market surveillance authorities;***

(b) ***monitor compliance with and enforce the obligations of the manufacturers or providers of ICT products, ICT services or ICT processes that are established in their respective territories and that carry out conformity self-assessment, and shall, in particular, monitor compliance with and enforce the obligations of such manufacturers or providers set out in Article 53(2) and (3) and in the corresponding European cybersecurity certification scheme;***

f) ***handle complaints by natural or legal persons in relation to European cybersecurity certificates issued by national cybersecurity certification authorities or to European cybersecurity certificates issued by conformity assessment bodies*** *in accordance with Article 56(6)* ***or in relation to EU statements of conformity issued under Article 53****, and shall investigate the subject matter of such complaints to the extent appropriate, and shall inform the complainant of the progress and the outcome of the investigation within a reasonable period*

g) provide an annual summary report on the activities conducted under point (b), (c) and (d)… to ENISA and the ECCG;

According to the European Cybersecurity Act, the national authorities are in charge of ensuring market surveillance related to the European cybersecurity certification schemes. The article 54 of the European Cybersecurity Act defines the elements of the European Cybersecurity certification schemes and mentions (i) the labels or marks as being part of a scheme.

> **Then, the sub group considers that if a reference to the label is integrated in a cybersecurity scheme, the surveillance market process foreseen for the whole scheme is then applicable to the label related to this scheme. Therefore, issues of compliance regarding labelling can be raised in the annual summary report in g).**

In addition to this market surveillance action, based on the provisions of the European Cybersecurity Act, other legal considerations could be explored, in particular concerning the actions open to the holder of intellectual property rights over the label (see point 3.5.3 of the report). Indeed, the owner of a label holds intellectual property rights over that label and is therefore able to take legal action, particularly on the basis of infringement of those rights (in the event of counterfeiting for example). This aspect can be clarified at a later stage or be dealt with in the annual summary report (see g)).

6.2.3 Complaints management

The establishment of a system for collecting and managing complaints is also an important tool in terms of credibility for the label.

> Article 58 (f.) of the European Cybersecurity Act provides, with regard to all certification schemes, that this prerogative must be ensured by the national authorities. This provision therefore also applies to the labels that result from these schemes.

However, given the European nature of the schemes and labels, as well as the communication that will be put in place around the forthcoming labelling, it would be useful and relevant that a unique desk is receiving any complaints. This desk will be accessible simply, by any applicant or end user, on the same communication portal. This complaints mechanism is not intended to replace, but to complement the system set up by the national authorities responsible for market surveillance in each country.

Indeed, in order to avoid a contradiction between the pan-European character of the certification and the label and the national character of the reporting and processing of complaints, it seems necessary to give an additional possibility to a complainant to express his or her complaint on the European website. This complaint will then naturally be redirected to the relevant national authorities, but this process must remain, in a way, transparent for the user.

These considerations terminate the current chapter. It is noted that additional exchanges, regarding the articulation of the different stakeholders' responsibilities will have to be further investigated in the coming months.

7. LABELLING WORKPLAN (2022-2025)

This report is the first step for the development of our labelling work plan for the next three years (2022-2025). It is already a solid base. Now logically, it requires developing a vision and a plan for 2022 onwards and, simultaneously with this current 2021 deliverables.

Therefore, I will kindly suggest that you also give your input regarding such a workplan. We will discuss and debate this Draft Work Programme early 2022 to start the new year with our first plenary meeting.

This Work Programme will follow the ENISA constant line in considering the cybersecurity of the whole IT eco-system in a consistent and holistic approach along its whole lifecycle across all levels of device or application, design and development, integrating security throughout the development, manufacturing, and deployment…

Please … possible chapters or road map

From 2022 to 2025, further works will be pursued:

- ❑ **General governance of the eco-system, such as the ownership of the labels, transparency,…**
- ❑ **Operational implementation of the labels, such as display, security, label generator**
- ❑ **Communication campaign, such as strategy and budget**
- ❑ **Compliance control and surveillance, such as articulation of the roles**
- ❑ **AOB… (please complete)**

Examples

Under Operational Implementation:

- how the technology and the legal conditions can ease the generation of labels and automating processes for the collection, processing and compilation or presentation of label-related data
- will we need to consider the attribution of certificates in a public key infrastructure (PKI), to authenticate a label and its representations?
- Digital labelling seals?

This part of the report will be on the agenda of the next plenary meeting scheduled in Q1-2022.

contact: marie-laure.lule@enisa.europa.eu

Marie-Laure LULE – Cybersecurity Expert MCS, ENISA

ATHINA, 15.11.2021

ANNEXES

- LIST OF ACRONYMS
- LIST OF TG MEMBERS REPRESENTATIVES
- DOCUMENTATION
- BIBLIOGRAPHY

ANNEXE : COMPOSITION

More than 42 participants[152] registered for our labelling activities. Various stakeholders from all sectors contributed their specific experiences in the field to our explorations. Additionally, our work was explained regularly in ENISA's consultative bodies, meaning SCCG and ECCG, whose members also contributed high quality inputs. This report reflects all these inputs with gratitude.

The following experts led the Labelling thematic group and its subgroups.

LABELLING Thematic Group
Marie-Laure LULE is a Cybersecurity Expert at ENISA in charge of establishing the Recommendations for Labelling Cybersecurity Certification in the framework of the certification schemes designed by ENISA

LABELLING Sub-Group LEGAL

Thomas NIESSEN is the Managing Director of Kompetenznetzwerk Trusted Cloud, a Certification expert, and a Member of Gaia-X and of the EUCS AHWG. He is our labelling expert with respect to legal issues.

LABELLING Sub-Group IMPLEMENTATION

Jose RUIZ-GUALDA is the Founder and CTO of JTSEC, and a Member of the SCCG. JTSEC also participates in the EUCC AHWG. He brings his expertise in the field of labelling requirements, approval processes and management.

LABELLING Subgroup AWARENESS

Danilo D'ELIA is Senior Policy Manager at ECSO and editor of the Cybersecurity Made In Europe label. This label aims at promoting customer awareness and communication strategy in the field of cybersecurity. He is our labelling expert with respect to a future communication plan to be defined and implemented between 2022 and 2025.

LABELLING Subgroup COMPLIANCE

Yoann KASSIANIDES is Delegue General at ACN, Alliance pour la Confiance Numerique, and Editor of the France Cyber Security label.

[152] see List of members of the Labelling TG available on CIRCABC (42) in Annex…

Timeline

Subgroup meeting IMPLEMENTATION	
Experts meeting	
EU-CS AHWG presentation	15/05/2021
Experts meeting	20/05/2021
Experts meeting	26/05/2021
Experts meeting	02/06/2021
Experts meeting	07/06/2021
TG LABELLINGPlenary Kick off Meeting	10/06/2021
Experts meeting	15/06/2021
Subgroup meeting MARKETING	17/06/2021
Subgroup meeting LEGAL & COMPLIANCE	18/06/2021
Subgroup meeting IMPLEMENTATION	21/06/2021
ECCG meeting: presentation	28/06/2021
Experts meeting	30/06/2021
TG LABELLING Plenary Meeting Q2-2021	01/07/2021
EU-CC AHWG presentation	02/07/2021
Experts meeting > Concept validation	14/07/2021
Subgroup meeting LEGAL & COMPLIANCE	14/07/2021
Subgroup meeting IMPLEMENTATION	27/07/2021
Subgroup meeting MARKETING	31/08/2021
Experts meeting: Preliminary deliverables	03/09/2021
SCCG meeting: presentation	17/09/2021
TG LABELLING Plenary Meeting Q4-2021	07/10/2021
Draft Report internal presentation	BTW 15/10 > 15/11/2021
Draft Report Transmission for comments	15/11/2021
Draft Report Validation	04/11/2021
SCCG meeting: transmission	19.11.2021
ECCG meeting: transmission	08.12.2021
EU-CC AHWG	29.11.2021
EU-CS AHWG	30.11.2021
Project closure Year 1	31/12/2021
Final Deliverable MT	01.02.2022
TG LABELLING Plenary Meeting Q1-2022	

Body Text Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

A.1 ANNEX SUBSECTION

Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui official deserunt mollit anim id est laborum.

A.2 ANNEX SUBSETCION

Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui official deserunt mollit anim id est laborum.

A.2.1 Annex Second Subsection

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

A.2.2 Annex Second Subsection

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

// MAKE SURE THAT THE OUTSIDE BACK COVER WILL BE A LEFT HAND PAGE. INSERT A BLANK RIGHT HAND PAGE IF NECESSARY.

XX-00-00-000-XX-X

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 000-00-0000-000-0
doi: 0000.0000/000000