EUROPEAN
COMMISSION

Brussels, 13.9.2017
SWD(2017) 500 final

PART 4/6

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

{COM(2017) 477 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

Table of contents:

1. Introduction 3

1.1 Methodological approach *5*

1.2. Data bottlenecks and methodological limitations *7*

2. What is the problem 8

2.1 Selective evidence on size and costs *8*

2.2 Root causes *10*

2.3. Information Asymmetry *14*

2.3 The Labelling Concept *18*

2.4. The problem of Fragmentation *29*

3. The ICT security certification landscape 31

3.1 International schemes and other initiatives 31

3.2. National initiatives 39

3.3. Main challenges and the need for a EU approach 44

4. Policy objective and intervention logic 47

4.1. Policy options *48*

Option 0 ..... **48**

Option 1 ..... **50**

Option 2 ..... **50**

Option 3 ..... **50**

1. Introduction

Every day, cybersecurity incidents cause major economic damages to European businesses and the economy at large. Such incidents undermine the trust of citizens and enterprises in the digital society. Theft of commercial trade secrets, business information and personal data, disruption of services - including essential ones - and of infrastructures result in economic losses of hundreds of billions of euros each year.

Cyberattacks are increasing at an alarming pace. The latest ransomware campaign, in May 2017, shows the potentially massive impact of cyber-attack across sectors and countries: more than 150 countries and over 190,000 systems were affected, including those related to essential services such as hospitals. This example is just the last of a series: more than 4,000 ransomware attacks have occurred every day since the beginning of 2016, a 300% increase over 2015. 50 % of businesses in the EU have suffered a cyber-attack and the projected growth of cybercrime is now higher than that of the internet. A recent survey[1] from 2016 revealed that number of security incidents across all industries rose by 38% in 2015, i.e. the biggest increase in 12 years.

Against this background, in its 2016 Cybersecurity Communication, the European Commission announced that, in view of the cybersecurity challenges and the overall effort to step up cooperation and knowledge sharing landscape, it would have advanced the evaluation of ENISA, due by June 2018, and present a proposal for a new mandate, as soon as possible. In particular, the Commission noted that the review of ENISA would provide an opportunity for a possible enhancement of the agency's capabilities and capacities to support Member States in a sustainable manner in achieving cybersecurity resilience by taking into account the agency's new responsibilities under the NIS Directive, new policy objectives to support cybersecurity industry, evolving needs in securing critical sectors, and new challenges linked to cross-border incidents, including coordinated response to cyber crises.

At the same time, the Commission noted that national initiatives are emerging to set high-level cybersecurity requirements for ICT components on traditional infrastructure, including certification requirements. Albeit important, these initiatives bear the risk of creating single market fragmentation and interoperability issues. Accordingly, the Commission announced that it would work, among others, on a possible European ICT security certification framework proposal, to be presented by end-2017, and to assess the feasibility and impact of a European lightweight cybersecurity labelling framework.

In the Communication on the Digital Single Market Strategy Mid-term Review, the Commission has further clarified that, by September 2017, it will review the mandate of ENISA to define its role in the changed cybersecurity ecosystem and develop measures on cyber security standards, certification and labelling, to make ICT-based systems, including connected objects, more cyber-secure.

Building on the findings[2] of the public consultation on the contractual Public Private Partnership on cybersecurity and possible accompanying measures, that took place from 18 December 2015 to 11 March 2016, and other technical studies, the following two main problems have been identified with regard to ICT security certification and labelling:

- Citizens' and companies do not have sufficient information concerning the security properties of ICT products and services they purchase
- The emergence of multiple national and sectorial certification schemes causes market fragmentation and barriers to the internal market

To evaluate the needs for policy action in the field of cybersecurity certification and labelling and carry out an impact assessment in light of the Commission's "Better Regulation" guidelines, the Commission needs a study to provide the evidence base needed.

Following a stakeholder consultation held in April 2017 by DG CNECT, the following policy options have been considered and discussed:

[1] http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/

[2] https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-contractual-ppp-cybersecurity-and-staff-working-document

- Option 0) *No action*
- Option 1) *Soft law tools*
- Option 2) *SOG-IS agreement mandatory for all EU Member States and extend its membership.*
- Option 3) *ICT Security Certification Framework*

In the following chapters of this Interim Report, the results of Task 1 are presented, after a quick recall of the adopted methodological approach. Within this Interim Report will be also summarized the results obtained from the desk research, the interviews with selected and impacted stakeholders and the online questionnaire properly structured by the Consortium. All data gathered will be used for Task 2 in order to duly evaluate and compare the policy options considered by the Commission.

In order to respond to the pressing time-line of the client we have modified the work plan originally presented within the proposal. This Interim Report is developed in accordance with all indications and agreements provided by the Commission during the project development, during the Inception Meeting of May 17th 2017 and in accordance with the Inception Report submitted on 19th May 2017. All activities were carried out in close cooperation between the Commission and the Consortium.

The final version of this Interim Report will take into account observations and comments raised by the Commission at the First Interim Meeting and will be made available to the Commission one week after the meeting.

1.1 Methodological approach

The European Commission - DG CNECT asked to the Consortium to gather evidence on ICT Security Certification and Labelling in order to assist the development of an Impact Assessment accompanying the foreseen regulation on certification and labelling. The Impact Assessment developed by the European Commission – DG CNECT has been substantiated empirically by the Consortium mainly through additional secondary sources, the use of more granular statistics (by country, sectors, affected groups), and a limited amount of field work. In particular, we have been fleshed out the IA by:

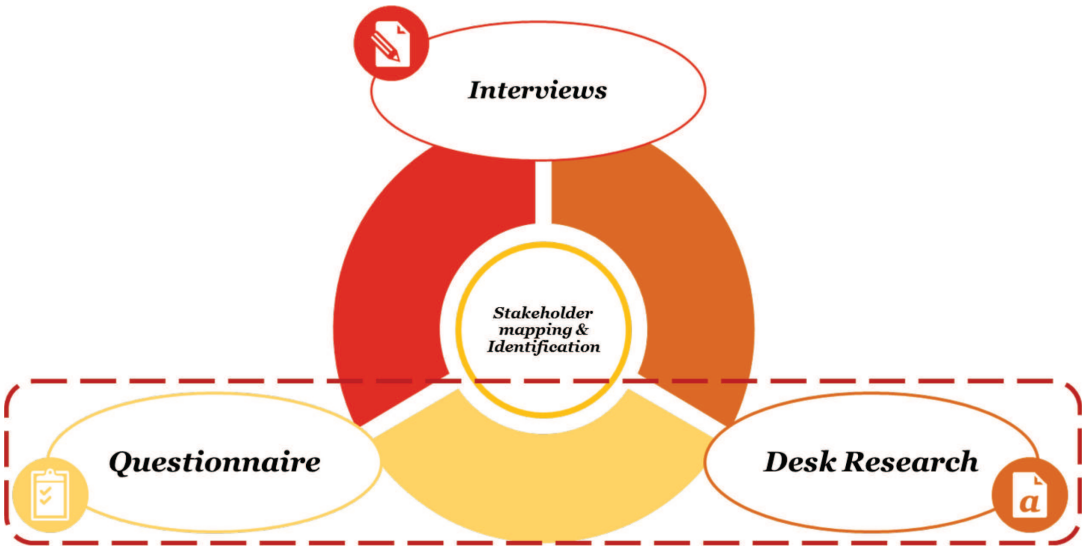
- Mapping all certification and labelling scheme, which enables to further substantiate the definition of the problem, the EU right to act, and the baseline and no action scenarios;
- Further describing and operationalising the policy options and their implications;
- Substantiate the market failures, fragmentation and their costs, including exemplifications and specific cases;
- Attempting to come up with some educated guesses on the different costs and benefits of certification;
- Further developing, commenting, and substantiating the options comparison and ranking

In close cooperation with the Commission, the Consortium will continue to flash out the Impact Assessment developed by the Commission in the same way explained above.

Methodological triangulation

The methodological triangulation refers to a fully structured and consolidated methodology for triangulating sources and methods, so that this will be a mixed methods study integrating quantitative and qualitative sources and methods.

Figure 1 Sources and methods triangulation



Source: own elaboration

Desk Research

Initial overall **desk research** was key for understanding the state of the art, for highlighting the complexities to be addressed and for laying the ground for **a solid methodology which builds over, but does not replicate, existing literature findings.** For this reason, PwC and FUB have been aligned with the EC Team concerning the study, which are currently being undertaken in closely related topics as to avoid overlap in research output. During the desk research activities, the Consortium has analysed all the documents provided by Commission including:

- European Commission Communications and studies
- JRC studies
- ENISA workshops
- Stakeholders consultations and workshops
- Results of ENISA Surveys

In addition to the documentation provided by the Commission, the Consortium has analysed other related and relevant documents from internal or secondary sources as:

- European Commission studies
- ENISA studies
- JRC studies
- Publications
- Stakeholders communications and studies
- Workshops

Moreover, in order to create synergies and not replicate parallel studies that are still ongoing, the Consortium has taken into account all the documentation including:

- IoT and Cybersecurity studies
- PwC studies
- IoT Market Studies
- Cloud Computing study

Other relevant information, evidences and data cost have been extracted through the interviews with selected stakeholders, that will be summarized in **chapter 5**. The desk research activities were also aim to find additional impacted stakeholder. A stakeholder mapping, taking in consideration all the inputs provided by the Commission, resulted fundamental to select the main stakeholder to be interviewed.

Interviews

Another step of the triangulation methodology was working with DG CONNECT to identify and validate the list of the stakeholders who are directly or indirectly impacted by the project. During the first preliminary meeting, on the 8th of May 2017, has been highlighted by the DG CONNECT Team that surveys have been conducted by **JRC**; this means that a mapping of stakeholders has already been developed. The stakeholders **mapping** has been integrated with the identification of **new selected stakeholder** included in specific and most impacted industrial sectors, taking in consideration the JRC surveys data received and analysed by the Consortium. A detailed stakeholder map has been necessary for identifying experts and participants for the **interviews** organized. The Map was constantly updated and improved during the project running and it is attached within the **Annex 7.3**.
More in particular, the Commission asked to contact National Certification Authorities and some representatives from smart-metering and semi-conductors industries. The Consortium has collected contacts to be interviewed from European Commission – DG CNECT, from internal sources and from online websites of companies and other impacted organisations.
In order to contact directly the selected stakeholders, many phone calls were made to have an appointment, asking also to spread the Questionnaire within the representatives of the Organization. Before any interviews, the Consortium sent by e-mail an interview template to inform the representative interviewed about the topics and the questions that would be later posed during the interview. Many organizations were also contacted only by e-mail with attached the interview template structured by the Consortium.
Once the appointment was scheduled, the interviews were conducted through a conference call with representatives from the organizations involved, representatives from PwC and representatives from FUB.

To this day, **18 representatives** have been interviewed from impacted sectors and national Certification Authorities. More in detail, the stakeholders interviewed are:

Type	Representatives interviewed
National Certification Authority	6
Conformity Assessment Bodies	2
Semi-Conductors Industry	1
Smart-Metering Industry	5
Critical Infrastructures	4

All the Minutes of the Interviews conducted by the Consortium are included within the **Annex 7.1** and all the contributes from stakeholder are also structured in Chapter 5 to convey the different views gathered on different aspects.

Questionnaire

The Consortium has structured an online questionnaire in order to gather additional evidence on ICT security certification and labelling across Europe. The Questionnaire has been put online on 6th June 2017 and will remain open until 19th June 2017.
The invitation to the Questionnaire has been sent by e-mail to all collected contacts. A detailed map of the stakeholders contacted is presented within the Annex 7.2 "Questionnaire". Within the same Annex, preliminary descriptive statistics of the type of organisations that have completed the questionnaire is presented. More detailed results and analysis of the answers provided will be presented within the next deliverables, after the expiration date of the Questionnaire on 19th June 2017. The results of the online questionnaire will also contribute to the data cost analysis. The Questionnaire results will be partly complemented also by **surveys' answers provided by JRC and DG CONNECT**.

1.2. Data bottlenecks and methodological limitations

A few considerations on data bottlenecks and methodological limitations that apply especially to the products, that will be delivered in five weeks but also more generally to the final products at the end of the five months' project duration.

There are clear bottlenecks in terms of gathering reliable data on certification costs and benefits that have a wide EU 28 coverage. Through secondary sources only some scattered, fragmented, and at times inconsistent figures are available. Some interviews with relevant stakeholders and experts (or a workshop) have been possible to be conducted but the quality of the data obtained will not warrant a full objective quantification. Even within the five months' period, though some more data and qualitative information will be obtained, we will never have a fully robust and representative dataset.

For the above reasons it is important to stress again that: a) the triangulation of sources and methods remains a key pillar of our approach; and b) the assessment of impacts and the comparison and ranking of policy options will have by necessity a mixed quantitative-qualitative nature and will be supported by narrative explanations and justifications.

2. What is the problem

1.1 Selective evidence on size and costs

As stated in the European Commission (henceforth EC) Communication on Resilience, despite previous initiatives and achievements *'the EU remains vulnerable to cyber incidents. This could undermine the digital single market and economic and social life as a whole'* (European Commission, 2016a, p. 2). The box below reports some selective evidence on cyber incidents dimensions and associated problems and costs.

Box 1 Exemplificative evidence

Total breaches 2014-2016 (Symantec, 2017)

- 2014: 1523 (with more than 10 million identities exposed: 11; total identifies exposed: 1.2B);
- 2015: 1211 (with more than 10 million identities exposed: 13; total identifies exposed: 564M);
- 2016: 1209 (with more than 10 million identities exposed: 15; total identifies exposed: 1.1B);
- In the last 8 years more than 7.1 billion identities have been exposed in data breaches;
- It takes two minutes for a IoT device to be attacked.

Global estimates (CSIS, 2014)

- The likely annual cost to the global economy from cybercrime are estimated in more than $400 billion;
- Hundreds of millions of people having their personal information stolen cost as much as $160 billion per year;
- As cybercrime have impacts on export related jobs, Europe could lose as many as 150,000 jobs due to cybercrime or about 0.6% of the total unemployed

Costs to firms (PwC, 2015)

- The 2015 Information Security Breaches Survey conducted in the United Kingdom showed that 90% of large organisations and 74% of small and medium-sized businesses reported they had suffered from an information security breach;
- For companies with more than 500 employees the average cost of the most severe breach was between €1.86 million and €4.01 million
- For SMEs it oscillated between €95,840 and €397,1675

Hindrances to online activity, (Eurostat data reported in European Commission 2016b)

- The proportion of internet users having experienced certain common security issues over the internet – such as viruses affecting devices, abuse of personal information, financial losses or children accessing inappropriate websites – stood at 25% in 2015
- Security concerns prevented some internet users in the EU from doing certain activities over the internet: almost 1 in 5 did not shop online (19%) or did not carry out banking activities (18%) in 2015, and 13% of them did not use the internet with a mobile device via wireless connection from places other than home.
- Notably, more than 1 internet user out of 5 did not buy or order goods or services on-line for private use due to security concerns

Skill shortage and risk of know-how out flow (Friedman 2015; ISACA, 2015; Optimity Advisors, 2015)

- The Global Cybersecurity Status Report indicates an alarming shortage of skilled cybersecurity professionals around the world
- According to different estimates the demand for the cybersecurity workforce will rise to 6 million globally by 2019, with a projected shortfall of 1 - 1.5 million
- The situation is similar in Europe where, although academic organisations are educating highly qualified and trained cybersecurity professionals, this talent is many a time not absorbed by the European cybersecurity market;

- Given barriers to growth of European cybersecurity companies, this could result into an outflow of knowhow from Europe

Hindrances to Open and Big Data Economy

- The potential for data-driven innovation, provided cybersecurity is achieved, is a two-fold source of economic growth (OECD, 2013). First, directly as a new market with great economic potential of generating revenues by itself; Second, as a way of increasing efficiency and reducing administrative bottleneck;
- In the EU, if all framework conditions were in place, the EU data economy could increase up to EUR 643 billion by 2020 to EUR 272 billion in 2015 ;

Even the smallest estimates of cybercrime costs to the global economy are larger than the national economy of some countries, while governments and companies underestimate how much risk they face from cybercrime and how quickly this risk can grow. The most important cost of cybercrime[3], however, comes from its damage to company performance and to national economies.

Cybercrime hinders trade, competitiveness, innovation, and global economic growth. The first largest source of direct loss from cybercrime is the theft of intellectual property. In fact, companies invest substantial amount of money in research and development (R&D) to create new intellectual property (IP). One UK Company told British officials that it incurred revenue losses of $1.3 billion through the loss of intellectual property and disadvantages in commercial activities. Anecdotal evidence about IP theft come from every major economy (CSIS 2014).

According to the OECD Digital Economy Outlook 2015 (2015), 'ransomware' is rising as a prominent challenge among digital security issues. Experts estimate that "CryptoLocker infected some 234 000 computers during its first two months alone, before being disrupted by a multinational law enforcement effort, involving Canada, Germany, Luxembourg, the Netherlands, Ukraine, the United Kingdom and the United States"

The 'threat landscape' continues to evolve, sustained by often profitable business models. For example, one of such models is based on 'ransomware, which is a type of file-encrypting malware increasingly deployed by cybercriminals to encrypt the computer files of an organisation or individual, who must then make a payment (i.e. the "ransom") in exchange for decryption of their files.

The most prominent strain of ransomware is "CryptoLocker", which is spread via email attachments. Experts estimate that "CryptoLocker infected some 234 000 computers during its first two months alone, before being disrupted by a multinational law enforcement effort, involving Canada, Germany, Luxembourg, the Netherlands, Ukraine, the United Kingdom and the United States". In addition, cyberattacks leading to data breaches where the personal data of millions of European individuals in the EU get compromised have become more and more common in the recent years.

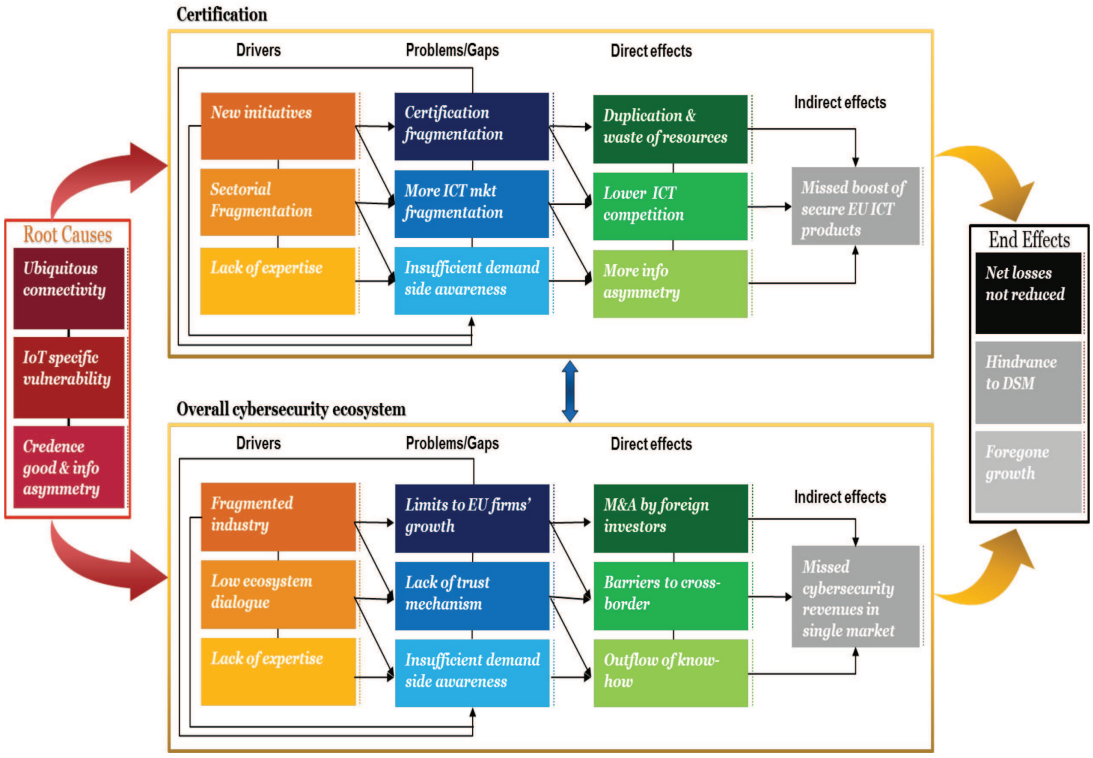
Similarly, to the business model behind ransomware, the breached company could be requested to pay a sum of money to the attackers in exchange for not publishing the data online. This type of incidents can have a direct impact on citizens in the form of e.g. identity theft or financial fraud (stolen credit cards) directly impacting the trust in the Digital Single Market (DSM).

ISACA (2015) conducted a global survey[4] of 3,439 business and IT professionals in 129 countries to capture their real-time insights on cybersecurity attacks, skills shortages finding that 86% of respondents see a global cybersecurity skills gap—and 92% of those planning to hire more cybersecurity professionals this year say they expect to have difficulty finding a skilled candidate. The survey also found that 83% of respondents say cyberattacks are among the top three threats facing organizations today, and only 38% say they are prepared to confront such threats. Moreover, 86% of respondents believe there is a shortage of skilled cybersecurity professionals. 48% of respondents are equally concerned about physical attack (e.g., terrorist attack or act of war) and cyberattacks.

[3] Symantec. (2017). Internet Security Threat Report: Volume 22, Symantec.
[4] ISACA. (2015). 2015 Global Cybersecurity Status Report: ISACA

In the picture below, we present a problem tree where effects are framed as foregone opportunities.

Figure 2 Problem tree



Sources: own elaboration based on EC sources (European Commission, 2016a, 2016b, 2016c, 2016d), and on various studies (Baldini et al., 2017; ECORYS, 2011; ERNCIP, 2014; IDC, 2009; Optimity Advisors, 2015)

1.2 Root causes

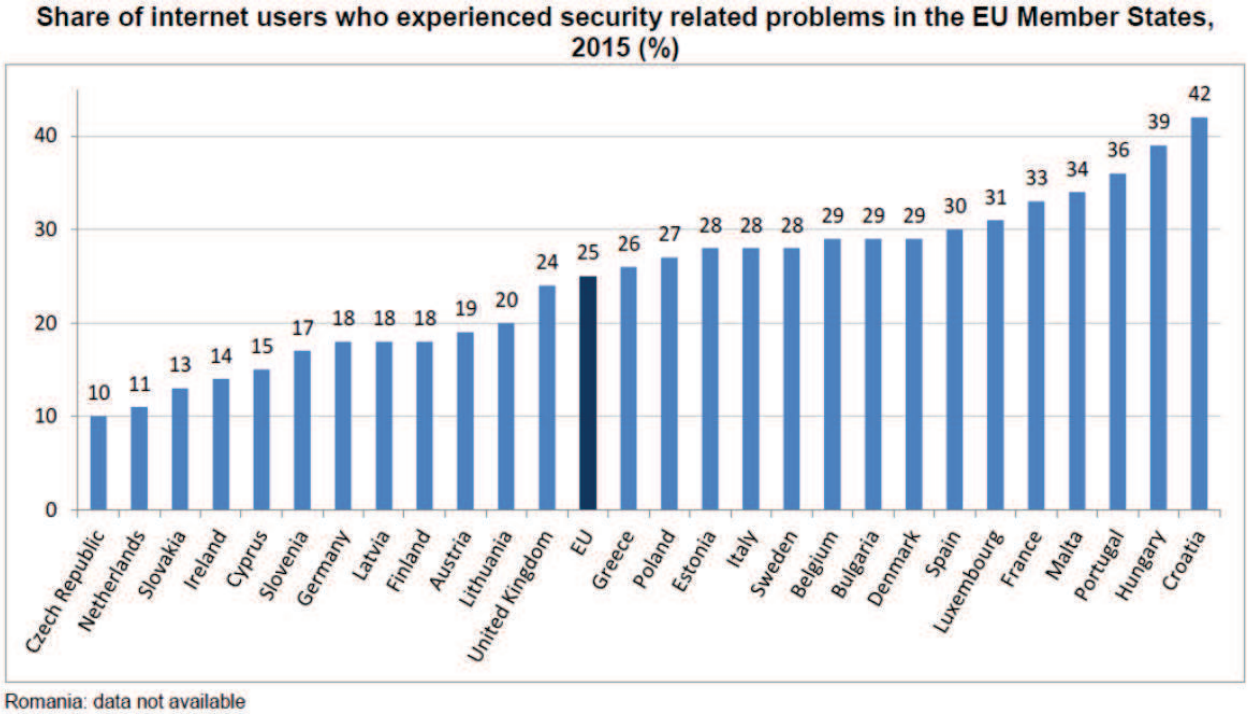
Universal ICT usage increase 'surface attacks'. Among the root causes or the increasing risk for, and occurrence of, cyber incidents there is the simple fact that the Internet and the cyberspace have become ever more important and are the backbone of our digital economies and societies. ICTs have become widely available to the general public, both in terms of accessibility as well as cost[5]. A boundary was crossed in 2007, when a majority (55 %) of households in the EU-28 had internet access. This proportion continued to

[5] http://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals

increase, passing three quarters in 2012 and four fifths in 2014. In 2016, the share of EU-28 households with internet access rose by two additional percentage points compared with 2015 to reach 85 %, 30 percentage points higher than in 2007. Widespread and affordable broadband access is one of the means of promoting a knowledge-based and informed society. Broadband was by far the most common form of internet access in all EU Member States: it was used by 83 % of the households in the EU-28 in 2016, approximately double the share recorded in 2007 (42 %).

Figure 3 Cyberspace as backbone of digital economy and society

Source: European Commission (2016b, p. 3)



Source: Eurostat

Security concerns prevented some internet users in the EU from doing certain activities over the internet: almost 1 in 5 did not shop online (19%) or did not carry out banking activities (18%) in 2015, and 13% of them did not use the internet with a mobile device via wireless connection from places other than home. Notably, more than 1 internet user out of 5 did not buy or order goods or services on-line for private use due to security concerns in Romania (35%), Sweden (34%), Portugal (30%), France (29%), Spain and Latvia (both 28%), Finland (27%), Italy and Malta (both 25%), Slovenia (24%), Denmark (22%) and the Netherlands (21%). Just as consumers, who take advantage of digital opportunities, businesses across Europe also largely depend on smoothly running information systems. This concerns not only the organisations, whose business model is based on online activity such as e.g. e-commerce platforms, but practically all types of businesses as the use of information and communication technologies influences the way that enterprises are run, information shared with partners and customers. Increasingly public and private sector business entities have the core business, operational critical data and "digital assets of their

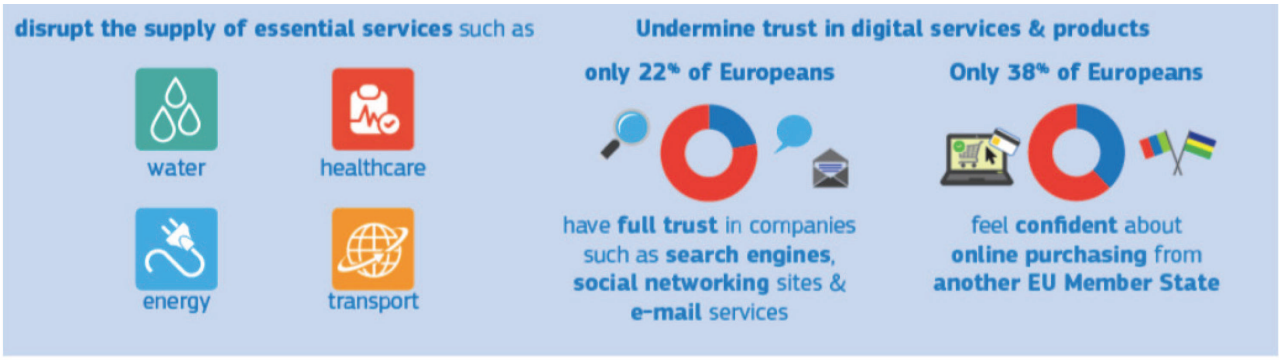
operations" in digital form, implemented by various ICT systems customer relation management, applications, services and operations (e.g. customer relationship management, supply chain management or enterprise resource planning). According to the survey on information and communication technology (ICT) usage in enterprises, only 3% of enterprises in the EU 28 do not have access to Internet. According to the **2015 Eurostat survey on ICT** usage in enterprises, the awareness among European enterprises related to cyber threats and the need to have a proper ICT security policy is growing, though there is still much room for improvement. In 2015, almost one out of three enterprises in the EU 28 had a formally defined ICT security policy. The share of large enterprises with such a policy was almost three times the share of small ones.

Surface attack increased and vulnerability amplified by IoT. The vulnerability is amplified by the fact that various sectors and industries heavily depends on ICT components and by the interdependence between current and future infrastructures (e.g. in smart cities environments, connected cars, energy smart grids). According to a recent report based on a Global IoT Executive Survey[6] on the impact of the IoT on companies around the world (Business Insider, 2017), the Internet of Things (IoT) is disrupting businesses, governments, and consumers and transforming how they interact with the world. Companies are going to spend almost $5 trillion on the IoT in the next five years — and the proliferation of connected devices and massive increase in data has started an analytical revolution. According to this report, there will be 22.5 billion IoT devices in 2021, up from 6.6 billion in 2016 and $4.8 trillion in aggregate IoT investment between 2016 and 2021. As pointed out in the latest BITAG (Broadband Internet Technical Advisory Group) unanimous report[7] (BITAG, 2016), the IoT and has brought with it new security and privacy risks. The number and diversity of consumer IoT devices is growing rapidly; these devices offer many new applications for end users, and in the future will likely offer even more. Many IoT devices are either already available or are being developed for deployment in the near future, including: sensors to better understand patterns of daily life and monitor health; monitors and controls for home functions, from locks to heating and water systems; devices and appliances that anticipate a consumer's needs and can take action to address them (e.g., devices that monitor inventory and automatically re-order products for a consumer). The same report points out that if IoT devices are compromised by malware they can become a platform for unwanted data traffic – such as spam and denial of service attacks – which can interfere with the provision of these other services. It also reports evidence that some devices do not abide by rudimentary security and privacy best practices. In some cases, devices have been compromised and allowed unauthorized users to perform surveillance and monitoring, gain access or control, induce device or system failures, and disturb or harass authorized users or device owners. Risks are linked to: lack of IoT supply chain experience with security and privacy; lack of incentives to develop and deploy updates after the initial sale; difficulty of secure over-the-network software updates; devices with constrained or limited hardware resources (precluding certain basic or "common-sense" security measures); devices with constrained or limited user-interfaces (which if present, may have only minimal functionality), and devices with malware inserted during the manufacturing process. With the IoT millions of devices are connected, which in jargon means that the 'attack surface' widely expands. Critical infrastructures, such as for example electricity generation plants or transportation systems, are controlled and monitored by Industrial Control Systems (ICS), including SCADA (Supervisory Control and Data Acquisition) systems. Today ICS products are mostly based on standard embedded systems platforms and they often use commercial off-the-shelf software. In particular, some sectorial industries such as transport, energy, health, and others do not have a solid and reliable scheme providing them assurance on the level of security of ICT components integrated into their systems (European Commission, 2016b, p. 10).

[6] http://www.businessinsider.com/the-internet-of-things-2017-report-2017-1?IR=T

7 BITAG. (2016). Internet of Things (IoT) Security and Privacy Recommendations. A Uniform Agreement Report: BROADBAND INTERNET TECHNICAL ADVISORY GROUP (BITAG).

Figure 4 The potential reach of cyber incidents



Source: European Commission (2016b, p. 4)

For these reasons, ICT embedded systems and the IoT are by themselves a new source of vulnerability and are placed in our problem tree among the root causes.

ICT products as computers or smartphones are often replaced regularly and this ensure a certain degree of security. Instead, ICT system are not replaced so often and, under the Directive for the security of networks and information systems (NIS), operators of critical infrastructures will be required to invest in their overall security in order to comply with the NIS Directive. However, not all IoT applications (e.g. smart home appliances) are linked to critical infrastructures and for those use cases, NIS directive would not be applicable.

Lack of full users' awareness due to information asymmetry. The third root cause has to do with the particular nature of cybersecurity as a 'credence good' and the implications in terms of information asymmetry. In order to shed light on this aspect it is useful to make the analogy with the various experiments and studies[8] conducted in the domain of environmental impact of home appliances and cars[9] (Codagnone et al., 2013; Codagnone et al., 2016). The "greenness" of a dishwasher or of a car are 'credence' goods; consumers cannot ascertain their environmental qualities during purchase or use. They are not present during the production process of the product and therefore cannot observe environmental friendliness of production. The objective of eco-labels based on certification standards and requirements is to reduce information asymmetry between the producer of green products and consumers by providing credible information related to the environmental attributes of the product and to signal that the product is superior in this regard to a non-labelled product. The implicit goal of eco-labels is to prompt informed purchasing choices by environmentally responsible consumers. This same reasoning applies to the cybersecurity ecosystem and in this respect a common certification framework and a lightweight labelling scheme may greatly reduce information asymmetry and increase demand-side awareness.
As more connected home devices enter the market at different price points, devices such as home security systems, smart thermostats and baby monitors are shifting from "nice to have" accessories to necessary gadgets. With every connected home device purchase, consumers are unknowingly providing hackers with new avenues to launch their attacks. In some instances, poor consumer security habits and vulnerabilities in connected devices are letting hackers into consumers' homes**.** According to 2016 Norton Cyber Security Insights Report[10], Fifty-one percent of consumers think it's becoming harder to stay safe and secure online than in the real world and one in five connected home device users don't have any protective measures in place for their devices. Over six in 10 (62 percent) consumers said they believe connected home devices were designed with online security in mind. However, Symantec researchers identified security vulnerabilities in 50 different connected home devices ranging from smart thermostats to smart hubs that could make the devices easy targets for attacks. Data show that there is a clear information asymmetry between designers and vendors on one side, and customers/users of ICT solutions on the other.

[8] Codagnone, C., Veltri, G. A., Bogliacino, F., Lupiáñez-Villanueva, F., et al. (2016). Labels as nudges? An experimental study of car eco-labels. Economia Politica, 33, 403-432.
[9] Codagnone, C., Bogliacino, F., & Veltri, G. (2013). Testing CO2/Car labelling options and consumer information. Final Report. Brussels: European Commission
[10] https://www.symantec.com/content/dam/symantec/docs/reports/2016-norton-cyber-security-insights-report.pdf

The UK government document "Using behavioural insights to improve the public's use of cyber security best practices"[11] provided by the UK government, it is argued that there is a considerable gap between what is currently known and what needs to be understood in order to address the cyber security behaviours of individual internet users. For instance, users report awareness and concerns about security but in practice never change privacy default settings and leave their devices always on and online.

There is certainly a need for good communication within the cyber security user community and a lack of knowledge and skills remains a problem. The '*provide information and they will use it*' approach does not appear to be effective in spreading the message fully or widely enough. It could be argued that communication should be through more diverse methods than a passive web page and key messages should be proactively pushed to the most relevant user communities. We know that interventions that rely solely on knowledge transfer may struggle. Even if people do find and read the information, behaviour change theories would tell us that while information is necessary it is not sufficient and the other influencers are important. Any knowledge-based intervention is more likely to be successful if other influencers, highlighted in behaviour theories are incorporated into the intervention – designing the right defaults; creating a security culture; having champions and opinion leaders etc.

2.3. Information Asymmetry

There are three classical market failures that according public economics warrant a policy or regulatory intervention: a) externality; b) market power; and c) information asymmetry. There can be no doubt in the fact that the cybersecurity market is currently affected by a clear case of information asymmetry; it is an information asymmetry that is particularly acute both because of the technicalities of the topic and because of fragmentation in certification scheme.

The security properties of a software product are a quality dimension, which is difficult to assess for an end user prior to purchase, at least not at a justifiable cost. In this situation, the market fails to provide optimal resource allocation. Consider a vendor A selling a product with desirable quality features (in this case strong security) and a vendor B selling a product without the desirable features (i.e. with weak or no security). Vendor A cannot reap the benefits of better quality because vendor B has lower costs and can therefore offer his product at a price which is prohibitively low for vendor A. As the customers cannot tell the difference due to the information asymmetry, they will buy from vendor B. This initiates a race to the bottom with regard to the desired quality property. This is commonly called a "market for lemons" referring to the seminal paper of Akerlof (1970).

This argument, however, can be further reinforced by an ongoing debate in the public and behavioural economics literature on whether or not the limited rationality, heuristics and biases that characterise the behaviour of both citizens and businesses as consumers may represent a fourth type of market failure lending further supports to policy or regulatory intervention (for a review of this debate see Lunn, 2015). Whereas the resolution of this ongoing theoretical and normative debate is yet to come, it is worth exemplifying the cognitive and behavioural limitations affecting both consumers and businesses when dealing with cybersecurity. There is no single behaviour that can keep people secure online, but rather cyber-security requires multiple interrelated behaviours, and each one is potentially influenced by different factors. The cognitive load on final users is heavy and many times they do not behave safely. This applies equally to consumers and businesses:

- Home users and small companies may lack the required expertise to set up the technical defences. Often, security is managed by an individual as one part of their overall role who may rely on help from family and friends, rather than an external specialist company. The worst-case scenario is small companies having no in-house staff being responsible for cyber-security.

- Company employees may not follow the cyber-security policies put in place by the company;

- Many do not perceive a risk. Small businesses believe they are safe from cyber threats, even though they have no policy or ways of knowing if this is the case. A National Cyber Security Association (NCSA) survey of small businesses in the US, conducted in 2012, suggested a cyber security disconnect where 77% of companies believed their company was safe from cyber threats and 47%

[11] https://www.gov.uk/government/publications/cyber-security-using-behavioural-insights-to-keep-people-safe-online

believed a data breach would have no impact on their business, yet 87% did not have a formal written Internet security policy and 69% did not even have an informal one. Finally, 18% said they would not even know if their computer network was compromised.

There are behaviours that increase the risks

- Always being connected has become both a habit and an expectation - The need to be connected at that place/at that time outweighs risk of insecure connection or interacting in a public space. For instance, in 2017, people in Italy spend an average of 6 hours per day on internet (through both laptops and mobile phones). In other countries, such as UK, France, Spain, Poland and Germany, the average ranges between 4h30 and 5h45[12].

- People are habituated to the "I accept" button and warning messages – do not read what they are agreeing to or think about the consequences of their behaviour, just click. They do not always make rational, thought through decisions. 73% of the people admit of not reading the whole fine print and only 17% of those who did understand it. [13]

- Convenience (or taking the easy way) always wins over security. An example of this could be a basic action like setting a password. Practices such as sharing a passwords and using the same ones on multiple platforms is still very common among individuals, even though it is highly recommended not do so.[14]

- Desirability wins over security – the desire to be connected, to download applications, music, video etc., to share information with people online. To do this at no expense or simply for information is also desirable. The Data-for-Access trades are in fact based on the desire and the convenience of being connected but at the cost of sharing private and sensitive information. [15]

- Financial costs do not justify security gains - security software is expensive, software upgrades are expensive. A recent investigation by the Polytechnic University of Milan's Information Security & Privacy Observatory[16] stresses that only 39% of large businesses have enacted a multi-year investment plan, and only one out of every two organizations has managers dedicated to these tasks. This is a precarious situation, with potential consequences not only for their offices but for the factories too, where modern machinery has become increasingly connected and dependent on the ability to gather, transmit, and analyze data. Companies often find it difficult to understand the benefits or gains of major investment in cyber security.

- Incentives for insecure behaviour mean that security risks are ignored– cost benefit analysis in favour of insecure behaviours (desire for immediate, concrete gain versus potential abstract risk in future). Especially Small Business do not perceive themselves as possible victims of cyber threats and therefore do not invest in cybersecurity measures. [17]

- Effort required is too high – to understand how to use the different tools, to keep up to date, to log in, to remember passwords, to complain. As a study from the National Institute of Standards and

[12] https://wearesocial.com/special-reports/digital-in-2017-global-overview

[13] https://www.theguardian.com/commentisfree/2014/apr/24/terms-and-conditions-online-small-print-information
[14] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4291202/#B1
[15]https://www.forbes.com/sites/marymeehan/2015/03/17/how-much-of-your-private-data-are-you-willing-to-share/#7d04406e3530
[16]http://www.italy24.ilsole24ore.com/art/business-and-economy/2017-05-29/cybersecurity-171538.php?uuid=AEX5bAVB
[17]https://staysafeonline.org/about-us/news/new-survey-shows-us-small-business-owners-not-concerned-about-cybersecurity

Technology (NIST) reports, individuals often deal with "Security fatigue" due to the many and various cybersecurity procedures that they have to follow. [18]

- No perceived benefit – belief that behaviours will not make a difference to security. Cybersecurity measures need to be constantly updated in order to face new possible cyberattacks. Because of this necessity, it is commonly believed that the companies that have not been hacked have not discovered it yet. [19]

- No perceived risk or risks downplayed - people justify their behaviours, e.g. being on an insecure connection for a short time is safe, personal information is not of value or simply thinking that attacks will not happen. For this reasons, illegal streaming websites[20] and social media are hackers' favourite target because people do not perceive them as not secure.[21]

- Do not perceive need for change – Lack of belief that negative consequences will result from noncompliance. The longer a person uses the internet with no negative consequences, the less they believe they are susceptible to risk.

- Lack of knowledge and skills – knowledge about what to do and how to do it, and skills to detect fraudulent activity. People must constantly update this knowledge. The Frost & Sullivan 2015 (ISC) Global Information Security Workforce Study lays bare the scale of the cyber security skills shortage, demonstrating that while demand for security professionals is growing, the supply of these professionals is not able to keep pace. The report estimates a global shortfall of 378,000 information security staff today, a figure that is projected to increase to 1.5million by 2019. Echoing these findings, Harvey Nash's 2015 CIO Survey found that 23 per cent of CIOs report a skills shortage in security and resilience and that only around a quarter (23 per cent) feel that they are very well prepared for a serious cyber security incident[22].

- Do not know which information to trust - who are the credible sources, who do you believe when different people make conflicting recommendations.

- Simply forget to behave securely when distracted by other things when online.

- Social etiquette – it is a sign of trust/intimacy to share information including passwords and devices.

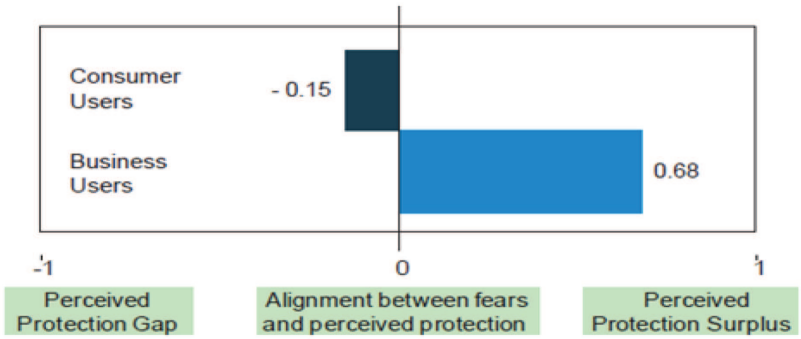
The certification, however, is only a signalling mechanism, if the criteria actually represent the desired property of the certified product, i.e. whether they are meaningful or not[23] (Schierholz & McGrath, 2010). A buyer needs to be able to assess whether the criteria match his needs. Usually this can only be achieved if the criteria are transparent to the buyer or even publicly available. However, the challenge remains to create a meaningful set of criteria applicable to a broad enough number of buyers to create a sufficient market for certified products. Testing a given product for vulnerabilities can only produce relatively short-lived test results, as attackers and security researchers continuously discover new ways of attacking systems and vulnerabilities in components used in products and systems (i.e. operating systems and applications). Thus, the test cases for certification have to be updated very frequently and for a product that has passed certification last month, today there may be a dozen known vulnerabilities and exploits. Lifecycle considerations Nowadays it is commonly accepted that the threat landscape is continuously changing and that target systems need to react to this change. One example is the significant number of researchers that search for vulnerabilities in products to which vendors react by publishing updates to their products. A

[18] https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly
[19] http://hbswk.hbs.edu/item/target-s-expensive-cybersecurity-mistake
[20] https://www.netnames.com/insights/blog/2016/02/the-dangers-of-illegal-streaming/
[21] https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/
[22] http://www.apmg-international.com/en/news-events/542074.aspx
[23] Schierholz, R., & McGrath, K. (2010). Security Certification – A critical review. ABB by DHS.

change to the product however invalidates the certificate and therefore requires a re-certification (incl. the time delay and additional cost associated with this). This puts an end-user organization which mandates certified products into the dilemma of either sticking to their policy of using certified products only versus fixing a known issue in their system. Similarly, product vendors are in a dilemma. They have to choose between fixing a known issue and loose certification for the latest release of their product (at least until re-certification can be achieved) or not fixing a known but maintaining the product certification (which again points out the limited meaningfulness of product certification). However, there are multiple points often criticized about security certification and the criteria against which certification happens, among them are lack of publicly accessible, standardized certification criteria and processes, meaningfulness of the results (or rather lack thereof) and cost of certification. Also The German Association of Electric Manufacturers, while recognising that in the domain of ICT certification product characteristics remain hidden and are not fully transparent, points out that there are multiple aspects often criticized about security certification and the criteria against which certification happens, among them are lack of publicly accessible, standardized certification criteria and processes, meaningfulness of the results (or rather lack thereof) and cost of certification[24] (ZVEI, 2017) .

At any rate, empirical evidence shows that there is still and awareness and information gaps among the final users of ICT products about security. The study conducted by IDC EMEA on "The European Network and Information Security Market"[25] (IDC, 2009), developed the Trust and Confidence Gap Indicator, which measures the gap between business and consumer users' fears of main security threats, and the perceived level of protection, thanks to the use of security solutions. The indicator varies between –1 and + 1. When fears are higher than the perceived protection there is a protection gap (indicator from 0 to –1); when perceived protection is higher than fears there may be a protection surplus (indicator from 0 to +1). According to this study, business and consumer users show a similar, moderate level of fear of main security threats (described by the statement "I am somehow worried"). The level of perceived protection instead is higher for businesses than for consumer users, but this is more due to lack of awareness than real implemented protection measures. Firstly, business users rarely systematically assess their security risks and damages in case of security breaches, so the perceived protection is more often based on assumptions than specific facts and assessments. In fact, the business demand survey calculated by the study shows a lack of correlation between the level of perceived protection and the frequency of security breaches.

Figure 5 IDC trust and confidence Gap Indicator, EU average



NOTE: The indicator measures the difference between the average rating of perceived protection and the average rating of fear of IT security threats. It varies between +1 and -1.

Source: IDC (2009)

The Trust and Confidence Gap Indicator for EU Consumers is slightly negative with an average level of –0.15, pointing out that consumers perceive a protection gap against the main security threats. The confidence

[24] ZVEI. (2017). Benefits and limitations of certifications and labels in the context of cyber security: German Electrical and Electronic Manufacturers' Association (ZVEI)

[25] IDC. (2009). The European Network and Information Security Market Brussels: Report delivered by IDC for the European Commission.

gap affects particularly two main security threats, the abuse of personal information and children accessing inappropriate websites. On the contrary, exposure to a virus is the only case in which perceived protection exceeds fears. Internet users are not so optimistic about spamming, which is rated low in terms of fears but a lot lower in terms of protection, meaning that there is not much confidence in solutions able to solve this problem. It is not unlikely that many users simply accept Spam as an unavoidable, but unwanted, consequence of being online.

1.3 The Labelling Concept

As illustrated in a DG SANCO report[26] (European Commission, 2006), Labelling is an important market tool which should be viewed as an integral part of communication between societal players (business to consumers, directly and via intermediaries, authorities to consumers, etc.). Labelling is no longer the only reliable route for communicating information to the consumer, as it once was, but it remains an effective tool. The benefits of consumer information in general and labelling in particular are clear. For the consumer, it provides the means for the operator to pass on essential information about products (use-by dates, safety warnings, etc.) as well as information which, perhaps not being essential, is still considered useful (nutrition labelling, recycling details, etc.). As such, the label allows the consumer to make an informed choice at the point of sale about whether to purchase a product and, if they do so, to consider how best it should be used. For the industry, labelling is a powerful tool which, when used effectively and responsibly, not only ensures the operators provide essential information, but also enables them to highlight the benefits of their products when compared to those of their competitors[27]. This is even more of an important factor if there are additional costs in providing these benefits and the operator needs to convince the consumer to pay a higher price with respect to competing products on the market. Indeed a sociological study[28] carried out in Europe revealed that a lack of labelling on production methods was preventing consumers from possibly shifting towards such products. However, although labelling should be a win-win situation for both the consumer and operator, in practice there is often a market failure and many stakeholders would argue that labelling schemes are not living up to their full potential. Simply put, consumer use of labels is inconsistent and the effectiveness of labelling as a communication tool can be questioned. The reasons for this failure are varied, but perhaps start with a simple lack of consumer interest in the information a label provides. Even if the consumer is interested, many find using labels difficult as they contain too much information, much of which is not understood, is confusing and is poorly presented.

The concept of applying a label on a product after a successful security certification is not new, as the EAL certificates from common criteria, the IACS (ERNCIP 2014), the four levels of FIPS can all be related to a labelling scheme, which gives an indication on the level of security protection or trust of a system (Baldini, et al., 2017). The critical task is how to associate the labels in a harmonized way across different certification schemes, protection profiles and so on. In France, the ANSSI has defined a label system for trusted products and service providers. The labelling concept could be extended to cover not only the traditional levels of Common Criteria (EAL), but to address specific security functions, which can be linked to specific protection profiles. For example, labels could be defined for specific security properties like confidentiality, integrity and authentication or for a specific Security Target (ST), which is defined in the related protection profile.
We can define different dimensions for which the label can be defined:

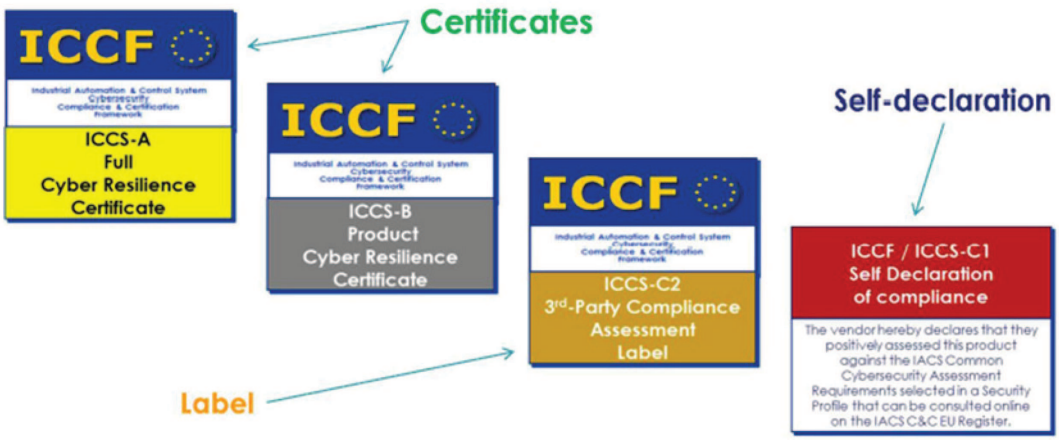
1. Level of assurance. This is the equivalent of the EAL in Common Criteria. We note that EAL level does not measure the security of the system itself, it simply states at what level the system was tested.
2. Protection profile for a specific domain (energy, road transportation and so on). Each protection profile can be associated to a specific level of assurance (dimension 1). Each domain has its own specific features and configuration environment, which must take in consideration for the security certification and deployment. For example, the security certification of a crypto-module for the road transportation may not be valid for the energy sector. This is why, the label must have a separate dimension to identify the domain.
3. To define how the certification was achieved: self-certification, third-party compliance assessment and so on how it is defined for IACS in section 3.3.1.

[26] https://ec.europa.eu/food/sites/food/files/safety/docs/labelling-nutrition_better-reg_competitiveness-consumer-info_en.pdf
[27] https://ec.europa.eu/food/sites/food/files/safety/docs/labelling-nutrition_better-reg_competitiveness-consumer-info_en.pdf
[28] "Consumer concerns about animal welfare and the impact on food choice". EU FAIR-CT36-3678. Dr Spencer Henson and Dr Gemma Harper, University of Reading.

The IACS scheme

The ICCF proposes (Thales, 2016) four possible approaches to certification in the form of four "schemes" named IACS Cybersecurity Certification Schemes (ICCS). The following diagram recapitulates these four schemes.

Definitions follow and the labels proposed for marking certified products, i.e. those that passed the evaluations with success, are presented in regard of each scheme. These graphic marks are only indicative and will need to be further validated and elaborated during the second phase of this feasibility study (to take place in 2017).



Example: Mark "ITC certified quality"[29]ITC has been providing professional services in the field of testing and certification for more than 15 years. The project of the new "ITC certified quality" mark is intended for producers and distributors that seek careful assessment of products and confirmation of their above standard properties by an independent accredited body. **Unlike common certification, the product quality and safety information reach directly the final consumer through this mark.** Continuous supervision of the product quality and safety throughout its sale provides a high degree of assurance that the product will keep its declared standard verified by the certificate. The objectives are:

- Providing information about higher level of product safety and quality to distributors and consumers;
- Marketing support of quality products on the expense of products meeting only the minimum legislative requirements;
- Visible information about successful product certification, which assessed conformity to the specified legislative and technical requirements.
- Guarantee of continuous safety and quality compliance of the products provided with ITC mark;

[29] http://www.itczlin.cz/en/certified-quality

- Support of communication between clients and suppliers in the field of competitive products with high standard of safety and quality.

- The mark is determined for placing on products, documents and in publications, where it shows conformity of the product properties to above standard requirements specified by a standard, specification or any other suitable document, while meeting all legislative requirements.

Industry associations have, however, expressed reservations on the applicability of a labelling approach in the domain of ICT security certification (see for instance: ZVEI, 2017; DIGITALEUROPE, 2017). Cyber security will be used across the board in the Internet of Things and will serve as a distinguishing feature. An excessively narrow and static certification and labelling system may actually restrict the range of technical security solutions, particularly if it does not only outlines the requirements but also the implementation measures. This prevents innovation and market diversity. In particular, the differences from energy efficiency labelling and security certification are stressed. The state of science and research clearly shows that cyber security cannot be measured using conventional means. The conditions change too quickly and, as a consequence, the requirements may no longer be met in the time between certification and product launches. In the case of cyber security, in/for the product this is equally dependent on the technical properties, processes, user competence, deployment environment and implementation within the overall system. This clearly distinguishes cyber security from energy efficiency, which is illustratively printed on relevant products in the form of a traffic-light label. Because of the existing design and methodical discrepancy, this approach cannot be applied to cyber security. Support the transfer of international security industry standards: in the area of cyber security, the international security standard IEC 62443 is concerned with requirements for technical aspects of products (through the security level) and process-organisational aspects of the company (through the maturity level), and combines these into an holistic approach (through the protection level). In particular, the approach discussed above is taken into account by means of process observation instead of product certification. This procedure has gained acceptance and agreement for numerous industrial applications across different sectors. It may therefore be possible to transfer the approach to other sectors. DIGITALEUROPE believes any future actions by policy makers in the field of cybersecurity certification and labelling should take into consideration the following criteria:

- **Cybersecurity is a global issue and requires international solutions** - Cyber-attacks know no borders and therefore standards and related certifications play a significant role in creating a safer ICT environment. In the last few years, various and not fully coordinated certification initiatives are increasing the problem of fragmentation across Europe. The lack of an EU wide approach for ICT Certification means that different Member States are developing their own National Certification Scheme with different cybersecurity requirements, different level of tests and different level of assurance. Germany, France and UK have developed their own National Certification Scheme and each certification scheme is not mutually recognised by each other, creating additional market barrier. Other emerging initiatives come for example from Italy, Netherlands, Norway and Sweden. In Italy, based on the national decree DPCM 17 February 2017[30], it should be established a National evaluation and certification centre for verifying security and non-vulnerability conditions for products, devices and systems for networks, services and critical infrastructures. In Netherlands, the BSPA scheme is in pilot phase since 2015. *Norway* and *Sweden* have the intention to develop a protection profile based on Common Criteria. The different international and national approaches will be widely argued within the chapter 3.
  Any future EU activity in the field of cybersecurity standards, certifications and labels should take into due account the existing international ecosystem.
- **Flexible cybersecurity solutions** - To stay ahead of malicious attackers, industry must be able to develop and deploy new tools to protect our digital economy against changing cyber risks.

[30] Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, Gazzetta Ufficiale n. 87 del 13 aprile 2017 (Italian Prime Minister Decree, 17/02/2017, Directive on guidelines for national cyber protection and cybersecurity, Official Bullettin n.87, 13/04/2017)

Policymakers should make sure that any regulatory action in this field keeps abreast of state-of-the-art technology.

- **One size does not fit all in a complex cyberspace** - A new EU certification framework would not be able to cover a broad set of products/services as the nature of products and services as well as the magnitude of cybersecurity risk vary significantly.
- **Promoting consumer protection and innovation** - Component/product labelling could potentially lead to a false sense of security for end-users in the consumer market. Benchmarking cybersecurity practices, on the contrary, would allow both consumers and organisations to compare situations and form an idea of the cybersecurity state-of-the-art.
- **Certification and competitiveness** - Regulated certifications and security **evaluation involve considerable costs**. It is important that they remain voluntary and that a range of agile self-certification mechanisms are allowed to flourish according to the existing market. It is important **not to erect market barriers to smaller companies** by mandating high entry costs.

A contrast is often made to energy-efficiency labelling, but there are some important differences. Firstly, while energy use can be subject to fairly homogenous or limited measurements (e.g. KwH), security is not as consistent. What matters for one set of products does not necessarily matter for others. Secondly, and most importantly, security is not static. While a product may achieve a top rating at the moment it is put on the market, six months down the line the fast paced changes of the threat landscape may render it insecure. **Labelling, therefore, creates the very real risk of a false sense of security.**

The Labelling Impact

Within these paragraphs, some examples and studies on labelling, experienced in different industry sectors, will be shown. Although there are no objective measurement methods to compare two labels of different sectors, the aim of this section is to provide some elements of comparison and possible scenarios or impacts in case of adoption of an EU labelling Scheme for ICT Products.

Energy Labels

The "Study on the impact of the energy label – and potential changes to it – on consumer understanding and on purchase decisions"[31] explores consumers' understanding of the individual elements of the energy label and how the label design influences consumer choice. The study has been conducted in two phases:

- *Phase I* is a targeted literature review and an online behavioral experiment.
  - The objective of the review is to investigate existing knowledge on consumer behavior and understanding under alternative energy labelling frames.
  - The online experiment tested choice and understanding in an incentivized experiment and understanding test. The behavioral experiment is conducted in seven Member States.
- *Phase II* is a bricks-and-mortar experiment that is carried out at retail stores and centralized locations in four Member States.

The findings from both phases of the study combined, along with literature review, indicate the following in terms of consumer choice and understanding under the label frames tested.

Consumer understanding

- Energy efficiency scales that include letters as opposed to numbers are generally better understood by consumers.
- Consumer understanding of the energy efficiency scale with A+++ to D and A to G scale is similar between the two.
- The differences in understanding between the alternate numeric scales tested is mixed and provides no clear indication as to which numeric scale may be best understood by consumers in the market.

31

https://ec.europa.eu/energy/sites/ener/files/documents/Impact%20of%20energy%20labels%20on%20consumer%20behaviour.pdf

- One third of consumers understand the meaning of the open ended scale. This increases to just under two thirds when consumers are provided with prior information in regard to the meaning of the open ended scale.
- Over half of consumers understand that the benchmark marker indicates best available technology.
- The provision of prior information can improve consumer understanding of the energy efficiency scale. As previously stated, this is particularly the case with the open-ended scale where understanding improves substantially if a prior explanation is provided.
- The majority of consumers were able to correctly identify the product that was least costly to use indicating that they understand the meaning of kWh/annum. Similarly, consumers that understand the meaning of kWh/annum are more likely to correctly identify the product that is least costly to run.
- Consumers are less likely to identify the least costly product to use when the product is affixed with a numeric or reverse numeric label compared to the A+++ to D and alphabetic label.
- Understanding the energy efficiency scale is an important determinate in whether the consumers choose the most energy efficient product; and, understanding is generally higher for the A+++ to D and alphabetic scale than the numeric scales.

Consumer choice

- There is some evidence that label frames which use alphabetic scales lead to more consumers choosing energy efficient products compared numeric scales.
- There is some evidence that labels with an A to G scale lead to more consumers choosing energy efficient products compared to the A+++to D scales.
- The choice between one and another label design has a greater difference in impact on behaviour for consumers who consider energy efficiency of low importance in their purchasing decision, compared to consumers that consider energy efficiency as an important criterion in product choice.
- The choice of label design is of greater importance in influencing behaviour for products where energy efficiency is not of key importance to consumers when selecting a product.

Average additional amount that participants are willing to pay for a more energy efficient product

The study analyse the average additional amount that participants are willing to pay for a more efficient product and whether this varies depending on the energy label framing, as known as the average minimum premium. To explain this using an example, if a participant from Italy was faced with the following two options for a television:

- Price: €150 and Energy efficiency rating: C
- Price: €180 and Energy efficiency rating: B

If they choose the second option, this shows that they are prepared to pay at least a €30 premium for the more energy efficient option. However, this participant may have been willing to pay a much higher premium for a television with an energy efficient of 'B' rather than one with an energy efficiency rating of 'C'. However, this potentially higher price premium was not included in the set of choices within the experiment.

The figure below shows the average minimum amount that participants are willing to pay for a more energy efficient product across each of the different framings and for each product. Results are divided depending on the energy efficiency rating difference between the two products involved in the choice experiment decision. Given the energy efficiency combinations used in the choice experiment the energy efficiency rating difference is either 1, 2 or 3 levels. For example, if a participant in the alphabetic closed scale framing is faced with a decision of choosing between a product with an energy efficiency rating of 'B' and another of 'C', the energy efficiency rating difference is 1. Similarly, if they are faced with a choice between a 'B' rated product and a 'D' rated product, the energy efficiency rating difference is 2. Finally, if they are faced with a chose between a 'B' or an 'E' rated product, the energy efficiency rating difference is 3. It is possible to observe in the Figure below that participants are willing to pay a higher premium for products with a larger energy efficiency rating difference, in the majority of cases. For example, participants in the numeric closed scale with benchmark marker framing are willing to pay €2 more for a television that is two energy efficiency

ratings higher than the alternative product (Energy rating difference = 2) than they would pay for a television that is one energy efficiency rating higher than the alternative (Energy rating difference = 1).

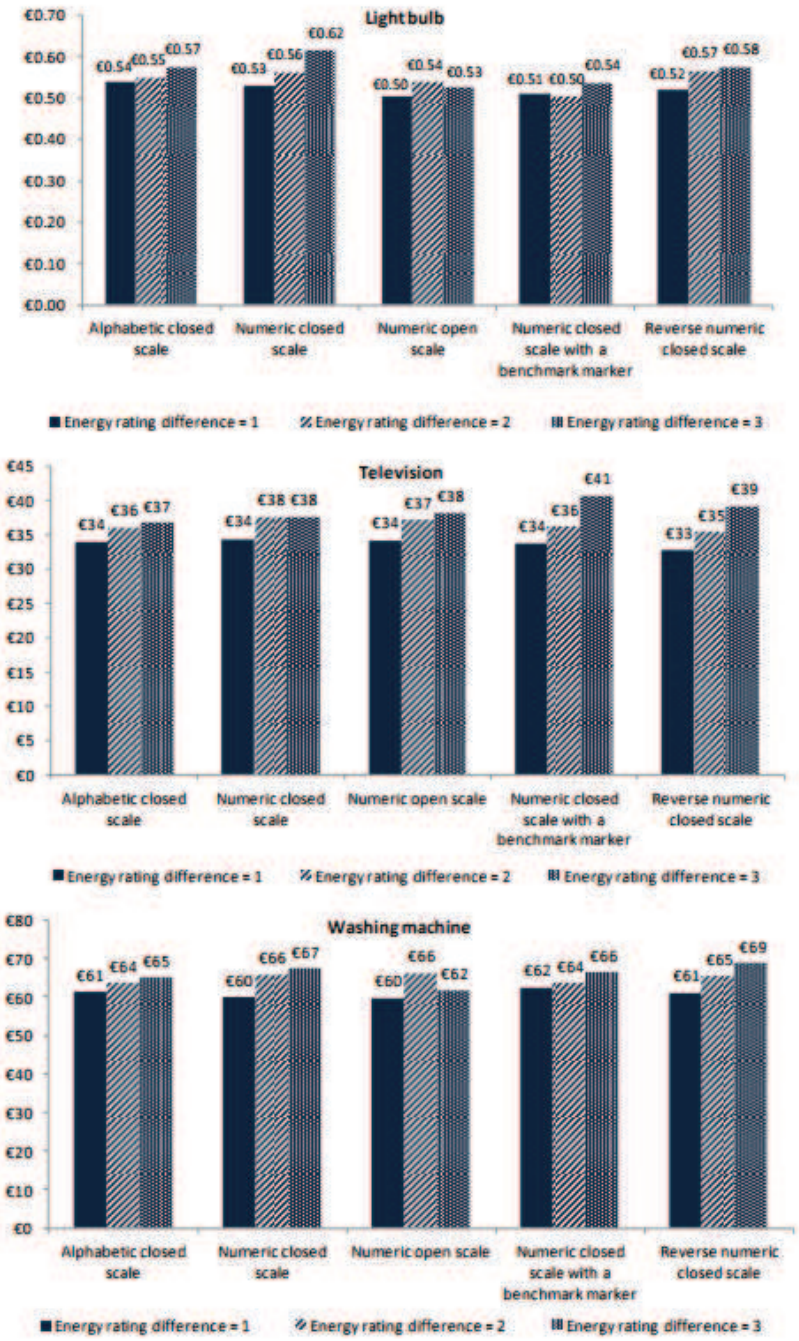


Figure - Average minimum premium participants are willing to pay for a more energy efficient

Another study entitled "Energy Labels: Formats and Impact on Consumption Behavior"[32] investigates the moderating role of energy labels on the relationship between consumer predispositions (energy consciousness) and purchase of energy saving products.

[32] http://www.duplication.net.au/ANZMAC09/papers/ANZMAC2009-334.pdf

Symbolic labels are used to communicate product information (e.g., nutritional ingredients, product safety warnings, and product ecological footprint) to consumers to increase their knowledge in purchase decisions. Energy labels are one of the widely used symbolic labels. They are legally required by many governments and technically endorsed by authoritative third parties in many nations. Different product categories are included in the labelling schemes in different countries, but high energy consuming appliances such as refrigerators and air conditioners are commonly included. Placed on the front side of the machine, energy labels certify the energy efficiency level of the appliance. The aim of using energy labels, like other ecological labels, is to encourage manufacturers and consumers towards more environmentally positive actions (OECD, 2005).

Researchers suggest that attitudes that are more accessible from memory are more predictive of behaviour, influence what messages are attended to, and how those messages are processed, and are more stable across time (Alwitt and Berger, 1993; Fazio, Herr and Olney, 1984; Fazio, Powell and Williams, 1989). Consumers with high energy consciousness may buy energy inefficient models due to the inactivation of their environmental attitudes (Alwitt and Berger, 1993). Considerable amount of information is processed at the point of purchase, and energy consciousness may not be the operant attitude. **The energy rating label can serve as a reminding notice, raising the accessibility and relevance of consumer energy consciousness in ecological consumption.**

Evidence presented within the report "Impacts of the EU's Ecodesign and Energy/Tyre labelling legislation on third jurisdictions"[33], shows that **international cooperation on equipment energy efficiency standards and labelling has contributed to delivering much greater energy, economic and environmental savings than would have occurred otherwise.** Willingness to share programmatic experience, learn from and emulate the successes of other programmes is an essential component of the product policy achievements made so far and this has led to the rapid promulgation of equipment energy efficiency measures round the world.

As stated within the paper "Consumer Response to Energy Labels - Insights from Choice Experiments"[34], **markets for energy-efficient goods are commonly characterized by information asymmetries**. Buyers are often not aware of the fact that the good they are about to purchase is also an energy service with running costs such as costs for electricity (Wilkenfeld et al., 1998). In addition, even those buyers who possess information about the existence of such costs are often not able to identify the level of energy efficiency of a good before their purchase decision. The energy consumption is therefore commonly an unobservable, or credence, characteristic; such characteristics can commonly lead to negative externalities of asymmetric information (e.g., Akerlof, 1970). In his seminal article on the market for lemons, Akerlof (1970) shows how the presence of information asymmetries can lead to market failure and adverse selection, and discusses signaling and screening as ways to overcome those challenges. One method of signaling that has received increasing attention from academics, policy makers and industry professionals is environmental or eco-labelling (De Boer, 2003; Pedersen and Neergaard, 2006; Rubik et al., 2007; Thøgersen, 2000**).**

Eco-Labels

Third party certified eco-labeling schemes are increasingly used worldwide as a means to overcome such information asymmetries and to increase trust in the validity of the environmental information. By providing information on the environmental performance of products, eco-labels can guide consumers towards more environmentally friendly purchasing behaviour (Grankvist and Biel, 2007). When consumer's see a third-party certification is displayed or visible on a product, customers believe that specific standards have been met because an outside organization has verified findings through an audit or a rigorous testing process[35]. Furthermore, such labels help manufacturers to gain a competitive advantage by producing environmentally friendly products (Thøgersen, 2000). Eco-labeling programs for promoting energy efficiency have gained particular importance for stimulating the sales of energy efficient electrical appliances and buildings worldwide. Energy labels can be used to provide information to consumers in order to enable them to compare the energy efficiency of a good on an equitable basis (Mahlia et al., 2002). **Labels can reduce uncertainty and**

[33] http://www.ecofys.com/files/files/ec-2014-impacts-ecodesign-energy-labelling-on-third-jurisdictions.pdf
[34] https://www1.unisg.ch/www/edis.nsf/SysLkpByIdentifier/4020/$FILE/dis4020.pdf
[35] https://www.uschamberfoundation.org/blog/post/certification-can-help-boost-consumer-trust/31481

overcome information asymmetry, but the optimal design of energy labels is a critical success factor and might even hinder energy labels' effectiveness when not carefully designed.

Eco-labeling could bring to a number of major benefits[36]:

1. **Informing consumer choice**: Eco-labeling is an effective way of informing customers about the environmental impacts of selected products, and the choices they can make. It empowers people to discriminate between products that are harmful to the environment and those more compatible with environmental objectives. An eco-label makes the customer more aware of the benefits of certain products, for example, recycled paper or toxic-free cleaning agents. It also promotes energy efficiency, waste minimization and product stewardship.
2. **Promoting economic efficiency**: Eco-labeling is generally cheaper than regulatory controls. By empowering customers and manufacturers to make environmentally supportive decisions, the need for regulation is kept to a minimum. This is beneficial to both government and industry.
3. **Stimulating market development**: When customers choose eco-labeled products, they have a direct impact on supply and demand in the marketplace. This is a signal which guides the market towards greater environmental awareness.
4. **Encouraging continuous improvement**: A dynamic market for eco-labeled products encourages a corporate commitment to continuous environmental improvement. Customers can expect to see the environmental impacts of products decline over time.
5. **Promoting certification**: An environmental certification program is a seal of approval which shows that a product meets a certain eco-label standard. It provides customers with visible evidence of the product's desirability from an environmental perspective. Certification therefore has an educational role for customers, and promotes competition among manufacturers. Since certified products have a prominent logo to help inform customer choices, the product stands out more readily on store shelves. Coveting the logo may induce manufacturers to re-engineer products so that they are less harmful to the environment.
6. **Assisting in monitoring**: Another benefit of an official eco-labeling program is that environmental claims can be more easily monitored. Competitors and customers are in a better position to judge the validity of a claim, and will have an incentive to do so should a claim appear dubious.

Food Labels

Firms typically have more information about the quality of their products than do consumers, creating a situation of asymmetric information[37]. It is prohibitively costly for most consumers to acquire nutritional information independently of firms. Firms can use this information to signal their quality and to receive quality premiums. However, firms that sell less nutritious products prefer to omit nutritional information. In this market setting, firms may not have an incentive to fully reveal their product quality, may try to highlight certain attributes in their advertising claims while shrouding others (Gabaix & Laibson 2006), or may provide information in a less salient fashion (Chetty et al. 2007). Mandatory nutritional labeling can fill this void of information provision by correcting asymmetric information and transforming an experience-good or a credence-good characteristic into search-good characteristics (Caswell & Mojduszka 1996). Golan et al. (2000) argue that the effectiveness of food labeling depends on firms' incentives for information provision, government information requirements, and the role of third-party entities in standardizing and certifying the accuracy of the information.

According to the survey conducted within the study "Labeling Policy for Genetically Modified and Organic Food: Impact on Consumer Choice"[38], more than half of participants (68.3%) expressed that they prefer to purchase foods with a non-GMO label versus foods without a non-GMO label. Furthermore, a majority of participants (87.8%) would like to see more labeling that distinguishes non-GMO and organic from GMO products. However, a small number of participants (24.4%) report that GMO food labeling impacts their purchasing decisions all the time, while approximately half of participants (51.2%) reported that GMO labeling affects their purchasing decisions only sometimes. Combined, 75.6% of participants allow GMO

[36] https://www.iisd.org/business/markets/eco_label_benefits.aspx
[37] http://kiesel.ucdavis.edu/AR%20KieselMcCluskeyvillasBoas.pdf
[38] http://www.fasebj.org/content/31/1_Supplement/640.32.short

labeling to influence their purchasing decisions. Those who believe organic foods have a *beneficial* impact on the environment reported that their views impact their purchasing decisions more frequently than those who were unsure of their effects.

Many consumers actively seek information about products that have qualities that serve their health needs and are consistent with their values[39]. As a result of these varied interests, food labels are increasingly being used to provide consumers with information about the environmental, technical and socioeconomic conditions under which the products were produced, as well as the health and safety aspects of food products. The growing consumer and industry interest in food labels presents challenges for government authorities, which **must ensure that the information that appears on food packages is useful, credible and presented clearly, so that it does not mislead the consumer.** With the increase in global trade in food, there is a need to harmonize food labelling so that product information is easily understood and is relevant to consumers in different markets.

As discussed within the paper "Is Organic Labelling Enough? Information Disclosure as Policy Instrument to Empower Consumer Choices"[40], **consumers are generally not satisfied with the availability of information that can guide their purchase decision**, and arguably, they are especially in a disadvantaged position to judge the potential compromises that the organic certification system creates. Information asymmetry, the gap of information with regard to the quality of organic products between consumers and producers, are expressly severe because of the nature of the products. In making choices for products, consumer typically relies on the dominant quality attributes, namely search, experience, credence and Potemkin attributes. A search attribute, such as freshness or appearance, is known before the purchase and consumers have the ability to examine it. Experience attributes, such as taste, are known after the consumption of the product. Credence attributes, such as nutrition or contamination, are difficult to be observed by consumers, but they can rely on third parties for quality assurance.

Recent expansion of organic food market has also been seen as the results of heightened awareness of the impact of food systems on environment. Such consumers are willing to pay a price premium for the additional benefits consuming the organic products. However, these values are not attributes that can be directly observed by consumers. Instead, **they rely on various information cues on the label when evaluating products under uncertainty. Labels or organic claims are widely used to transmit important quality information to consumers.** Organic labeling has been observed to be associated with a higher level of perceived healthfulness, hedonism, environmental friendliness and food safety. Since organic eggs are credence and Potemkin products, labels bearing organic certification elicit certain level of confidence of the values acquired through consuming organic egg. Not all organic labels, however, elicit the same level of trust. **In general, a third-party certification schedule is considered to be more trustworthy than producers' or retailers' private labelling scheme[41].** Label agency makes a difference to consumers' perception and willingness to pay. For example, in Switzerland, organic consumers were willing to pay a higher premiums for products with the Bio Suisse's label, a label backed by the farmers' umbrella organization, compared to products with other organic label. Consumers in Denmark and Czech Republic are willing to pay the highest price premium for governmental logo. The reputation and brand image of the label agency lend creditability to the label, and enhance the level of consumer trust. Although consumers are not willing to automatically assume fidelity of quality assurance behind of every label, they may place greater level of trust over the logos backed by ethical practices and stringent legal requirements. In the US, USDA organic has been an established logo with high level of consumer awareness and positive perception of the certification scheme behind it, consumers are responding to USDA organic milk more positively then generic organic labels.

It is important to remark that the perception of overall quality depends on both the consumer's awareness of the label and the label's subsequent ability to generate positive descriptive and inferential beliefs. Label

[39] http://www.fao.org/docrep/018/i0576e/i0576e00.pdf
[40] http://hl-128-171-57-22.library.manoa.hawaii.edu/bitstream/10125/41482/1/paper0333.pdf
[41] S. Eden, "Business, trust and environmental information: Perceptions from consumers and retailers," Business Strategy and the Environment, vol. 3, no. 4, pp. 1-8, 1994.

equity thus enhanced purchasing intention.[42] The impact on overall quality and purchase intention only emerged, for example, when the unrecognized PGI (Protected Geographical Indication) label was explained to consumers, thus highlighting the importance of building awareness of a values-based label. When it was explained, the values-based label was shown to operate as an effective market signal that generated both descriptive and inferential beliefs in relation to the products bearing the label. **These beliefs in turn explained consumers' perception of overall quality and influenced purchasing intention. Finally, consumers – individually and collectively – will be better served by labelling schemes that incorporate an understanding of their perspective and thus reduce misinformation.**[43]

The study "Consumer market Study on the functioning of voluntary food labelling schemes for consumers in the European Union"[44] has identified a large number of food labelling schemes across the EU Member States, Iceland and Norway but with important country variations. The study identified Spain, Germany, Italy and Portugal as the countries with the highest number of schemes while Romania, Cyprus and Malta were found to have a very limited number of food labelling schemes.

Increasing transparency and minimising consumer confusion seem to be the key drivers for schemes to follow the guidelines while lack of awareness, administrative burden and cost of compliance were identified as key obstacles for compliance. The guideline criteria most often met by food labelling schemes that were identified in the websweep were provision of contact information and/or feedback mechanisms on scheme websites for which 100% of schemes met this criterion. Clarity and transparency of scheme requirements and claims made was also met by a large number of food labelling schemes. Here we observe that between **91% and 82% of schemes clearly state their objectives**; between 79% and 73% have claims and requirements which are clearly linked to their stated objectives, and similarly the scope of the scheme in regard to the products and process it covers are clear. However, when seeking more detailed information on scheme requirements and specifications this is not always available for free on the website. Only 59% of schemes met this criterion in the websweep index. Further, when these specifications are available they can often be difficult to understand from the point of view of a consumer. An important recommendation would be to encourage schemes to provide information on their websites about their requirements, their specifications and their membership fees, and fees for certification, in a form that is easy to understand for all relevant actors, including consumers. This would help improve compliance of schemes against the 2010 Commission guidelines. In addition, encouraging schemes to provide information on the evidence used to make any claims about scheme requirements easily available on their websites, (again) in a form that is easy to understand for all relevant actors, including consumers is recommended.

To improve transparency, a recommendation would be to encourage schemes to clearly state whether, where and to what extent their specifications go beyond the relevant legal requirements. Provisions for enabling and promoting the participation of small scale producers could also be explored as this was met by a low proportion (35%) of schemes that responded to the scheme operator survey. Further, clearly stating that the scheme is public or private and whether it is certified or self-declared would be useful for consumers as this information is often hard to find on scheme websites. While not specifically addressed in the assessment of schemes, the provision of a web address on the scheme label affixed to the product may also help consumers as they could then easily find additional information on the scheme if they want. Methods to minimize the administrative burden and costs for producers and scheme operators in complying with the guidelines could also be explored.

Overall, results of the consumer survey show that consumers are aware of food labelling schemes, **they buy products affiliated to food labelling schemes, believe there are benefits to these products and to some extent are willing to pay a premium price for labelled products.** Providing consumers with more and better accessible information on the different types of labelling schemes and the meaning of

[42] Third party labeling and the consumer decision process, HEC - https://basepub.dauphine.fr/bitstream/handle/123456789/12755/CR891Flarceneux.pdf?sequence=1&isAllowed=y

[43] Third party labeling and the consumer decision process, HEC - https://basepub.dauphine.fr/bitstream/handle/123456789/12755/CR891Flarceneux.pdf?sequence=1&isAllowed=y

[44] http://ec.europa.eu/consumers/consumer_evidence/market_studies/food_labelling/docs/final_report_food_labelling_scheme_full_en.pdf

the most common ones, as well as educating them through, for example, an information campaign would be a good way of reducing this risk. Improved information provision, information campaigns or educational initiatives could help consumers distinguish between the different types of schemes, in particular between certified and self-declared or between public and private. This could also increase their knowledge of regulations for schemes and help them make more informed choice. A clear indication on the scheme label about whether the scheme is public or private (where it is possible to qualify clearly), certified or self-declared could also be an easy way of increasing scheme transparency without adding a lot of text on the label.

To improve understanding and access to information about food labelling schemes for all interested parties, a model scheme could include the following key elements.

- Clear statement of the scheme name and website address on the label affixed to the product.
- Website with scheme contact details.
- Statement of the scheme objectives and the types of products and process it covers.
- Clear statement of the organisations or bodies that own and manage the scheme, including their contact information.
- If the scheme is endorsed by third parties, the names and contact details of the parties should be provided.
- Clear statement of whether the scheme is public or private, and certified or self-declared.
- If a certified scheme, the name of the certification body should be provided and clear and transparent information on the key certification processes and requirements for nontechnical readers should be available.
- If the scheme covers areas where there are specific legal requirements, such as organic farming or animal welfare this should be clearly stated, and the extent to which the scheme goes beyond the relevant legal requirements should be understandable to nontechnical audiences.
- Provision of clear guidance on how to meet the scheme main requirements for parties interested in joining the scheme. Contact details, question forms or other mechanisms to access assistance with understanding and meeting the requirements for membership should be available.

Healthcare Labels

A pre-requisite for a market to be able to function properly is transparency on prices and quality so that the end user can inform himself fully and correctly before making a purchasing decision. In the case of medical devices, between demanders and providers there is an 'unbalanced' spread of knowledge of the market. **Manufacturers have the benefit of having much more information than users**: they know the functioning (and limitations) of their product, know the cost structure, etc. The demand side of the market, on the other hand (specialists, nurses, buyers, management/board), is very fragmented, both in terms of knowledge of the (sometimes very specialized) use of the devices and also knowledge about what other (substitutable) devices are available. The users of medical devices are therefore strongly dependent on the knowledge, expertise and information provided by manufacturers (for example with specialised operations, with the use of equipment, etc.). The fact that the users share little or no information between themselves (price, quality, etc.) is also a factor, with the result that the problem of information remains[45].

Transparency and better information are crucial to give more autonomy to patients and health professionals and enable them to take decisions with full knowledge of the facts, in order to give a solid base to regulatory decision-making process and to make sure the latter is trust-worthy. To do so, it is essential that Eudamed (European Database on Medical Devices) electronic systems related to existing devices, concerned economic operators and certificates allow public opinion to be well informed about devices circulating on the market. The clinical investigation electronic system should serve as a tool for cooperation between Member States and enable promoters to deliberately introduce a unique application process for several Member-States, and in this case to report serious incidents. Otherwise, manufacturers should convey the main safety and performance characteristics and the clinical evaluation results for high-risk medical devices via a public

[45] Sector Study Medical Devices Study of the structure and functioning of the market for medical devices

document The well-functioning of notified bodies is also essential to guarantee a high level of health and safety protection, as well as citizen trust in the system.[46]

Medical device labeling assists patients or their lay caregivers in understanding the device; its operation, care, and maintenance; the way it interacts with the body to accomplish its purpose; its place and purpose in the patient care regimen; and any safety or disposal issues. Medical device labeling is essential to assure safe and effective use of many, but not all, devices. It informs patients or their lay caregivers about proper use, risks, and benefits of the device in language they can understand. Adequate directions for operating the devices are needed to make devices safe and effective. For example, as more patients use complex medical devices at home, medical device patient labeling becomes necessary to better communicate to the lay person how to operate the device. Devices that might have labeling that would include instructions for use would be those the patient or lay caregiver have to set up, operate, clean, etc. They might include such devices as suction equipment, intravenous infusion pumps, physical therapy equipment, or transdermal electrical nerve stimulation (TENS) devices. Devices that would have labelling consisting primarily or completely of risk/benefit information might be implants that have no external patient interface, once they are implanted, or prescription, diagnostic or therapeutic devices that the patient is actively involved in choosing (e.g., laser eye surgery, lithotripsy, intraocular lenses)[47].

2.4. The problem of Fragmentation

One of the key drivers of increasing cybersecurity risk is that the European cybersecurity industry is fragmented for historical reasons and remains fragmented[48]. Historically, firms grew in this sector as a result of governmental demand and remain largely dependent on this very domestic revenue stream, which reduce cross-border purchases and the incentives for firms to grow outside their national market. The EU cybersecurity market is dominated by a small group of global vendors, competing with a high number of smaller European suppliers that remain regional or national players (IDC, 2009)[49]. The EU suppliers, while showing a positive dynamism, remain mostly national or regional players. The presence of third country suppliers drives the competitiveness and innovation in the market (Optimity Advisors, 2015)[50].

Box 2 Key evidence on the cybersecurity market

- The **global size** of the privacy and cybersecurity (PAC) market vary from **EUR 47bn to EUR 76bn (2014)** and the industry is expected to**grow by around 7–8% per annum over the next 5–6 years**.
- The total EU market (including non-EU countries) is worth **26% of the global market:** EUR 12bn–EUR 19bn (2014) and is considered the second largest cybersecurity market behind North America, which controls a large segment (43%) of the global market;
- Governance is fragmented at EU level due to the fact that **security in general, and cybersecurity in particular** – especially as a component of critical infrastructures and national assets protection – **remains a national responsibility within the EU treaties;**
- Governance fragmentation is visible also at Member States level where the arrangements between national civilian and military CERTs fragmented;
- Another barrier for the emergence of a more cooperative European industry is the presence of entrenche **third-country companies** that tend to be preferred to EU domestic companies with similar or better solutions, due to **reputation and maturity of ì third-country suppliers;**

[46] Françoise Grossetete, Revise the Rules Relating to MD Advertising to Ensure the Right Information and Optimal Patients Protection, http://www.ealth.org/images/speak-about-us/european-files-magazine-march-2013.pdf
[47] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3255430/
[48] European Commission, SWD(2016) 216 final, Communication: Strenghtening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry
[49] IDC. (2009). The European Network and Information Security Market Brussels: Report delivered by IDC for the European Commission.
[50] Optimity Advisors. (2015). Study on Synergies between the civilian and the defence cybersecurity markets Brussels: Report delivered by Optimity Advisors for the European Commission.

- Summing up **EU weaknesses** that could jeopardise innovation and synergies in the cyber domain, the key factors are **fragmentation in governance**, **lack of consistency in the EU data collection** and data analysis and lack of **end-user knowledge** of the cybersecurity market. There is also a shortage of EU companies that can offer the **whole value-chain of cybersecurity solutions**, and that are able to absorb the talent on the market, and there is l**imited entrepreneurial activity** when compared with the US.

Source: Optimity Advisors (2015)

This situation results in the the difficulty to compete on the European and global levels and to grow (***problem***), which often leads to mergers and acquisitions of Europe's SMEs by non-European actors, weakening the European sector and leaving Europe also more vulnerable and technologically dependent on others (***direct effect***); furthermore this also cause the risk of know-how outflow as the European cybersecurity firms cannot absorb the newly skilled professionals produced by European academic institutions who end up working for foreign global companies . Second, there is the European cybersecurity ecosystem is characterised by low dialogue and coordination (***driver***), which result (***problem***) in the lack of 'a well-functioning mechanism ensuring trustworthiness & readability of cybersecurity products and solutions' (European Commission, 2026b, p. 10); this further creates barrier to both cybersecurity and other cross-border activities (***direct effect***). Finally, leaving aside the cyber-security sector itself, there is a lack of expertise both in ICT producing firms and in ICT using firms as regard cybersecurity (***driver***), which contributes to low demand-side awareness (***problem***); the latter further reinforce the cross-border barriers (**direct effect**). Taken altogether these drivers, problems, and direct effects, contribute to the ***indirect effect*** of missing the growth opportunities that would derive from a more dynamic and competitive European cybersecurity industry.

The certification landscape. First, various and not fully coordinated certification initiatives (***driver***) increase fragmentantion in the domain of certification (***problem***), resulting in duplication of efforts and waste of resources (***direct effect***). Second, the sectorial fragmentation of initiatives (***driver***) increase fragmentation in the ICT market for lack of product comparability with respect to cybersecurity (***problem***), resulting in lower competition in the ICT sector (***direct effect***). Third, lack of expertise on the users' side (***driver***), cause an insufficient demand side awareness (***problem***), and combined with the other problems leads to an increase rather than a decrease of the information asymmetry (***direct effect***). The earlier cited literature on energy labels shows, in fact, that lack of credibility or understanding and proliferation of different and not comparable labels create confusions and negative reactions on the side of users. The fragmentation of certifications schemes (and possibly of associated label) would have the same effects and induce more rather than less information asymmetry also in relations to cognitive phenomena such as heuristics and biases. Taken altogether these drivers, problems, and direct effects, contribute to the ***indirect effect*** of missing the growth opportunities that would derive from boosting cybersecure European ICT products in the global market. The certification fragmentation is further discussed in the next sections of this document.

Common end effects. The problems and effects of the ecosystem as whole combined with, and compounded by, those of the certification landscape cause the end effects of: a) not reducing the net losses from cyber incidents for citizens, businesses, and public administrations; b) creating hindrances to the full implementation of the DSM strategy; c) foregoing several sources of potential growth for European economies.

3. The ICT security certification landscape

Certification can be defined as: '*a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system*' (NIST, 2010).

The certification of products generally requires the following four phases:

1) Application. A company applies a product for evaluation to obtain a certification;
2) An evaluation is performed to obtain certification. The evaluation can be mostly done in three ways:
    a) The evaluation can be done internally to support self-certification;
    b) The evaluation can be performed by a testing company, which is legally belonging to the product company;
    c) It can be third party certification where the company asks a third party company to perform the evaluation of its product;
3) In case of an internal company or a third party company evaluation, the evaluation company provides a decision on the evaluation.
4) Surveillance. It is a periodic check on the product to ensure that the certification is still valid or it requires a new certification.

In the following, we review international and emerging national schemes to highlight the main problems and challenges, and conclude with a qualitative analysis of the costs of benefits of no EU action as compared to a broadly conceived EU Intervention. The following sections have been drafted extracting information from various sources including the JRC report[51] (Baldini et al., 2017), a report (Enisa, 2014) and the proceedings of two workshops by Enisa (Enisa, 2016a, 2016b), two key reports delivered by Ecorys (2011) and ERNCIP (2014), documents from the French and German Certification Authorities (ANSSI, 2015; ANSSI & BSI, 2017), as well as the Communication and supporting SWD on Security Industrial Policy (European Commission, 2012a, 2012b). In addition, information has been retrieved from interviews with National Certification Authorities and from the websites of Certification Authorities and similar institutions, which are indicated in footnotes.

3.1 International schemes and other initiatives

Common Criteria (also known as ISO 15408)[52]. The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA). It is a framework in which computer system users can specify their security functional and assurance requirements, vendors can then implement and/or make claims about the security attributes of their products, and security Conformity Assessment Bodycan evaluate the products to determine if they actually meet the claims. It ensures that:

- Products can be evaluated by competent and independent Conformity Assessment Body so as to determine the fulfilment of particular security properties, to a certain extent or assurance;

- Supporting documents, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies;

- The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation;

[51] Baldini, G., Giannopoulos, G., & Lazari, A. (2017). Analysis and recommendations for a European certification and labelling framework for cybersecurity in Europe. JRC Science for Policy Report. Luxembourg: Publications Office of the European Union.
[52] https://www.commoncriteriaportal.org/

- These certificates are recognized by all the signatories of the CCRA.

The CC permits comparability between the results of independent security evaluations and is flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT products. It can be used in the smart grid to verify if a product meets the claims regarding the technical implementation of those security functions (Enisa, 2014). CC certified products provide assurance an a wide range of product categories from, databases, operating systems, accesso control systems, network devices, to Trusted platform modules, biometric systems and devices[53]. Namely, for certified products and Protecion Profiles are currently defined 15 categories (in fact, one of these ("Other devices and systems") capture s everything not included in the other 14 categories). A certified product/Protection Profile no longer recognised within CCRA is reported as "Archived" (Notice that, an official resolution, effective at June 1st, 2019, limits to 5 years the validity of recognition. Starting from that date, all certificates issued from 5 or more years will be archived.). In the next tables the current state is shown by official CCRA statistics showing, for the period 1999-2017, valid and archived certificates for products and protection profiles, per year, per scheme (country), and per assurance level (EAL).

2206 Certified Products by Category *

Category	Products	Archived
Access Control Devices and Systems	64	57
Biometric Systems and Devices	3	0
Boundary Protection Devices and Systems	77	124
Data Protection	60	75
Databases	33	51
Detection Devices and Systems	15	49
ICs, Smart Cards and Smart Card-Related Devices and Systems	1063	21
Key Management Systems	23	27
Mobility	26	3
Multi-Function Devices	137	165
Network and Network-Related Devices and Systems	235	188
Operating Systems	94	69
Other Devices and Systems	264	276
Products for Digital Signatures	92	7
Trusted Computing	20	0
Totals:	**2206**	**1112**
Grand Total:		**3318**

* A Certified Product may have multiple Categories associated with it.

[53] See also the certified product list (cpl) of CCRA portal at, www.commoncriteriaportal.org/products.

Certified Products by Assurance Level and Certification Date

EAL	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	Total
EAL1	0	0	0	0	0	0	1	1	6	3	1	0	1	10	2	2	4	3	2	36
EAL1+	1	0	0	0	0	0	0	0	17	0	2	11	2	0	1	2	1	0	0	37
EAL2	0	0	0	0	0	0	1	0	8	1	7	2	3	2	10	12	18	15	6	85
EAL2+	0	0	0	1	1	1	2	2	8	8	8	4	5	20	23	29	59	76	21	268
EAL3	0	0	0	0	0	0	0	0	10	4	1	9	5	13	11	12	9	2	3	79
EAL3+	0	0	0	0	0	2	1	1	37	10	12	12	12	28	20	23	17	18	2	195
EAL4	0	1	0	1	0	0	0	0	28	5	9	4	6	2	7	2	0	5	1	71
EAL4+	0	1	1	2	2	3	3	2	142	58	67	56	60	91	64	52	58	56	19	737
EAL5	0	0	0	0	0	0	0	0	6	3	2	0	1	0	0	0	0	3	0	15
EAL5+	0	0	0	0	0	0	3	0	50	27	31	43	35	28	56	53	44	69	30	469
EAL6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EAL6+	0	0	0	0	0	0	0	0	0	0	2	3	0	4	6	6	13	11	4	49
EAL7	0	0	0	0	0	0	0	0	0	0	1	0	0	0	4	0	0	0	0	5
EAL7+	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
Basic	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Medium	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
US Standard	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
None	0	0	0	0	0	0	0	0	0	0	0	0	0	1	4	10	41	67	36	159
Totals:	**1**	**2**	**1**	**4**	**3**	**6**	**11**	**6**	**312**	**119**	**143**	**145**	**130**	**199**	**208**	**203**	**264**	**325**	**124**	**2206**

Certified Products by Scheme and Assurance Level

Scheme	EAL1	EAL1+	EAL2	EAL2+	EAL3	EAL3+	EAL4	EAL4+	EAL5	EAL5+	EAL6	EAL6+	EAL7	EAL7+	B	M	S	N	Total
Australia	2	1	9	7	2	3	5	12	0	0	0	0	1	0	0	0	0	19	61
Canada	1	0	8	129	0	9	0	8	0	0	0	0	0	0	0	0	0	21	176
Germany	9	4	10	26	14	56	15	310	8	169	0	20	0	0	0	0	0	3	644
Spain	8	8	7	7	4	12	0	30	0	3	0	0	0	0	0	0	0	2	81
France	1	18	1	15	0	39	4	276	3	259	0	14	4	0	0	0	0	0	634
India	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	3
Italy	4	6	0	1	2	0	1	9	0	0	0	0	0	0	0	0	0	0	23
Japan	0	0	6	41	35	38	0	0	0	0	0	0	0	0	0	0	0	0	120
Republic of Korea	3	0	5	8	9	15	24	15	0	15	0	0	0	0	0	0	0	1	95
Malaysia	6	0	14	6	0	4	1	2	0	0	0	0	0	0	0	0	0	0	33
Netherlands	0	0	4	1	1	1	1	19	0	13	0	15	0	1	0	0	0	1	57
Norway	0	0	1	17	2	11	15	16	3	7	0	0	0	0	0	0	0	0	72
New Zealand	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sweden	1	0	9	2	5	4	5	4	1	0	0	0	0	0	0	0	0	1	32
Turkey	0	0	7	1	3	0	0	9	0	0	0	0	0	0	0	0	0	0	20
United Kingdom	0	0	3	7	1	3	0	26	0	3	0	0	0	0	0	0	0	2	45
United States	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	109	110
Totals:	**36**	**37**	**85**	**268**	**79**	**195**	**71**	**737**	**15**	**469**	**0**	**49**	**5**	**1**	**0**	**0**	**0**	**159**	**2206**

344 Protection Profiles by Category *

Category	PPs	Archived
Access Control Devices and Systems	10	7
Biometric Systems and Devices	7	5
Boundary Protection Devices and Systems	36	24
Data Protection	15	4
Databases	9	7
Detection Devices and Systems	17	17
ICs, Smart Cards and Smart Card-Related Devices and Systems	88	20
Key Management Systems	15	11
Mobility	7	4
Multi-Function Devices	4	3
Network and Network-Related Devices and Systems	35	22
Operating Systems	17	15
Other Devices and Systems	63	18
Products for Digital Signatures	21	2
Trusted Computing	9	4
Totals:	**353**	**163**
Grand Total:		**516**

* A Protection Profile may have multiple Categories associated with it.

Protection Profiles by Assurance Level and Certification Date

EAL	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	Total
EAL1	0	0	0	0	0	0	0	5	0	1	0	2	0	0	0	0	0	0	0	0	8
EAL1+	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	4
EAL2	1	1	1	3	1	0	0	5	3	0	1	0	1	2	1	0	1	4	1	0	26
EAL2+	1	0	2	1	2	0	0	1	7	12	2	0	6	0	1	0	2	4	1	2	44
EAL3	2	4	1	0	0	0	0	0	0	0	2	2	1	0	0	0	1	1	0	0	14
EAL3+	0	0	0	1	3	0	2	0	0	2	9	1	1	3	0	0	1	3	0	0	26
EAL4	0	0	2	1	1	0	0	1	0	1	2	1	0	4	1	0	0	0	1	0	15
EAL4+	0	8	1	11	7	7	0	3	3	5	9	14	15	4	5	4	4	7	10	4	121
EAL5	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
EAL5+	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
EAL6	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1
EAL6+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EAL7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EAL7+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Basic	0	0	0	0	0	0	0	2	7	2	0	1	0	0	0	0	0	0	0	0	12
Medium	0	0	0	1	0	1	1	1	4	15	1	2	0	0	0	0	0	0	0	0	26
US Standard	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
None	0	0	0	0	0	0	0	0	0	0	0	0	2	2	3	9	11	12	5	1	45
Totals:	**4**	**16**	**7**	**19**	**14**	**8**	**3**	**18**	**24**	**39**	**26**	**23**	**26**	**15**	**12**	**13**	**20**	**31**	**18**	**8**	**344**

Protection Profiles by Scheme and Assurance Level

Scheme	EAL1	EAL1+	EAL2	EAL2+	EAL3	EAL3+	EAL4	EAL4+	EAL5	EAL5+	EAL6	EAL6+	EAL7	EAL7+	B	M	S	N	Total
Australia	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Canada	0	1	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	1	4
Germany	6	0	2	9	3	7	3	59	0	0	0	0	0	0	0	0	0	0	89
Spain	2	0	2	1	2	0	4	0	0	0	0	0	0	0	0	0	0	0	11
France	0	1	0	8	0	11	0	34	1	1	0	0	0	0	0	0	0	6	62
India	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Italy	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Japan	0	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	5
Republic of Korea	0	1	0	0	0	0	2	5	0	0	0	0	0	0	0	0	0	0	8
Malaysia	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Netherlands	0	0	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	0	3
Norway	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
New Zealand	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sweden	0	0	0	3	0	0	1	0	0	0	0	0	0	0	0	0	0	0	4
Turkey	0	0	6	2	0	0	0	2	0	0	0	0	0	0	0	0	0	0	10
United Kingdom	0	0	1	0	5	0	3	3	0	0	0	0	0	0	0	0	0	0	12
United States	0	1	15	21	2	7	2	11	0	0	1	0	0	0	12	26	0	38	136
Totals:	**8**	**4**	**26**	**44**	**14**	**26**	**15**	**121**	**1**	**1**	**1**	**0**	**0**	**0**	**12**	**26**	**0**	**45**	**344**

The CCRA framework, within the definition of Collaborative Protection Profiles (cPP), introduces the concepts of "technical community (TC)" and Essential security Requirements. Two or more Schemes can declare their interest in setting up a TC in charge of facing a specific issue in a specific Technical Domain (TD). The TC will produce an ESR in order to take into account requirements as much as possibile shared with all the Schemes in the CCRA and then will be define the cPP and the relative supporting documents to be used to evaluate a specific product in the TD against the cPP.

CCRA Schemes can chose to

1) [Invonved Schemes] - contribute to the TC from the beginning of the project (interested nations): this contribution can be interpreted as the willing of the Scheme to evaluate the results of the community and eventually to propose the solution for a national procurement.

2) [Position Statement] - officially communicate a "position statement" in support of the ESR, meaning that the ESR is a correct and shared instantiation of the requirements in order to solve the issues defined for the setting up of the TD. A correct definition of a cPP in this area can be promoted in a national procurement.

3) [Endorsement] - officially communicate an endorsement of the cPP that means that the cPP as has been defined by the TC (and relative supporting documents) can be promoted for a national procurement.

The following table shows the EU schemes involved in the CCRA Technical Domains ant the position statements to the relative ESR (for all CCRA nations)

Technical Domain

	Position Statement		**EU Involved Schemes**
	EU Nations	**Non EU nations**	
USB Protable Storage devices	**DK,SE,FI,UK,GE**	**AU-NZ,JP,USA,**	**SE,UK,GE, (TK), NL**
FDE	**UK, NO,**	**USA, AU-NZ, CA**	**SE,UK, (TK), NO**
Network Devices	**UK**	**USA, AU-NZ, CA**	**UK, (TK), NO**
Application Software			**SE, (TK), UK**
Dedicated Security Component			**UK, SE, NL**
Biometric Security			**SP, (TK)**

The following table shows the Endorsment statements of CCRA Schemes to the cPP defined in a specific technical domain

	Endorsment	
Collaborative Protection Profiles	**EU Schemes**	**Non EU schemes**
Stateful Traffic Filter Firewalls	**UK**	**US, CA, AU-NZ**
FDE- Encryption Engine v.2.0		**US**
FDE - Authorizaion Acquisition v.2.0		**US**
FDE- Encryption Engine v.1.0	**UK**	**US, CA, AU-NZ**
FDE - Authorizaion Acquisition v.1.0	**UK**	**US, CA, AU-NZ**
Network Devices V.2.0	**US**	
Network Devices V.1.0	**UK**	**US, CA, AU-NZ**

SOG-IS. SOG-IS is the main certification mechanism existing at European level. However, it only includes 12 Member States plus Norway and has developed only a few protection profiles regarding digital products (such as digital tachograph and smart cards)[54]. Moreover, Member States often request certification as a pre-condition to be admitted to national public procurement tenders. Additional national certification frameworks and schemes are expected to develop in the coming years. Here are presented some statistics for some producing members of SOGIS agreement. Differences between the numbers of recognized certificates issued by the scheme are represented only where present.

Next table reports some CC certification statistics for the Italian Common Criteria Scheme (OCSI).

		CCRA & SOGIS					
Product type (CCRA categories)	#	2012	2013	2014	2015	2016	2017
Products for Digital Signatures	7		1	1	2	2	1
ICs, Smart Cards and Smart Card-Related Devices and Systems	4				2	2	
Multi-Function Devices	3				2	1	
Data Protection	1				1		

[54] A Protection Profile (PP Profile (PP) is a document used as part of the certification process. A PP states a security problem of a given system or products and it specifies the security requirements needed to address that problem.) is a document used as part of the certification process. A PP states a security problem of a given system or products and it specifies the security requirements needed to address that problem.

Operating Systems	1			1			
Total	16		1	2	7	5	1*

Italian CC certification statistics - *14 evaluation processes in progress (July, 21 2017)

Next table reports some CC certification statistics for the French Common Criteria Scheme (ANNSI)

		SOGIS/CCRA									
Product Type	**#**	**#**	**<2010**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
Smart Card	347	333/332	57	32	29	36	38	37	34	52/51	18
Digital Tachograpgs	6	6	5	0	0	1	0	0	0	0	0
Miscellanous	5	5	0	0	0	2	0	1	0	1	1
Micro-chips	182	180	71	15	4	15	22	14	8	20	11
Product for PC and servers	35	31	8	3	5	7	0	1	0	6	1
Network Product	23	22	9	2	1	1	1	4	0	4	0
Systems	1	1	1	0	0	0	0	0	0	0	0

Next table reports some CC certification statistics for the Dutch Common Criteria Scheme (NLNCSA).

		SOGIS/CCRA									
Product Type	**#**	**#**	**<2010**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
Smart Card	14	11/14	1/4	0	0	1	5	1	1	0	2
Digital Tachograpgs	3	3	1	1	0	0	1	0	0	0	0
Miscellanous	14	11/13	1/3	0	3	0	1	1	1	2	2
Micro-chips	4	4	1	0	1	0	0	0	1	1	0
Product for PC and servers	3	2/3	0	0	0	0	0	0	0	1	1
Network Product	8	7	1	0	0	2	0	1	1	0	2
Systems	2	2	0	0	0	0	1	0	1	0	0
HW devices	6	6	0	0	0	0	0	1	2	1	2
Crypto Library	8	8	0	0	0	1	1	0	3	2	1

Next table reports some CC certification statistics for the German Common Criteria Scheme (BSI).

		SOGIS/CCRA						
Product Type	**#**	**#**	**2012**	**2013**	**2014**	**2015**	**2016**	**2107**
Digital Signature	7	7	2	2	3	0	0	0
Digital Tachograph	5	5	1	2	0	2	0	0
eHealth	6	6	0	0	1	3	2	0
electronic ID documents	41	41	8	11	12	1	7	0
Network devices and system	18	18	1	3	4	8	2	0
operating system	13	13	4	3	2	2	2	0
other devices and systems	9	9/6	1	4/2	2/1	0	1	0
server applications	17	17	1	6	3	5	1	0
smart card and similar devices	72	72	9	14	14	14	17	0
smart metering systems	1	1	0	0	0	0	1	0

Next table reports some CC certification statistics for the UK Common Criteria Scheme (NCSC). Note that UK statistics are represented only on CCRA website and product categorization is same as CCRA.

		SOGIS/CCRA						
Product Type (*)	**#**	**<2012**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
Access Control Devices and Systems	4	1	1	0	0	2	0	0
Boundary Protection Devices and Systems	2	2	0	0	0	0	0	0
Smart Cards and Smart Card-Related Devices and Systems	22	0	2	0	6	10	3	1
Network and Network-Related Devices and Systems	5	2	1	0	1	1	0	0
Operating Systems	2	1	1	0	0	0	0	0
Other Devices and Systems	6	5	1	0	0	0	0	0

Information Technology Security Evaluation Criteria (ITSEC)[55]. Used for evaluating computer security for IT products and systems. It is a structured set of criteria for evaluating computer security within products and systems. The ITSEC was first published in May 1990 in France, Germany, the Netherlands, and the United Kingdom based on existing work in their respective countries. Following extensive international review, Version 1.2 was subsequently published in June 1991 by the European Commission for operational use within evaluation and certification schemes. It is still used for some evaluation in the classified information but it has to be considered superseded by the publication of ISO 15408 Common Criteria for ICT security product evaluations.

ISA Secure Certification Programme[56]. It independently certifies industrial automation and control (*IAC*) products and systems to ensure that they are robust against network attacks and free from known vulnerabilities. It is by the the IEC/ISA standardisation recognised, but the ISASecure is ye only existing certification service and is available at Certification Authorities in the US and Japan, and recognised by ANSI (American National Standards Institute).

Federal Information Processing Standards FIPS-140[57]. These are U.S. government computer security standards, which specify requirements for cryptography modules.

Industrial Automation and Control Systems (ISA/IEC-62443 /IACS)[58]. ISA/IEC-62443 is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems. These documents were originally referred to as ANSI/ISA-99 or ISA99 standards, as they were created by the International Society for Automation (ISA) and publicly released as American National Standards Institute (ANSI) documents. In 2010, they were renumbered to be the ANSI/ISA-62443 series. This change was intended to align the ISA and ANSI document numbering with the corresponding International Electrotechnical Commission (IEC) standards.

EN50128. It specifies procedures and technical requirements for the development of programmable electronic systems for use in railway control and protection applications

IEC61508. It is aimed at the electrotechnical industry.

ISO 27001[59]. ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature. The ISO 27001 standard provides a framework that helps organisations: protect clients and employee information; manage risks to information security effectively; achieve compliance; protects the company's brand image.

[55] See official document published on the website of the German Certification Authority BSI at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile

[56] http://www.isasecure.org/en-US/

[57] http://csrc.nist.gov/groups/STM/cmvp/standards.html

[58] See: https://www.isa.org/isa99/ and

[59] https://www.iso.org/standard/54534.html.

IASME is a UK-based standard for information assurance at small-to-medium enterprises (SMEs). It provides criteria and certification for small-to-medium business cyber security readiness. It also allows small to medium business to provide potential and existing customers and clients with an accredited measurement of the cyber security posture of the enterprise and its protection of personal/business data. IASME was established to enable businesses with capitalization of 1.2 billion pounds or less (1.5 billion Euros; 2 billion US dollars) to achieve an accreditation similar to ISO 27001 but with reduced complexity, cost, and administrative overhead (specifically focused on SME in recognition that it is difficult for small cap businesses to achieve and maintain ISO 27001). The cost of the certification is progressively graduated based upon the employee population of the SME (e.g., 10 & fewer, 11 to 25, 26 - 100, 101 - 250 employees); the certification can be based upon a self-assessment with an IASME questionnaire or by a third-party professional assessor. Some insurance companies reduce premiums for cyber security related coverage based upon the IASME certification.

ISO/IEC 19790 and ISO/IEC 24759 are applicable to validate whether the cryptographic core of any security product is properly implementing an approved suite of cryptographic protocols, modes of operation and key sizes, while protecting this implementation and the critical security parameters, such as keys, in accordance to the design and specification requirements laid out in the standards. There are four levels of security defined, and ISO/IEC 19790 includes a variety of possible implementations, both software and hardware.

IECEE CB Scheme[60]. It is operated by the IEC System of Conformity Assessment Schemes for Electrotechical Equipment and Components (IECEE), is an international system for mutual acceptance of test reports and certificates dealing with the safety of electrical and electronic components, equipment and products. It is a multilateral agreement among participating countries and certification organizations, which aims to facilitate trade by promoting harmonization of national standards with International Standards and cooperation among accepted National Certification Authorities (NCBs) worldwide. By achieving this, it brings product manufacturers a step closer to the ideal concept of "one product, one test, one mark, where applicable'.

In the specific domain of smart grids the list of applicable schemes includes the following (Enisa, 2014): ISO 9001; ISO/IEC 27001; IEC62443; ISO/IEC 15408, Common Criteria; ISO/IEC 19790; CPA, CSPN; and IASME. The latter, for instance, is a British standard that is not widely recognised outside the UK

1.1. National initiatives

France[61]. The National Cybersecurity Agency of France (Agence nationale de la sécurité des systèmes d'information – ANSSI) established in 2008 the Certification Sécuritaire de Premier Niveau (CSPN), which is an IT Security Certification Scheme. Its main purpose is to offer a faster and cheaper alternative for IT Security Certification as compared to the Common Criteria (see below) approach. The security criteria as well as evaluation methodology and process are based on an ANSSI created standard. Similarly, to the CPA, there is no MRA for CSPN, which means that products tested in the France will not normally be accepted in other markets. CSPN is regnosized only by ANSSI in France[62]. As reported in an ANSSI presentation (2015) the CSPN was developed as shorter and cheaper alternative to the Common Criteria evaluations, whose cost and duration are considered a barrier for the security industry development. The CSPN can be used when a low level of assurance is required and it ensures a product evaluation in 25 days (while CC evaluation of a smart card can take from 6 months to 1 year). ANSSI provides around 25 CSPN certificates (mainly on software) and 100 CC certificates (mainly hardware) per year. Currently, ANSSI recognises and issues two main types of labels. These labels are used for:

- certifying products
- qualifying products and services

[60] https://www.iecee.org/about/cb-scheme/.
[61] Based on information from website (http://www.ssi.gouv.fr/administration/produits-certifies/cspn/) and from official case study presentation (ANSSI, 2015).
[62] ENISA - Smart grid security certification in Europe.

Germany[63]. The German Federal Office for Information Security (**BSI**) is developing an approach for low level assurance to improve the efficiency of Common Criteria evaluation. The approach is still under development and is very close to the CSPN French framework.
The *IT-Grundschutz Certificate*[64] offers companies and agencies the possibility of making transparent their efforts regarding IT security. After consulting with registered IT-Grundschutz users and IT security experts, the BSI has defined three variants of the IT-Grundschutz qualification: the IT-Grundschutz Certificate and the self-declarations "IT-Grundschutz entry level" and "IT-Grundschutz higher level". The issuance of the IT-Grundschutz Certificate is based on an audit carried out by an external auditor licensed with the BSI. The outcome of the audit is an audit report which is submitted to BSI that decides on the granting of the IT-Grundschutz Certificates.

UK. The *Commercial Product Assurance* (CPA)[65] is the UK national scheme for commercial off-the-shelf products; products successfully evaluated according to CPA obtain a Foundation Grade certification, meaning that they proved to be good commercial security practice and are suitable for lower threat environments. CPA is open to all vendors, developers and suppliers of security products with a UK sales base. However, there is no Mutual Recognition Agreement (MRA) for CPA, which means that products tested in the UK will not normally be accepted in other markets. CPA is similar to common criteria, however not so widely recognised outside of UK (Enisa, 2014). Information about products certified and cost to sustain for CPA certification can be retrieved on the online website of CPA scheme. Certified Products[66] under CPA scheme are actually **37** and **15** products are in evaluation.
The Costs[67] to sustain to certify a product under the CPA scheme are:

- Paid by Test Lab to NCSC for each task = £4,640
- Membership fees = £2,220
- Certified Consultancy for Large Companies = £10,100
- Certified Consultancy for SMEs = £1,010
- Additional Head Consultant with a single service offering = £1,010
- Each additional service offering for existing Head Consultant = £1,010

Cyber Essentials[68] is a government-backed, industry-supported scheme to help organisations protect themselves against common cyber-attacks. The full scheme, launched on the 5 June 2014, is used to "give assurance" to wider industry. For central government procurement of technology products and services, which involve handling of personal information, it is required that the Cyber Essentials scheme, or Cyber Essentials Plus, is in place[69]. The evaluation criteria currently recognised by the UK certification scheme, and the methodologies associated with them, are: a) the Common Criteria (CC) ISO/IEC 15408 and the Common Methodology for IT Security Evaluation (CEM) ISO/IEC 18045; b) the IT Security Evaluation Criteria (ITSEC) and the IT Security Evaluation Manual (ITSEM).

The Netherlands. Dutch approach Baseline Security Product Assessment (BSPA) scheme is intended to judge the suitability of IT security products for use in the "sensitive but unclassified" domain: the requirements are expressed in the Dutch "Baseline Informatiebeveiliging Rijksdienst" (Government security baseline, BIR). The BSPA scheme is in pilot phase since 2015. During the pilot phase BSPA scheme received **6 requests** for certification: three of them are completed and the other three are starting up. The average costs of a certification under BSPA scheme are approximately **40 thousand euros**. An evaluation performed under the BSPA scheme has the following main characteristics: it is carried out in constrained time frame and with limited resources; it determines the conformity of the product to the security specification in the Security Evaluation Target and it determines the effectiveness of the security features offered by the product. The evaluation process should take 25 person days within a calendar period of 8 weeks. The BSPA scheme is comparable to the CSPN scheme of ANSSI. Dutch scheme is then in charge of overseeing the entire process, to validate the report and to publish a "statement of conformity". The Dutch

[63] Based on information reported in Baldini et al. (2017).
[64] https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCertification/itgrundschutzcertification_node.html
[65] https://www.cesg.gov.uk/scheme/commercial-product-assurance-products-foundation-grade
[66] https://www.ncsc.gov.uk/index/certified-product?f[0]=field_assurance_scheme%3A226&f[1]=field_assurance_status%3AAssured
[67] https://www.ncsc.gov.uk/articles/products-and-services-scheme-fees
[68] https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
[69] https://www.gov.uk/guidance/public-sector-procurement-policy#procurement-policies-for-technology

national organization of DSO's "Netbeheer Nederland", has also developed the Dutch Smart Meter Requirements (DSMR). In December 2014, The Netherlands was considering developing a protection profile based on Common Criteria, anyhow, in order to be recognized among participants of any Mutual Recognition Arrangement based on Common Criteria certification (e.g. SOGIS, CCRA), any protection profile will need to be certified in a scheme that has been recognized as "certificate producing member".
The objective of the Netherlands scheme for Certification in the Area of IT Security (NSCIB) is to enable IT products and systems to be evaluated and certified in the Netherlands in a way that conforms to the 'Common Criteria' methodology (ISO-standard 15408) for Evaluation and Certification.
A concrete example where the Dutch Certification scheme is requested in public procurement acts is represented by all taxis (more than 10 thousand) in the Netherlands, which have to contain an On-Board Computer (Dutch BCT). The relevant regulatory act came into force on 1 October 2011. The regulations specify that all taxi operators must purchase an on-board computer and have it installed and activated before 1 February 2015. On-board computers in taxis must have a type-approval and must comply with the requirements for (software) security[70].

Pricelist for certification under the Netherlands Scheme for Certification in the area of IT Security (NSCIB)

Certification of a Protection Profile / Product

NSCIB new certification € 3.300,00
Certificate is valid for a maximum of 5 years
Includes one certificate in Dutch or English and web publication of certification report
NSCIB re-certification (minor change) € 275,00
Original certificate remains
Based on Impact Analysis Report of changes, no updated vulnerability assessment
Certifier creates maintenance report
TUV updates records and adds maintenance report to web publication

NSCIB re-certification (major change) € 550,00
Re-issue of original certificate, original expiry date remains
Re-use possible of previous results, new vulnerability assessment
Certifier updates certification report
TUV updates records, re-issues certificate and updates web publication

Site Certification

NSCIB site certification € 1.900,00
Site certificate is valid for a maximum of 2 years
Includes one certificate in Dutch or English and web publication of certification report

Translation per certificate € 275,00

Use of internal non-commercial certifiers (very limited availability) - Free
Use of external commercial certifiers (for regular certifications) - 175,00 p/h

All cost are exclude VAT and travel costs

[70] https://www.rdw.nl/sites/tgk/englishversion/Paginas/On-board-computers-for-taxis.aspx

	Total	Certification fee	Certifier costs	Certifier hours
New certifications EAL4-6				
Small TOE (simple applet)	€20.800,00	€3.300,00	€17.500,00	100
Normal TOE (IC, Crypto Library, ePassport, HSM)	€29.550,00	€3.300,00	€26.250,00	150
Big TOE (JavaCard, complex HSM)	€33.925,00	€3.300,00	€30.625,00	175
Re-certification Major change ("Maintenance")				
Big TOE medium delta	€13.675,00	€550,00	€13.125,00	75
Re-certification Minor change	€9.425,00	€275,00	€9.150,00	50
New certifications EAL2-3				
Small TOE (e.g. simple network device)	€13.800,00	€3300,00	€10.500,00	60
Normal TOE (e.g. BCT)	€17.300,00	€3300,00	€14.000,00	80
Big TOE (complex network device)	€20.800,00	€ 3300,00	€17.500,00	100

Figure - Average certification costs (ex VAT)

Number of NSCIB certificate applications received

Year	Type	New certifications	Recertifications	Maintenance
2011	Smartcards	4		1
	Network devices	1		
2012	Smartcards	3		
	Datadiode	1		
	Boundary protection	1		
2013	Smartcards	6	1	
	HSM	1		
	BCT	3		
2014	Smartcards	3		2
	Network devices	1		
	BCT			1
	POI (payment terminal)	1		
	Boundary protection	1		
	Site certificates	5		
2015	Smartcards	4	5	
	Network devices	1		
	PP BCT		1	
	Site certificates		1	
2016	Smartcards	5	3	6
	Network devices	3		
	Tachograph	1		
	Site certificates		4	

Year	Type	New certifications	Recertifications	Maintenance
Total 2011 - 2016	Smartcards (EAL4-6)	25	9	9
	HSM, POI (EAL4)	2	0	0
	Network devices (EAL2-3)	6	0	0
	BCT (EAL3)*	3	1	1
	Tachograph (EAL4)**	1	0	0
	Other (EAL3-7)	3	0	0
	Site certificates (EAL6)	5	5	0

*National Regulation (Taxi)
** EU Regulation

Year	Type	New certifications	Recertifications	Maintenance
Completed 2017	Smartcards	6	4	0
	Network devices	2	1	0
	HSM	1	0	0
	Datadiode	1	0	0
Ongoing 2017	Smartcards	3	3	0
	Network devices	1	0	0
	HSM*	3	0	0
	Datadiode	1	0	0

*eIDAS Regulation

Selective examples of emerging certification schemes across Member States. In the *Czech Republic* the Institute for Testing and Certification (ITC) issue reports and certificates that, however, are not widely recognized[71]. *Norway* and *Sweden* have the intention to develop a protection profile based on Common Criteria. *SERTIT* (Sertifiseringsmyndigheten for IT-sikkerhet) is currently representing *Norway* as a member of the international community called "Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security (CCRA)". The average number of certificate applications received by SERTIT for the last five year period (2013-2017) is 11,6 per year. The annual numbers of applications from 2013 – 2017 (up to the 3rd of August 2017) are: 14, 9, 13, 13, 9. SERTIT does not charge for the certification as it is a Governmental service, but companies have to cover travel expenses related to progress-meetings and site-visits. The cost of the evaluation itself is a matter between the Evaluation Facility and the Industry. SERTIT is not involved in the commercial part between the ITSEF and the Industry. Mandatory requirements for Certification are stated in the Security Act. The average number of certificate applications for the last five year period linked to the before mentioned mandatory requirements is 3,2 per year. The annual numbers of such certifications from 2013 – 2017 (up to the 3rd of August 2017) are: 6, 0, 4, 1, 5. In *Ireland* the *Cyber Essentials* scheme is used to "give assurance" to wider industry and interested parties that the certified organisation is applying basic levels of IT related security to address the threat of cyber-attacks. *Poland* recently joined SOG-IS[72] and will be able to self-assess and certify IT products in compliance with the international standard ISO/ IEC 15408 adopted by the Polish legal system. This standard allows formal verification of information systems security. This will increase the level of cyber security and raise the competitive efficiency of Polish companies on the global market. In *Spain* the CCN (Centro Certificacion Nacional) adopts as common evaluation criteria those included in the following schemes: Common Criteria for Information Technology Security Evaluation» (CC); ISO/IEC 15408, Evaluation Criteria for IT Security; Information Technology Security Evaluation Criteria (ITSEC). The Number of certificate applications received by the CCN are 112 applications since January 2013 to August 2017. On average, the CCN receive around 22 applications per year. The Certification Authority does not request any fee for the release of the certificates. The costs come from the labs, which are not controlled by CCN. In the Spanish regulation, the National security Framework (Eqsuqema nacional de seguridad, defined

[71] http://www.itczlin.cz/en/certification-products
[72] http://commoncriteria.pl/index.php/en/common-criteria-standard/common-criteria-in-poland

in the "Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica") operates a classification of the system to be adopted in the public administration; at a high level, a certification against recognized european and international standard is requested. ISO 15048, is an explicit option described in the National Security Framework. In Italy, based on the national decree DPCM 17 February 2017[73], it should be established a National evaluation and certification centre for verifying security and non-vulnerability conditions for products, devices and systems for networks, services and critical infrastructures.

1.2. Main challenges and the need for a EU approach

From the analysis of the international and national schemes the JRC Report[74] (Baldini et al., 2017) identifies a number of challenges, including:

- **Re-certification and patching**. This require the definition of a new process or a modification of the existing approach for Common Criteria;
- **Security and trust coverage**. Security certification with Common Criteria may not be enough to provide full security and trust of a product;
- **Certification costs**. Common criteria certification is considered a long and expensive process, which does not make it suitable for fast market deployment or relative short product cycles as in the consumer market
- **Non-applicability to specific products and systems**. Some classes of system and products are difficult to certify due their intrinsic features and characteristics.
- **Comparability and visibility of the certification**. Users do not have a clear metric of comparison among different certified products.
- **Usability**. The Common criteria certification does not give a clear and simple indication to the users of the provided level of trust. Metrics are missing for this purpose.

The report further stresses that in the energy sector some of the potential security threats are still not clearly understood and there is a growing body of research on security and privacy aspects of the energy sector including its evolutions to the Smart Grid. The complexity and scale of future power systems that incorporate smart-grid concepts will introduce many security challenges. With respect to the issue of the energy sector and of smart grids the Enisa report (2014) draws the following conclusions:

- **Price**. Current certification schemes are considered rather expensive due to fragmented national policies, lack of resources, the need for repeatability and consistency of the results and the large number of components involved in the smart grid supply chain;
- **Lack of a uniform approach**. Stakeholders are facing a fragmented situation where different initiatives regarding the cyber security of smart grids are being developed;
- **Long life cycle**. The certification process takes some time which usually is more than the time needed for new vulnerabilities to appear in the cyberspace.
- **Legal framework**. There are only a few legal texts concerning security in smart grids and this is leaving enough space for grey zones and/or interpretations.
- **Common Criteria**. Although is the predominant certification scheme in the market, it will be unrealistic to have a Common Criteria certificate for the whole smart grid supply chain; it should be

[73] Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, Gazzetta Ufficiale n. 87 del 13 aprile 2017 (Italian Prime Minister Decree, 17/02/2017, Directive on guidelines for national cyber protection and cybersecurity, Official Bullettin n.87, 13/04/2017)

[74] Baldini, G., Giannopoulos, G., & Lazari, A. (2017). Analysis and recommendations for a European certification and labelling framework for cybersecurity in Europe. JRC Science for Policy Report. Luxembourg: Publications Office of the European Union.

extended to include specific protection profiles for the smart grid, similar to those related to the smart card industry, where a joint interpretation library was developed.

During the February 2016 Enisa workshop (2016a) MS representatives, among other things, voiced the following concerns:

- Certification should be, in general, voluntary. Mandatory certification might be justified for some areas, or specific products, with high security requirements;
- Mandatory certification should be assessed carefully, as it may introduce economic/administrative burdens for European industry;
- During the design of the EU certification framework it should be taken into account that some Member States have national certification schemes for certain high assurance sectors, and both schemes should not be confused
- As SMEs are key to ensure economic growth in EU, any future mandatory certification scheme should not introduce unjustified barriers for SMEs to enter the market.
- Any proposed certification scheme should not create bottlenecks for introducing products to the market.
- Certification based on international standards (e.g. on ISO standards) would facilitate EU industry to operate globally.
- European certification is one pillar of the European Digital Single Market (DSM). While global interests should be taken into account, Europe and EU legislation have specific requirements due to a risk-based approach.
- European Member States which are non-members of the SOG-IS, were invited to join the mutual recognition agreement.

In a subsequent worshop taking place in October of 2016 (Enisa, 2016b) the following conclusions were adopted:

- Need of a roadmap for a European security certification framework;
- Certification framework should be based on different certification levels/schemes including self-certification (compliance assessment);
- Need of harmonized security requirements at European level;
- Accredited/licensed European security certification labs;
- Definition of roles and governance aspects for European security certification;
- Combination of security and privacy certification, when possible;
- Security certification per domain (sector) when necessary (e.g. IACS);
- Label as marketing / certificate recognition tool. If feasible, ICT security labelling could be associated with any certification level;
- Identification of the need to develop new underling criteria for certification;

During a workshop organised by the French and German Certification Authorities (ANSSI & BSI, 20179) it was recognised that in the absence of an EU-wide cybersecurity certification scheme:

- Companies have to be certified individually in each country (except within SOG-IS);
- The Digital Single Market (DSM) is too fragmented;
- The reinforcement of digital security in Europe and user's trust can't be properly achieved;
- EU legislations adopt different approaches to security evaluation adding to the fragmentation of the DSM.

The same document concludes that, the development of an EU cybersecurity certification scheme should support the development and the well functioning of the Digital Single Market by:

- Reinforcing the security and trust in digital products, systems and services in Europe;
- Reducing fragmentation thus facilitating access to market for products, systems and services within the EU;
- Increasing companies' competitiveness through security;
- Building a leading security evaluation ecosystem in Europe ;
- Contributing to making the EU an attractive and competitive digital player;

At the more general level of the security industry as a whole the problems that the EU is facing have been fully documented in the Communication and supporting SWD (European Commission, 2012a, 2012b). Although ICT security is only a part of the broader system of industrial security, it suffers from the same challenges evidenced in these two documents. First, the fragmentation along national and even regional lines has created 28 different security markets, a situation that is an anachronistic rarity in the European Union with several negative consequences for both the supply and the demand side creating market barriers and higher costs. Second, in large part the security market remains largely an institutional market where the larger buyers are public authorities. The SWD (European Commission 2012b) stresses that: a) no common system of certification exists at a European level for security equipment; b) there is no mechanism of mutual recognition across countries. Therefore, a producer of security technologies has to go through the costly and lengthy certification processes for each country in which he wants to commercialise his technologies.

The analysis of the above sources confirm that need for a European certification scheme that had already been suggested by various studies including (ECORYS 2011) and (ERNCIP 2014). A European security certification scheme should be set-up to overcome the national differences on security certification and support a European-wide cybersecurity market. The majority of countries, with or without a national framework, expressed their favourable opinion of setting a common European scheme that they could be part of, either as producers or consumers of certifications. To sum up the main drivers are:

- The need to harmonize the current national certification schemes (Germany, UK and France) and to cover areas not fully addressed in order to create a common European certification scheme based on a common approach
- Testing and certifying the cyber-security of IACS components/devices it is a needed step to take as it would bring a higher level of cyber-confidence to industry buyers and users.
- The need to establish a practical scheme guaranteeing mutual recognition of certificates across Europe and compatible with similar requirements beyond. The current collaboration schemes like CCRA and SOG-IS could be a starting point for the establishment of a common format and semantic of the certificates.

4.Policy objective and intervention logic

Needs and strategic objective

In terms of needs the following three can be identified:

(1) Reduce the current EU vulnerability and equally protect citizens, businesses, and public administrations

(2) Forster dialogue, coordination, and trustworthiness in the cybersecurity ecosystem

(3) Respond to the DSM, which identified cybersecurity gap as a key hindrance to the achievement of a digital single market and the cybersecurity standardisation was defined as one of its priorities (European Commission, 2015b)

As a result, the overall strategic objective of a EU cybersecurity certification and labelling scheme can be formulated as follows: *Create a European ICT Security Certification Framework that at the same time, avoids the fragmentation resulting from different approaches across European Union and is as close as possible up to international standards in order reduce trade hindrances*

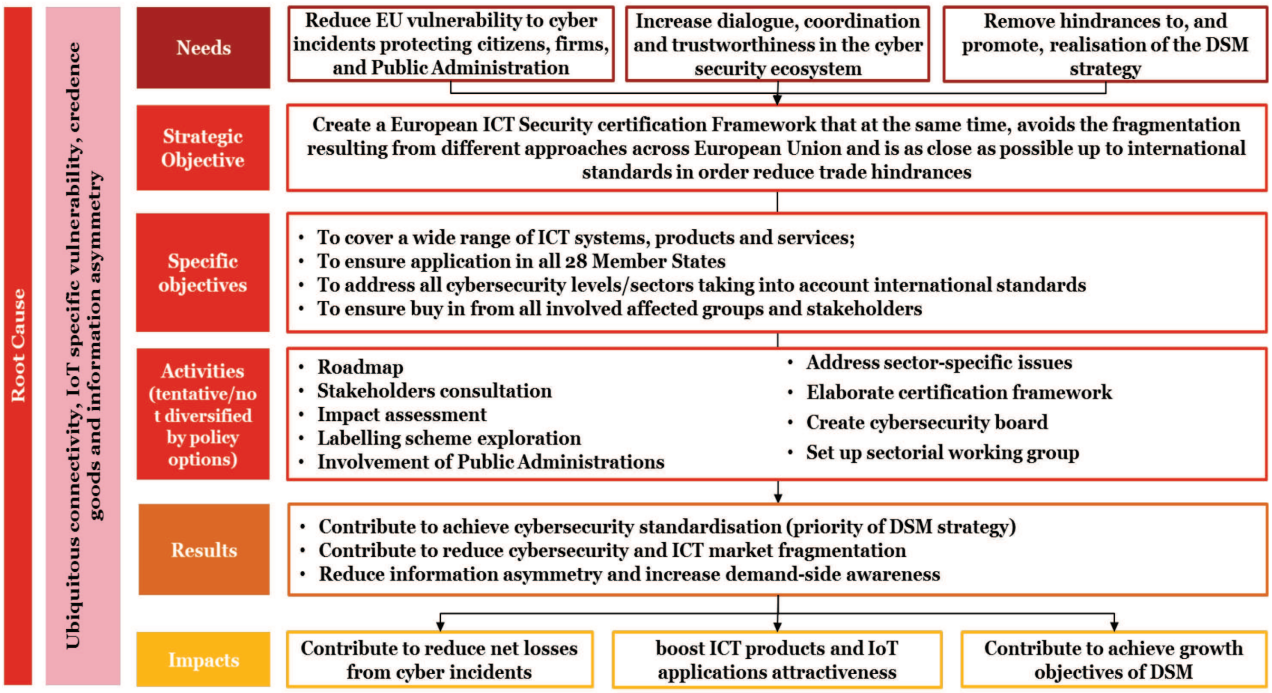
Specific objectives

Descending from the analysis of the problem and from the formulation of the needs and of the strategic objectives the specific objectives are in our view the following: a) To cover a wide range of ICT systems, products and services; b) To ensure application in all 28 Member States; c) to address all cybersecurity levels/sectors taking into account international standards; d) to ensure buy in from all involved affected groups and stakeholders.

Preliminary and simplified intervention logic

The Intervention Logic derived from the above sub-paragraph is depicted below and require no further comments.

Figure 6 Certification scheme and labelling: preliminary Intervention Logic



Source: own elaboration on secondary sources (obtained by the Commission and retrieved ourselves)

1.3. Policy options

The rise of cybercrime and security threats has spurred in recent years stimulating the emergence of national initiatives to set high-level cybersecurity requirements for ICT components on traditional infrastructure, including certification requirements. Albeit important, these initiatives bear the risk of creating single market fragmentation and barriers for interoperability. The proliferation of national certification and labelling initiatives increase costs for businesses operating cross-border and is likely to create obstacles for the internal market, as it raises the costs for companies/vendors operating across borders. This barrier is more significant for small and medium sized enterprises, which have usually less resources to dedicate to certification programmes. The risk of fragmentation of security requirements and related certification schemes emerges as an important concern for the industry. In the context of the public consultation related to the cPPP, some respondents emphasized that no reliable certification scheme exists at the moment at the European level, while some others pointed to the fact that existing national schemes act as barriers to market entry, complaining about the costs of complying with several certification schemes in Europe. Some of the industry associations state that further fragmenting the market with numerous certification schemes should be avoided.

On the other hand, while a European certification framework can reduce the costs and risks broadly sketched above and produce some benefits for both supply and demand, potentially negative impacts should not be overlooked. A mandatory security certification can introduce additional costs on the manufacturer and the citizen. While some types of products would require secure certification because of safety reasons (healthcare, road transportation) other products may be based on a voluntary basis approach. From an economic point of view, there is also the risk to introduce market distortion because large/midsize companies would be able to invest more money on the security certification process, while small companies could be excluded by some markets. The dynamicity of specific domains or technologies (e.g., IoT) introduces the issue of the staticity of security certification and of considering the life-cycle of the various products. This means that if a product is submitted to frequent changes, the security certification will be not worth the effort involved in the initial phases (on this see more also in the section on ICT certification labelling).

In April, a stakeholder consultation with DG CNECT (EC/ENISA, Towards a European ICT Security Certification Framework, April 27, 2017) concerning policy options was held. The presented options are briefly described here along with the results from the discussion with the stakeholders (as provided by DG CNECT):

Option 0

No action. The overwhelming majority of stakeholders stated that “no action” is not a viable possibility.

Under this option, the Commission would maintain the status-quo and not undertake any policy or legislative action. The option would result in the following situation:

1. The problem relating to the **limited information asymmetry and ineffectiveness/inefficiency of the current certification** schemes is **unlikely to be solved** in the absence of intervention.
2. As technology becomes increasingly complex and pervasive, it will be more and more **difficult for buyers to ascertain the security qualities of ICT** products and services.
3. In the lack of the proper economic incentives, it is also **unlikely that operators could establish self-regulatory measures fixing the existing information gap**. Such incentives are likely to exist only for markets where institutional or very organised buyers are present and can therefore exercise pressure on the side of the vendors.
4. The problem of **market fragmentation is very likely to increase** in the short-medium term (next 5-10 tears) as a number of national and sectorial certification schemes are emerging.
5. The lack of coordination and interoperability across such schemes **hampers** the potential of **the digital single market**.

The **SOG-IS** agreement and the CCRAs **will not solve the problem** in the short-medium term. The criticism towards common criteria, on which SOG-IS is based, will remain an issue as the limited geographical and substantive coverage of the agreement.

Under the **Do-Nothing scenario,** the current situation would be continued and there would be no common EU wide system of Conformity Assessment and Certification (CAC). Security products subject to approval/certification requirements would continue to undergo national testing, validation and approval/certification procedures. No priority would be given to certain products. Furthermore, no additional development of EU-level structures and processes for the implementation of conformity assessment and certification requirements and procedures would take place.

Under this scenario the main impacts for **producers and suppliers** would be:

- **Costs of complying with multiple national procedures**. Multiple certification and conformity assessment country by country entails substantial costs.
- **Delay in 'time to market' of products**. Such multiple procedures prevent EU producers to enter rapidly all EU markets and achieve economy of scale and volumes to compete with third-country players.
- **Adaptation costs to meet national CAC systems**. Additional production costs may apply if variants of products are needed to get the certification in a given country.
- **Slow development and diffusion of new solutions**. Limited market access and scale reduce the incentives to R&D and innovation.

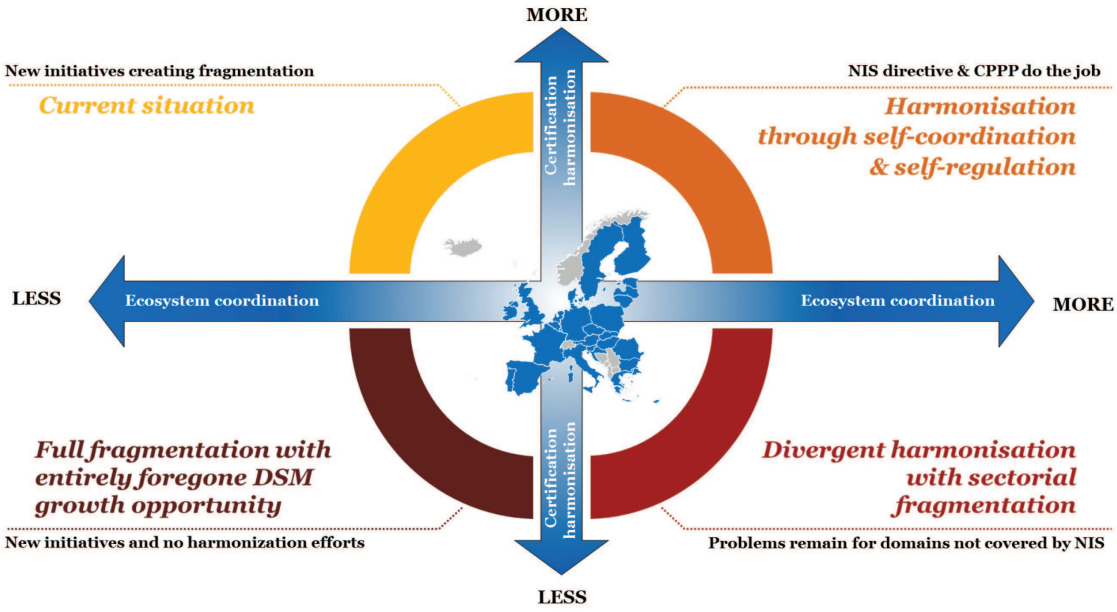
For **procurers** the status quo also entails lack of transparency and especially limited choices of suppliers, reducing the possibility to get the best value for money.

With no intervention in the Member States, only a limited number of **Certification Authorities** operate with quasi-monopolistic power. Obviously, this condition persists only because suppliers of security products are obliged to have their products certified in each Member State and cannot opt to have their product certified once for the entire EU.

In certain countries with well-functioning certification systems **regulators** may not perceive any immediate need for an EU-wide CAC scheme. However, many countries lack the technical expertise and capacity to support such functions. This may limit the scope for developing and implementing regulations requiring conformity assessment of security products and may result in insufficient or appropriate national regulatory frameworks for security products. Such circumstances may necessitate that Member States make reference to, and are reliant upon standards to certification procedures available from other Member States but which may not be aligned to their own national situations.

As a result of the various negative impacts illustrated above, costs are passed onto final users (both citizens and businesses) representing the negative impacts for **society** as a whole. Users of security products are not always able to buy the best security products at the lowest price.

Figure 7 Scenarios under no action



Source: own elaboration on secondary sources (obtained by the Commission and retrieved ourselves)

Option 1

Soft law tools. EC would encourage MS and industry initiatives, such as developing relevant guidelines and methodologies, and promote MS participation to SOGIS-MRA. This solution should have low costs but is not expected to adequately address the fragmentation risk.

Option 2

SOGIS mandatory. EC would make SOGIS-MRA mandatory for all MS. This solution would allow only the Common Criteria approach, so leaving out, e.g., some national approaches based on low time/cost/assurance requirements.

Option 3

Framework option. EC would mandate the creation of the EU cybersecurity certification and labelling framework based on a board made of the 28 cybersecurity agencies. The framework could initially rely on Common Criteria and (extended participation to) SOGIS-MRA. Different certification approaches would be submitted to the board, and, if accepted, would gain mutual recognition within EU. A secretariat run with the assistance of an EU agency or body (e.g., ENISA) would ensure efficiency within the framework. Working group under the board would capture/anticipate the certification needs from different industry sectors, so triggering, via board approvals/decisions, the creation of the needed tools (e.g., the relevant protection profiles). Even though the corresponding costs need to be well analysed, this solution seems to be flexible and manageable enough to meet the relevant expectations, as confirmed by a majority of the participant stakeholders.

The following points demonstrate the potential positive and negative impact of having an EU general ICT Security certification and labelling framework structured by type of affected player.

Producers:

- **Reduction of costs associated to multiple testing to obtain national certification and labels.** Security products will have to be certified only once rather than multiple times, thus reducing overall conformity assessment and certification costs;

- **Reduction of adaptation costs to meet national product standards/specifications.** Common EU product standards reduce the need to produce product variants adapted to meet different national standards;
- **Reduction of the need for product trials for Priority and sensitive security products[75].** The possibility to certify products meeting EU requirements after initial trials should reduce the subsequent need for further national and/or client trials;
- **Reduction of the 'time to market' of products.** Having obtained EU certification, products may be introduced to the whole EU market without delays caused by the need to obtain national certification;
- **Improved alignment of production to the expected EU market as a whole.** Production (of certified products) can be aligned at the outset to the expected size of the EU market rather than being conditioned on the uncertain timing associated with obtaining national certification;
- **Reduction of risk that competitors are able to 'replicate' new product developments and innovations.** Simultaneous access to the EU market as a whole limits the opportunities for competitors to use in a strategic manner delays in obtaining national certification to launch competing products;
- **Enhanced transparency of performance requirements and standards / specifications.** Common EU performance requirements and conformity assessment protocols should enable producers to better develop products according to 'predetermined' criteria, reducing uncertainty of product conformity assessment outcomes;
- **Acceleration of development process.** A common regulatory framework with reference to defined product standards/specifications should make it easier for producers to direct their RTD efforts to meeting regulatory/market requirements.
- **Negative impacts**. Potentially negative impact for producers relates to the additional costs of obtaining EU certification and labelling (for products that are currently not covered by national conformity assessment and certification and labelling requirements but that will be brought within a future EU-wide system). However, in a longer-term perspective, certification could be an investment for companies and transformed in a market advantage. In fact, the savings obtained from one certification instead of multiple certifications could be reinvested, for example, in research and innovation.

Market conditions:

- **Increased transparency regarding product performance.** EU certification and labelling provides an indicator of product performance based on common standards/specifications and, hence, increases market transparency**;**
- **Increased market openness.** Increased market transparency should reduce market entry barriers by facilitating market acceptance of (certified) products offered by new market entrants and reducing the importance of ''reputation effects';
- **Increased competition in security product markets.** Greater market transparency and openness should reduce fragmentation and increase the level of competition within markets. Existing suppliers will be more easily able to serve different national markets, which may be particularly beneficial to SMEs. The EU market would also be more attractive to new entrants, both new business start-ups and non-EU based suppliers. Increased competition should put downward pressure on the price of security products, which reduces costs for procurers / users of the products;
- **Increased competitiveness of European manufacturing industry.** Increased competition should drive improvements in productivity performance by forcing improvements in production

[75] Priority and sensitive security products are security products and solutions addressing 'unfamiliar' or new types of threats that require the development or application of new technologies, and equipment and may be extended to changes in organisation and implementation of security functions; for example through the automation of security functions.

efficiency and/or raise value added (e.g. higher value-added products). At the same time, improved market access that increases the size of the potential market for new products, should provide a positive incentive for producers to engage in RTD activities and promote innovation. Finally, EU certification may support exports of products to markets outside the EU if it engenders greater recognition in international markets than the existing multitude of national certification schemes.

- **Negative impacts**. The main identified potentially negative impact on market conditions concerns the possibility that minimum EU standards may become de facto market requirements. This may, in turn, reduce the market opportunities for products with performance levels above minimum requirements and, reduce, incentives for investments in RTD to raise product performance. Similarly, it may limit market acceptance of 'alternative' or innovative' products, particularly if they are costlier than standard products that comply with minimum requirements.

Procurers and users:

- **Lower price for security products.** As outlined above, there are a number of impacts that affect producer costs and prices and that should feed through to the purchase cost of security products;
- **Increased product choice / availability.** Increased market openness should result in more suppliers on the market. At the same time, a less fragmented EU market should promote RTD and innovation and raise entry into the market of new technologies and innovative solutions;
- **Enhanced information / transparency on product performance.** An EU-wide conformity assessment and certification scheme should increase market transparency and provide potential purchasers with greater information on product performance. This should contribute to reducing information asymmetries between purchasers and producers;
- **Facilitation of procurement procedures.** Procurers – and where relevant regulatory authorities – would be able to include EU standards and an EU certification as a requirement in their contracts. Furthermore, an EU wide scheme with mutual recognition of certification should support greater openness in procurement procedures by making it easier for potential suppliers

Certification Authorities

- **Change in the volume of demand for CAC (Conformity Assessment and Certification) services.** A single 'one-stop' EU-wide approach should decrease total number of CAC procedures required for each individual product. However, bringing products currently not covered by national CAC requirements within the scope of an EU-wide scheme should increase in the volume of demand for CAC procedures. The overall balance will depend on the actual scope of an EU-wide conformity assessment and certification scheme(s);
- **Increased competition for the provision of CAC services.** For Type-1 products, the introduction of an EU-wide CAC scheme should remove the controlling position that CAC bodies are able to occupy over their national markets, thus promoting competition between CAC bodies. For Type-2 products, the scale of the existing infrastructure for conformity assessment and testing relatively limited, making it difficult to assess the impact of a 'one stop' EU system on competition and on the cost and quality of CAC service provision;
- **Strengthened EU-wide accreditation.** For Type-1 products, it is foreseen that there will be EU accreditation of conformity assessment and Certification Authorities following common rules and requirements for obtaining accreditation. For Type-2 products, it will be essential that appropriate checks are made to assure the quality and independence of CAC service providers. This implies a strong emphasis on the accreditation of conformity assessment and Certification Authorities. Accordingly, part of the implementation of an EU CAC system for Type 2 products would relate to the development and operation of the infrastructure and procedures for accreditation of conformity assessment (e.g. Conformity Assessment Body) and Certification Authorities;

- **Increase of administrative costs related to the CAC system.** For Type-1 products it is foreseen that conformity assessment and Certification Authorities will be EU accredited, which will result in corresponding (additional) administrative costs. For Type-2 products, the introduction of an EU-wide CAC system together with the definition of product requirements and technical standards/specifications would require the development of a corresponding organizational structure. Again, this implies some additional administrative costs.

Regulators

- **Conformity with EU standards as a basis for national regulations.** The development and introduction of European Standards and an EU-wide CAC scheme may make it easier for national authorities to introduce national regulations setting product requirements aligned to these standards;
- **Facilitation of regulations through existence of conformity assessment infrastructure.** The existence of an EU-wide CAC system could remove the need to countries to independently develop such an infrastructure. This may reduce the associated CAC infrastructure costs from introducing regulatory requirements for security products. In turn, this may speed-up the adoption of regulations as there will be lower cost and shorter delay in meeting the corresponding requirements for a CAC infrastructure/scheme to verify compliance with regulations.

Society

- **Raised average security performance characteristics of deployed products.** By ensuring that all products meet minimum requirements, an EU-wide CAC system should raise the average performance level of deployed security products. However, there may be risks that an EU-wide CAC system may have a negative impact on overall security performance if it reduces incentives for the development of products with performance characteristics above EU (minimum) requirements;
- **Accelerate the deployment of security products.** To the extent that an EU legislative and CAC 'package' accelerates the deployment of security products (e.g. reduced time to market), particularly to address new threats, it should have a positive impact on security.

The costs of fragmentation: indicative estimations

Lack of standardisation of technical rules and of mutual recognition together with the cost of multiple conformity assessments and certification has long been recognised as one of the main barriers to the single market (Ilzkovitz et al., 2007, pp. 59-63). The fragmentation of in ICT security certification and labelling is just one manifestation of such phenomenon. Depending on the industry such fragmentation and the need of multiple conformity assessments can cost to enterprises between 2% and 15% of their production costs (Ilzkovitz et al., 2007, p. 61). Based on this estimation produced by DG ECFIN economists, it is possible to first produce the following high level and indicative calculation:

- According to PwC and LSEC Cyber Security market study[76] the EU cyber security market is estimated at 157 € billion;
- To be conservative, we assume that industry aggregate production costs are 40% of the market value (63 € billion), and that only 60% of products require certification, so that the total relevant value for production costs is 38 € billion (60% of 63 € billion);
- Again remaining on the conservative side, if we use only the lower bound (2%) from DG ECFIN analysis, the total costs of multiple testing due to fragmentation for the entire EU cybersecurity industry would amount to 760 € million per year.

[76] The study is still ongoing and the preliminary results presented within the Interim Report are updated to June 6, 2017.

This high level and indicative aggregate calculation could be further contextualised and applied in more granular fashion to very specific sectors. Ecorys (2011, p. 48 and pp. 209-211) has applied the same line of reasoning illustrate above for the very specific sector producing 'intruder alarm systems'. Currently a producer of a security alarm system seeking to supply their product throughout the EU will typically need to apply for 10-15 certificates from different Member States. This certification including but not limited to:

- **CertAlarm**[77]**:** The CertAlarm Certification Schemes provide a proof of conformity the European (EU) product, system, installation and service standards. The scheme is based on the principle of independent third-party assessment and certification of security products. In February 2011, the European cooperation for Accreditation (EA) confirmed the status of CertAlarm as a scheme covered by the EA Multilateral Agreement (MLA). The CertAlarm Certification includes some standards on IP interoperability implementation based on Web services for each kind of alarm[78].
- **Common Criteria**
- **EuroPriSe** (Privacy for IT products): EuroPriSe, the European Privacy Seal, is a European scheme providing privacy and data protection certification for IT products and IT-based services. The European Privacy Seal embodies a visible trust mark certifying that a product or service has been checked by independent experts and approved by an impartial privacy organisation. The EuroPriSe website privacy certification is awarded to websites that are compliant with EU data protection law and that meet all of EuroPriSe's high-quality data protection requirements. Specifically, the evaluation covers publicly available parts of a website and focuses on the interaction between a web server and the browser of a visitor on the website. This includes topics such as cookies, IP address processing and social plugins[79].
- **ONVIF and PSIA** (Video surveillance): the Open Network Video Interface Forum (ONVIF) and the Physical Security Interoperability Alliance (PSIA) are two recently created organisations with the aim of developing interoperability standards for Internet Protocol (IP) based security systems. Both these bodies are promoting conformity schemes based on manufacturers undertaking their own conformance testing. ONVIF's Profile Q offers the advanced security required in today's technological world, giving integrators and end users the necessary protections from today's cyber security threats, in addition to providing out-of-the-box interoperability[80].
- **Alarm System Certificate**[81]**:** The alarm system Certificate is the UL Mark for programs designed to meet the needs of alarm service providers, their customers, and interested stakeholders. It is the alarm company's declaration that the system will be installed, maintained, tested and monitored in accordance with applicable codes and standards. The Alarm System Certificate includes a cybersecurity standard (UL 2900)[82]
- **ISA/IEC-62443 (formerly ISA-99)**: ISA/IEC-62443 is a series of cyber security standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems. The concept of manufacturing and control systems electronic security is applied in the broadest possible sense, encompassing all types of plants, facilities, and systems in all industries. Manufacturing and control systems include, but are not limited to[83]:
    - hardware and software systems such as DCS, PLC, SCADA, networked electronic sensing, and monitoring and diagnostic systems

[77] ECORYS. (2011). Security Regulation, Conformity Assessment & Certification. Brussels: Report delivered by ECORYS for the European Commission.
[78] http://www.certalarm.org/ca/sites/default/files/Scheme%20Rules-2-Iss_5.pdf
[79] https://www.european-privacy-seal.eu/EPS-en/website-privacy-certification-overview
[80] https://www.ifsecglobal.com/onvif-introduces-profile-q-to-tackle-cyber-security-challenges/
[81] http://industries.ul.com/blog/alarm-system-certificate
[82] http://industries.ul.com/wp-content/uploads/sites/2/2016/04/UL_CAP-Overview-Info.pdf
[83] https://www.isa.org/isa99/

- associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

- **IECEE CB Scheme[84]:** The CB Scheme is an international program created by the International Electrotechnical Commission for Electrical Equipment (IECEE) for the acceptance of product safety test results among participating laboratories and certification organizations around the world. The CB Scheme offers manufacturers a simplified way of obtaining multiple national safety certifications for their products — providing entry into over 50 countries.

Their estimation is that, under an EU-wide system of conformity assessment and certification that provides for mutual recognition of certification throughout the EU and would avoid multiple testing in several national market, the cost savings for intruder alarm systems would amounts to a range of EUR 4.7 million to 9.9 million per year. As this is a very tiny sector within the broader cybersecurity industry, the above estimate of total costs of fragmentation in the range of 760 € million per year seems reasonable.

[84] http://www.intertek.com/marks/cb-scheme/