Council of the European Union

Brussels, 14 September 2017
(OR. en)

12183/17
ADD 8

Interinstitutional File:
2017/0225 (COD)

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	13 September 2017
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2017) 500 final PART 5/6
Subject:	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")

Delegations will find attached document SWD(2017) 500 final PART 5/6.

Encl.: SWD(2017) 500 final PART 5/6

EUROPEAN
COMMISSION

Brussels, 13.9.2017
SWD(2017) 500 final

PART 5/6

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:

5. Stakeholders' support

The following section described the information gathered through interview activities to selected participants from these categories:

- Smart meters Industry
- Semiconductors industry
- Other private sector representatives
- Members of ICT Certification Authorities

Questions were asked in order to cover the following areas of interest:

- Evidence of fragmentation
- Labelling and information asymmetry
- Policy Option 1: Non-legislative "Soft-law" measures
- Policy Option 2: EU legislative act to extend SOG-IS agreement to all MS
- Policy Option 3: EU general ICT security certification and labelling framework
- Institutional costs

5.1 Evidence of fragmentation

Interview data gathering activities provided key examples of fragmentation of ICT Security Certification across Europe pinpointing what are the cross-border trade challenges the industry must face when entering the market of several EU countries.

Representatives from smart meters industry provided a position on fragmentation in the field of smart metering products, which is worth reporting: "*If the question is: Are there countries that accept each other certificates? The answer is no*". As example, it has been explained that there are currently three certification for smart-meters in three countries. In the UK, the certification scheme is called the CPA (Commercial Product Assurance), which is a scheme applied for smart-meters but also for other products. In France they have the CSPN (Certification de Sécurité de Premier Niveau) certification scheme and in Germany they have their own protection profile based on Common Criteria. There are also national communications infrastructure for devices connected to smart-meters including interfaces with the different stakeholders involved such as the German Smart Meter Gateway and in the UK the so-called "Communication Hub". These are all examples where additional certification requirements are needed for a vendor to access the market of these countries.

Specific examples of fragmentation are widespread. For instance in the field of VPNs related network products, although VPNs are certified against a "collaborative" protection profile (cPP), meaning that the PP has been harmonized with International Mutual Recognition Arrangement, vendors wanting to access the French market have to undergo the additional CSPN certification process (and in some cases a completely new common criteria evaluation). This means that the VPNs requirements must be certified through national approval which in the French case will last from 6 to 9 month and the costs are estimated to around 80k euros as well as the EU approval process which is free of charge but takes 2 months to be completed.

Market fragmentation within the EU exists even for trust service products, which have been certified against US FIPS certification schemes. For Hard Security Modules initial certification of the crypto module acquired through the American FIPS), and the SOGIS members, via CEN, request for additional Common Criteria certificates with related vulnerability analysis. Some

European countries accept FIPS certifications for electronic signature products as equivalent to Common Criteria certified, yet other certify their products exclusively through the CC. The share of products certified with both systems, therefore allowing the vendor to sell its product in both US and European markets is even narrower.

Additionally for SSCD products, there are examples in SOGIS Member States where the original common criteria certification is not sufficient for national needs and the product has to undergo again the certification process of that country.

Respondents from National ICT Certification Authority pointed out the fact that fragmentation may exist even within the same country. This may happen as in the case of Italy, where procurement requirements may be established by administrative subject with a fair degree of autonomy. There is also a second example. In Italy, a public local authority (Provincia di Trento), in a public procurement procedure[1] has recommended the security certification of a video surveillance system according to Common Criteria (low assurance, i.e., EAL 1). Duration and costs of this security certification can be estimated in about 6 months and 20K euros.

The interviewees from smart meters industry provided some concerns on the future scenario of multiplication of national certification schemes for what concerns the industry of smart-metering if no action is taken. If MS continue not to accept each other Certification schemes, each MS will continue to improve its own Certification scheme and this could create a strong legacy making harmonisation more difficult. Furthermore, such fragmentation is also happening on the evaluation side. There are only limited number of Conformity Assessment Body that are able to certify against the requirements of different schemes. In this way, additional market entry barrier are created. The interviewers explained that the single most important barrier to trade for the smart metering industry are the costs for certification. Without specifying better the unit of analysis, the respondent stated that the cost of certification is about 1 million and the SMEs are out of this gain. In Germany, only one of the biggest smart-metering companies is starting a certification to enter other markets and all the other companies are present only in the German market".

5.2 Labelling and information asymmetry

Interviewees from several interviews addressed the issue of information asymmetry. For Semiconductors industry representatives the situation is today polarised between products for public security and consumers' product. For the former certification is long and costly and only the big company can manage such processes. At consumers' product level the requirements are lighter, but what is currently needed are solutions that are in between these two extremes. Currently, there is also the need to raise awareness about the importance of security using some forms of labelling schemes. On the other hand, according to some respondents the market problem is not one of fragmentation but rather of awareness and demand.

For Semiconductors industry representatives it is paramount to distinguish customers from users when trying to assess whether there is an information asymmetry with behavioural impacts. The final consumer is not well informed on the security properties of ICT products/services, this is due to a lack of awareness due to absent labelling. From the point of view of industry and government customers, the information in labelling schemes is likely to have an impact on its behaviour and purchases. An example can be found in cable TV that need to be connected to a router for internet connections, these products do not respond to specific security requirements and are vulnerable to hacker attacks. On the other hand, consumers are not aware of this kind of deficiencies, so they continue buying products without considering security requirements.

[1] Further details are not available

According to Smart meters industry representatives the situation on information asymmetry is different if we consider business-to-business products. The suppliers buy millions of meters and they of course have good understanding of security specifications of the products and in this domain labelling would not be of much use.

On the other hand, labelling and other means to reduce information asymmetry are important to increase trust in the public and the government should be very interested in this topic. The public opinion is more concentrate on privacy issues (e.g. personal data). For smart-meters, in UK, there is a display connected to the meters and consumers can simply read data on this display. There are devices connected with meters and you could be connected to the meters and read data where you want. The consumer decision to buy a product is often on the utility of the product. You should differentiate what products/device needs to be certified and what devices needs to be labelled.

5.3 Policy Option 1: Non-legislative "Soft-law" measures

Whilst some interviewees explained that voluntary labelling schemes and other non-legislative measures may provide some benefits to the industry, this policy option does not stands on its own feet as a way to address the main concerns of market fragmentation and information asymmetry.

On the positive note by letting the industry voluntarily put forward their own labels in coordination with public authorities it allow it to provide information to the users in a cost-efficient way.

The value of voluntary schemes and industry labelling initiatives is positive when considering the national level. Yet when considering cross-border trade of ICT products voluntary labelling approaches seem to pose additional problems. In fact, consumers may have awareness for labels existing at the national level but less so for labels from other countries, which do not abide to a certain degree of cross-country standardisation.

Furthermore, voluntary labelling initiatives may avoid some market inefficiencies that arise with regulated certification schemes, particularly for national or regional schemes that define standards and evaluation methodology and only recognise certain certification bodies within their own territory. Therefore, mandatory certifications which may introduce economic/administrative burdens could be limited by relying on voluntary schemes, which provide greater industry flexibility and rely on a lightweight system to demonstrate to their customers the security level of the products they market.

Against this background, labelling schemes without a sound legal and mandatory framework may lose their purpose in terms of trust and reliability. In fact, the deficiency of such non-legislative policy measures depends on the good will of the industry that adopt such measures and on the likelihood of providing trusted and reliable information to the users.

Labelling also depends on the user perception and quality of information. In fact, for the end-user such labels may lead to more confusion. If the label is too simple, the user could misunderstand the corresponding information. If the label is too complex, the user could be unable to understand it. With respect to business-to-business, marketing the impact of voluntary labelling may not be the most conducive argument in reducing market fragmentation and information asymmetry. When having to purchase very high quantity of products the certification behind the label and the security specifications of the product may be considered more important.

5.4 Policy Option 2: EU legislative act to extend SOG-IS agreement to all MS

To face the challenges of market fragmentation and information asymmetry in the ICT security sector the option of extending the SOG-IS agreement to all EU member states did not receive support from any of the interviewees.

The reasons are varied. For Smart meters industry representatives, decision-making between all EU countries may be too burdensome. At the moment SOG-IS goes up to EAL-4 and up to EAL-7 for specific domains. The challenge with SOG-IS is the unanimity of the Member State.
One critique addressed to the extension of the SOG-IS is that the agreement is based on the Common Criteria, which is not the right solution for ICS at the moment (please refer to Annex 7.4 for a developed overview of the criticism of the Common Criteria). Common Criteria costs 500k and lasts more than one year, which is a problem for a vendor. Common Criteria may be a good approach for some kinds of components and products. When the lifecycle of a product is longer than 20 years, we have to find approaches at a system level based on procedures and self-declaration.

The extension of SOG-IS agreement to all MS is not a valid policy option to be considered since there are Member States which are too small and for which the start-up and maintenance of a Certification Authority may be too costly. Not all countries have the ability to join the SOG-IS agreement. Therefore, there is a question of trust between governments. Procedures in France may receive more trust compared to certification procedure in other countries, making their activities superfluous and too costly.

5.5 Policy Option 3: EU general ICT security certification and labelling framework

According to the opinions provided by stakeholders interviewed, an EU ICT certification scheme could be a valuable policy options to face the challenges of market fragmentation and information asymmetry of ICT security products.

Representatives from ICT Certification Authority claims that there is an urgent need to establish a proper EU framework that will analyse, select and improve, where necessary, the acceptable approaches for EU wide certification, and will rationalize the certification decisions for both MSs and industry. Harmonizing will only be possible through technical exchanges between the MSs Schemes, which obviously relies on open certification approaches.

The interviewees from ICT Certification Authority think that a mutual recognition agreement of certification schemes existing in different countries have indeed a positive impact on industry costs. As remarked by the Certification Authorities, obviously a recognition agreement would eliminate the need and cost of re-certification in the domain covered by the agreement.

For Smart meters industry representatives it would be welcome to have one methodology on how you asses the risk, how you define security requirements and how you go through certification and a recognition across Europe. It is very important to have flexibility in certification scheme, determine on the risk connected to the product evaluated and the risk connected to the location of the product. Moreover, if MS continue not to accept each other Certification schemes, each MS will continue to improve its own Certification scheme and this will create a strong legacy to be later overcome in order to introduce a general EU framework.

Questions were also addressed on the institutional responsibilities that an EU management board of a possible EU wide certification framework would have. An interviewee explained that ENISA could play a role within industries to help to understand the concerns of the different national agencies. For smart-metering industry representatives, ENISA can play a key a role to harmonize Members States' Agencies on definition of national requirements and assurance, by making sure that the solutions meet the needs of the industry. ENISA should also cooperate with European and international standardisation institutions. Working with ENISA, it would be important to understand and harmonize the security language of the energy sector, in order to understand each other complementing both energy and smart-meters sectors. Therefore, representative from Smart meters industry explained it would be important to combine the approach of DG CNECT with the approach of DG ENERGY.

5.6 Institutional costs

Insights from the interviews to representatives of national ICT Certification Authorities as well as desk research on start-up and maintenance costs of institutions similar to ENISA have been done to provide the following estimates:

1. Costs incurred by an IT Certification Authority for the participation in the SOG-IS MRA
2. Costs incurred for the start-up of an IT Certification Authority
3. Costs incurred for the operational management of an IT Certification Authority
4. Costs estimated for the start-up of an EU wide ICT framework management board (6 months)
5. Costs estimated for the running of an EU wide ICT framework management board

These estimates are supported by a separate excel file listing the data entries and underlying calculations presented below in a more extended and narrative mode.

1.2.1. Costs incurred by an organization for the participation in the SOG-IS MRA

In relation to the costs incurred by an organization for the participation in the SOG-IS agreement the consortium asked its interviewees to provide the related break down of costs such as the ones to support harmonization activities and to participate into SOG-IS technical meetings.

Representative from National Certification Authority explained that MC meetings take place 1-2 times per year and the JIWG meetings 3-4 times per year respectively. The interviewee explained that on average the yearly travelling costs for **three members** attending **six meetings** are approximately **33 thousand euros**. In addition, for the preparation of meetings, attendance and national reporting the personnel cost estimated for 0,5 FTE of an Assistant is approximately **25 thousand euros**.

Therefore, for one of the Certification Authority that were interviewed the costs incurred for the participation in the SOG-IS MRA are approximately **58 thousand euros**.

1.2.2. Costs incurred for the start-up of an IT Certification Authority

Secondly, the consortium aimed at gathering data on the costs incurred for the start-up of an IT Certification Authority such as the costs related to staff competence building on ICT security certification, process setup, accreditation of Conformity Assessment Body and institutional communication etc.)

However for one of the interviewees it was impossible to provide any cost estimate for the start-up of the ICT Certification Authority as it was were created long time ago and most of the personnel initially involved is no longer operative. Moreover, in some cases, analytical cost records on IT Certification Authorities creation were not collected. However, the interviewee stated that the most time-consuming activities were related to drafting of IT Certification Authorities procedures and overall organization compliant to mandate received from the Government law and international standards.

Another interviewee from ICT National Certification Authority stated that costs estimate for setting up a Certification Authority is approximately **1.2 million** euros for 3 years. Total costs for the whole scheme, consisting of one Certification Authority and two ITSEFs (Conformity Assessment Body) is estimated to approximately **5 million Euros.**

1.2.3. Costs incurred for the maintenance of the operational management of a Certification Authority

Thirdly, we asked to ICT Certification Authorities representatives to provide some estimates of the costs incurred for the management of their institution (i.e. costs related to infrastructure and personnel, maintenance of technical expertise, management of the schemes etc.).

For one of the interviewees two main cost items must be considered. For the maintenance of the operational management of a Certification Authority, an organization needs 5 person/year. Work force is needed, on the one hand, for product certification activity, on the other hand for the management of the scheme at national level (initial accreditation and periodic reassessment of private Conformity Assessment Body, exams for evaluators and other experts assisting the scheme). The total personnel cost, considering the estimate of approximately 140 thousand euros for 2 Administrator (AD5) and 150 thousand euros gross (with taxes and contributions paid by the employer) for 3 Assistant (AST3), is **approximately 290 thousand euros**.

1.2.4. Costs estimated for the start-up of an EU wide ICT framework management board (6 months)

In the context of an EU wide ICT Security Certification Framework, the costs estimated by the Consortium for the start-up phase of a Management Board are described below, taking into account all the assumptions and data considered. However, the Consortium provides a raw estimate considering that a more detailed analysis would be necessary in order to have a more accurate capacity plan. The following proposal is based on a preliminary analysis of the existing ENISA organizational structure and desk research on the functioning of other European Agencies (e.g. EASA[2]).

As provided in the ENISA Regulation (EU) No 526/2013, the bodies of the Agency comprise[3]:

- A **Management Board:** The Management Board is ensuring that the Agency carries out its tasks under conditions which enables it to serve in accordance with the founding Regulation.
- An **Executive Board:** The Executive Board is preparing decisions to be adopted by the Management Board on administrative and budgetary matters.
- **An Executive Director**: The Executive Director is responsible for managing the Agency and performs his/her duties independently.
- **A Permanent Stakeholders' Group**: The PSG advises the Executive Director in the performance of his/her duties under this Regulation.

[2] EASA is the competent authority to issue type certificates for aircraft, to approve changes to the type design etc. Before issuing the certificate or approval, the Agency has the obligation to assess the design and that the applicant has demonstrated compliance. This can be done by a 100% check of everything, by sampling some parts etc.; in the end of this process the Agency needs to be "convinced" that that the design is safe (airworthy) and that it can legitimately issue the certificate / approval."Level of Involvement (LOI)" is a method / concept trying to formalise this checking / verification function. EASA does it already today, but not in a formalised, objective and transparent manner. Only few guidance is given by EASA to its staff members: based on his/her engineering judgement, experience with the applicant etc. The Agency has to determine its involvement on a risk based approach and will provide the criteria that the Agency should use in that exercise. The risk, as it will be defined in the law, is that a design is not compliant with the rule, because the Agency has not verified this part of the project, and that this non-compliance has an impact on safety. The objective is to focus in the future the resources to where it is necessary: where the highest risks are.

[3] https://www.enisa.europa.eu/about-enisa/structure-organization

A new Certification Unit or a specific team within one of the existing ENISA units (depending on the size of the team) would be necessary in order to ensure the functioning of an EU wide Certification scheme. Here after is presented a proposal of the new ENISA structure and organization, based on the information gathered during the first part of the activities and on a preliminary analysis of the existing European agencies (e.g. EASA):

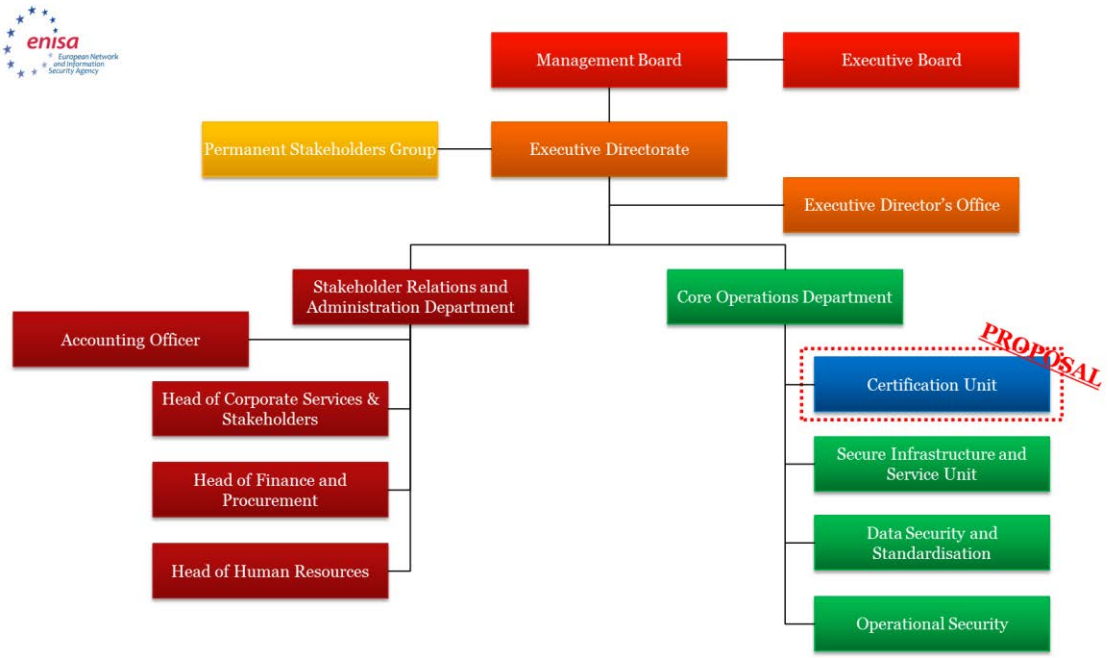


Figure – Proposal for the New ENISA Structure and Organisation

The start-up activity is estimated in 6 months. This phase would include all activities needed to set up the Framework, the definition of the organizational structure and responsibilities for each role. It would also include the definition of procedures rules and the terms of reference of the Board as well as the negotiation and validation with the Member States.

The corresponding main costs can be clustered as follows:

A. External Experts
B. Skills development and training
C. Website Creation

Taking into account all the data and assumptions shown above, the total cost estimated for the start-up phase is **280 thousand euros.**

Description	Unit #	Unit of measure	Occurance	Unit price	Sub-Total	Total	Cost Tipology
Expert	3	Person	1	€ 75.000,00	€ 225.000,00	€ 225.000,00	Event-based
Skills Development and training	**0,4**	**Person**	**1**	**€ 75.000,00**	**€ 30.000,00**	**€ 30.000,00**	One-time
Website Creation	**1**	**Price**	**1**	**€ 25.000,00**	**€ 25.000,00**	**€ 25.000,00**	One-time

GRAND TOTAL € 280.000,00

A) The major costs are related to Personnel expenditures. Three Experts would carry out the activities during the 6 months duration. The three external experts will have to be followed and coordinated by at least two ENISA employees that do not represent additional costs as they are already remunerated by ENISA. According to ENISA procurement rules[4], each selected Expert can be remunerated with a fixed fee of €450 per person-day plus any travel and subsistence related costs, which will be based on the European Commission's standard 'Daily allowance' or per diem rates for each European Country. To better estimate the travelling cost and allowances for each experts, the Consortium have taken into account a study specifically conducted for another EU Agency on the "Experts Meetings". During the start-up phase, considering for each experts 130 working days in 6 months, a very rough estimate of the total fee is:

   Total Fee for each Expert: 130 working days * 450€ + 11'000€ (Travelling cost estimate) + 5'000€ Allowances ≃ **75'000€**

   Travelling cost includes:

   - Tickets
   - Travel Agency Fees
   - Catering
   - Shuttle
   - Allowances (attendance fee, accommodation allowance, other transportation cost to be reimbursed)

   In addition to the travelling cost, 5 thousand euros of other Allowances (e.g. health insurance) are to be considered.
   Considering three Experts for the Start-up phase, the total estimated cost for personnel is **225 thousand euros**.

B) Moreover, during the start-up phase, cost for skills development and training of the new Administrators and Assistants of the Certification Unit must be considered. For this activities the estimate cost is approximately 0,4 FTE of an Expert for a total of **30 thousand euros**.

C) The estimate cost for the website creation is calculated considering two information: an interview with representative from National Certification Authority and desk research. During an interview with representative from National Certification Authority, the estimated cost for the creation of the website which includes a registry of all certification undertaken in that country is around 10 thousands euro. Assuming that the European Commission will story in its registry information concerning product certification of all EU countries and not merely information from a single country. A more reasonable estimate cost could be **25 thousands euros** which is based on the costs for this database characteristics[5]:

- **Number of pages**: 10 - 50
- **Style of design**: Moderately stylized
- **Copywriting # of pages**: 5-10
- **SEO w/ Placement Guarantee**: 30 keywords
- **Responsive Design**: Yes

[4] https://www.enisa.europa.eu/procurement/cei-list-of-nis-experts/technical-description-cei-list-of-nis-experts/at_download/file
[5] https://www.webpagefx.com/How-much-should-web-site-cost.html

- **Database Integration**: Full development
- **e-Commerce Functionality**: None
- **CMS**: Standard

1.2.5. Costs estimated for the running of an EU wide ICT framework management board

In order to consider different options for the maintenance costs of Institutions similar to ENISA in the context of an EU wide ICT Framework, costs related to the creation of a Management Board have been analysed.

In the context of the creation of an EU general ICT Certification scheme, representatives from National Certification Authorities expect not negligible costs to run a European certification boards. At least, the following costs should be considered: costs to produce/maintain the relevant competencies in the Framework (e.g., security specification, evaluation, certification), costs to call/launch ad hoc projects on relevant security requirements and corresponding security certification requirements, and costs for logistics. Costs could be in fact reduced to those needed to coordinate and/or extend pre-existing structures and/or tools and/or standards.

Interviewees from ICT Certification Authority said that a very quick estimation of manpower needed to run a European Certification board is not that obvious, however if we consider the existing SOG-IS MRA and EU Authorities (ENISA, JRC), ICT Certification Authority representatives suggest that a permanent secretariat of 5 people could support the MSs to:

- Organize the appropriate exchanges of strategies to address the certification needs in the EU and establish roadmaps
- Approve the certification methods considered applicable for EU certification and recognized by all MSs
- Offer a front office for new certification needs expressed by vertical sectors
- Publish certificates and promote certification activities

A proposal of the new Structure and Organisation of the new Certification Unit is shown below:

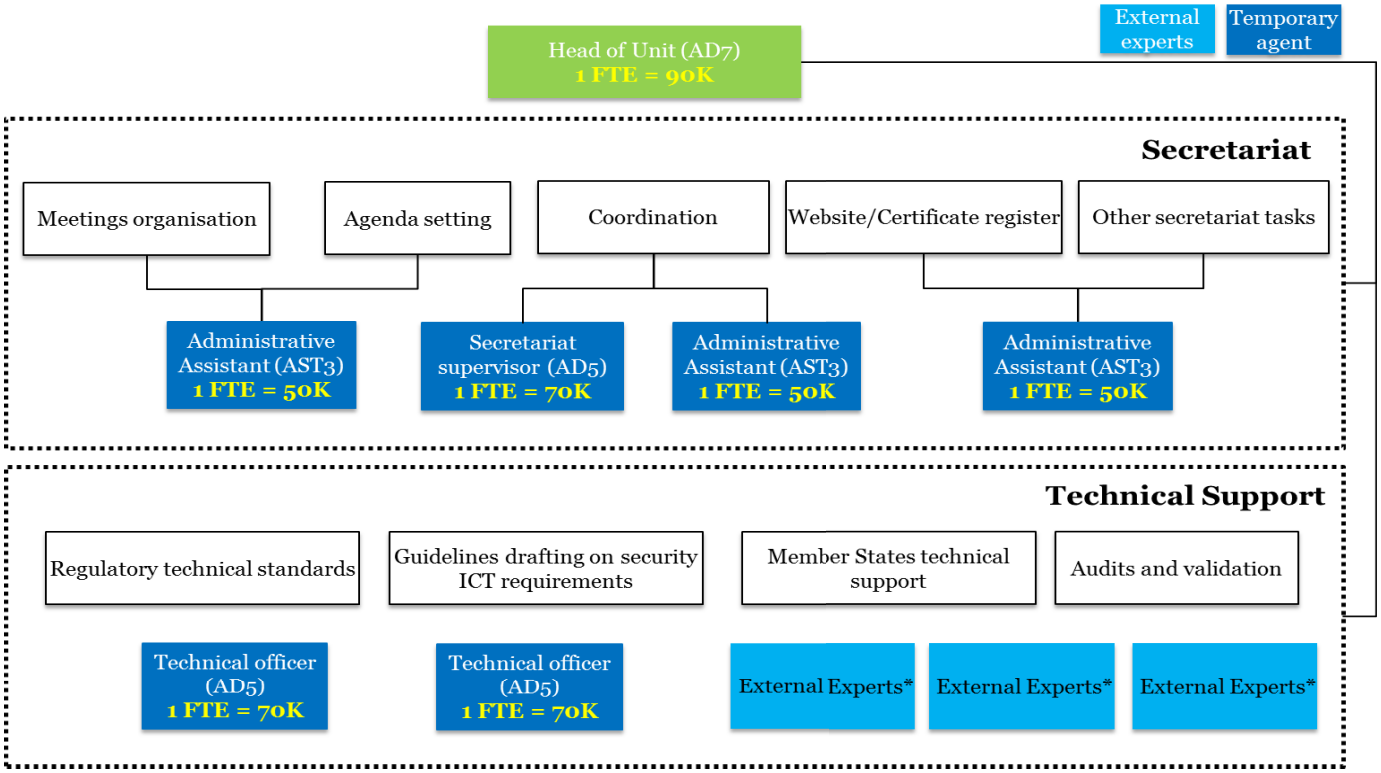


Figure - Proposal for the new Certification Unit

The new Certification Unit could be composed by:

- **1 Head of Unit (or Team Leader)**: For the estimate cost, the Consortium considered a salary for a Temporary Agent (AD7). The Head of Certification Unit will be responsible for maintaining relationships with ENISA Management Board as well as EU Member States and supervising the Secretariat Team and the Technical Support. **The total cost estimated is 90k/€ per 1 FTE.**

Under the Head of Certification Unit, the Secretariat will be composed by one Administrator Temporary Agent (AD5) and three Assistants (AST3) that will be responsible for the following activities:

- **Coordination:** coordinate department functions, identifying needs, information sharing
- **Meetings organization:** organize transfers and technical and/or support meetings to MS and industry
- **Agenda setting:** draft agenda and the decisions/opinions of the Board, maintaining relations with MS
- **Website/Register of Certificates:** maintain/update the website and the register of the certified products and the list of products under evaluation
- **Other secretariat tasks:** provide support to and/or participate in various (technical) meetings, working groups etc.

Assuming for the Administrator a salary of 70 thousand euros per year and for the Assistants a salary of 50 thousands euros per year , the total cost estimated for running and maintain the Secretariat is **220k/€ for** 1 Administrator (AD5) and 3 FTE Assistant (AST3).

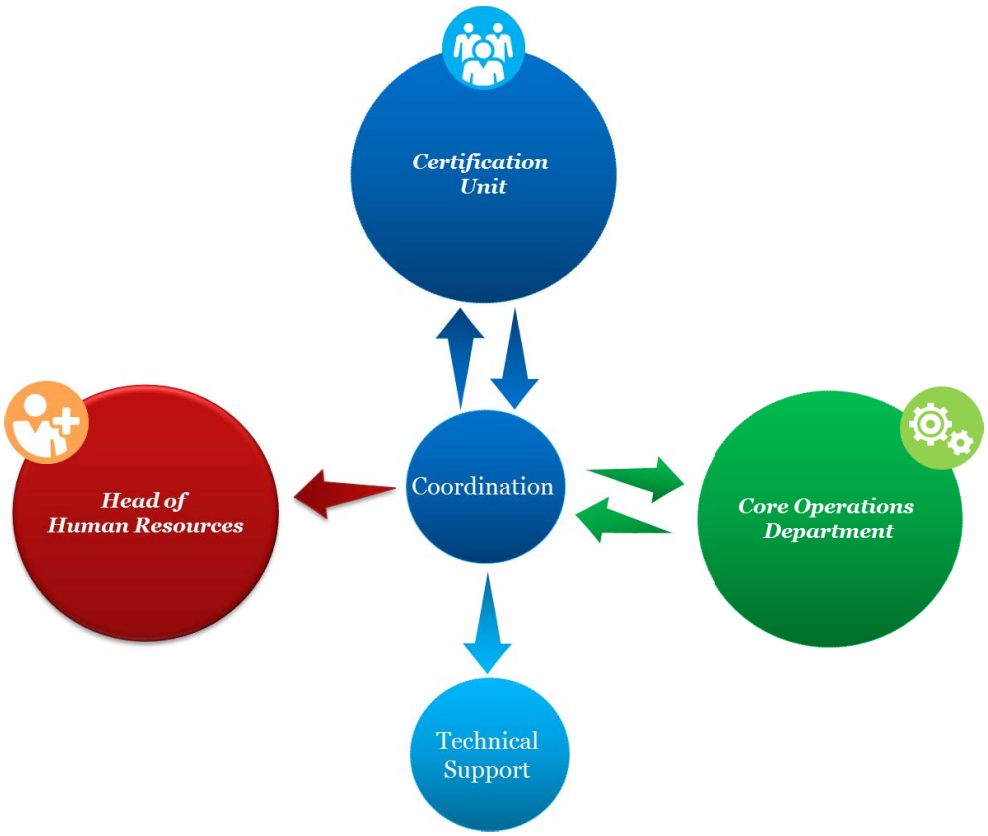


Figure - Roles Interrelationships

The Secretariat of the Certification Unit will need of Technical Support responsible for the following activities:

- **Regulatory technical Standards:** Responsible for evaluating standards and the certification scheme's security requirements, preparing and collecting reports
- **Guidelines drafting on security ICT requirements: involve industry and certification authorities stakeholders to draft guidelines on given ICT requirements**
- **Member States technical support:** Responsible for providing technical expertise to MSs (e.g.: MSs taking part in the framework on issues related to ICT Products
- **Audit and Validation:** Conduct audit on Conformity Assessment Bodies and Certification Authorities and validate the products/services certified

To run and maintain the Technical Support Unit, two Administrators and three External Experts must be recruited. Assuming for the Administrators a salary of 70 thousand euros per year and for the External Experts a salary of 75 thousands euros per year (Total Fee for each Expert: 130 working days * 450€ + 11'000€ + 5'000€ Allowances ≃ 75'000€ as explained in detail in the previous pages), the total cost rough estimation for running and maintaining the Technical Support is **365 thousand euros per year** for 2 FTE Administrator (AD5) and 3 External Experts.

In addition to the personnel cost, the following costs must be considered:

- Costs for meetings and events (e.g.: catering; rooms rent, etc.)

- Costs for travelling of ENISA Certification Unit personnel

ENISA could organize 6 major events per year with representatives from all Member State as actually organized by SOG-IS. The estimate costs for each events should be include at least:

- Catering
- Event Room Rent

Assuming for the Catering approximately 100 euros for each participants (including breakfast, lunch and dinner) and for the room rent an estimated cost of 500€ per day, the total estimate cost for 6 events of two day and 60 participants is **42 thousand euros**.

Moreover, audit activities must be undertaken by ENISA Certification Unit personnel on MS having national certification authorities. We assume that after the creation of an EU wide certification framework around 15 country of the total 27 EU countries will be audited. Considering for each travel abroad an estimated cost of 2 thousand euros per participants and considering an average of 15 travel per year, the total cost is **45 thousand euros**.

In the end, for minor meeting organised at the ENISA Headquarter, a light brunch could be offered. We estimate that in general for the working of an organisation such as ENISA in order to involve industry and certification stakeholders around 5-6 working meetings per month. In total 72 minor meetings per year could cost up to **1'440 euros.**

To have an overview of the estimated costs explained above, here after all the costs details are shown in table:

Description	Unit #	Unit of measure	Occurance	Unit price	Sub-Total	Total	Cost Tipology
Event Room Rent	2	Day	6	€ 500,00	€ 1.000,00	€ 6.000,00	Event-based
Catering for Event	60	Person	6	€ 100,00	€ 6.000,00	€ 36.000,00	Event-based
Catering for Meeting (ENISA Headquarter-based)	1	Day	72	€ 20,00	€ 20,00	€ 1.440,00	Event-based
Travelling Costs for Meetings abroad	1,5	Person wage	27	€ 2.000,00	€ 3.000,00	€ 45.000,00	Event-based
Head of Unit (AD7/9)	1	Person wage	1	€ 90.000,00	€ 90.000,00	€ 90.000,00	Recurring
Maintenance Costs - Secretariat (AD5)	1	Person wage	1	€ 70.000,00	€ 70.000,00	€ 70.000,00	Recurring
Maintenance Costs - Secretariat (AST3)	3	Person wage	1	€ 50.000,00	€ 150.000,00	€ 150.000,00	Recurring

Secretariat - Meetings organisation	0,5	Person wage	1	€ 50.000,00	€ 25.000,00	€ 25.000,00	Recurring
Secretariat - Agenda setting	0,5	Person wage	1	€ 50.000,00	€ 25.000,00	€ 25.000,00	Recurring
Secretariat – Coordination	1,0	Person wage	1	€ 70.000,00	€ 70.000,00	€ 70.000,00	Recurring
Secretariat – Coordination	1,0	Person wage	1	€ 50.000,00	€ 50.000,00	€ 50.000,00	Recurring
Secretariat - Website/Certificate register	0,5	Person wage	1	€ 50.000,00	€ 25.000,00	€ 25.000,00	Recurring
Secretariat - Other secretariat tasks	0,5	Person wage	1	€ 50.000,00	€ 25.000,00	€ 25.000,00	Recurring
Technical Support - Technical Support (AD5)	**2**	**Persone wage**	**1**	**€ 70.000,00**	**€ 140.000,00**	**€ 140.000,00**	Recurring
Technical Support - External Experts	**3**	**Person wage**	**1**	**€ 75.000,00**	**€ 225.000,00**	**€ 225.000,00**	Recurring
			GRAND TOTAL		**€ 788.440,00**		

Figure - Total estimate costs for the running of an EU wide ICT framework management board

1.2.6. Costs estimated for the running of an EU wide ICT framework managed by an Expert Group

In the context of the creation of an EU wide ICT Certification scheme, costs estimated for the running of an EU wide ICT Framework managed by an Expert Group have been also considered.

The costs for the **EU** institutions, **ENISA** and **Member States** coincide with the establishment and maintenance of this European Framework. In particular, the European Commission would have to place resources to support the establishment of the framework, notably for the adoption of the European schemes by means of delegated acts or implementing acts. It is estimated that this would require three FTEs working full time basis (e.g.two administrators and one assistant).

The EU institutions would also bear the costs related to the set up of the Expert Group. Typically, the Commission allocates 600 Euro per expert who will qualify for travel reimbursement. Since each Member State will appoint a representative, the total cost of the group is estimated to be in the region of 16,000 - 17,000 Euro per year.

ENISA is expected to bear the bulk of the costs related to both the functioning and maintenance of the framework, as it will be in charge of a) preparing the candidate schemes and b) issuing guidelines and c) providing the secretariat for the Group. The instituional costs related to ENISA are included in the economic estimates for ENISA (see Annex 6).

As an alternative to ENISA, it has been estimated that establishing a new body with the appropriate expertise in such a complex area would take between 5-7 years. Approximately, the costs of setting up a new European body amount to EUR 21,9 million. ENISA as the EU agency for cybersecurity with strong links with Member States has been considered to be best placed to ensure a coordinated and efficient approach to any European effort on security certification, for example by bringing all relevant stakeholders together, coordinating their work on certification schemes, preparing certification schemes and provide technical expertise.

Member States appointing a competent certification authority are expected to bear costs that would approximately amount to 1,600,000 Euro per year. This estimate include costs related to personel (e.g. min. three), equipment, subcontracting, operations (incl. training conferences) as well as set up of evaluation facilities. The operational management of a certification authority would also require investments for carrying out enforcement and supervision activities. Costs related to these activities are in the region of 290,000-300,000 Euro (per year). Generally, the overall impact will be significantly lower (or neutral) on Member States that are already part of the SOG-IS MRA and that have a supervision authority already in place.

This Option would not impose additional costs for the industry in the short term, namely because certification will remain essentially a voluntary tool. As is the case today, businesses will remain free to choose whether to certify their products or services. By contrast, the possibility to obtain an EU wide certificate would certainly act as a cost reductor for those firms that already certify their products or as an incentive for those that are willing to do so.

Since the process involved in future European schemes would depend on the associated level of assurance, cost and duration of certification would be more proportionate compared to the current SOG-IS MRA, built on the lenghtly and bureaucratic CC methodology.

5.7 Summary of the Interviews with Experts on Cyber Resilience of Critical Infrastructures

The following paragraph summarize the information gathered through interview activities to selected participants from these Critical Infrastructures Sectors:

- Finance
- Transportation
- Energy
- Telecommunication
- Healthcare

Questions were asked in order to cover the following areas of interest:

- Evidence of fragmentation
- Labelling and information asymmetry
- Advantages of adopting cybersecurity certification
- Cyber resilience of Critical Infrastructures
- Impacts of an EU wide ICT Security Certification and Labelling Scheme
- Costs related to Certifications

Almost the totality of interviewees from different critical infrastructures sectors agree that there are many advantages adopting security certified ICT components/products for Critical Infrastructures. For example, a security certified product allows the entrance to several markets that have particular requirements and gives advantages for the transparency of the information for the customer or the regulator. However, an interviewee from Finance Sector stressed that being compliant does not mean being safer. In fact, the Finance Sector is one of the most regulated sector in the world and operators need to be compliant with lots of National and International Requirements.

The fragmentation across Europe related to National and International ICT Security Certification Schemes is highlighted by many interviewees. One of the Scheme mentioned by interviewees is Common Criteria but it is stated that this Certification Scheme does not work and it is little used to certify critical infrastructure products or components. Moreover, the certification processes are too difficult to go through because there is too much bureaucracy and paper forms to fill and the related costs are too high. An interviewee from Communication Sector said that in 2016 they requested 20 Common Criteria certifications with a cost of several hundred thousand euros each, including the external resources, laboratories etc.

Two clear examples of fragmentation are related to the French National Certification Scheme developed by ANSSI and the German National Certification Scheme developed by BSI. These two National Certification Schemes do not recognise each other. Another example mentioned is the National Certification Scheme recognised only in UK. An interviewee from Communications Sector said that his company needs to be certified on a variety of schemes in order to provide their service. In UK, there is the CAS(T) scheme, which is a telecom specific version of ISO27001 and that is a fundamental security certification for any product and service that is sold. Furthermore, the Public Services Network need to be certified every year as a prerequisite. It will not be possible to sell services in UK, without certifying them. For the same company, costs related to these certification are very high. For example, for one of thei network platform the overall budget was of 500 thousand UK pounds. It includes 39 different services, whose price range from 10 to 15 thousands UK pounds each. CAS(T) Certification, an equivalent of the ISO 27001, it is issued by the National Cyber Security Council and it is valid only for the UK. Therefore, it is more UK centered and not European. Furthermore, there are actually a lot of standards for products' security certification. There are at least four schemes that are run by the UK National Technical Authority. They range from test marking, encryption etc. and there is no doubt that the cost of certification would be a barrier for vendors who want to enter the UK market.

A representative of an association of critical infrastructure stated that in Italy there isn't any mandatory certification but it is necessary to be compliant with Standards and National requirements. For example, as stated by interviewee from the Communication Sector, there are lots of products and components such as firewall, IPM, intrusion detection systems, routers with different criteria and standards that are required. In

some cases, multiple certifications are necessary because other markets require them. For example, in France, it is requested an authorization issued by the Prime Minister Office for network devices used in Critical Infrastructure. It is common for government to require certain standards for Critical Infrastructure and security products and services.

In the Finance industry services must have secure encryption and the use of Hardware Security Module (HSM), which are incredibly expensive. In order to use a HSM component, the cost is around 20 thousand euros and it is a cost for a single component, not for the whole device.

The fragmentation of ICT Security Certification Schemes combined with the increase of National Approaches across Europe are defined by interviewees a real market problem. Without a European wide Certification Framework, it would be very difficult to sell products in more than one European Country especially for small and medium companies. It is important however that the requirements of the certification are appropriate.

Critical infrastructures are by definition more critical than IoT, in general. However, the fragmentation is a common theme for both of them and it is unhelpful. Interviewees stated that the best solution to solve such fragmentation would be a moderate option that keeps in consideration both the European Market and each jurisdiction. According to representatives from Telecommunication Sector, it would also be positive if European Commission, instructed by ENISA, could define a set of best practices.

Regarding the lack of information related to security requirements of ICT products and components, according to all interviewees, an EU wide Certification and Labelling Scheme could be a valid instrument to raise the awareness and trust of customers. Interviewees stress that customers should be divided in companies and end-users. Companies are generally more aware on security requirements of ICT products purchased than the end users are. This is due also to the different nature, cost and complexity of the product that are purchased. There are medical devices that are expensive and complicated machines, which can be bought only by operators (for example, Tomography machines cost approximately one million euros). Before an operator buys such an expensive machinery, surely it will ask for more information about security requirements than a normal user that wants to buy a medical smart device that measures the level of glucose.

For critical infrastructure operators it is crucial to have the correct information about security tests made on certified products or information related to security requirements. As argued by an interviewee of Communication sector without a certification applied it is difficult to know if the information provided to the customer/end-user are true and complete. Each company could claim that their product is secure but it is better to have third parties to test it independently. Without any information related to security requirements of ICT/IoT products, the choices are based merely on the producer name. The company brand from which consumer purchases the components is like a security guarantor. For instance, buying from Scheneider Electric and Siemens is probably more reliable than purchasing from a Chinese producer. There is, however, an issue to point out: most of systems and products on the European Market have embedded components that come from China where the security standards are less available to check. An appropriate EU labelling Scheme for ICT/IoT products could reduce these problems. Interviewee from Communication Sector said that, during the last year, his company discussed on the idea of IT trust labels for devices. They believe that a Labelling Scheme could be a more effective solution, especially for critical infrastructure. Also for a representative of Transportation and Logistic sector, the current situation with the lack of transparency of security requirements could still be improved. Making the information more available and clearer would definitely help the operators and avoid certain situations. If the label would be reassuring for the customer, it would also increase the trust in the company.

The totality of the interviewees agreed that a European cybersecurity certification Framework that support the mutual recognition of cybersecurity certification would have a positive impacts. However, it is important to establish in a proper manner what are standards, minimum security requirements to adopt and the evaluation processes of the laboratories. For an expert on cyber resilience of critical infrastructures, having multiple certification laboratories is very expensive. It is required to prepare the maintenance staff of these structures and, with an EU wide Certification Scheme, it would be possible to reduce these laboratories. It will be therefore possible to reduce costs related to laboratories on the long term.

Representative from a Transportation and Logistic association claims that an EU wide Certification Scheme would not only increase the security levels of all Member States but it would also be good for the European market. Even in this case, however, it is stated that the EU wide Certification Scheme has to be made in a proper manner: the certification needs to be designed based on the needs of the industries and the Member States. Moreover, the mutual recognition across EU might even have positive effects globally. An EU wide Certification Scheme could attract other non-European countries to join the mutual recognition. States like US and Canada and many others might be interested in the future to join such mutual recognition. All interviewees stated that it is also important that an EU wide Certification scheme would not be a mandatory scheme.

Another example, related to cybersecurity and the actual European ICT landscape, comes from Cloud Computing Services. Interviewees from Finance, Energy and Telecommunication Sectors stated that there is a barrier from using Cloud Services considering that, without clear and mutually recognized security requirements, companies have not perception of data stored in a secure way, especially according to the various jurisdictions. Most of the banks are struggling with this challenge. There are many problems because the European data might be stored in South America, or in another Country, under a different jurisdiction and with different perception of security. If Cloud Services would be certified under an EU wide Certification Scheme, it would be easier to be compliant and more confident about the respect of common security requirements.

6. Work Plan

This chapter of the Interim Report is based on the submitted Inception Report, and briefly summarizes how activities were undertaken in the first reporting periods and the extent to which they coincided with Tasks as planned. Furthermore, also key issues and how they were tackled are included.

The timetable represented here below (Overall Gantt chart) illustrates the general scheduled work plan for carrying out the whole project, as agreed within the Inception Report, with the red line indicating where we currently stand:

Overall Gantt Chart

Sub-Task	Description	May			June				July				August				September				October	
		W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15	W16	W17	W18	W19	W20	W21
	Task 0 – Project Management																					
0.1	Organisation and management of project meetings	IM						FIM														
0.2	Submission of deliverables and quality control	IRd	IRf		FIRd	FIRf			SIRd	SIRf	FRd	FRF										
0.3	Regular reporting to the EC																					
	Task 1 – Gather the evidence base																					
1.0	Project set up		IRf																			
1.1	Desk Research & Field Work																					
	Literature / Input analysis provided by the Commission																					
	Desk Reasearch																					
	Stakeholders re-mapping																					
	Interviews/ Online Questionnaire																					
1.2	Mapping and assessment of existing certification and labelling schemes																					
1.3	Problem definition and assessment																					
1.4	Analysis of the baseline scenario and its evolution				FIRd	FIRf																
	Task 2 – Assess the impact																					
2.1	Classification and analysis of the impacts of each policy option																					
2.2	Comparison of options and elaborating the preferred one								SIRd	SIRf	FRd	FRF										
2.3	Desk Research; interviews to new stakeholders; definition of three case studies																					
	Task 3 – Other specific tasks																					
3.1	Economic annex explaining the analytical model																					
3.2	Support in answering to specific requests coming from the Board																					
3.3	Elaboration of the intervention logic																					
3.4	Follow-up of the submission of the IA to the RSB																					

1.1. Update on Project Tasks

We have been following clear and logical procedures at all stages of the engagement until now. Below we outline, in reference to each of the foreseen Tasks, main activities carried out, including those methodological elements that characterized these Tasks. Furthermore, at the beginning of each paragraph describing the Task, we have detailed each one of them in a number of more operative Sub-Tasks, indicating for each of them their implementation status.

1.1.1. *Task 1: Evidence Gathering and Analysis*

Macro-Task 1 will be broken down into five sub-tasks (1.0, 1.1, 1.2, 1.3 and 1.4) each one containing the various activities indicated with letters in the ToR. Task 1 will involve the following sub-tasks:

Task 1: Evidence Gathering and Analysis	Implementation status
Sub-Task 1.0: Project set up	Completed
Sub-Task 1.1: Desk research and Field work	Completed
Sub-Task 1.2: Mapping and assessment of existing certification and labelling schemes	Completed
Sub-Task 1.3: Problem definition and assessment	Completed
Sub-Task 1.4: Analysis of the baseline scenario and its evolution	Completed

Here below the implementation timetable referring specifically to project Task 1, dedicated to Evidence Gathering and Analysis.

The output consisted of addictions and integrations to what has been described in literature provided by the commission (e.g. JRC report, ENISA questionnaire), a desk research activity, an ongoing activity which consists in interviews of the main stakeholders mapped (mainly Certification Authorities, smart meters and semiconductors representatives). Furthermore it has been conducted a depth analysis of the problem definition and the baseline scenario and its evolution, using the output coming from the above mentioned evidences gathered.

Task 1 Timetable – 5 Weeks

Sub-Task	Description	May			June				July
		W1	W2	W3	W4	W5	W6	W7	W8
	Task 1 – Gather the evidence base								
1.0	Project set up		**IRf**						
1.1	Desk Research & Field Work								
	Literature / input analysis provided by the Commission								
	Desk research								
	Stakeholders re-mapping								
	Interviews/Online Questionnaire								
1.2	Mapping and assessment of existing certification and labelling schemes								
1.3	Problem definition and assessment								

1.4	Analysis of the baseline scenario and its evolution				**FIRd**	**FIRf**			

Sub-Task 1.0 Project set up

As part of the Project set up, Pwc & FUB delivered on the 17th of May 2017, the Draft Version of the Inception Report to the DG CNECT Team one day before the inception meeting. The goal of the Inception Meeting at week 1 was to scope the methodology, resources and objectives, which have been initially proposed in the technical offer and thanks to a preliminary data collection. This was necessary to set out, share and validate the approach to be followed throughout the whole duration of the study, laying out the grounds, in particular to the mapping and assessment of existing security certification and labelling schemes, the problem definition and assessment as well as providing the discussion over the policy options.
Following the Inception Meeting, the Inception report has been finalised taking into account all observations and comments raised at the meeting and delivered on the 19th of May 2017.

Sub-Task 1.1: Desk research and field work

The goal of the data gathering activities was to find quantitative data or estimates, experts' views, and any kind of useful information on:

- State of play of certification and labelling frameworks by Member States, including level of diffusions, their key features (i.e. self-regulation vs. mandatory frameworks), level of success and their added value
- Evidence of obstacles to cross-border trade and market fragmentation stemming caused by fragmentation in national certification framework
- Costs (i.e. cost and duration of certification procedure) and benefits (for final users and as positive externality for the Digital Market Strategy) of certification frameworks (see later our typology)

DG CONNECT has provided a list of sources to be examined that include also the results of workshops organized by DG CONNECT with stakeholders in the previous months. In addition to the sources provided and listed above, one market study elaborated by PwC integrated.

During the first preliminary meeting, on the 8th of May 2017, and the kick off meeting, on the 17th of May 2017, the DG CNECT Team has highlighted the need to have within the Draft Interim Report the analysis of all the evidences supporting the impact assessment. It was therefore asked to focus on the documentation provided by DG CNECT and for this reason the activities to be carried out has been reorganized as follows:

1.1.0. Literature / Input analysis provided by the Commission;

1.1.1. Desk Research;

1.1.2. Re-mapping of key stakeholders not yet engaged in past activities and organization of related interviews;

1.1.3. Interviews/Online Questionnaire.

Since the beginning of the project, we have been working to identify and validate a list of the stakeholders who are directly or indirectly impacted by the project. The list has been updated and enriched several times during the first weeks. An updated release of the stakeholders map is included already now in Annex.

This fundamental database represented a key element to identify Certification Authority agencies and the representatives of the main industrial sectors participating to the interviews and questionnaire, to identify evidences supporting the analysis. When identifying key stakeholders, we have been taking into account the following:

- Geographical coverage (EU 28 MS),
- Coverage of the various types of stakeholders (Certification Authority Agencies, Industries, etc.)
- ICT vendors,

- Policy makers.

To get more resources in support of *Literature / input analysis provided by the Commission*, the Consortium requested to have access to a study on cloud computing certification, the study is not completed and the Consortium had a preview of the ongoing activities. Furthermore, within the Report have been included preliminary data coming from the study on the Cyber Security Industry Market Analysis (CIMA), conducted by PwC and LSEC. This study is not yet completed and the data included by the Consortium within the present report are the very first information shared and updated at the 6th on June 2017.
As regard the results of the 2017 Enisa Survey, the DG CNECT Team shared the results with the Consortium and these results are part of the analysis included within the previous chapters.

The chapter of this report, named Stakeholders' support, contains a synthesis of the interviews conducted so far and, it gives an overview of the point of view of the main stakeholders involved. In addition to the interviews, the Consortium has prepared a Questionnaire (see Annex 7.2) sent to all stakeholders mapped during the first two weeks of the project, which aimed at gathering more evidences. The due date to submit the said Questionnaire was the 19th of June, the Annex includes also the results gathered.

Sub-Task 1.2: Mapping and assessment of existing certification and labelling schemes

Evidence on the current state of the art in the 28 EU countries and selected extra EU countries has been identified and provided, performing a systematic research of secondary sources on the following:

- Available materials (from e.g., EU project CRISP, ENISA, BSA) that formed the initial reference for relevant entities in cybersecurity (and, hopefully, for the derivation of the cybersecurity certification status) in EU (and outside).
- Missing data gathered on the basis of explorations by the above mentioned questionnaire and interviews submitted to selected stakeholders in specific and impacted industry sector (mainly smart meters, semiconductors, Certification Authorities, etc.)

As highlighted by the DG CNECT Team during the Inception Meeting, on the 8th of May 2017, the specific theme of labelling will be discussed in September.

Sub-Task 1.3: Problem definition and assessment

Sub-Task 1.3 has been developed performing the following phases:

Analysis of the state of play and why EU intervention is needed (or not);

A preliminary qualitative assessment of the current fragmentation and its costs has been developed during these weeks, to perform the test prescribed in impact assessment to ascertain whether EU action is required. Practical examples and specific cases to prove the market fragmentation have been gathered and it is presented within this report. The activity is ongoing and it will be completed within the 19th of June 2017.

Further Development

Based on the documents/data/information that the Consortium have analysed, it has been developed and improved the evaluation of the core problem and its whole definition.

Sub-Task 1.4: Analysis of the baseline scenario and its evolution

The approach used to develop scenarios started from the definition of gaps, needs and state of play. The trajectories that the State of Play Model pointed out, as well as the analysis of barriers and needs, interpreted in terms of how they can evolve in terms of trends. The scenarios, thereby, investigated the type(s) of future(s) to which these trends may lead following the various steps explained in the following.

The trend analysis followed five steps:

1. **Identify the main trends**. The trends has been derived from the baseline and state of play, which also shaped by the general description framework.
2. **Classification of the trends**. This step required that trends have been clustered using an uncertainty - impact matrix. The rationale is that trends having a high uncertainty and high impact may result in contradictory and alternative futures and thus feed into different scenarios. On the contrary, trends having a high impact and low uncertainty should result in one type of future that has been forecasted. Trends with expected low impact are irrelevant and has not be considered.
3. **Organization of trends**. The trends classified as having a high uncertainty and high impact has been organized and clustered into a limited number of key uncertainties that defined a number of key dimensions (possibly two). These dimensions are the variables of the scenarios axis. In doing so trends related to each other will be merged into key uncertainties having a high impact.
4. **Derive concerted scenarios**. By combining the key dimensions of uncertainties (each one taking an extreme value), a number of scenarios has been derived. Each scenario has been given a typical, easy-to-recognize, and understandable name.
5. **Develop scenario stories and description**. The last step aimed at enabling communication of the scenarios. An easy to read and understandable sketch or story will be of each scenario, as well as the values taken by the main aspects (contextual macro-level environment, transactional environment, technology, etc.)

1.1.2. Task 2: Assess the impact

During Task 2 will be provided quantitative and qualitative empirical evidence of the likely economic, social and environmental impacts of each of the identified preliminary options. Task 2 has been broken down into two sub-tasks detailed as follows:

Task 2: Assess the impact	Implementation status
Sub-Task 2.1: Classification and analysis of the impacts of each policy option	**Closed**
Sub-Task 2.2: Comparison of options and elaborating the preferred one	**Closed**
Sub-Task 2.3: Desk Research; interviews to new stakeholders; definition of three case studies	**Closed**

The Sub-Task 2.2 is ongoing considering that, during the interviews, the Consortium has started to gather, from the main stakeholders, data and information on the options proposed by the European Commission.

Here below the implementation timetable, referring specifically to project Task 2, dedicated to assess the impacts:

Task 2 Timetable – 10 Weeks

Sub-Task	Description	June				July				August				September				October	
		W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15	W16	W17	W18	W19	W20	W21
	Task 2 – Assess the impact																		
2.1	Classification and analysis of the impacts of each policy option																		
2.2	Comparison of options and elaborating the preferred one					**SIRd**	**SIRf**	**FRd**	**FRf**										
2.3	Desk Research; interviews to new stakeholders; definition of three case studies																		

Sub-Task 2.1: Classification and analysis of the impacts of each policy option

As agreed with the European Commission DG Connect Team, this activity is currently drived and performed by the Commission and the Consortium is supporting through the evidences gathering and an in depth analysis of the information gathered throw the interviews conducted.

Within this inception report, it has been drafted a previous potential impact analysis for each policy option identified by EC.

Sub-Task 2.2: Comparison of options and elaborating the preferred one

The overall objective of the comparison of options is to provide an overview of the positive and negative impacts of each policy option with regards to the objectives. This comparison, using a multi-criteria analysis, will help us to compare the different policy options in terms of effectiveness, efficiency and coherence

concerning the delivery of the policy objectives as well as prepare evidence and recommendations for decision-making.

The comparison of policy options is consisting in:

- Summarising positive and negative impacts for each policy option;
- Comparing policy options in terms of effectiveness, efficiency and coherence according to the results of task 1;
- Ranking the options by order of preference and recommend a preferred option.

Sub-Task 2.3: Desk Research; interviews to new stakeholders; definition of three case studies

In order to gather more information to be used for the impact assessment, the Consortium has organized a second phase of direct interviews and a second online questionnaire specifically designed and structured for Critical Infrastructures (which include organizations coming from transportation, healthcare, energy, finance, telecommunication sectors). Considering that the questionnaire has been submitted at the end of July, a complete overview of the results would be consultable in the first week of September. As regards the interviews the main results have been included within the present report.

The report includes three case studies specifically defined through the interview conducted and an additional desk research. The case studies regard:

- Smart Meters industry
- Alarm Systems industry
- Cloud Computing services

1.1.3. *Task 3: Other specific tasks*

During this Task 3 we have to provide additional elements/services in order to support the Commission through the following actions:

1. Provide the economic annex referred to in the Better Regulation Toolbox (Tool #8), explaining the analytical models used in preparing the impact assessment;
2. Assist the Commission in establishing an adequate implementation plan for the preferred policy option;
3. Assist the Commission in the elaboration of the intervention logic linking the identified problems with the problem drivers and the policy options and in the drafting of the main charts and tables to be included in the impact assessment;
4. Support in the follow-up of the submission of the impact assessment study to the Regulatory Scrutiny Board (RSB) of the Commission (in particular in helping to respond to questions from the RSB).

The following sub-tasks:

Task 3: Other specific tasks	Implementation status
Sub-Task 3.1: Economic annex explaining the analytical model	**Ongoing**
Sub-Task 3.2: Support in answering to specific requests coming from the Board	**Closed**
Sub-Task 3.3: Elaboration of the intervention logic	**Closed**

Sub-Task 3.4: Follow-up of the submission of the IA to the RSB	Ongoing

Here below the implementation timetable, referring specifically to project Task 3, dedicated to additional elements/services aimed at supporting and assisting the European Commission:

Task 3 Timetable – 15 Weeks

Sub-Task	Description	May	June				July				August				September				October				November				December		
		W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15	W16	W17	W18	W19	W20	W21	W22	W23	W24	W25	W26	W27	W28	W29	W30
	Task 3 – Other specific tasks																												
3.1	Economic annex explaining the analytical model																												
3.2	Support in answering to specific request coming from the Board																												
3.3	Elaboration of the intervention logic																												
3.4	Follow-up of the submission of the IA to the RSB																												

Sub-Task 3.1: Economic annex explaining the analytical model

With specific reference to the economic impacts, in the present subtask we are developing an economic annex to the impact assessment report with detailed explanations on the analytical models used in preparing the impact assessment.

More precisely, for each of the analytical model used we are defining an explanation box with technical explanations (in accordance with the ToR - Section 5.1 “Deliverables”) containing, at least, the following main information about the model:

- a brief description of the model;
- the model developer and nature (public/private/open source) of the model;
- model structure and modelling approach with any key assumptions, limitations and simplifications;
- intended field of application and appropriateness for the specific impact assessment study;
- model validation and peer review with relevant references;
- the extent to which the content of the model and input data have been discussed with external experts;
- explanation of the likely uncertainty in the model results and the likely robustness of model results to changes in underlying assumptions or data inputs;
- explanation as to how uncertainty has been addressed or minimised in the modelling exercise with respect to the policy conclusions;
- the steps taken to assure the quality of the modelling results presented in the IA;
- a concise description of the baseline(s) used in the modelling exercise in terms of the key assumptions, key sources of macroeconomic and socio-economic data, the policies and measures the baseline contains and any assumptions about these policies and measures.

Sub-Task 3.2: Support in answering to specific request coming from the Board

In order to assist DG CNECT in answering to the Board comments and requests, we have supported the team in respond to the main comments received. To achieve this purpose the Consortium contacted again some of the main stakeholders and add information through desk research activity.

Sub-Task 3.3: Elaboration of the intervention logic

Underlying causes (or "drivers") of the problems identified in the task 1 “Evidence Gathering and Analysis”, the present subtask supported in the elaboration of the “intervention logic” as the link between problem-drivers and policy options.

The intervention logic model that we have developed to justify the public policy action is a method used to explain of what the intervention - the policy proposals - is meant to achieve (the objectives) and how it is supposed to achieve it (the tools). The intervention logic regroups all the activities, expected effects and assumptions of an intervention. It also presents in a clear way how the policy will lead to the intended effects in the present and future context.

Developing the intervention logic, we have taken into account that it may evolve over time according to the political, economic or social context. This implies that the intervention logic model may need to be reconstructed several times, for successive periods to fit in with developing events.

During this sub-task, the intervention logic has been detailed for the policy option that results as the preferred option considering the ranking.

Sub-Task 3.4: Follow-up of the submission of the IA to the RSB

After the draft Impact Assessment has been produced, the Regulatory Scrutiny Board (RSB) will scrutiny it in order to assess the quality and provide recommendations on how this draft report should be improved by the Commission services. As part of the Commission’s renewed commitment to better regulation, a new Scrutiny Board has been established, replacing the Impact Assessment Board, with the aim of strengthening the existing system of quality control.

The new Regulatory Scrutiny Board will scrutinize the quality of all impact assessments, major evaluations and fitness checks of existing legislation and issue opinions on the draft of the related reports in line with the relevant guidelines. According to the Commission’s Working Methods 2014-2019 any impact assessment should be accompanied by a positive Board opinion before an initiative can proceed.

Our support in this task will consist in helping to respond to RSB questions concerning the impact assessment study already submitted and in supporting the commission services in the follow of the RSB recommendations considering that the activities have to be finalized within the end of September.

1.1.4. *Task 0: Project Management*

This Task is focused on the provision of ongoing project management services throughout the duration of the project. In detail, project management activities are involving the following three Sub-Tasks, together with the production of most of the foreseen project Deliverables:

- **Sub-Task 0.1**: Organisation and management of project meetings
- **Sub-Task 0.2**: Submission of deliverables and quality control
- **Sub-Task 0.3**: Regular reporting to the EC

Here below the implementation timetable, referring specifically to project Task 0, dedicated to project management and coordination activities:

Task 0 New timetable 1 – First 15 Weeks

Sub-Task	Description	May			June				July				August			
		W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15
	Task 0 – Other specific tasks															
0.1	Organisation and management of project meetings	**IM**						**FIM**								
0.2	Submission of deliverables and quality control	**IRd**	**IRf**				**FIRd**	**FIRf**	**SIRd**	**SIRf**	**FRd**	**FRF**				
0.3	Regular reporting to the EC															

Task 0 New timetable 2 – Second 15 Weeks

Sub-Task	Description	September				October	
		W16	W17	W18	W19	W20	W21
	Task 0 – Other specific tasks						
0.1	Organisation and management of project meetings						
0.2	Submission of deliverables and quality control						
0.3	Regular reporting to the EC						

Sub-Task 0.1: Organisation and management of project meetings

The kick-off meeting took place in Brussels on the 17th of May 2017. Furthermore, in order to ensure frequent communication with EC Team throughout the entire project, conference calls have been scheduled during the first weeks with EC Project Manager in order to discuss project activities, progress on deliverables and any other key issues.

The main project Reports already presented, include the Inception report (D1), delivered at the beginning of engagement activities (on the 19th of May).

Sub-Task 0.2: Submission of deliverables and quality control

All deliverables are going through a rigorous quality review process covering both scientific excellence and standard of English. Feedback received during Project Meetings has been and will be considered and the reports duly amended.

Sub-Task 0.3: Regular reporting to the EC

The Team Manager will lead regular reporting on behalf of the entire team to the Commission, primarily through day-to-day email exchange as well as regular project status report via conference calls.

Meetings and Reports

A number of meetings are foreseen to ensure discussions on the most important project issues. Meetings will be relevant to each deliverable.

The main project Reports already presented, include the Inception report (D1), delivered at the beginning of engagement activities and the First Interim Report (D2), the Second Interim Report (D3) and the present and Final Report. The final study report summarizes how activities were undertaken and the extent to which they coincided with tasks as planned. Key issues and how they were met will be included. The Final study report will show key conclusions and all information gathered so far.

7. Annex

7.1 Minutes of the interviews

June 7, 2017

Interviews results from representative of a National ICT Certification Authority

1- Do you know EU cases where an ICT product/service is requested or recommended to be equipped with a given security certificate in order to enter the market of a given MS?

In all EU MSs, a security certification is requested in the digital signature context, namely for secure signature/seal devices as defined in EIDAS regulation[6]. As specified in EIDAS secondary legislation[7], this is a security certification according to "Common Criteria EAL 4+" with given Protection Profiles. The corresponding duration and cost are in the order of 18 months and 100K euros. Notice that, in Italy, a procedure has been established to cover cases where the Protection Profiles mentioned before cannot be used. The Italian procedure is still based on Common Criteria EAL4+ as well.

2. Do you know cases in the EU, where national approaches for the security certification of any ICT products/services have been/are being established?

Yes. In Italy, based on the national decree DPCM 17 February 2017[8], 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.

3. Do you know EU cases, where a customer is not provided with enough/reliable information about the security properties of any ICT products/services?

Yes. The provided information is usually not reliable enough. Notice that, to improve the situation, a security certification is a necessary but not a sufficient condition. A significant solution would be to have a security certification against security requirements established by super partes bodies and possibly recommended by statutory authorities.

[6] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union L 257, 28 August 2014.

[7] Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, Official Journal of the European Union L 109/40, 26 April 2016.

[8] 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)

4. Do you think a mutual recognition agreement of certification schemes existing in different countries may have a positive impact on industry costs?

Yes. Clearly, a recognition agreement would eliminate the need and cost of re-certification in the domain covered by the agreement.

5. In the context of the possible creation of a European ICT security certification Framework, building on existing ICT certification mechanism, such as SOG-IS MRA, what do you think are the estimation of costs needed to run a European Certification Board?

I expect not negligible costs. At least, the following costs should be considered: costs to produce/maintain the relevant competencies in the Framework (e.g., security specification, evaluation, certification), costs to call/launch ad hoc projects on relevant security requirements and corresponding security certification requirements, and costs for logistics.

Interviews results from representative of a National ICT Certification Authority

1- Do you know EU cases where an ICT product/service is requested or recommended to be equipped with a given security certificate in order to enter the market of a given MS?

Yes. In Italy, a security certification is requested for secure signature/seal devices. In fact, due to EIDAS[9], this applies to all EU countries. As specified in rules for EIDAS implementation[10], the security certification has to be executed according to "Common Criteria EAL 4+" with given Protection Profiles. Duration and cost can be estimated in about 12 months and in the range of 50K-100K euros.

There is also a second example. In Italy, a public local authority (Provincia di Trento), in a public procurement procedure[11] has recommended the security certification of a video surveillance system according to Common Criteria (low assurance, i.e., EAL 1). Duration and costs of this security certification can be estimated in about 6 months and 20K euros.

2. Do you know cases in the EU, where national approaches for the security certification of any ICT products/services have been/are being established?

Yes. In UK, an approach known as CPA (Commercial Product Assurance) has been established for COTS products to be used in low risk environments. This approach has been derived by the Common Criteria (for low assurance certification).

Moreover, in France, an approach known as CSPN (Certification de Sècuritè de Premier Niveau) has been established.

This is a black box testing approach for low assurance certification requirements and the evaluation/certification process has limited duration and costs.

3. Do you know EU cases, where a customer is not provided with enough/reliable information about the security properties of any ICT products/services?

Yes. In fact, for many products of large diffusion (e.g., the smart phones), no information is provided about the relevant ICT security properties, and the user is left alone with many questions and no answer. A security certificate would improve the situation making some significant information available, and reliable as well.

[9] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union L 257, 28 August 2014.

[10] Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, Official Journal of the European Union L 109/40, 26 April 2016.

[11] Further details are not available

4. Do you think a mutual recognition agreement of certification schemes existing in different countries may have a positive impact on industry costs?

Yes. As in similar cases, the mutual recognition agreement would eliminate the cost of certification duplication, at least within the validity (range of products, set of countries, etc.) of the relevant agreement.

5. In the context of the possible creation of a European ICT security certification Framework, building on existing ICT certification mechanism, such as SOG-IS MRA, what do you think are the estimation of costs needed to run a European Certification Board?

I would estimate medium costs. At least in the case where already available structures (e.g., EU Agencies), tools (e.g., SOGIS-MRA), and standards (e.g., Common Criteria) were exploited to the maximum extent. Costs could be in fact reduced to those needed to coordinate and/or extend pre-existing structures and/or tools and/or standards.

Interviews results from representative of a National ICT Certification Authority

1- Do you know EU cases where an ICT product/service is requested or recommended to be equipped with a given security certificate in order to enter the market of a given MS?

Yes. A security certification is requested in the EU digital signature context. According to EIDAS[12] and the corresponding technical rules[13], a secure signature/seal device has to be certified according to Common Criteria EAL 4+ with given Protection Profiles. Duration and cost of this security certification depend on the type of secure signature device (either smart card or HSM- Hardware Security Module) and on the maturity of the security certification market. My estimates hold for countries where the relevant market is consolidated[14]. For the smart card type, the duration of the evaluation/certification process is of some months; whereas, for the HSM type, the duration is of some years.

Another example is available for Italy, where, in a public procurement procedure defined by Provincia di Trento (Italian local authority), a video surveillance system has been recommended to be provided along with a Common Criteria - Low Assurance security certification[1].

2- Do you know EU cases where an ICT product/service vendor due to requested or recommended additional security certifications (see previous question) in order to enter the market of another MS, has given up in entering that market?

As concern questions 2, 3 and 4, relevant cases were possible before the establishment of EIDAS regulation

3- Do you know EU cases, where a customer is not provided with enough/reliable information about the security properties of any ICT products/services?

Yes. The typical case is that the relevant information is not provided at all. In fact, in EU, we are very far from the case where, as far as ICT security is concerned, a product is provided along with a set of reference information for the customers which allow to understand, e.g., how the product can be/cannot be used. The current concept of product information to be provided to a product user do not cover at all the ICT security domain.

4- Do you think a mutual recognition agreement of certification schemes existing in different countries may have a positive impact on industry costs?

[12] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union L 257, 28 August 2014.

[13] Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, Official Journal of the European Union L 109/40, 26 April 2016.

[14] Further details are not available

Yes. At least in the countries and for the products (positively) affected by the agreement, multiple security certifications would no longer be needed.

5- In the context of the possible creation of a European ICT security certification Framework, building on existing ICT certification mechanism, such as SOG-IS MRA, what do you think are the estimation of costs needed to run a European Certification Board?

I would expect low costs, since already available structures/components (e.g., EU Agencies) could be exploited for the Framework realisation. I'd suggest the Framework to consider the possible infeasibility to take a unique approach (e.g., unique evaluation/ certification criteria) to security certification. In fact, based also on the operating context, ICT products/services usually have large variability in terms of severity of security requirements severity and assurance level of the corresponding certification processes, and this is probably better addressed by several suitable solutions.

Interviews results from representative of a National ICT Certification Authority

1- Do you know EU cases where an ICT product/service is requested or recommended to be equipped with a given security certificate in order to enter the market of a given MS?

The interviewed is aware of cases where an ICT product service is requested or recommended to be equipped with a given security certificate in order to enter the market of a given Member State: the interviewed provided examples where a Common Criteria certification is EU-wide requested (e.g. the case of digital tachographs) and where the same certification is requested (e.g. the case of the electronic Identification Authentication and Signature, eIDAS, regulation).
The duration of such certification is around 6 months and the costs can be estimated between 50 and 100 thousands Euro.

2- Do you know EU cases where an ICT product/service which is equipped with some certificate security certificate is requested or recommended (e.g., preferred within public procurement) to get additional security certificates in order to enter the market of any MS?

The interviewed provided information of the smart meter case where the product is requested to get additional security certificates in order to enter at least the German market. In order to provide information to the fragmentation, the interviewed explained the health card example in Germany where a certification of the health cards is required by the National Approach; unfortunately the interviewed was not aware of the cost of the certification for the cases of smart meter and health card.

3- Do you know cases in the EU, where different certification approach from two different countries are deemed equivalent to establish the security of a same product (through Mutual Recognition Agreements)?

Regarding the approach of a mutual recognition arrangement, the position of the interviewed is that such approach will have positive impact on the costs of industry. On the other hand, regarding the possibility to establish a European certification framework, the interviewed commented that costs are still not predictable because it depends on the tasks and on the mandate of the European Certification Board in charge of managing the framework.

June 8, 2017

Combined answers from two interviewees from a National ICT Certification Authority

1. **Do you know EU cases where an ICT product/service is requested or recommended to be equipped with a given security certificate in order to enter the market of a given MS?**

   The interviewed provided several cases where there is a requirement on certification of an ICT product.

   Regarding the Hardware Security Module (HSM), a product that falls in this category has to be certified against the common criteria standard in order to access to the French market. HSM common criteria certification can last 6 to 9 months and the cost can be estimated on around 200k euros.

   Another example where common criteria certificate is required, in the EU, is the Secure Signature Creation Devices (SSCD): like the previous example, a certification process can last 6 to 9 month and the cost can be estimated in around 200k euros.

   The interviewed provided then information on the case of detection sensors where a qualification against the French national approach CSPN is required by national law. In this case, the duration of the qualification is 2 months and the costs is around 35k euros.

   Regarding network devices related to the creation and management of VPNs (Virtual Private Networks), requirements are defined in France and in the EU on certification based respectively on a national approval (which is Common Criteria based), and on a EU approval process: the French national approval process for VPNs will last from 6 to 9 month and the costs are estimated around 80k euros. The EU approval process is free of charge and takes 2 months to be completed.

2. **Can you provide a case where the certification of an ICT components component is accepted in one country but it was not accepted in another EU country as another certification was required? In that case, did the company undertake a second certification or did it restrain itself from entering the market of that second country?**

   With reference to the previous examples, the interviewed noted that for HSM an initial certification of the crypto module is requested (FIPS), and the SOGIS members, via CEN, request for additional Common Criteria certificates with related vulnerability analysis.

   For SSCD products, there are examples in SOGIS Member States where, if the original common criteria certification is not sufficient for national needs, the product has to undergo again the certification process.

   VPNs related network products are a good example to demonstrate that in absence of an EU common certification approach, some national schemes may have the need to define their own framework requesting another certificate: even if the product is certified against a “collaborative” protection profile, cPP (meaning that the PP has been harmonized between International Mutual Recognition Arrangement members), and even if the product is certified against the FIPS requirements, the additional certification CSPN (and in some cases a completely new common criteria evaluation) is required to access to the French market.

   Other example can be provided for other ICT products like Firewall.

3. **National certification approaches**

The interviewed confirmed that some vendors of HSM, SSCD or other EU regulated products, after completing the certification process in non EU countries (e.g. USA, but there are also examples of products certified in UK and Sweden), quit the common criteria certification required in the EU because, in most of the cases, evidences required at security level for the evaluation process cannot be made available outside the country of origin.

The interviewed provided examples of national approaches for low-level assurance with the CSPN in France, and the parallel approaches in Germany and Netherlands. The interviewed commented that alternative certification programs have been established to complement existing ones, in order to allow more entries into certification (case of CSPN), or to fill the gap of non-existing certification solutions.

4. Do you know cases in the EU, where different certification approach from two different countries are deemed equivalent to establish the security of a same product (through Mutual Recognition Agreements)?

The interviewed thinks that a mutual recognition agreement of certification schemes existing in different countries have indeed a positive impact on industry costs. Based on the SOG-IS MRA, France can for example certify an e-passport application on a chip that was certified in another SOG-IS qualified member by just composing on the chip certificate. It applies as well for all smart card based products.

For eIDAS, any SOG-IS certificate on a HSM or SSCD will be considered as immediately valid for French procurement, as it probably is for all SOG-IS MRA members.

A very quick estimation of manpower needed to run an European Certification board is not that obvious, however if we consider the existing SOG-IS MRA and EU Authorities (ENISA, JRC), we could suggest that a permanent secretariat of 3 to 5 people could support the MSs to:

- Organize the appropriate exchanges of strategies to address the certification needs in the EU and establish roadmaps
- Approve the certification methods considered applicable for EU certification and recognized by all MSs
- Offer a front office for new certification needs expressed by vertical sectors
- Publish certificates and promote certification activities

5. Do you know EU cases, where a customer is not provided with enough/reliable information about the security properties of any ICT products/services?

Unless a product or service has been certified, interviewed answered that there is no proper evidence that a product or service is secure enough for its customer.

Only a certification allows to deliver a certification report that identifies the assessed security level and associated documentation (user guidance, especially) to customers (who have to carefully examine these evidence to make sure the product/service is adequate to their security needs).

6. Do you think a mutual recognition agreement of certification schemes existing in different countries may have a positive impact on industry costs?

Therefore, there is an urgent need to establish a proper EU framework that will analyse, select and improve, where necessary, the acceptable approaches for EU wide certification, and will rationalize the certification decisions for both MSs and industry.

Harmonizing will only be possible through technical exchanges between the MSs schemes, which obviously relies on open certification approaches.

Interviews results from representative of a Semi-conductors industry

1- Do you know EU cases where an ICT product/service is requested or recommended to be equipped with a given security certificate in order to enter the market of a given MS?

An illustration of present certificates needed for ICT products is the Italian passport, which has a chip certified for example in Netherlands, produced in Germany and approved by the national statement of Polygraph of Italy.

Another example given was related to the banking sector and especially for the bankcards. All bankcards in Europe must be certified in two ways: credit cards or debit cards.
Passports, bankcards and many documents must be certified under European Regulation but there are also National Regulation to be considered that could require additional certification. For instance, in Italy there is the CNS (Carta Nazionale dei Servizi) Card that is certified under the Italian Government. In Germany there is a similar program called Telematik-Infrastruktur. Another example of ICT products that must be certified are all cards reader for hospitals.

All laptops using Microsoft, Office, Windows software needs TPM (Trusted Platform Module) which is the name of the requirement for building a microchip which aims at guaranteeing the encryption of the email of personal computers and laptops. All pc, laptops must have certified microchips and the certification is uniquely recognized worldwide. The chip of a laptop could be produced in Germany and the motherboards produced in China but all components must be certified.

2- Do you know EU cases where an ICT product/service which is equipped with some certificate security certificate is requested or recommended (e.g., preferred within public procurement) to get additional security certificates in order to enter the market of any MS?

One problem of fragmentation for ICT Certification is that one product needs to be certified more times for each single component: the hardware of one product needs one dedicated certification, the software integrated of the same product needs another certification and, for example, the chip a third one. This is a real problem for the semi-conductor industry.

Fragmentation is related to the existence of multiple national and sectorial certification schemes not mutually recognized especially in reference to National programs and regulations. The Italian health care cards are completely different from French health care cards, because they have different data, different functions and different type of certifications.

3- Do you know EU cases where an ICT product/service that has been requested or recommended to be equipped with additional security certifications (see previous question) in order to enter the market of another MS, has actually gone through the certification process?

For example, Taxi cards have to be certified within individual National specific programs (one example is the Dutch program) but in Italy there is no such a program established. Within the Member State there are too many National programs which are not harmonized. The fragmentation exists in terms of specific products and specific regulation of member states.
Software, Hardware and chip are certified with different levels of certification according to EAL Common Criteria.

4- Do you know EU cases, where a customer is not provided with enough/reliable information about the security properties of any ICT products/services?

It is paramount to distinguish customers from users when trying to assess whether there is an information asymmetry with behavioural impacts. The final consumer is not well informed on the security properties of ICT products/services, this is due to a lack of awareness through labelling. From the point of view of industry and government customers, the information in labelling schemes is likely to have an impact on its behaviour and purchases.

An example can be found in cable TV that need to be connected to a router for internet connections, these products do not respond to specific security requirements and are vulnerable to hacker attacks. On the other hand, consumers are not aware of this kind of deficiencies, so they continue buying products without considering security requirements.

5- Do you think a mutual recognition agreement of certification schemes existing in different countries may have a positive impact on industry costs?

Benefits of Mutual recognition agreement within Member States comes from more than 20 years of experience.

6- Do you think that the extension of the SOG-IS MRA to all Member States could be a viable policy options?

The extension of SOG-IS agreement to all MS is not a valid policy option that must be considered because there are Member States which are too small and do not have a Certification Authority. Not all countries have the ability to join the SOG-IS agreement.

June 12, 2017

Combined answers from two interviewees from Smart Metering Industry

1. **Do you know EU cases where an ICT product/service which is equipped with some certificate security certificate is requested or recommended (e.g., preferred within public procurement) to get additional security certificates in order to enter the market of any MS?**

   The fragmentation meant as the existence of multiple national and sectorial certification schemes not mutually recognized exists especially talking about National specific programs. There are currently three certification that are ongoing: one in UK, one in France and one in Germany. Our company currently knows this three different certification scheme and do not knows if other initiatives are ongoing. There are at least three Member State that request different certifications and they do not accept each other certificates, so for each country it is request a different certification.
   All the three Countries (France, UK, and Germany) have their own scheme: in the UK is called CPA (Commercial Product Assurance) that it is a scheme that is applied for smart-meters but also for other products. In France it is request the CSPN (Certification de Sécurité de Premier Niveau) certification scheme and in Germany there is a certification scheme based on Common Criteria. Another kind of fragmentation is then also happening on the evaluation side. There are only limited number of Conformity Assessment Body that are able to certify against the requirements of different schemes. In this way, a certain kind of market entry barrier is created.

2. **Do you see the emergence of multiple national or sectorial certification schemes as a likely scenario in the future, especially in view of the growing cybersecurity risks?**

   If MS continue to do not accept each other Certification schemes, each MS will continue to improve its own Certification scheme. Our company started many activities with DG CNECT in order to prevent a situation with 27 different national certification schemes in Europe.

3. **Do you think the extension of the SOG-IS to all member states represents a valuable policy option? Can you please elaborate what do you think are the criticalities and positive aspects?**

   In Germany, smart-meters needs to be certified against EAL-4. It is not very easy to evaluate again smart-meters for example in France or somewhere abroad. The competition is limited. Moreover, Smart-meter industry is beginner in security. A European certification scheme beyond the SOG-IS, would be great and it would increase the competition. Actually, the processes, the procedures and the burocracy for certification is too much for smart-meters industry and security industry.

4. **What do you think in this context would be the difference between the SMEs and the Large Sized Enterprises? Do you think that the size of the Company may impact its ability to access in another market and then having additional certification?**

   The cost of certification is about 1 million and the SMEs are out of this gain. In Germany, only one of the biggest smart-metering companies is starting a certification and all the other companies are present only in the German market.

5. **Do you think that the processes and tools used for ICT security certification should be sufficiently flexible and take into account different levels of assurances according to market needs (e.g. more stringent testing/assessment standards for**

more sensitive products/applications and less stringent for less sensitive products/applications)?

It would be great to have one methodology on how you affect the risk, how you define security requirements and how you go through certification and a recognition across Europe. It is very important to have flexibility in certification scheme, determine on the risk connected to the product evaluated and the risk connected to the location of the product.

6. Do you have an estimate about cost and direction of these certifications?

Looking at the German scheme, the cost of certification is very expansive. The cost of certification is about 1 million euro and the SMEs are out of this gain. For BSI "Smart Meter Gateway" certificate the cost is much more than one million. Our company also checked with meters manufacturers the price for smart meters certification and in UK is almost 150K euro. In Germany, only one of the biggest smart-metering companies is starting a certification and all the other companies are present only in the German market. In France, the cost of certification is something between Germany and UK. The cost it is similar to the UK, so it is about 150K euro or more. In terms of cost, it is also important to note that the evaluation processes are different between MS.

7. Can you provide a case where a customer/user is not provided with enough/reliable information about the security properties of any ICT products/services? What is the problem for consumers: that information 1) is not is not provided at all 2) is not reliable 3) is not enough

Concerning the Labelling topic, the representative of the Smart meter industry underlined that it is fundamental to distinguish the kind of customer. The suppliers buy millions of meters and they have good understanding of security specifications of the products. For Business-to-Business products, the labelling aspect is not much relevant. On the other side, the public opinion is more concentrate on privacy issues (e.g. personal data) and the transparency of data collected by smart-meters. In UK, smart-meters have a display connected to the meters and consumers can simply read data on this display. The consumer decision to buy a product is more on the utility of the product than security aspects. It is important to differentiate which devices needs to be certified and which devices needs to be labelled.

Additional Remark

Working with ENISA, it would be important to understand and harmonize the security language of the energy sector, in order to understand each other, both energy and smart-meters sectors. It is important to combine the approach of DG CNECT with the approach of DG ENERGY.

Interviews results from representative of Smart meters industry

1- Can you provide a case where the certification of an ICT component is accepted in one country but it was not accepted in another EU country as another certification was required? In that case did the company undertake a second certification or did it restrain itself from entering the market of that second country?

We need to distinguish between ICT and ICS (Industrial Control System) products, since the two categories have different requirements and currently this is not so clear to the certification environment.
In France exists the CSPN certification (a kind of light common criteria), which is a low level assurance approach, initially used for ICT products but now moving in covering also ICS and critical infrastructure products.
Relating to product to be used in critical infrastructure, we are not aware of any other request for products certification in other EU countries.
In our product range, we have not seen any overlapping in product certification relating to activities in other countries. Not even in the field electrical infrastructure used by the military world.
We are not aware of cases where a vendor renounced to certificate its products in other countries due to different certification requirements for the same product.
We are aware that, in Germany, BSI is investigating on a low-level assurance framework which is in line with the French CSPN approach.

(Additional question) Based on your experience, what is your view of costs and durations of certification processes?

The French Certification Authority defined the framework CSPN which a light version of common criteria. CSPN certification costs about 50k euros and the duration is around 6 months. Behind these costs, there are a number of activities to be performed by the vendor to fulfil CSPN requirements and such activities are estimated to cost around 300k euros.
France has in place other types of certification framework (for COMSEC and for system integrators). It is very important to apply international standard to harmonize requirements between Members States and to give the vendor the opportunity to be competitive at international level. In the ICS world, we are aligned with the standard ISO 15443.
We are a European and international industry. We have to follow different certification approaches in different countries. Common Criteria are much more expensive for us: just as an example, the cost of a Common Criteria certification is not less than 500k euros. We do not feel that the Common Criteria approach is the good solution, at least for ICS.

(Additional question) As for security certification, do you proceed on voluntary basis or on a request/recommendation basis?

We think that certification is a driver to improve the level of security, and this applies not only in Europe. There are also requirements like the French one to apply to CSPN. However, the choice to undergo the certification of a product is of course market driven.

2- Do you think that the processes and tools used for ICT security certification should be sufficiently flexible and take into account different levels of assurances according to market needs (e.g. more stringent testing/assessment standards for more sensitive products/applications and less stringent for less sensitive products/applications)?

Devices that are more critical should have a higher level of security. Definitively some products have a very low risk. On top of some certifications, it would be good to consider self-declaration: in some area,

there is a high attention on vulnerability assessment approaches. For me it is much more important to have certification based on procedures in charge to the user managing the critical infrastructure. A certification has also to be considered in a system model: if the product is not used or configured in a secure way, there are vulnerabilities in charge of the critical infrastructure owner. We need a sort of way to certify requirements and we need to be able to specify which components are more critical and need a higher security assurance than others. One way to do that could be the self-declaration approach.

3- Can you provide a case where a customer/user is not provided with enough/reliable information about the security properties of any ICT products/services? What is the problem for consumers: that information 1) is not is not provided at all 2) is not reliable 3) is not enough

I do think that information provided to customer is not enough at least for critical infrastructure owners. Today we, as vendors, have in place cyber security programs to fulfil the information needs of critical infrastructure operators.

4- Would you be in favour of the introduction of a common label signalling that the products have been certified within a certification scheme in accordance with EU rules?

I definitely think that, even with the label, the customers need to understand what the label means and there is the need for some information behind. I mean there should be a transparent information about how this process of certification has been carried on.

5- Do you think a mutual recognition agreement of certification schemes existing in different countries may have a positive impact on industry costs?

We agree that a certification recognised between member states is required. We prefer to have a certification that is done in one country and is recognized in others Member States. We also prefer to refer to international standard to remain competitive at international level.

6- Do you think the extension of the SOG-IS to all member states represents a valuable policy option? Can you please elaborate what do you think are the criticalities and positive aspects

We feel that Common Criteria and SOGIS are not the right solution for ICS at the moment. Common Criteria costs 500k and lasts more than one year. This is a problem for a vendor. Common Criteria is a good approach for some kinds of components and products. In situations where the lifecycle of a product is more than 20 years, we have to find approaches at a system level based on procedures and self-declaration. ISO 15443 is an example of standard that we think is adequate for ICS context.

7- Concerning an EU wide certification framework, do you think it would have a positive impact on costs for your industry? Can you please elaborate what do you think are the criticalities and positive aspects?

In ICS context, we think that other levels of the system have to be certified as well, not only the product level. We need to make sure that the certification takes into account the different actors involved in the whole process. Some nations may have different needs on ICS and ICT requirements too. The application of a specific international standard has be debated, not only the framework. For non-critical devices, we also find that the solution could rely on a self-declaration process.

8- In your opinion, what role the EU Agencies (such as ENISA) might have in the management and the operational tasks of an EU wide cybersecurity certification scheme?

I think ENISA could play a role within industry to help to understand the concerns of the different national agencies. ENISA can play a key a role to harmonize Members States' Agencies on definition of national requirements and assurance, and assuring that the solution meets the needs of industry. ENISA should also cooperate with standardization institutes.

(Additional question) Would your company be willing to actively contribute to the realization of the said EU framework?

Industry would be available to contribute to the realization of the EU Framework. We are involved in cyber security taskforces and industry experts from these taskforces would be happy to participate. We also produced a policy paper that shows the position of pan-European vendors about relevant requirements.

Interviews results from representatives of Conformity Assessment Body

1- **Can you provide a case where the certification of an ICT component is accepted in one country but it was not accepted in another EU country as another certification was required? In that case, did the company undertake a second certification or did it restrain itself from entering the market of that second country?**

My organization has in fact certified some products with vendors who have been successively requested to re-certify the same products. This was needed to enter the market of another country. Notice that the problem is not the recognition of certificates (Common Criteria), but the suitability of a certificate against country specific requirements (e.g., assurance level (Common Criteria EAL) and/or security requirements (Common Criteria SFRs). Vendors expect certificates to be valid for all customers, but most of the times this is not the case because of country specific requirements. This applies especially for governmental customers. Most of the problems arise from the semantics and the content of certificates (Common Criteria) and not from the lack of certificate recognition.
There are cases where a vendor, having already certified its product, has applied for a second certification to enter the market of the requesting country.
I do not know about cases where a vendor renounced to apply for a second certification.

2- **Do you think that the processes and tools used for ICT security certification should be sufficiently flexible and take into account different levels of assurances according to market needs (e.g. more stringent testing/assessment standards for more sensitive products/applications and less stringent for less sensitive products/applications)?**

In some cases, end users are addressed with wrong needs and the concept of a single view on assurance is not useful at all (an example is the mandatory usage of cPP (collaborative Protection Profile) within CCRA to get certificate recognition for assurance level greater than EAL2). Certification has to be very flexible to provide what the market is asking for. ISO 15408 (Common Criteria, in fact) has sufficient room for flexibility.

3- **Are you aware of national approach to security certification of some products which are being established in some MS? Do you expect new approaches established in the near future?**

No.

4- **Can you provide a case where a customer/user is not provided with enough/reliable information about the security properties of any ICT products/services? What is the problem for consumers: that information 1) is not is not provided at all 2) is not reliable 3) is not enough**

I think there is a general lack of understanding of the security properties of a product from the user/customer. The information is not really provided.

5- **Assume a labelling framework where a product can be security labelled after a successful security certification. Would this approach improve the situation?**

The problem with such a label is that it could lead to more confusion. If the label is too simple, the user could misunderstand the corresponding information. If the label is too complex, the user could be unable to understand the corresponding information. To be useful, the label should be well balanced.

6- **Do you think a mutual recognition agreement of certification schemes existing in different countries may have a positive impact on industry costs?**

I think we definitively need a pan European solution to security certification in view of a single market. This solution could be in the form of MRA or of a European legislation. MRA are slow and difficult to manage, and they could in fact be ruled (or more or less controlled) by some nations only. I would prefer a European legislation applied to all member states.

7- Do you think the extension of the SOG-IS to all member states represents a valuable policy option? Can you please elaborate what do you think are the criticalities and positive aspects

The fact that the SOG-IS does not include all member states is a real problem: it is a must to expand SOG-IS to all members states.

8- Concerning an EU wide certification framework, do you think it would have a positive impact on costs for your industry (ITSEF)? Can you please elaborate what do you think are the criticalities and positive aspects?

I think we need that: as an ITSEF, the framework is fundamental to my organisation. Note that 80% of our customers come from countries outside Europe. The rest are national vendors: certification in Europe is too much based on national reference (vendors in one country certify in that country). In general, there is no single market in EU.

9- In your opinion, what role the EU Agencies (such as ENISA) might have in the management and the operational tasks of an EU wide cybersecurity certification scheme?

Current schemes, which are governmental, do not really have resources and capabilities to suitably certify according to the current market requests. EU certification framework need to consider capabilities and to open the door to private certification activities. There is room for European Agencies (like ENISA) but there is also the need to find a role for private certification bodies and companies. I do not think a successful design can be done with just certification bodies: the EU certification framework has to open other realities such as ENISA, representatives from industry, etc.

13th July 2017

Combined answers from two interviewees from Smart Metering Industry

1- **Based on your knowledge, is the smart meters industry a highly regulated sector? Across Member States, are there existing security provisions and standards indeed override the need for labels and certification?**

We will both answer to this question. In the current situation there are few countries that are asking for a security certificate that are UK, Germany and France. Their process of certification is based on national requirements that they started to write. In the UK they are called security objectives. Based on these requirements and objectives they defined a security certification approach at a national level. So far, I haven't seen any reference to any international standards because these standards are still quite high level and very general. They are not suited for a certification. That's why there are national definitions based on which national certification takes place. It's mainly that you have to repeat three times different methodologies to prove that you have secured your device, which means that you'll have to face three times more costs. This is not possible.

2. **If France, Germany and UK did not introduce the national requirements, what would smart meters operators be required to do as security measures?**

The motivation for the industries to invest and to innovate on this topic is limited because of the market structure. Another thing is that the liability for damages for operators in different countries is not even when they comply with the legal environment. I would like to stretch that the three methodologies that France, Germany and UK use are all standards, which is not a problem. The problem is that there are too many standards. Another problem is a problem of European accordance of minimum requirements of documentations and tests results, for the same functionality and in the same language, ready and accepted by the different authorities of different countries. This is an important message that should pass to the Commission.

3. **So, the introduction of these three different strandards made operators to go through other tests three more times, by adding more costs?**

Yes, It also block the innovation. The additional costs could be invested in other innovations.

4. **We talked about the different standards from Germany, France and UK before and it was said in the previous interview that the costs for the German certification is approximately one million. Is that correct?**

Yes, and it would include the indirect cost, which is the non existent market. Companies invested for six years and they do not have anything back so far.

5. **For France and Uk, it was said that it could reach almost 150 thousand euros. Is it right?**

Yes, it was in the Smart Meter sector. We received these information from the meters manufacturers so it's specific for the Smart Meter Certification. This information is related to the Uk. For France it should be a similar range, around 150 thousand euros for one certificate.

6. **For which reasons is there such a wide range of costs? Are there big differences between these Smart Meter industries? Is it related to the different approaches in these three countries?**

The approach in France is for instance more focused on testing in a fixed time: given the products and the deadline for certification, all the security tests have to be completed during that time. At the end of the fixed time, you receive a report on whether it is working fine or not. In the German approach, they have a higher level of certification. The standards are the same but they have higher levels of tests for the certification. How thoroughly you can test the device is the difference. The Germans are using the

Common Criteria as standard. They started in 2011 to use these security certification standards as requirements. They also added requirements for privacy and security as well as other processes to maintain these standards during the lifecycle. The testing methodology is end to end: for instance for software coding you need to have your own site, where only authorized coders and cleaners can enter the room. On the other hand in UK and in France they put just a security assessment on one product, while in Germany the whole infrastructure need to be tested and certified. The basic functionalities and requirements are the same but it doesn't mean that at other levels the German certification might be more efficient. There are in fact different architectures for different smart meters. For instance, the French ones won't work in Germany. The data and the controlling is different. Same is for Uk. However the basic function requirements are the same.

7. **Would the higher costs for certification in Germany be a barrier to the market for small and medium industries? If the architectures are different, wouldn't a European certification framework also require different standards?**

There is clearly a difference in attitude in different countries. There will be for sure some countries that believe that their approach is better than any other one. They will have different architecture and different security measures like in Germany. What would be interesting is to see how the market would respond to this. German Manufacurers will probably follow this standard but other European producers will probably prefer other countries. It is our expectation however that the majority of the European States would agree with the European approach for certification. They will accept certifications made by other European countries. If a particular Member State would require additional test, they should be able to demand it. The basic requirements on security are very similar in all the European countries. If we say that 80% of the requirements is the same for all countries, then there will be only a 20% of the standards that should be covered in order to enter the market of another European Country. This would be more attractive economically and financially. It would in fact be a basic certification for everybody and, maybe, even Germany would accept that basic requirement since it might be the same.

8. **Another advantage might be that the money that won't not be spent for other national certification, they could be invested in the cyber security sector. Is it correct?**

Yes, absolutely. For instance, for my company, I won't have to find several solutions for each country for security and there for invest the money of those costs in development of other cybersecurity measures, that require constant updates. Maintaining certain levels of security in various different countries would also be way more expensive and difficult than if they were in European certification framework. On a national level, the ICT guys are imposing their visions on the Energy guys and their approach is not very successful. At the same time, the Energy guys are ignoring all the risks. They are not reliable.

9. **I would like to deepen the aspects related to the small and medium enterprises. Considering the previous hypothetical situation of an 80% of states that will use the European standards, do you think that smaller and medium enterprises would be favored to penetrate in these countries?**

Basically, with a European framework the barrier for the market entry would be easier. It's hard to define if they would be able or not to enter the market because it will depend on that 80% of common costs. For sure, it would lower the barrier so they would have more chances to do it. For the markets that won't accept the certification would still have problems. There might be two sides of the company. In a very fragmented market, there might be few national champions with certain innovations but biggers player might eat them but this is not related to the security certification. In Germany 5 out of the seven companies that are putting their products on the certification are smaller companies. Only one player is global. The challenge however is that in the Smart Meter sector, the product cannot leave the German market, at the moment.

July 13th, 2017

Interview results from Expert on Cyber Resilience of Critical Infrastructures

1. **Based on your knowledge, what are the main advantages, if any, of adopting security certified ICT/OT components in critical infrastructures? Please consider possible advantages also in the field of attack prevention and/or resilience**

   I worked on these issues as I was working for the ERNCIP (European Reference Network for Critical Infrastructure Protection). The aim would be to arrive to a certification framework for the Critical Infrastructure. The discussion on a certification of the components started two years ago or so because of the French and German influence, as well as DG CNECT. If I am not wrong, last year there was even a Call of Proposal in order to fund projects in this field. I'm still skeptical about certifications and benefits that they could have on the improvement of the Critical Infrastructure resilience.

2. **Do you know cases in the European Union where some ICT components of critical infrastructures, even though already equipped with some security certifications accepted in some MS, are requested or recommended to get additional security certifications in order to access the market of other MS?**

   Yes, there is. Certification means to certify towards other referential standards. There is the Common Criteria but it doesn't work and there is proof of its inefficiency. Only by checking their website, it is easy to understand that there are only few products for the critical infrastructures that had been certified by the Common Criteria. Furthermore, the ISA Security Compliance Institute release the ISA SECURE certifications: even in this case there are only few certified components. It's a too little number for such a complex system. They are way too expensive and they don't have a future. These certification processes are too difficult to go through because there is too much bureaucracy and paper forms to fill. Another problem is the definition of Standard. What are the reference ones? In the critical infrastructure domain, it takes too much time –even more than 10 years – to decide them. In France with the ANSII and in Germany with BSI, there is fragmentation. In Italy, on the other hand, there is no requirement and in all the other Member States there isn't any mandatory certification. You only have to comply with the Standards. I come from a background in the Nuclear Sector, where standard compliance to certain standard is mandatory and extremely strict. As for the certification I think that it's only useful for the creation of procedures that turn out to be long, complicated and expensive.

3. **Do you know ICT products/components/service deployed in critical infrastructures require mandatory cybersecurity certification?**

   No

4. **As for operators that purchase and adopt components and products for the critical infrastructures, do you think that their choices are based on product certifications or on other features?**

   I believe that their choices are based merely on the producer name. The company brand from which they purchase the components is like a security guarantor. For instance, buying from Scheneider Electric and Siemens is probably more reliable than purchasing from a Chinese producer. There is, however, an issue to point out: most of systems and products on the European Market have embedded components that come from China where the security standards are less available to check. So, how can I be sure that Chinese components respect security standards and certifications that will protect me from risks? For example, the microprocessors of PLC (Programmable Logic Controller) components have Chinese origins.

5. **Do you know any National Certification Scheme in Europe?**

Besides France (ANSSI) and Germany, I know the existence of the national schemes in UK and the Netherlands.

6. **In your opinion, to what extent does the current (or possible) existence of multiple cybersecurity certification schemes represent a barrier to EU market entry in the critical infrastructure domain?**

   Yes, it's definitely a market problem. If the European Commission would be able to apply a European label, components and products with an Italian certification would be able to be sold in Finland. If we could manage to have European standardized framework, the market would benefit from it. It's similar to the food labels. Without a free movement of goods in the EU, there would definitely be market limitations. Without a European Certification, it would be very difficult to sell products in more than one European Country.

7. **In your opinion, would a European cybersecurity certification framework that support the mutual recognition of cybersecurity certification reduce costs for manufacturers of components or service providers used in critical infrastructures? Can you please provide your view on other possible positive or negative aspects?**

   Yes, sure. Furthermore, having multiple certification laboratories is even more expensive. You need to prepare the maintenance staff of these structures and, with European certification, it would be possible to reduce these laboratories. It will be therefore possible to reduce these costs on the long term.

8. **By adding an information label on the product that certifies the security standards – as it happens for medical devices – do you think that it would be possible to reduce the information asymmetry? Would it be possible for the consumer to compare more products and have more information on its security standards?**

   Yes, absolutely. As for the medical devices, we are talking about expensive and complicated machines that are bought by operators, for example Tomography machines that cost approximately one million euros, and not by normal citizens. It is more a Marketing issue: as I use a label to certify my product, it can be sold more easily on the European Market. Should I be surer about its security, though? Not really, as far as I am concerned.

9. **What are the benefits for a certified product? Would a costumer buy it more likely?**

   It's always a matter of Trade-Off, whether to put a certified product on the market or not. If the certified product is three times more expensive than the not certified one, I am not sure I would buy it. It's an old dilemma if the security costs are a long term investment or not. Through mutual recognition of a certification framework it would be better. However, it should not add any other cost on the producers.

10. **Would you be in favor of a European Scheme of mutual recognition between the member states?**

    Yes, I am because of the free market benefits and not because of the possible improvements of security in the Critical Infrastructures. I am positive towards a European Label. The certification, however, should be discussed on different levels: what about the compliance standards? And what about the laboratories? They are different discussions.

11. **Are there any regulations that makes certifications mandatory?**

    There isn't any mandatory certification in Europe. There are other private activities such as the Norwegian DNV and the German Thuf but there isn't any mandatory certification.

12. **We are wondering if a certified product might guarantee more openess to the different markets. What do you think about the functionalities of it?**

Let's take an example. A PLC is well defined functionally. It is more difficult however for SCADA systems. The certification won't guarantee only their functionalities but also its immunity to external threats and other vulnerabilities.

13. For these components, the security requirements are very important. Are there security tests of the components?

After the functional tests, they check the security of the component from external threats through tests in laboratories, like the penetration test. Recently, in the United States, hackers managed to hack in to cheap CCTV cameras, produced in China. They were extremely common because of their affordable price but they had lower security standards. Therefore, Hackers managed to enter their system and block the whole network. Enel is going to sell 24 million Smart Meters. If these devices would have a security certification, we would definitely be safer. On the other hand, if they have vulnerabilities, hackers would be able to enter a network of 24 million devices and turn off the lights of Italy for at least one day. There is a lot that should be done: defining the limits of a certification, what are the standards and what is its contribution to security. I worked with ENISA and I think that we should work more on the meaning of this certification/label and on the real effects that it could have on resilience.

Interview results from representative of a manufacturer operating for Critical Infrastructures

1- Based on your knowledge, what are the main advantages, if any, of adopting security certified ICT/OT components in critical infrastructures? Please consider possible advantages also in the field of attack prevention and/or resilience

There are different advantages and some of them are quite obvious. It allows the entrance to several markets that have particular requirements. It is also an advantage for the transparency of the information for the customer or the regulator. By certifying products, you can step up versus a competitor and be in a better position on the market. For the security of the product itself, it can be helpful but I think that the major advantages would still be related to the transparency of the information and the entry on the markets.

2- Do you think that operators of essential services have a sufficient level of information regarding the securities features of the IT/OT products /services they use for the lifecycle of their infrastructures?

As for critical infrastructure operators is crucial. If you do not have a certification, you cannot know if the information is true. Each company could claim that their product is secure but it is better to have third parties to test it independently. That is definitely another advantage that a certification could represent. However, I still believe that the main one would be the entrance on the market.

3- Do you know cases in the European Union where some IT/OT components deployed in critical infrastructures are requested, mandeted or recommended to be provided with some type of cybersecurity certification?

It depends on what products are compelled. It is primarily around security products and services, such as firewall, IPM, intrusion detection systems, routers, so this kind of networking devices, like routers and switches. There are different criteria and standards that are required. In some cases, we do multiple certifications because other markets require them. For example, in France, you need to have an authorization issued by the Prime Minister Office for network devices in Critical Infrastructure. It is common for government to require certain standards for Critical Infrastructure and security products and services.

4- Do you have any example of national certification or scheme?

As a company, we rely a lot on Common Criteria. Getting certifications in each member state is complicated, expensive and time consuming. On standard sides, we follow ISO standards. As for local ones, we have specific requirements by the military law for security devices. In Germany, we have some requirements from BSI.

5- In your opinion, would a European cybersecurity certification framework that support the mutual recognition of cybersecurity certification reduce costs for manufacturers of components or service providers used in critical infrastructures? Can you please provide your view on other possible positive or negative aspects?

I am not sure what the framework is exactly trying to achieve, a part for mutual recognition. There are many basic and common requirements at a national level but they can also be certified through the Common Criteria. I am not sure about what Europe can achieve for security issues. I am not against the Commission having a board and controlling the situation but I am a little bit skeptical about the results. There is a problem of fragmentation, especially since more European countries became skeptical on Common Criteria. There is a lot of work for ensuring security of products.

6- Do you know cases in the European Union where some ICT components of critical infrastructures, even though already equipped with some security certifications accepted

in some MS, are requested or recommended to get additional security certifications in order to access the market of other MS?

Yes, it depends on the type of product and the Member State. Even with the Common Criteria most of the time you have to do other tests because they cover only the basics. Furthermore, certain devices require specific extra certifications such as networking devices. At a national level, for instance, in Germany, for security devices, they have to cover by the Common Criteria but also they have to go through specific tests locally to prove that your devices are reliable. There are also type of products that need to be certified against additional requirements for critical infrastructures in France made by ANSSI.

7- Can you provide us some information about the costs of certifications?

Yes, on Common Criteria alone, last year, we had 20 certifications and it costed us around several hundred thousand euros each, including the external resources, laboratories etc.

8- Do you think that these costs represent a market barrier for smaller and medium enterprises?

It depends on the type of the companies we are talking about. If you are a Germany encryption company, you have Philips on the other side so you will probably have to look on other markets. Unless you decide to collaborate with the bigger Germany companies. Otherwise, you will probably struggle in finding German customers. From the costs perspective, if you are a smaller company and you are trying to enter on other MS's markets you will struggle.

9- Do you think that operators of essential services have a sufficient level of information regarding the securities features of the IT/OT products /services they use for the lifecycle of their infrastructures?

The biggest problem is the fragmentation. There are different kinds of certifications but they guarantee certain standards. Only at lower levels, there might be a problem of lack of transparency on security measures. It is harder to understand if they are secure.

10- Is there any information or issue on this topic that you would talk about? Something concerning labelling?

Yes, actually there is. In our company, during the last year, we have been discussing on the idea of IT trust labels for devices. We think that it might be a more effective solution, especially for critical infrastructure. Instead of a common framework, labels might be more useful as a solution for the information asymmetry. Now, most of the end devices for Critical infrastructures are regulated but not checked. A label would be different from a Common Criteria because it would more of an insurance in order to enter the market. The best would be to have both a label for the basic requirements and another one for the specific and higher ones.

July 24th, 2017

Interview results from representative of a European Association for Forwarding, Transport, Logistics and Custom Services

1- Based on your knowledge, what are the main advantages, if any, of adopting security certified ICT/OT components in critical infrastructures? Please consider possible advantages also in the field of attack prevention and/or resilience

Yes, there are many. When it comes to security equipment, especially Air Cargo, it is important to have secured components. Security is also very important for screen technology and other IT components as well. A standard security certification of the components is always a good thing. It something that should now exist on a general basis in cargo screen technology. We support in fact a harmonization of the various markets on security standards and certifications. Our only concern is whether logistics is considered a critical infrastructure. Germany considered it as such and it is the most advanced on this issue. However, not all the Member States consider it as such, because in case of a problem with a particular company, you can always ask to another one. However, this point of view does not consider the possibility of a larger cyber-attack, which goes across the whole industry. Not the whole logistic sector should be considered as a critical infrastructure, but there are for sure certain structures that should. Airports are a clear example of this. Furthermore, another entity that we need to deal with, for security standards, are the governments.

2- Do you know ICT products/components/service deployed in critical infrastructures require mandatory cybersecurity certification? Do you know European National Certificaton Scheme?

No, no that I know of. There might be some, but from the discussion we had on cybersecurity, it never came out.

3- Before you mentioned the German approach, do you have any examples of certifications or any experience related to it? Do you know costs and/or procedures that it might require?

No, I do not, unfortunately.

4- In your opinion, would a European cybersecurity certification framework that support the mutual recognition of cybersecurity certification reduce costs for manufacturers of components or service providers used in critical infrastructures? Can you please provide your view on other possible positive or negative aspects?

Yes, I think an EU certification might have a positive effect. We support this kind of policies because we believe that is always preferable to have a common European Scheme. We believe so because it would not only increase the security levels of all Member States but it would also be good for the market. It has to be made properly however. The certification need to be designed based on the necessities of the industries and the member states.

5- Do you think that an EU wide Certification Scheme could brings advantages also for smaller and medium companies reducing market barrier?

Yes, sure. Being able to buy certified products from every member state would help even smaller and medium companies to enter the market. You would be able to buy different components for your network more easily. It is important however that the requirements of the certification are appropriate. It would be helpful also because on the European market the majority of the enterprises are SMEs.

6- Based on your experience, do you think that critical infrastructures are at greatest risk because of outdated security practices / policies and limited regulatory oversight?

We had a lot of discussion about this issue with the European Commission on the current cybersecurity situation and the latest cyber-attacks. As it turned out, most of the companies that had been attacked were underprepared and there was not enough information sharing between them and on what they needed to do. It is extremely important to have updated practices, update processes and updated technologies. This should not happen, once the cyber-attack took place. Operators need to act in advance to prevent them and share information. We think that standardizing security will bring down the costs that could be invested elsewhere. Mandating certain practices will not be the best solution because security requires continuous updates. Rather than prescribing procedures, it would be better to have a constant evaluation of risk assessments through a security check approach.

7- Do you think that certification and labelling of ICT products/services may contribute to enhance the level of assurance of critical infrastructures? Do you think that certification and labelling of ICT products/services may contribute to enhance the level of information?

Yes, sure. It would be more effective.

8- Do you think that operators of essential services have a sufficient level of information regarding the securities features of the IT/OT products /services they use for the lifecycle of their infrastructures?

Yes, I think that in general they do. It probably depends on individual experiences but I think that they receive the basic security information on the component. I think that the situation could still be improves. Making the information more available and clearer would definitely help the operators and avoid certain situations.

9- Do you think that this approach of mutual recognition in Europe would have advantages for the different stakeholders of the market? Do you think that it might have other benefits?

Yes, I think it would be a good solution. It would make the security easier to obtain. The mutually recognition across EU might even have positive effects globally. I think that it would be good if the risk agenda of the EU could attract other non-European countries to join the mutual recognition. States like US and Canada and many others might be interested in the future to join such mutual recognition.

July 25th, 2017

Interview results from representative of a European Bank

1- **Based on your knowledge, what are the main advantages, if any, of adopting security certified ICT/OT components in critical infrastructures? Please consider possible advantages also in the field of attack prevention and/or resilience**

Yes, sure. There are for sure some advantages of using security certified components. I think that a certification adds a lot of value. For instance, I use HSM devices (Hardware Security Modules) that fit with security standards compliance. It allowed us to store critical data on a secure device. It's mainly from compliance assessment that I get advantages. With compliance, it doesn't always mean that is more secure than other devices though.

2. **Do you know whether the critical infrastructure operated by you adopts some ICT/OT products which come with some types of cybersecurity certifications? In this case, do you have any idea of costs of this certification?**

In the finance industry, as an example, our services must have secure encryption and use HSM, which are incredibly expensive. In order for us to use a HSM component, it is going to cost us around 20.000 euros and that is not the whole device. Devices with five of them like a hot standby, business computing and others are going to cost around 100.000 euros. All of that would be needed just to store key credentials of the encryption.

3. **Do you know cases in the European Union where some ICT components of critical infrastructures, even though already equipped with some security certifications accepted in some MS, are requested or recommended to get additional security certifications in order to access the market of other MS?**

In the Finance Sector, we have to follow the EU directives for payment services. With other countries, like the US we do not have to do it. I have to be compliant with the 54 jurisdictions of countries we are operating in. These procedures become very prescriptive and we have to deal with many descriptive requirements that sometimes might even be contradictory.

4. **Do you think that operators of essential services have a sufficient level of information regarding the securities features of the IT/OT products /services they use for the lifecycle of their infrastructures?**

It is not really a lack of a transparency; it is a lack of understanding of security requirements. There is a perception that if everybody performs by following the prescription, it will be secure. However, this is partially true. The problem is that most of the time the prescription doesn't' cover everything and they can still be breached. For me, there is a dichotomy between compliance and security. I spend a lot of money and a lot of effort for the compliance, which is not necessary a guarantee for security.

5. **Do you think that the costs, due to this fragmentation of compliances and the duplication of costs, could be invested in other security solutions?**

Yes, absolutely. For example, there are security organizations that require more people to work on the compliance than the ones working on security solutions.

6. **In your opinion, would a European cybersecurity certification framework that support the recognition of ICT security certificates reduce costs for operators of critical infrastructures? Can you please provide your view on other possible positive or negative aspects?**

If it became too prescriptive, it might be too difficult to comply to, as it happens for the other jurisdictions.

7. **Do you think that a soft approach, which only give guidelines to different stakeholders, could be more useful? What kind of approach would you suggest otherwise?**

   If you look at the GDPR regulation, it is not prescriptive around the world. I think it would be an appropriate approach.

8. **What do you think about a label on the products with the security information?**

   I think it would not make too much difference. As an example at the Data Centers, engineers would configure the devices without physically seeing them. Therefore, they won't be seeing it.

9. **What would be the effect of a European certification scheme on SMEs? Do you think they might have advantages?**

   Many of the security products are very technical. Even if there would be a certification, I am not sure that the SMEs would actually understand the security standards and tests of the product. I think that they would not know all the distinctions.

10. **Do you have any information on Cloud Computing? Do you think that this ICT certification in this field would have advantages?**

    At the moment we are not using Cloud Computing. There is a barrier from using them because we cannot be sure that the data is stored in a secure way, especially according to the various jurisdictions. Since we are a regulated entity, that is a barrier for us. Most of the banks are struggling with that challenge. There are problems because the European data might be stored in South America, or in somewhere else, under a different jurisdiction. It would also be more expensive because of that.

11. **Do you think that a certification might give more advantages on the security of the Cloud?**

    If they are certified it would definitely be more cheap and it would be easier for the security compliance of the different jurisdictions. However, I still don't feel comfortable with them because they are not secure enough by design.

August 3rd, 2017

Interview results from representative of a Telecommunications Company

1. **Do you know ICT products/components/service deployed in critical infrastructures require mandatory cybersecurity certification?**

   I am going to answer you with an insight from the UK perspective. First, we are contractually obliged to look for security certification on products and services for the national infrastructure. They have to be certified on a variety of schemes in order to provide their service to the critical national infrastructure. In the UK, there is the CAS(T)[15] scheme, which is a telecom specific version of ISO27001 and that is a fundamental security certification for any product and service that is sold. Furthermore, the Public Services Network need to be certified every year as a prerequisite. It will not be possible for us to sell it in UK, without certifying them.

2. **Can you provide some information related to costs of the certification?**

   Yes, for example for one of our network platform the overall budget was of 500.000 UK pounds. It included 39 different services, whose price range from 10 to 15 thousands UK pounds each.

3. **Do you have an idea if this certification is recognized through Europe or if it is only for the UK?**

   I would say that it is valid only for the UK. If we look at the CAS(T), the equivalent of the ISO 27001, it is issued by the National Cyber Security Council. Therefore, it is more UK centered and not European. However, in terms of what it is asked for, it is based on an ISO standard.

4. **Do you have any idea if a certified product in another country has to go through the UK certification process, before entering the market?**

   Any product worldwide of this sector, which should be sold in UK, has to go through the certification scheme. There are by use non UK certification that have value like the Common Criteria, but they still need a formal approval to sell it by the UK.

5. **In your opinion, would a European cybersecurity certification framework that support the recognition of ICT security certificates reduce costs for operators of critical infrastructures? Can you please provide your view on other possible positive or negative aspects?**

   There are many security standards that we have to comply to and there is one on cyber security resilience coming soon in the UK. If all of the certification bodies would recognize these security tests, we would save a lot of money. We have just started to see the benefits of the interventions to try to facilitate mutual recognition of the national security certification. We support this kind of initiative.

6. **Do you think that the current situation of certification could represent a barrier for European market, especially for the SMEs?**

   In the UK, there actually a lot of standards for product security certification. There are at least four schemes that are run by the UK National Technical Authority. They range from test marking, encryption etc. and there is no doubt that the cost of certification would be a barrier for vendors who want to enter the UK market.

7. **Do you think that operators or customers have a sufficient level of information related to the security of their IT devices?**

[15] CAS (T) is a certification scheme for clients providing telecommunications services. The scheme supports the government Public Services Network (PSN), which requires all telecoms services procured by public sector bodies.

This is a personal opinion but I think that there is a lot of confusion on the meaning of each standard. Most of the people do not understand what the security certification means and what does it guarantee you, on the purchase side. I think that too much information sometimes might create a lot of confusion.

8. **Do you think that a label with the main information might be a solution for this problem?**

   I am not sure. I think it depends if they understand the meaning of the label mark on the product. It would be useful to distinguish between two products but I am still skeptical about it. I think it depends on which customer group we are talking about here. I have to say that most of the organizations, who purchase components and products for the critical infrastructure, have the technical knowledge to distinguish between different levels of security protection. In the case of IT devices in general, I believe that –yes- a security label might be useful for consumers. Furthermore, for the case of IoT devices, I think there is still a rationale for a certain type of labelling framework. It's a difficult questions to answer to because it is too general.

9. **Considering the current situation, do you think that the critical infrastructures are at a greater risk because of the fragmentation across the market?**

   Yes, I think so. The security level change across Europe and I think it might be problematic for the critical infrastructure.

10. **We are doing a case study on cloud computing. Do you think that the lack of a certification on this kind of service could affect the choice of companies to use it? Do you have any experiences to share with us, related to the Cloud services?**

    There are definitely several issues related to the Cloud, including trust ones. It is more difficult because it is not suitable for all certification. I have an example related to critical national infrastructure. Virtualization and Cloud have many benefits for the management of the critical infrastructure but it is important to know every technical aspect and functionality of it.

11. **Do you have any other suggestion or advice for the European Commission on the topics we discussed before?**

    Critical infrastructures are by definition more critical than IoT, in general. However, the fragmentation is a common theme for both of them and, as we have seen, it unhelpful. For this reason, we support what the Commission is trying to do. With that said, we think that the European Commission, in her impact assessment, is going in the other direction, for what concerns certain solutions. We would not support the extreme one such as support mandatory requirements. We think that the more moderate attempt, that keeps in consideration both the European Market and each jurisdiction, would be better. I think that it would also be positive if European Commission, instructed by ENISA, could define a set of best practices. As we started working on the IoT with the European Commission, there were different opinions regarding the possibility of a label. We were supportive. In fact, if the label would be reassuring for the customer, it would also increase the trust in the company. There are two issues however. First, it is quite difficult to communicate security levels through a label. Secondly, there would still be some kind of fragmentation. The labelling in itself is good but there should be a proper discussion on how does it communicate.

7.2 Questionnaire

In order to assist the **European Commission - DG CNECT in gathering evidence on ICT security certification and labelling**, the consortium made an online questionnaire open up to 19th June 2017.
The Questionnaire will help the Consortium and the European Commission to build additional specific evidence to the results of the ENISA survey on "EU certification and labelling framework", which is a key step to **support the design of a European policy/regulation which is close to the needs of the European ICT industries**.

The questionnaire has been designed by putting multiple closed questions and some open questions where the selected stakeholders can more detail some relevant aspect. The Questionnaire template can be consulted here below:

A. Introduction
This questionnaire is organised by PwC and Fondazione Ugo Bordoni FUB to assist the European Commission in gathering evidence on ICT security certification and labelling. It takes into account the results of the ENISA survey on "EU certification and labelling framework" and aims at building additional evidence. By answering to the questionnaire, you will provide critical support for the collection of data on the impact of vendor's strategic operations, consumer's behaviours and what is the most desirable policy option and most conducive regulatory environment for such critical area of activity.
This questionnaire includes multiple-choice and open questions. You can only choose one option for each question. If a question is not applicable to you, or you do not know which option to choose, simply skip that question. Once an option is selected, it can be changed to another option, but you cannot completely remove your response.
All responses recorded, including any personal information you provide, will be kept strictly confidential. Your input will only be used in combination with the responses of others participating in the questionnaire. Our research examines the opinions of groups of respondents. Your individual responses will not be shown to anyone outside the study team.

B. Registry questions

What is your first name?

What is your last name?

What is your email address?

Please provide your email if you accept being contacted on the subject of the study
What is your type of organization?

- ☐ Evaluation lab
- ☐ Certification Authority
- ☐ Public Administration
- ☐ ICT Security expert
- ☐ Vendor (service/product)
- ☐ User (service/product)
- ☐ Other

What is your role/profession?

What is the name of your organisation?

What is the country where your organisation operates?

C. Evidence section

1. In your opinion what is the best strategy/policy option to increase consumer's trust and confidence in ICT products?

☐ Implement a bill of rights giving to customers a chance to make claims after having purchased ICT devices
☐ Adopt a certification and labelling scheme allowing customers to compare in an informed way which products offer the highest level of security
☐ Hard-law approach, increasing trust through the introduction of disciplinary sanctions
☐ Financial incentives to vendors encouraging them to regularly replace and/or update old products
☐ Other

If option "other" is ticked please provide further explanation:

2. Do you think security labelling of ICT products/services (whether certified or non-certified) is likely to impact consumers' behaviours despite any price considerations?

☐ Very likely
☐ Likely
☐ Indifferent
☐ Not likely
☐ Not likely at all
☐ Don't know

3. Do you think the consumer trust in the security properties of product/service is likely to increase when certifications are performed according to security requirements set by third party entities, as opposed to security requirements being freely chosen by vendors?

☐ Very likely
☐ Likely
☐ Indifferent
☐ Not likely
☐ Not likely at all
☐ Don't know

4. To which extent do you think the quality, reliability and exhaustiveness of information on the security property of ICT products is likely to influence consumer/user choice over other type of factors such as costs?

☐ Very likely
☐ Likely
☐ Indifferent
☐ Not likely
☐ Not likely at all
☐ Don't know

5. On average what is the range of costs for certifying an ICT service/product?

☐ < 10.000 €
☐ 10.000 € – 100.000 €

☐ 100.000 € – 1.000.000 €
☐ > 1.000.000 €

6. On average what is the range of costs of labelling of an ICT service/product (excluding any cost related to the certification process)?

☐ < 1.000 €
☐ 1.000 € – 50.000 €
☐ 50.000 € – 100.000 €
☐ > 100.000 €

7.* Can you please provide an example you are aware of a security certification requirement a company had to undertake to access the market of an EU country? *(specify at least name of certification, type of ICT product, country) (Include average costs from questions below)

Could you provide an educated estimate of compliance costs and time:

8.* Can you please provide an example you are aware of a security labelling requirement a company had to comply with in order to access the market of an EU country? *(specify at least name of labelling scheme, type of ICT product, country)

Could you provide an educated estimate of compliance costs and time:

9. Can you please provide an example you are aware of a case of national procurement bids/practices restricting open competition in favour of mandatory national certifications? *(specify type of ICT product, country, procurement procedures and enforcement e.g. mandatory or recommended)*

10. How likely do you think a large-sized company which has certified its product in a given EU country would restrain itself from entering the market of a second MS in consideration of additional security certifications requirements?

☐ Very likely
☐ Likely
☐ Indifferent
☐ Not likely
☐ Not likely at all
☐ Don't know

11. How likely do you think a SME which has certified its product in a given EU country would restrain itself from entering the market of a second Member State in consideration of additional security certifications requirements?

☐ Very likely
☐ Likely
☐ Indifferent
☐ Not likely
☐ Not likely at all
☐ Don't know

12. From your experience, what is the likelihood of an ICT product/service vendor to accept bearing the costs of a second certification/labelling process in order to access the market of another EU country?

☐ Very likely
☐ Likely
☐ Indifferent
☐ Not likely
☐ Not likely at all
☐ Don't know

13. In reference to commercial strategies, do you think a foreign vendor is likely to favour accessing an EU country having in place a mutual recognition agreement (in relation to security certification and labelling) with other EU countries?

☐ Very likely
☐ Likely
☐ Indifferent
☐ Not likely
☐ Not likely at all
☐ Don't know

14. In your opinion, in the context of a European ICT security certification Framework what role the EU Agencies (such as ENISA) might have at the management level (e.g. Establish transparent procedures)?

15. In your opinion, in the context of the creation of a European ICT security certification Framework what role the EU Agencies (such as ENISA) might have at the operational level (e.g. Identifying needs, cooperation, coordination, alerting)?

16. How likely do you think a European ICT security certification Framework would produce the following benefits?

1) higher consumer trust in the security properties of the product/service

☐ Very likely ☐ Likely ☐ Indifferent ☐ Not likely ☐ Not likely at all ☐ Don't know

2) higher number of certified/labelled products/services

☐ Very likely ☐ Likely ☐ Indifferent ☐ Not likely ☐ Not likely at all ☐ Don't know

3) lower time and cost of certification/labelling

☐ Very likely ☐ Likely ☐ Indifferent ☐ Not likely ☐ Not likely at all ☐ Don't know

4) reduction/elimination of fragmentation (meant as the existence of multiple national and sectorial certification schemes not mutually recognised)

☐ Very likely ☐ Likely ☐ Indifferent ☐ Not likely ☐ Not likely at all ☐ Don't know

Results

The Questionnaire results have been collected and analysed. Twenty-five Representatives from different type of organisation gave their contributes to the online Questionnaire. In the graphic below, the percentages of the types of organisation that have completed the Questionnaire are shown:

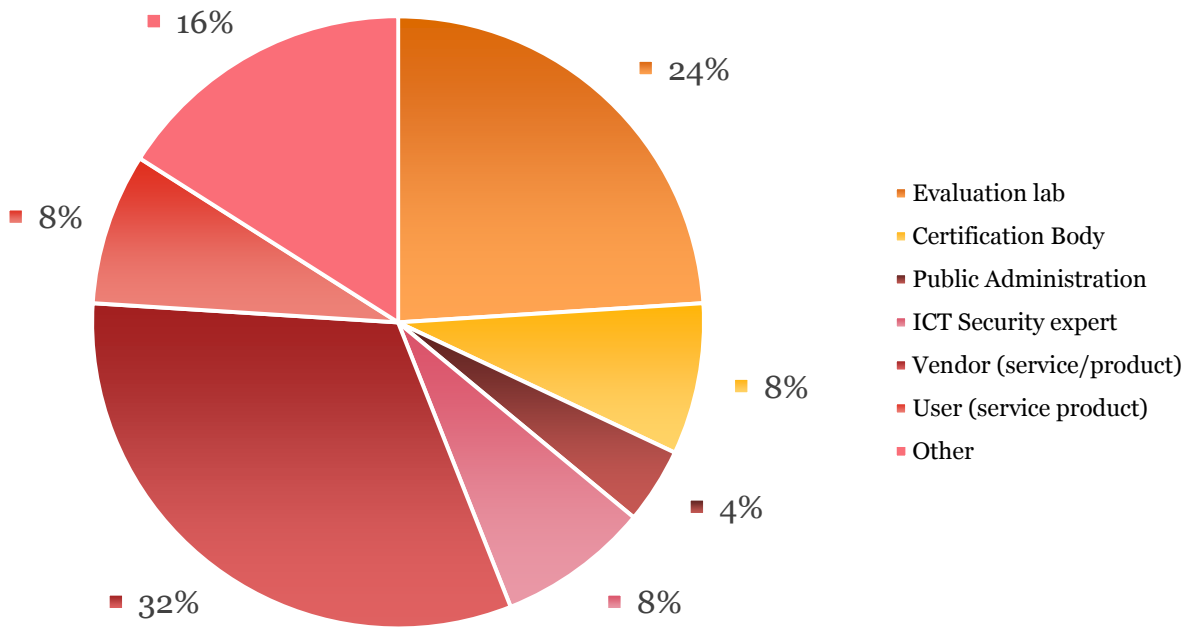
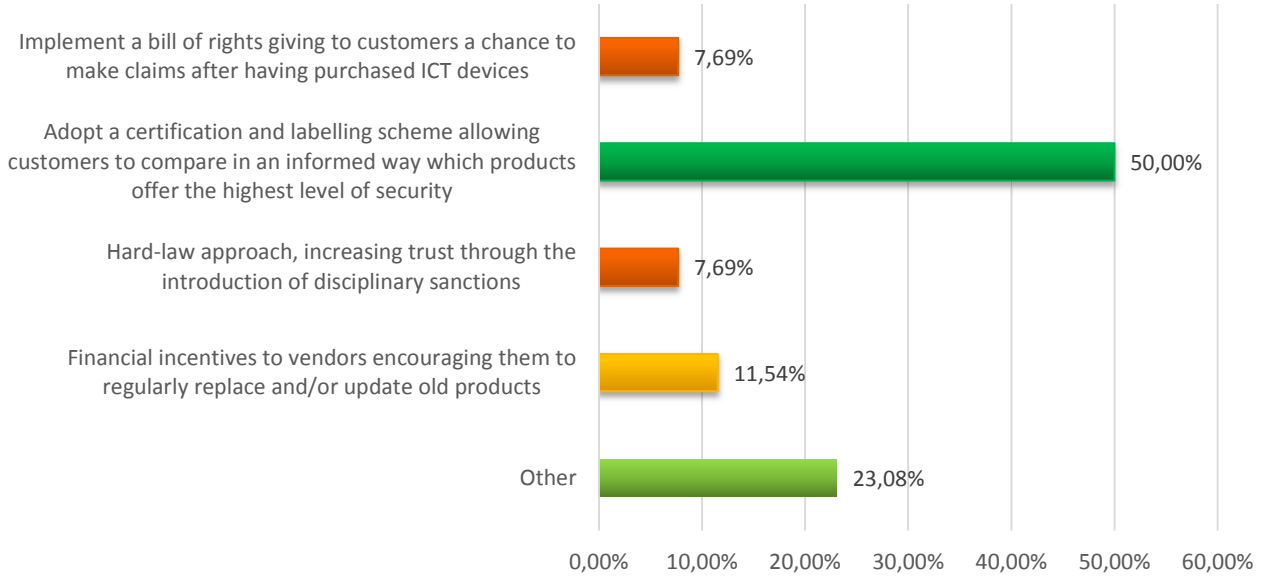


Figure - Type of Respondents

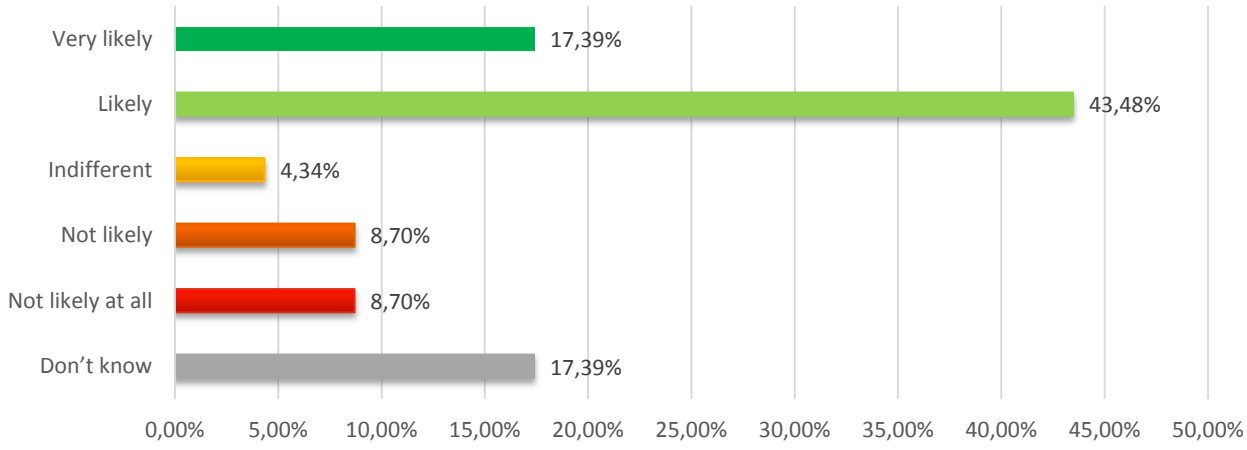
1. In your opinion what is the best strategy/policy option to increase consumer's trust and confidence in ICT products?



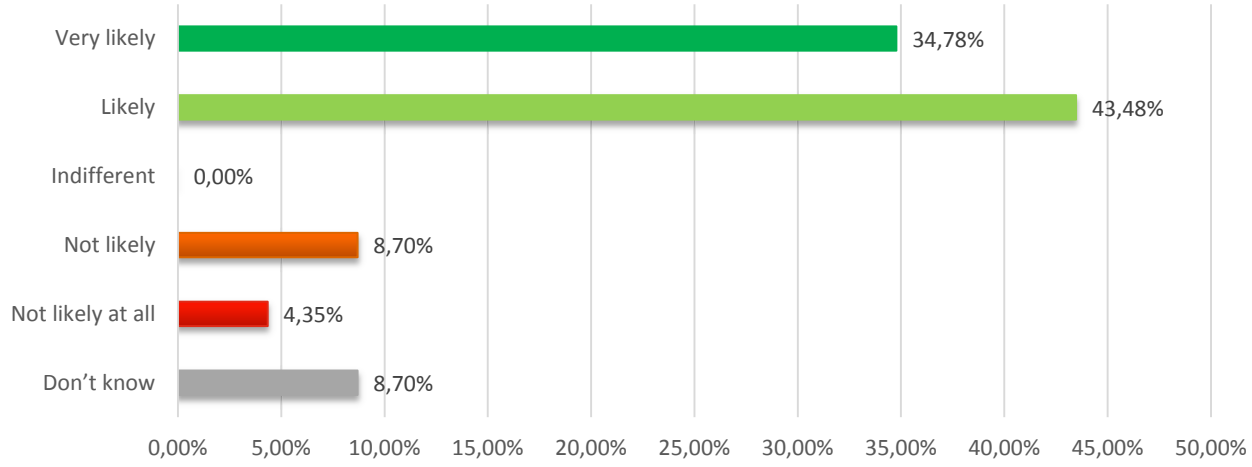
Explanations provided for the option "other":

1. Evidence of conformance with applicable, recognised standards
2. Hard-law approach translating IT security Requirements in Protection Profiles supporting CC evaluation/certification plus financial incentives to vendors encouraging them to certify their IT products/system and maintain the certifications through time
3. A mix of above-mentioned proposals would be the best strategy to increase consumer's trust and confidence, adopting an EU-wide certification and labelling scheme shall constitute the core of the future strategy of the European Commission. To be efficient, certification and labelling shall apply to all ICT products and services, therefore a hard-law approach is necessary. Remark: With regards to certification, Eurosmart advocates for a scalable approach linked to risk management. Depending on the different security and assurance levels, and on the robustness to be provided, the metascheme could encompass different certification schemes from self-assessment up to Common criteria highest levels.
4. Industry-led best practices (with government input) on cybersecurity baselines -> similar to the NIST Cybersecurity Framework as a model (could be adapted for EU needs) which is based on existing international security standards (and for which certifications are available) are critical in an effort to increase customer's trust and confidence in ICT products. In addition, financial incentives and government procurement power can play helpful roles if applied sensibly.

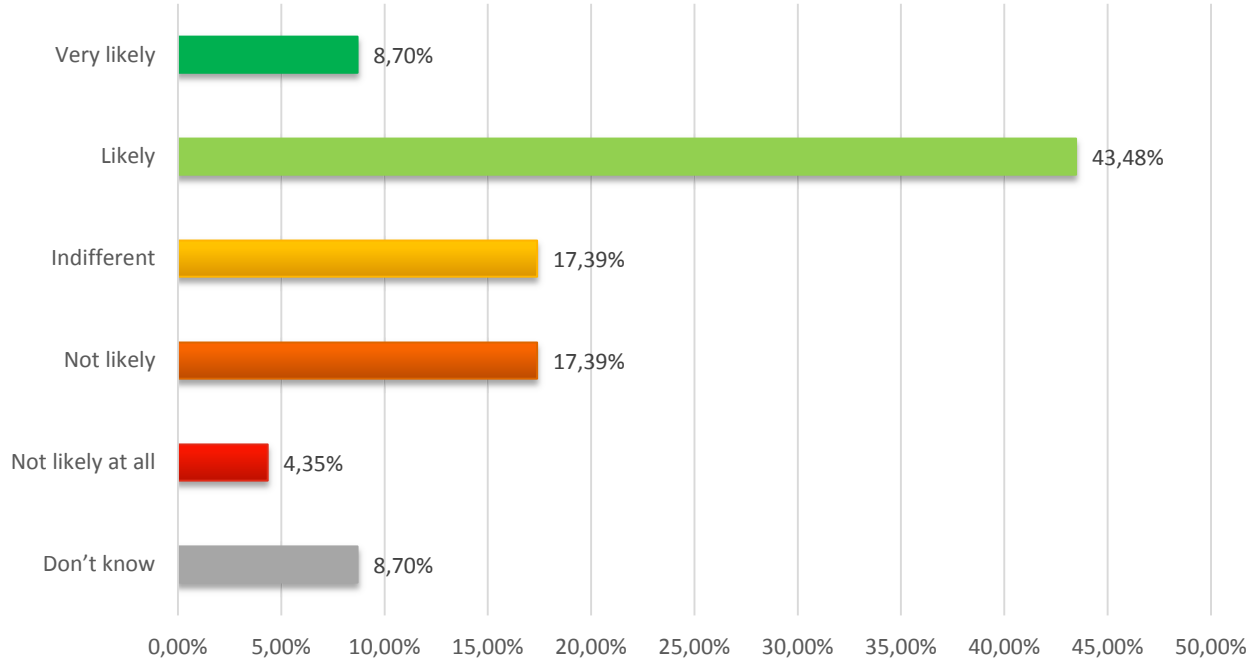
2. Do you think security labelling of ICT products/services (whether certified or non-certified) is likely to impact consumers' behaviours despite any price considerations?



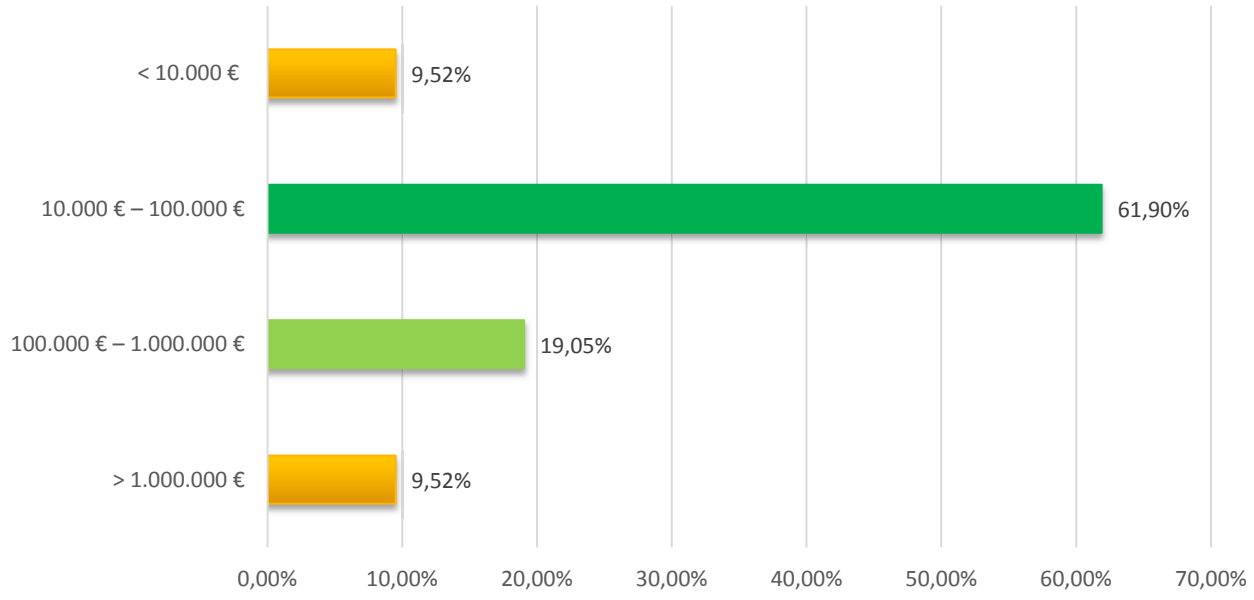
3. Do you think the consumer trust in the security properties of product/service is likely to increase when certifications are performed according to security requirements set by third party entities, as opposed to security requirements being freely chosen by vendors?



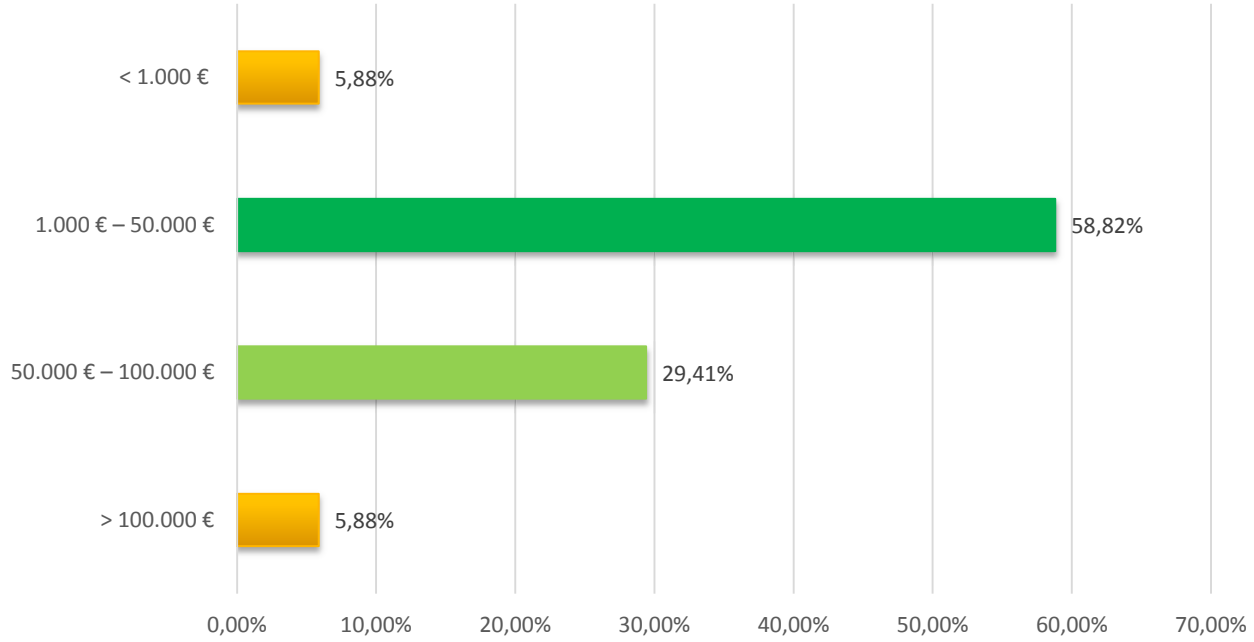
4. To which extent do you think the quality, reliability and exhaustiveness of information on the security property of ICT products is likely to influence consumer/user choice over other type of factors such as costs?



5. On average what is the range of costs for certifying an ICT service/product?



6. On average what is the range of costs of labelling of an ICT service/product (excluding any cost related to the certification process)?



7. Can you please provide an example you are aware of a security certification requirement a company had to undertake to access the market of an EU country? (Specify at least name of certification, type of ICT product, country) (Include average costs from questions below)

- "C5" standard is or will be required for public sector procurement of cloud services in Germany (note: C5 compliance is road mapped, but I am not sure if it's been completed yet) EN 301 549 is required for public procurement of ICT products and services ISO 27001 certification provides the basis for our compliance with EU Standard Contractual Clauses under the EU Data Privacy Directive ISO 27001 and 27018 also provide the basis of our compliance with other legal requirements under various privacy laws in the EU, including without limitation NEN 7510:2011 covering health information in the Netherlands and NHS data in the UK. UK G-Cloud is required to sell cloud computing to government customers in the UK.
- Mobile Network Operators require SIM cards to be certified using Common Criteria EAL4+ certification scheme
- ANSSI CSPN in France
- eID card in Germany. Cost are difficult to evaluate as it includes costs of hardware certification and cost of the composite (+/- €500.000).
- French CSPN certification
- Server signing according CEN protection profile
- smart metering, CSPN certification, France
- C-SEC Payment Terminal needed to sell in Germany and UK
- CSPN in France
- Not directly, however I have been assisting several healthcare / medical device manufacturers to implement ISO27001 and GDPR requirements. This has some overlap with the proposed certification
- Security certification requirement is not requested to access the market. Providing of Services (eg trusted services) is required to certify.
- Smart metering Gateway, BSI CC PP EAL 4+ certification
- eIDAS QSCD products

7.1 Could you provide an educated estimate of compliance costs and time:

- Compliance costs are well above $1M and time is in the 18 months range
- We do not disclose this information publicly.
- For Certification alone it would be 50k€ and 6 months. This does not include R&D costs.
- New common criteria certificates take between 9 and 12 months. For 2 CC certificates for the hardware running in parallel and another one for the composite it takes 1 year ½. It can be faster if hardware is already certified.
- 25k€ and 2 months
- 150000€
- 6 weeks, between 15 to 30 K euros
- 80K and 4 months
- 25 + 10 if crypto
- Very hard, depends entirely on the complexity of the product and the organizational structure.
- Currently only CCEAL4+ is requested as mandatory certification for trusted services. Few months and X0.000€ for smart cards, Many months for HSM and X00.000€ for HSM. Depending on manufacturer experience on Certification.
- 1 Mio / 5 Years
- 60000

8. Can you please provide an example you are aware of a security-labelling requirement a company had to comply with in order to access the market of an EU country? (Specify at least name of labelling scheme, type of ICT product, country)

- See above. Note that most requirements are "soft" – not required by law per se (except for public sector procurement) but a practical reality for customers who want assurances beyond a "trust me" approach by vendors.
- No
- IIF from BSI are German specific.
- No
- Digital Tachograph – Vehicle Unit (PP-0057) & Tachograph Card (PP-0070) & Motion Sensor (PP-0093
- CSPN
- See before, ISO 27001
- NO evidence of labelling requested outside the field of certification
- eIDAS QSCD product certification

8.1 Could you provide an educated estimate of compliance costs and time:

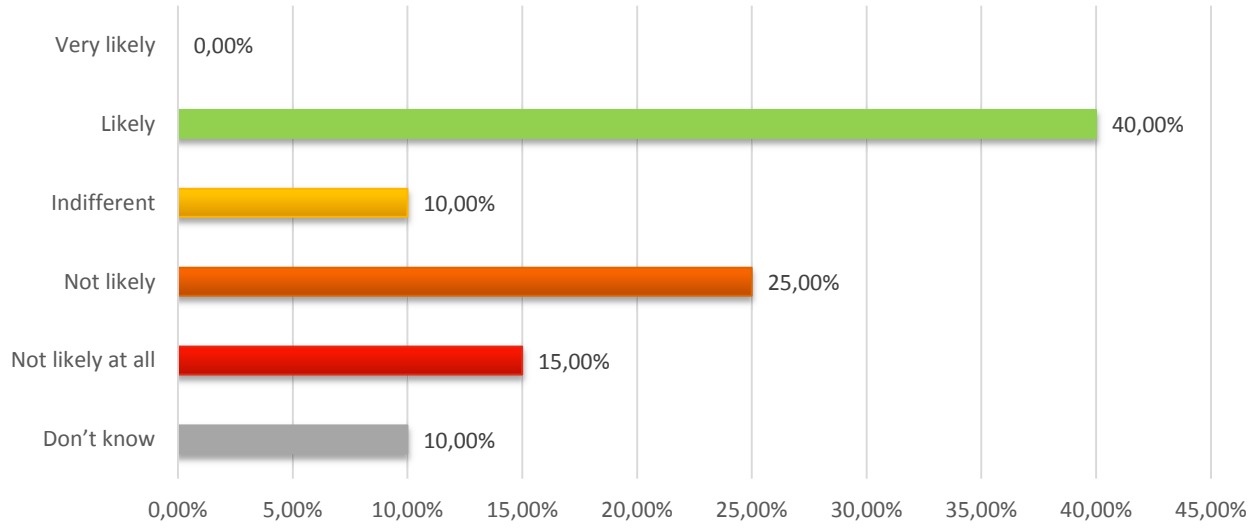
- We do not disclose this information.
- No
- 300000€
- Again, completely product and organization dependant.
- NO
- 60.000 EUR and 3-5 months

9. Can you please provide an example you are aware of a case of national procurement bids/practices restricting open competition in favour of mandatory national certifications? (Specify type of ICT product, country, procurement procedures and enforcement e.g. mandatory or recommended)

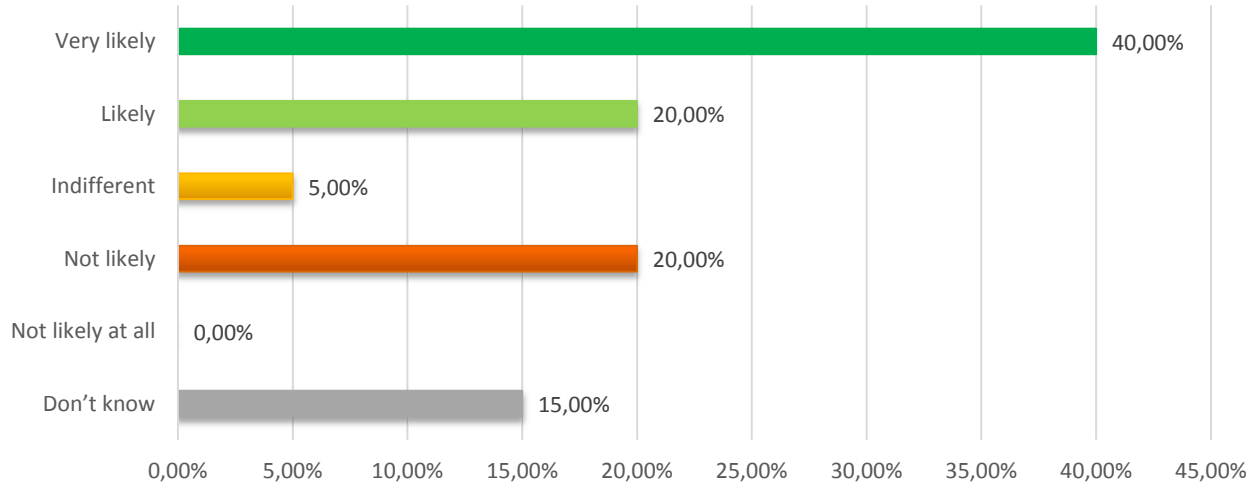
- CSPN in France for Military applications for Electrical Distribution
- No
- Passport, ID card, Driving licence,

- Common Criteria EAL4+, electronic passports
- German ePassports, ID cards, Healthcards, French SIM-cards
- In NL there have been several attempts over time to increase the adoption of open standards in general, not directly security related. All have been quite unsuccesful so far due to resistance from IT departments.
- Surveillance system - Italy - Public procurement - CC Certification
- Smart Metering around Europe / mainly in Germany
- eIDAS product e.g. eID documents and infrastructures. It is mandatory having the eIDAS compliance
- Certification by the Chinese Financial Authentication (CFA) scheme is required to enter the Chinese payment market for card (Secure Element) based payment
- To our knowledge, there is no national procurement practice that restricts open competition in favour of mandatory certification. Instead, most national procurement practices tend to have both open competition and certification requirements.

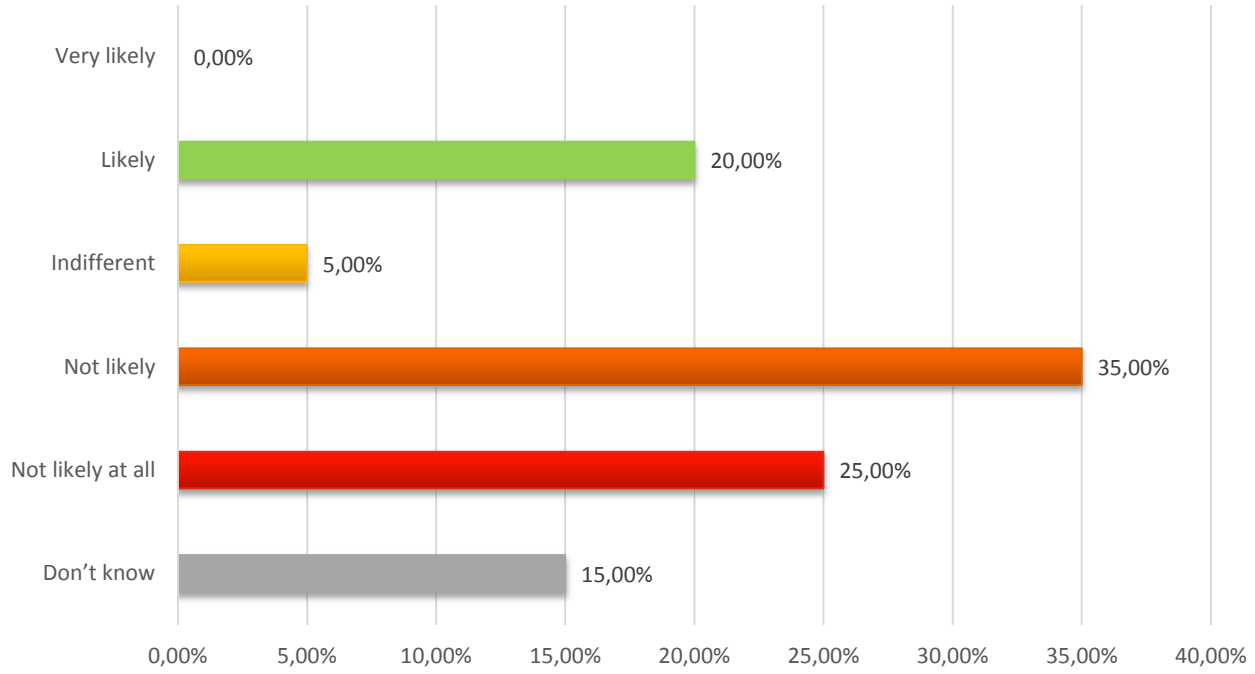
10. How likely do you think a large-sized company which has certified its product in a given EU country would restrain itself from entering the market of a second MS in consideration of additional security certifications requirements?



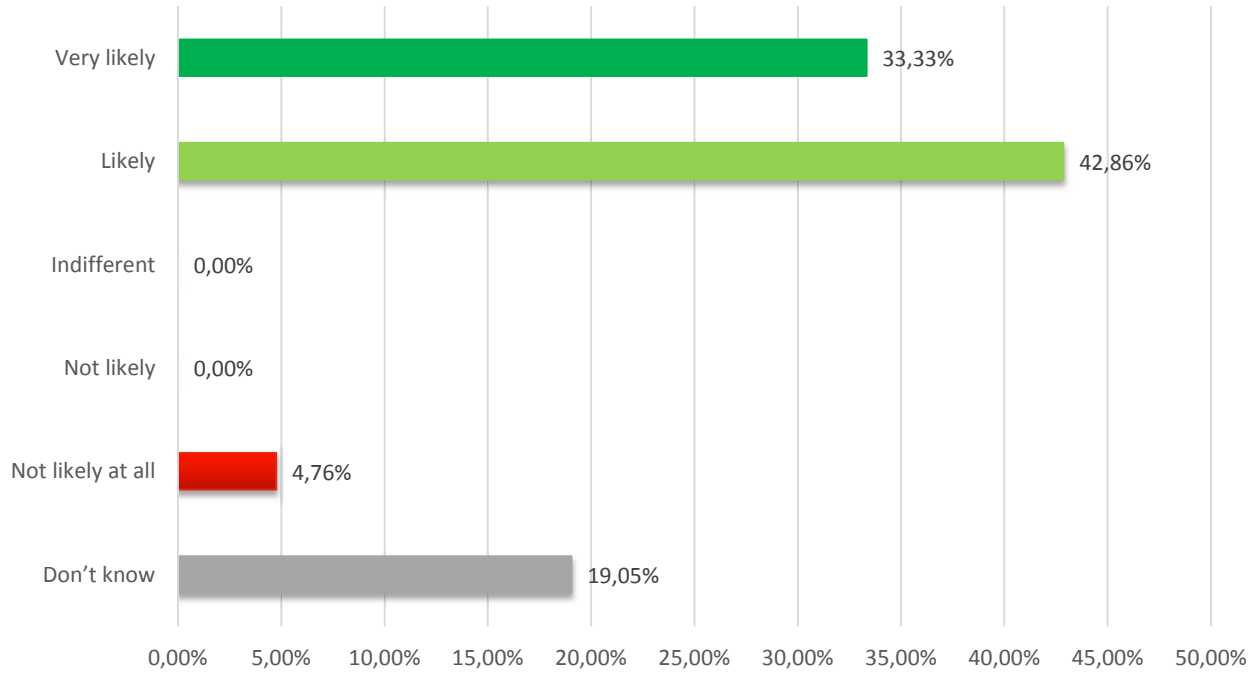
11. How likely do you think a SME which has certified its product in a given EU country would restrain itself from entering the market of a second Member State in consideration of additional security certifications requirements?



12. From your experience, what is the likelihood of an ICT product/service vendor to accept bearing the costs of a second certification/labelling process in order to access the market of another EU country?



13. In reference to commercial strategies, do you think a foreign vendor is likely to favour accessing an EU country having in place a mutual recognition agreement (in relation to security certification and labelling) with other EU countries?



14. In your opinion, in the context of a European ICT security certification Framework what role the EU Agencies (such as ENISA) might have at the management level (e.g. Establish transparent procedures)?

- Raising awareness, education, etc.
- The EU should ensure that in the context of ICT security certifications that 1) neither the EU nor Member States completely "re-invent the wheel" but instead leverage existing standards and certifications based on international standards. 2) The EU should strive to enable mutual recognition between comparable cybersecurity certifications - again ideally based on existing international standards.
- Governance, co-ordinate mutual recognition
- ENISA could endorse the role of a transversal agency which could be continuously active in identifying and registering expert groups that will be in charge of defining adequate certification levels per sector. ENISA could monitor what is enforced in terms of certification, and could be given a mandate to specific experts groups that would be in charge of defining in details these sectorial certifications.
- establish the same rules for the security certification scheme in the various CS
- ENISA will have a key role
- Coordination of National Security Agencies Technical Referential and procedures
- Identify the products/services, Establish procedures/methodologies, Maintain and harmonize the asurance level and competences (like SOG-IS is doing for Common Criteria evaluations)
- Partner
- Implement laws ensuring support and updates for released devices. And establish clear and transparent implementation procedures.
- define Directives for better integration
- Push for standardisation among member states of such ICT security certifications;
- Third party body as in any other EU Certification Scheme
- Harmonization of security certification requirements (eg security level required) and harmonization of approaches to certification of ICT security features in EU states
- Conformity Assessment Body centrally in order to enhance EU wide competition
- Drive mutual recognition, define procedures and frameworks e.g. Common Criteria

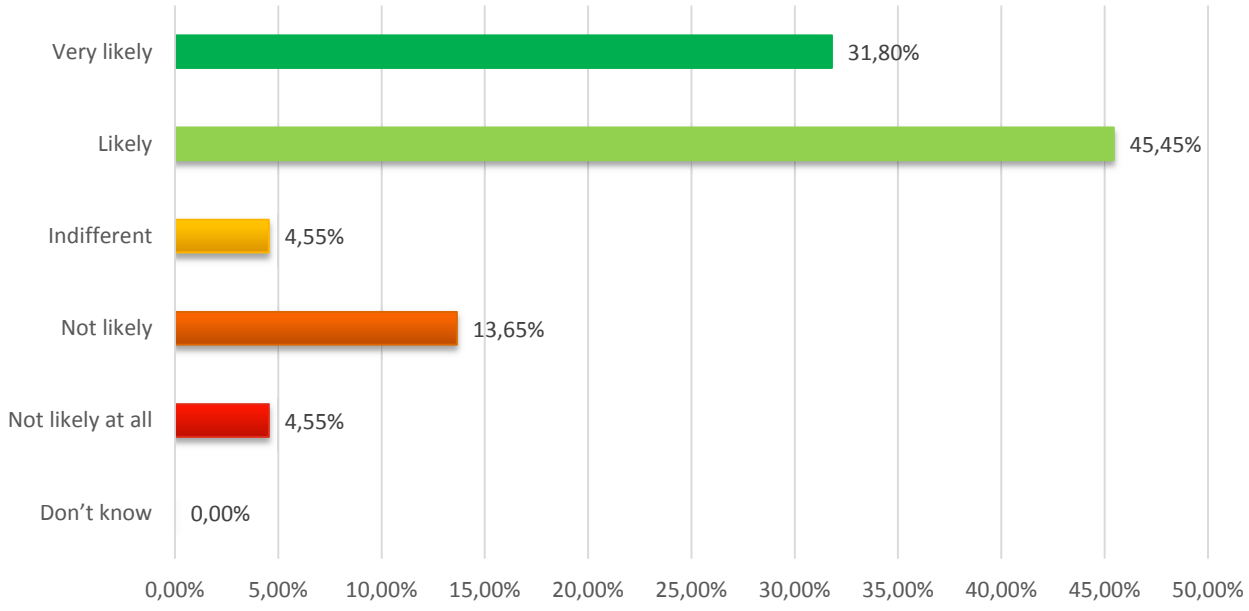
15. In your opinion, in the context of the creation of a European ICT security certification Framework what role the EU Agencies (such as ENISA) might have at the operational level (e.g. Identifying needs, cooperation, coordination, alerting)?

- Yes, all of those examples
- ENISA could help ICT vendors in Europe by deepening their mapping of available ICT security standards across the EU as well as other leading certifications (and/or industry led best practices), working to identify commonalies, overlap and opportunities for harmonization. ENISA is currently not set up to play an operational role and/or to advise on the implementation of particular certification frameworks.
- Co-ordination, information sharing
- ENISA could be a registration office for all new applicable certification schemes and standards depending on a specific market segmentation. Given its neutrality and independency, the European Union could be devolved the role of managing a potential labelling scheme for cybersecurity once certification schemes have been put in place.
- guarantee the skills of the different national certification scheme
- ENISA should be involved in CERT for ICT
- Promoting the security evaluation scheme, Providing market analysis, Funding security evaluations when ICT products or services are use by the EU

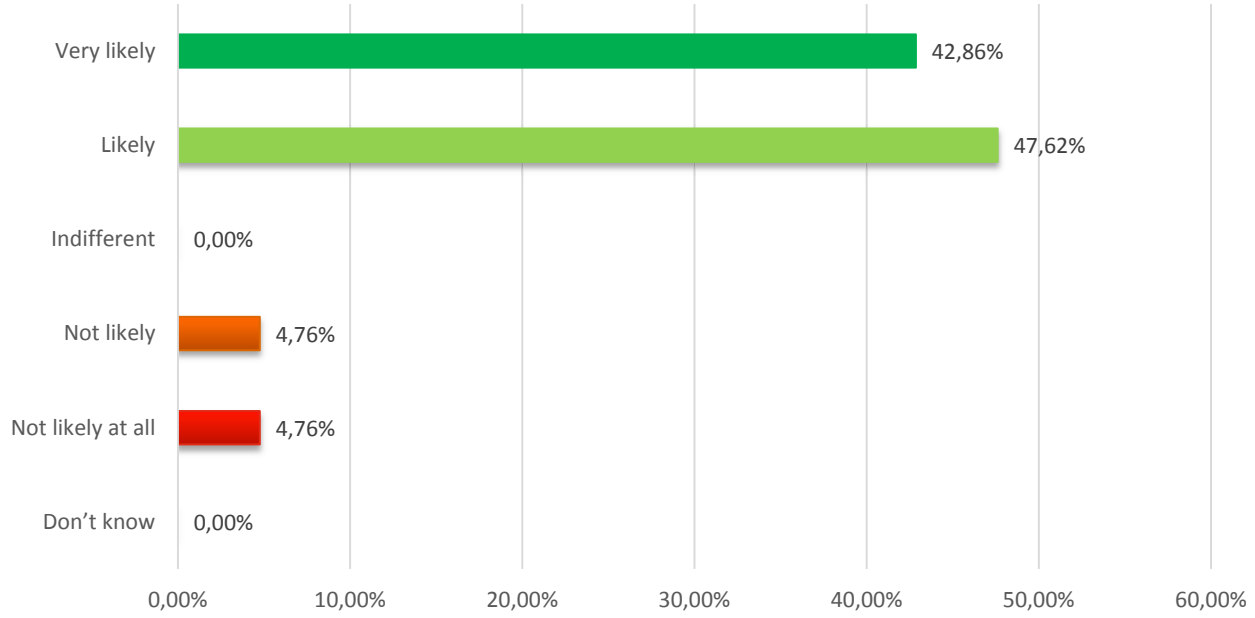
- Identifying needs through technology watch, ensuring the interoperability of the framework (very improtant), update the procedures/methodologies, maintain the list of certified products/services
- Coordination
- Verification, audits and validation.
- Analyse the market and the situation in different MS and provide support and/or encourage them to share and reuse best practices.
- Coordinating and Guarantee of fair behavior
- identifying needs, coordination, supervision
- Merge with SOG_IS and manage EU wide valid PPs for minimum security requirements
- Identifying needs and define and plan focus areas. Drive international cooperation

16. How likely do you think a European ICT security certification Framework would produce the following benefits?

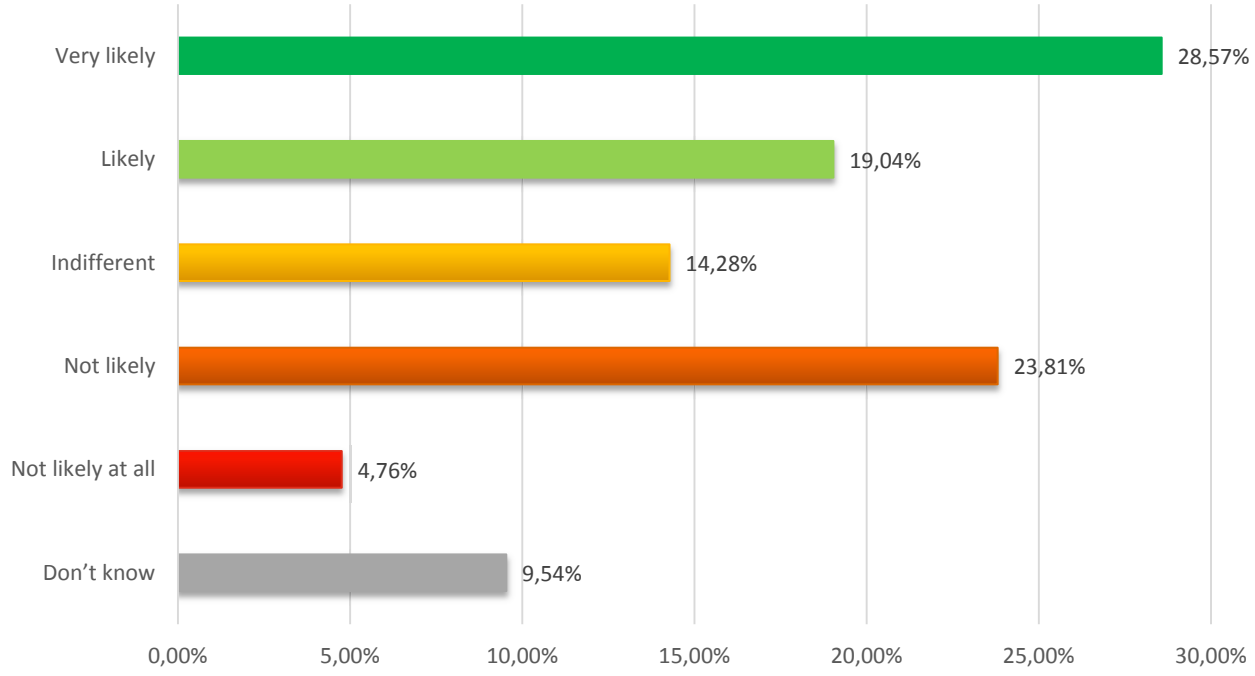
1) higher consumer trust in the security properties of the product/service



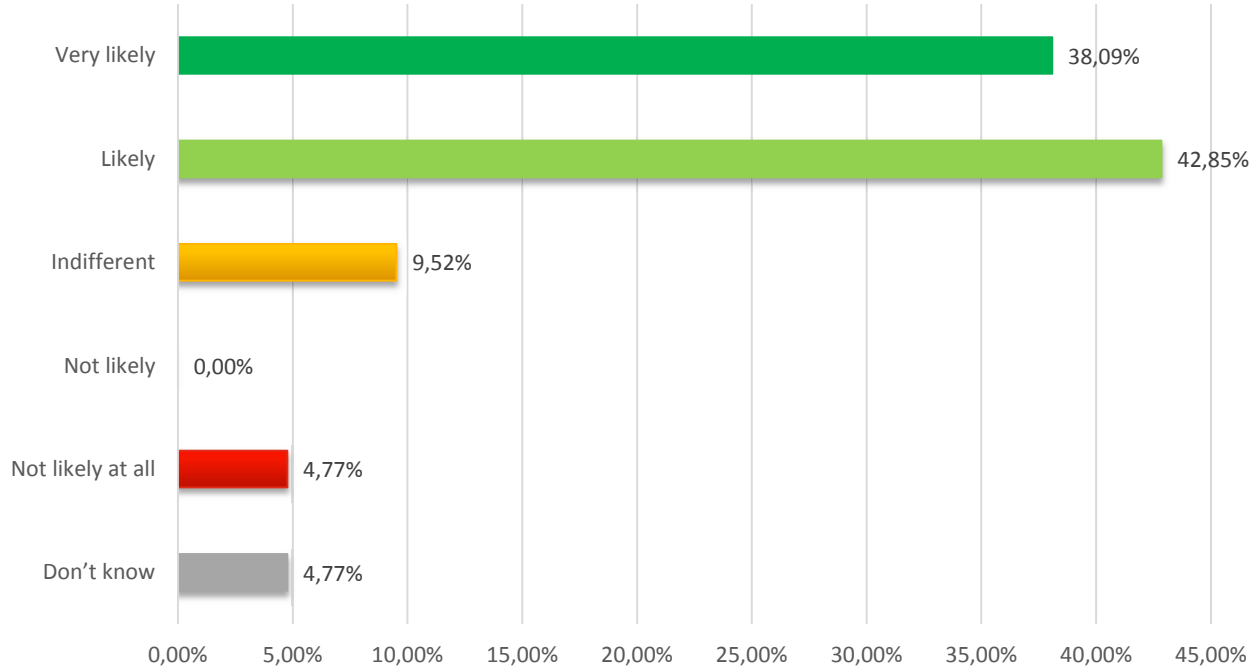
2) higher number of certified/labelled products/services



3) lower time and cost of certification/labelling



4) reduction/elimination of fragmentation (meant as the existence of multiple national and sectorial certification schemes not mutually recognised)



Analysis

The online Questionnaire has been broadly publicised sending email to selected and impacted stakeholders, albeit within the confined certification community, and contacting representatives of impacted organisations during events and workshop. To facilitate the presentation of the results, the survey questions have been grouped across four thematic areas, namely:

- **Consumer Trust & Labelling** comprising of questions 1, 2, 3 and 4
- **Time/Costs for Certifying/Labelling** comprising of questions 5, 6, 7.1, 8.1
- **Fragmentation** comprising of questions 7, 8 9, 10, 11 and 12
- **Policy Options and envisioned features** comprising of questions 13 through to 16

Consumer Trust & Labelling

In order to increase consumer trust and confidence in ICT products, **50%** of questionnaire participants agreed on the necessity to *adopt a certification and labelling scheme* allowing customers to compare in an informed way which products offer the highest level of security. A smaller percentage, 23,08%, of the respondents indicated the answer "Other" as the best policy/strategy option to follow, providing, for example, the following assertions:

- Hard-law approach translating IT security Requirements in Protection Profiles supporting CC evaluation/certification plus financial incentives to vendors encouraging them to certify their IT products/system and maintain the certfications through time
- A mix of policy/strategy options proposed would be the best strategy to increase consumer trust and confidence
- Industry-led best practices (with government input) on cybersecurity baselines. In addition, financial incentives and government procurement power could play helpful roles.

The majority of the questionnaire respondents think that security labelling of ICT products/services is likely to impact consumers' behaviours despite any price considerations. Indeed, **17,39%** of participants chosen

the answer "*Very likely*" and **43,48%** of respondents chosen the answer "*Likely*". Moreover, according to the large majority of respondents, consumer trust is likely to increase when certifications are performed according to security requirements set by third party entities as opposed to security requirements freely chosen by vendors.

Time/Costs for Certifying/Labelling

61,90% of questionnaire respondents indicated that the cost incurred for certifying an ICT service/product is between 10 thousand euros and 100 thousand euros. A smaller percentage, 19,05% answered that the cost incurred for certifying an ICT service/product are between 100 thousand euros and 1 million euros and only 9,52% of respondents indicated as 1 million or plus the cost incurred for certification. To better understand the answers provided, many examples can be mentioned according to the question 7.1:

- 25 thousand euros and 2 months
- 6 weeks, between 15 to 30 thousand euros
- 80 thousand euros and 4 months
- 1 million euros and 18 months
- 60 thousand euros

Looking at the answer provided by the respondents regarding time and cost of certification, it is necessary to distinguish the product/service that must be certified. In fact, time and cost depend entirely on the complexity of the product/service and the organizational structure. The same reasoning applies also to the costs of labelling. Being labelling a process not yet widely used for ICT products, the questionnaire respondents have not been able to give many examples of labelling time and costs. The only two quantitative answers are:

- 300 thousand euros
- 60 thousand euros and 3-5 months

Fragmentation

The issue of fragmentation is central to the study. Respondents gave many examples of ICT products that companies have to certify in order to access the market of an EU country. For example:

- eID cards in Germany
- Smart-metering devices
- SIM cards
- QSCD products

In many cases, as widely argued within this Interim Report, additional certifications are requested in order to access to other EU countries For example:

- CSPN
- BSI German Scheme

Many example were give for cases of national procurement bids/practices restricting open competition in favour of mandatory national certifications. The respondents gave the following answers:

- CSPN in France for Military applications for Electrical Distribution
- Common Criteria EAL4+ for electronic passports
- German ePassports, ID cards, Healthcards, French SIM-cards
- Surveillance system - Italy - Public procurement - CC Certification
- Smart Metering around Europe / mainly in Germany
- eIDAS product e.g. eID documents and infrastructures. It is mandatory having the eIDAS compliance

40% of respondents, giving the answer "*Likely*", think that a large-sized company which has certified its product in a given EU country would restrain itself from entering the market of a second MS in consideration of additional security certifications requirements. The same percentage of respondents gave the answer "*Very Likely*" talking on the same issue for SMEs. Is therefore evident that the greatest difficulties are faced by SMEs that in the vast majority of cases are not able to cope with the costs of a certification.

In the end, the majority of respondents, 35%, gave the answer "*Not Likely*" regarding the question asking the likelihood of an ICT product/service vendor to accept bearing the costs of a second certification/labelling process in order to access the market of another EU country.

Policy Options and envisioned features

A large majority of respondents indicated with the answers "*Very Likely*" and "*Likely*", respectively **33,33**% and **42,86%** of respondents, that a foreign vendor is likely to favour accessing an EU country having in place a mutual recognition agreement with other EU countries.
In the context of a European ICT security Certification Framework, all the respondents answered that the EU Agencies (such as ENISA) would play a key role both at management an operational level.
Very high percentages are observed regarding the benefits that could be produced by a European ICT Security Certification Framework:

- Regarding an increase of consumer trust in the security properties of the product/service, the respondents answered with "*Very Likely*" in the **31,80**% of the answers and with "*Likely*" in the **45,45**% of the answers
- Regarding an increase of certified/labelled products/service, the respondents answered with "*Very Likely*" in the **42,86**% of the answers and with "*Likely*" in the **47,62%** of the answers
- Regarding the reduction/elimination of fragmentation, the respondents answered with "*Very Likely*" in the **38,09%** of the answers and with "*Likely*" in the **42,85%** of the answers
- Regarding a decrease of time and cost of certification/labelling, the respondents answered with "Very Likely" in the **28,57**% of the answers and with "Likely" in the **19,04**% of the answers

It is clear that the vast majority of respondents believe that an EU ICT Security Certification Framework would produce many benefits, reducing fragmentation and increasing competitiveness of ICT market companies.

7.3 Stakeholder Mapping

Working with DG CONNECT it was possible 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. In particular, as requested by the Commission, the Consortium has contacted especially many representatives from National Certification Authorities, Smart-metering and Semi-conductors industries.
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.

The Consortium selected the most impacted stakeholders which are mapped below:

Recipient	Brief Description	Classification	Domain
Amossys	Security evaluations	Conformity Assessment Body	SOG-IS, CSPN, CC
Applus Laboratories	EVALUATION LAB	Conformity Assessment Body	SOG-IS, CC
Atsec	Laboratory and consulting services for information security	Conformity Assessment Body	SOG-IS, CC
Atsec	Laboratory and consulting services for information security	Conformity Assessment Body	SOG-IS, CC
Brightsight	Security evaluation specialist	Conformity Assessment Body	SOG-IS
Leti Cea Tech	Player in research, development and innovation	Conformity Assessment Body	SOG-IS, CSPN
INTA	Public Research Agency specialized in Aerospace technological research and development	Conformity Assessment Body	SOG-IS
CGI	Provide end-to-end IT and business process services	Conformity Assessment Body	SOG-IS
COMBITECH	Independent technical consulting company	Conformity Assessment Body	SOG-IS
Consorzio RES	Security Evaluation Laboratory; Evaluation Centre; Global Consultant	Conformity Assessment Body	SOG-IS
Datenschutz		Conformity Assessment Body	SOG-IS
DFKI	German Research Center for Artificial Intelligence	Conformity Assessment Body	SOG-IS
Epoche and Espri	IT security evaluation and testing services	Conformity Assessment Body	SOG-IS
IMQ	Certification Authority and a European leader in conformity assessments and laboratory tests	Conformity Assessment Body	SOG-IS
SELTA	Leading in the design of solutions for network's automation in the field of energy and transport	Conformity Assessment Body	SOG-IS
MTG	Independent consulting and software company	Conformity Assessment Body	SOG-IS
Norconsult	Multidisciplinary consultancy firms in the Nordic re	Conformity Assessment Body	SOG-IS
NTT Security	Consulting services, managed security services and technology solutions	Conformity Assessment Body	SOG-IS
Oppida	Evaluation and consulting services	Conformity Assessment Body	SOG-IS, CSPN

Recipient	Brief Description	Classification	Domain
Riscure	Global security test lab	Conformity Assessment Body	SOG-IS
Secuvera	Security Consulting	Conformity Assessment Body	SOG-IS
Serma-Safety-Security	Security formal evaluation, Security expertize and consulting; Safety expertize and consulting.	Conformity Assessment Body	SOG-IS, CSPN
Sogeti	Technology and Engineering Services	Conformity Assessment Body	SOG-IS, CSPN
Src-Gmbh	Provide service in the areas of information technology and information security	Conformity Assessment Body	SOG-IS
Cclab	Evaluation services	Conformity Assessment Body	SOG-IS
Technisblu	IT consulting	Conformity Assessment Body	SOG-IS
Thalesgroup	Safety and Security Solutions	Conformity Assessment Body	SOG-IS, CSPN
T-Systems	Integrated solutions for the networked future of business and society	Conformity Assessment Body	SOG-IS
Tuvit	IT security	Conformity Assessment Body	SOG-IS
UL	Global leader in safeguarding security, compliance, and global interoperability	Conformity Assessment Body	SOG-IS
Roke	Evaluation LAB	Conformity Assessment Body	CPA
KPMG	Evaluation LAB	Conformity Assessment Body	CPA
Context	Evaluation LAB	Conformity Assessment Body	CPA
Dnv-Gl	Evaluation LAB	Conformity Assessment Body	CPA
Info-Assure-Ltd	Evaluation LAB	Conformity Assessment Body	CPA
NCC Group	Evaluation LAB	Conformity Assessment Body	CPA
Siventure	Evaluation LAB	Conformity Assessment Body	CPA
CGI IT UK Ltd	Evaluation LAB	Conformity Assessment Body	CPA
EDSI	Evaluation LAB	Conformity Assessment Body	CSPN
Lexfo	Evaluation LAB	Conformity Assessment Body	CSPN
QuarksLab	Evaluation LAB	Conformity Assessment Body	CSPN
Serma Safety	Evaluation LAB	Conformity Assessment Body	CSPN
Synacktiv	Evaluation LAB	Conformity Assessment Body	CSPN
Trusted Labs	Evaluation LAB	Conformity Assessment Body	CSPN
Blancco	CPA-CC -CSPN fragmentation example		CPA, CC, CSPN
ANNSI	French CB	Conformity assessment and Certification Authorities	

Recipient	Brief Description	Classification	Domain
CCN	Spanish CB	Conformity assessment and Certification Authorities	
BSI	German CB	Conformity assessment and Certification Authorities	
BSI	German CB	Conformity assessment and Certification Authorities	
BSI	German CB	Conformity assessment and Certification Authorities	
NSCS	UK CB	Conformity assessment and Certification Authorities	
FICORA	Finland CB	Conformity assessment and Certification Authorities	
SERTIT	Norvegian CB	Conformity assessment and Certification Authorities	
NLNCSA	Netherlands CB	Conformity assessment and Certification Authorities	
OCSI	Italian CB	Conformity assessment and Certification Authorities	
NASK	Poland CB	Conformity assessment and Certification Authorities	
Bundeskanzleramt	Austria CB	Conformity assessment and Certification Authorities	
FMV	Sweden CB	Conformity assessment and Certification Authorities	
JHAS	Smart card JIL WG	Vendor(Product/Service)	
JEDS	HW devices JIWL WG	Vendor(Product/Service)	
Eurosmart (gemalto)	Smart card Community	Vendor(Product/Service)	
ESMIG	Smart Meters Association	European & International Organizations	Smart-meters
ESMIG	Smart Meters Association	European & International Organizations	Smart-meters
EMVco		End-users	
NXP	Semi condusctors Industry	Vendor (Product/Service)	Semi-conductors
Infineon	Semi condusctors Industry	Vendor (Product/Service)	Semi-conductors
BEAMA	UK association for T&D europe	Vendor (Product/Service)	Smart-meters
GIMELEC	FR association for T&D europe	Vendor (Product/Service)	Smart-meters
AFBELL	SP association for T&D europe	Vendor (Product/Service)	Smart-meters
ANIMEE	PT association for T&D europe	Vendor (Product/Service)	Smart-meters
ANIE	IT association for T&D europe	Vendor (Product/Service)	Smart-meters
SWISSMEM	CH association for T&D europe	Vendor (Product/Service)	Smart-meters
FEEI	AT association for T&D europe	Vendor (Product/Service)	Smart-meters
ZVEI	GE association for T&D europe	Vendor (Product/Service)	Smart-meters

Recipient	Brief Description	Classification	Domain
AGORIA	BE association for T&D europe	Vendor (Product/Service)	Smart-meters
FEDET	NL association for T&D europe	Vendor (Product/Service)	Smart-meters
EMSAD	TK association for T&D europe	Vendor (Product/Service)	Smart-meters
AEM		Vendor (Product/Service)	Smart-meters
Bitron		Vendor (Product/Service)	Smart-meters
CESI		End-users	Smart-meters
e-distribuzione		End-users	Smart-meters
Prodti	Academics / no profit foundation		Smart-meters
Sagemcom Broadband Sas		End-users	Smart-meters
Schneider electric		Vendor (Product/Service)	Smart-meters
TelecontroSTM		End-users	Smart-meters
Atmel		Vendor (Product/Service)	Smart-meters
Ayesa		Vendor (Product/Service)	Smart-meters
MAC		Vendor (Product/Service)	Smart-meters
landgyr	Smart meter vendor, CPA certified smart meter product	Vendor (Product/Service)	Smart-meters
EDMI Europe	Smart meter vendor, CPA certified smart meter product	Vendor (Product/Service)	Smart-meters
Siemens		Vendor(Product/Service)	Smart-meters
ST Microelectronics	Global Semiconductors company	Vendor(Product/Service)	Semi-conductors
ESIA	Voice of the Semiconductor Industry in Europe	European & International Organizations	Semi-conductors
UEAPME	Voice of SMEs in Europe	European & International Organizations	SMEs
Digital SME Alliance	European association exclusively focused on representing the interests of the SME community in the ICT sector.	European & International Organizations	SMEs
SBS	Represent and defend small SMEs interests in the standardisation process at European and international levels	European & International Organizations	SMEs
ANIE		Vendor (Product/Service)	Semi-conductors
Fraunhofer Group	Service provider for R&D in the areas of microelectronics and smart systems integration	Vendor (Product/Service)	Semi-conductors
GlobalFoundries	leading full-service semiconductor design, development, fabrication and innovation company with locations across the globe.	Vendor (Product/Service)	Semi-conductors
Imec	R&D solutions, innovation services applicable to both products and services	Vendor (Product/Service)	Semi-conductors

Recipient	Brief Description	Classification	Domain
Micron	global leader in the semiconductor industry	Vendor (Product/Service)	Semi-conductors
TDK	Semiconductor Solutions for Automotive and Industrial Electronics	Vendor (Product/Service)	Semi-conductors
Namium	Advanced assembly and test services to a global customer base of semiconductor companies	Vendor (Product/Service)	Semi-conductors
Rhom	Semiconductor Corporate	Vendor (Product/Service)	Semi-conductors
FAB	The world's largest analog/mixed-signal foundry group	Vendor (Product/Service)	Semi-conductors
Texas Instruments	Global semiconductor company operating in 35 countries	Vendor (Product/Service)	Semi-conductors
Nuki	Turn smartphone into smart keys	Vendor (Product/Service)	Smart-Lock Door
August	Design products and services that let everyday people monitor and manage entry into their homes from wherever they are	Vendor (Product/Service)	Smart-Lock Door
Igloohome	Makes homes and properties smarter	Vendor (Product/Service)	Smart-Lock Door
Mul-T-Lock	High Security Locking and access control solution	Vendor (Product/Service)	Smart-Lock Door
Friday	The world's smallest smartlock	Vendor (Product/Service)	Smart-Lock Door
SmartLOCK	market leader in connected access solutions	Vendor (Product/Service)	Smart-Lock Door
DanaLock	Danish smart-lock company	Vendor (Product/Service)	Smart-Lock Door
Clay	Wireless, cloud-based smart lock technology company	Vendor (Product/Service)	Smart-Lock Door
Smart Video & Sensing Limited	Value Added Reseller (VAR) of optical based survey solutions, Video Incident detection systems / Video Analytics and high end digital CCTV	Vendor (Product/Service)	Smart-CCTV
Smartvue	IoT video solutions	Vendor (Product/Service)	Smart-CCTV
Swann	Global leader in security monitoring, consumer electronics and security-centric solutions for the smart homes and businesses of today and tomorrow	Vendor (Product/Service)	Smart-CCTV
Graz University, Austria		Other	Semi-conductors
STMicroelectronics		Vendor (Product/Service)	Semi-conductors
Infineon Technologies		Vendor (Product/Service)	Semi-conductors
Infineon Technologies		Vendor (Product/Service)	Semi-conductors
Infineon Technologies		Vendor (Product/Service)	Semi-conductors
Leonardo		Vendor (Product/Service)	Semi-conductors
Radboud University, The Netherlands		Other	Semi-conductors
ENS, France		Other	Semi-conductors

Recipient	Brief Description	Classification	Domain
Eurosmart	Is an international association located in Brussels representing the Voice of the Smart Security Industry for multi-sector applications	European & International Organizations	Smart Security Industry
Eurosmart	Is an international association located in Brussels representing the Voice of the Smart Security Industry for multi-sector applications	European & International Organizations	Smart Security Industry
Eurosmart	Is an international association located in Brussels representing the Voice of the Smart Security Industry for multi-sector applications	European & International Organizations	Smart Security Industry
ST Microelectronics	Global semiconductor company	Vendor (Product/Service)	Semi-conductors
ST Microelectronics	Global semiconductor company	Vendor (Product/Service)	Semi-conductors

Critical Infrastructures

Recipient	Brief Description	Classification	Domain
World Energy Council	Network of Energy stakeholders	Operator	Energy
ServiTecno	Software and Iot for companies	Producer	Energy, Healthcare
STE S.p.a	Innovation and & Communication Technology	Operator	Energy
RSE Spa, T&D Techologies Dpt	Ricerca Sul Sistema Energetico	Operator	Energy
AIIC	Associazione Italiana esperti Infratttutture Critiche	Operator	Energy, Healthcare, Transport, Finance
Marsh	Insurance Broking, cybersecurity services for transports	Operator	Transportation
Avantune	startup, cloud services, Member of the AIIC	Producer	Finance
Digital Europe	Services for Digital transfromation in the fields of finance and Healthcare	Producer	Fianance, Healthcare
Data Security Solutions	Data security solutions, including for the Healthcare system, based in Riga, Latvia	Producer	Healthcare
CER (Community of European Railway and Infrastructure Companies)	CER represent the interests of its members on the EU policy-making scene, in particular to support an improved business and regulatory environment for European railway operators and railway infrastructure companies.	Operator	Transport
Taxify.eu	ridesharing app in Europe & Africa - Estonia	Operator	Transportation
NewBanking	Based in Denmark. Services for Financial digital security and blockchains. NewBanking (www.newbanking.com) delivers verified money - KYC with payments - as a service to enterprise customers	Producer	Finance
ESI Group	The ESI Group specialise in Material Physics and are innovators in Virtual Prototyping addressing the need for products and processes which are both smart and autonomous, thus supporting industry in digital transformation	Operator	Energy
Kraft CERT	Cybersecurity for the National Energy Sector in Norway	Producer	Energy
Ansaldo Energia S.p.A.	leading international player in the power generation industry,	Producer	Energy
SOFTECO	IT Solutions for business development, Transport, Finance,	Producer	Transportation,

Recipient	Brief Description	Classification	Domain
	Energy		Finance, Energy
Newron Pharmaceuticals	Leader in the development of innovative therapies for Central Nervous System (CNS)	Producer	Healthcare
Bayer AG	Major Pharmaceutical company in Europe	Producer	Healthcare
Philips	A leading health technology	Producer	Heathcare
Air France KLM	France's major airline	Operator	Transportation
Easyjet	Europe's leading airline	Operator	Transportation
FERROVIE DELLO STATO ITALIANE S.p.A.	Italy's railway company	Operator	Transportation
SNCF	France's railway company	Operator	Transportation
Deutsche Bahn AG	Germany's railway company	Operator	Transportation
F. Hoffmann-La Roche Ltd	A global pioneer in pharmaceuticals and diagnostics	Producer	Healthcare
Finance Norway	Financial services in Norway	Operator	Finance
ING Group	Financial products and services	Producer	Finance
AXA	Pan European and global Insurance player headquartered in France. AXA strives for an integrated single market in the Insurance sector.	Operator	Finance
Assicurazioni Generali S.p.A	Leading insurance company in Italy	Operator	Finance
Société Générale	French Bank	Operator	Finance
HSBC Holdings PLC	HSBC is one of the world's largest banking and financial services organisations	Operator	Finance
Aviva Plc	UK's largest insurer with strong businesses in selected European markets	Operator	Finance
Shire	Leading global biotechnology company	Producer	Healthcare
Sanofi	Global healthcare leader	Producer	Healthcare
AstraZeneca	Global research-based biopharmaceutical company headquartered in the UK.	Operator	Healthcare
Alitalia	Italian ariline	Operator	Transportation
Meridiana fly S.p.A.	Italian ariline	Operator	Transportation
Tap Portugal	Portoguese Airline	Operator	Transportation
GlaxoSmithKline	Global healthcare company, based in UK	Operator	Heathcare
Crédit Agricole S.A.	Bank and Insurance	Operator	Finance
BNP Paribas Personal Finance	Bank and Insurance	Operator	Finance
UK Finance	UK Finance represents nearly 300 of the leading firms providing finance, banking, markets and payments-related services in or from the UK.	Operator	Finance
Nederlandse Waterschapsbank	Nederlandse Waterschapsbank N.V. (NWB Bank) is a leading financial services provider for the public sector.	Operator	Finance
PPRO Financial Ltd	PPRO Group is a cross-border e-payment specialist removing the complexity of international e-commerce payments by acquiring, collecting and processing an extensive range of alternative payments methods for PSPs under one contract, through one platform and one single integration.	Producer	Finance
CLECAT - European association for forwarding, transport, logistic	CLECAT was established in 1958 in Antwerp, it is now located in Brussels and it represents the interests of 24 members (consisting of national organisations of EU freight related service providers, as well as various observer and	Operator	Transportation

Recipient	Brief Description	Classification	Domain
and Customs services	associate members).		
Virtu Financial Ireland Limited	Virtu Financial Ireland Limited is a wholly owned subsidiary of Virtu Financial, Inc. and is a market-leading liquidity provider in European markets with a focus on equities, exchange traded funds and exchange traded derivatives.	Operator	Finance
Morgan Stanley	Morgan Stanley (NYSE: MS) is a leading global financial services firm providing investment banking, securities, wealth management and investment management services.	Operator	Finance
FEXCO Merchant Services Unlimited Company	Provider of Innovative Fintech, Payments & Business Solutions for merchants, acquirers and other businesses	Operator	Finance
Kreditech Holding SSL GmbH	Improving financial freedom for the underbanked by the use of technology.	Operator	Finance
Groupe GTI	Financial operations, with a focus in the field of structured finance and asset securitization.	Producer	Finance
Febelfin	Febelfin vzw/asbl (non-profit association) is the Belgian Financial Sector Federation. It tries to reconcile the interests of its members with those of the policy makers, supervisors, trade associations and pressure groups at the national and European level.	Operator	Finance
Fintech France	Promoting French Fintech Abroad	Producer	Finance
UIRR, International Union for Road-Rail Combined Transport	The International Union for Road-Rail Combined Transport (UIRR) represents European road-rail Combined Transport operators, as well as Transhipment Terminal Managers, who organise this ecologically and economically sustainable system of freight transport.	Operator	Transportation
UITP - International Association of Public Transport	UITP covers all modes of public transport - bus and other road collective transport, rail including tramway, metro, light rail, regional and suburban railways, and waterborne transport. It represents collective transport in a broader sense.	Operator	Transportation
Olivetti	Olivetti S.p.A. is an Italian manufacturer of typewriters, computers, tablets, smartphones, printers, etc. Today it is also specialized in Cloud Computing, ICT and much more	Producer	Energy
Cisco	American multinational technology conglomerate, specialised into specific tech markets	Producer	Energy
ING Group	Dutch multinational banking and financial services corporation headquartered in Amsterdam. Its primary businesses are retail banking, direct banking, commercial banking, investment banking, asset management, and insurance services.	Operator	Finance
Addison Lee	London-based private hire company	Operator	Transportation
Allianz	German financial services company headquartered in Munich, Germany. Its core businesses are insurance and asset management	Operator	Finance
Banco Santander	Spanish banking group	Operator	Finance
HSBC	British] multinational banking and financial services holding company	Operator	Finance
Orange	French multinational telecommunications corporation	Operator	Telecommunications
Vodafone	Multinational telecommunications company	Operator	Telecommunications
Telefonica	Spanish multinational broadband and telecommunications provider	Operator	Telecommunications

Recipient	Brief Description	Classification	Domain
Ryanair	Irish low-cost airline	Operator	Transportation
CIPRE	Critical Infrastructure protection & resilience europe	Expert	Energy
FCA	Financial regulatory body in the United Kingdom	Operator	Finance
Payments UK	300 firms in the UK providing credit, banking, markets and payment-related services	Operator	Finance
London Digital Security Centre (LDSC)	ActionFraud is the UK's national fraud and cyber crime reporting centre	Operator	Finance
Belgian Cybersecurity Coalition	The Cyber Security Coalition brings together the academic world, the public authorities and the private sector in Belgium to fight against cybercrime.	Operator	Telecommunications, Security
CISQ	The Consortium for IT Software Quality (CISQ) is an IT industry group comprising IT executives from the Global 2000, systems integrators, outsourced service providers, and software technology vendors committed to making improvements in the quality of IT application software	Operator	IT, Certification
Deutsche Bahn (DB)	German railway company	Operator	Transport
ATOS R&I (ARI)	Global leader in digital transformation with approximately 100000 employees in 72 countries and annual revenue of around € 12 billion.	Operator	Security
NATO ENERGY SECURITY CENTRE OF EXCELLENCE	Energy security research center of NATO	Expert	Energy
Royal Holloway University of London	University of London with an Information Security Group	Expert	Energy
University of Twente	University of Twente, with a Cyber Security and Safety Group	Expert	Energy
Universität der Bundeswehr München & Cyber Security Research Lab of Airbus	Cyber Security Laboratories	Expert	Energy
Fire Eye	Cybersecurity company that provides products and services to protect against advanced cyber threats,	Producer	Finance
RSE (ricerca sistema energetico)	Research company in the energy field	Expert	Finance, Security
Certiquality	Italian certification body	Expert	IT, Certification
University of Malaga, Spain	University of Malaga	Expert	Energy
Acris GmbH	Manufacturer of Healthcare products and technologies	Producer	Health Care
European Cyber Security Organisation (ECSO) ASBL	ECSO represents the industry-led contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP).	Operator	IT, Security
EOS' Civil Aviation Security Working Group Chair	EOS Security Screening and Detection Technologies Working Group	Operator	Transport
EOS Urban security project	EOS' Working Groups seek the establishment of a meaningful public-private dialogue to further their domains' objectives in partnerships where user demands are met by feasible security solutions and services for the protection of Europe and its citizens'	Operator	Transport
Smiths Detection	Industry expert manufacturer of security detection devices	Producer	Transport

Recipient	Brief Description	Classification	Domain
SC SAFETECH INNOVATIONS SRL	Cyber security solutions, including infrastructures	Operator	Finance
Easy Smart Grid GmbH	Developing an innovative smart grid solution	Producer	Energy
European Electronic Component Manufacturers Association	Under the EECA's umbrella organization, there are 2 autonomous industry associations with members coming from the manufacturing and related industries as well as from national associations	Producer	Energy
European Passive Components Industry Association	Represent and promote the common interests of the Passive Components Manufacturers active in Europe to ensure an open and transparent market for Passive Components in Europe as part of the global market place	Producer	Energy
Oracle Utilities	Solutions for Global Utility companies, including the Energy Sector	Producer	Energy
Vattenfall	Swedish power company	Operator	Energy
EVB Energy Solutions	German Energy company	Operator	Energy
Alliander	Energy network company	Operator	Energy
Echelon	IoT Company, specialized in Smart Cities	Operator	Energy
Ferranti Computer Systems	Ferranti Computer Systems helps organizations improve their business through smart implementation, also in the energy field	Operator and Producer	Energy
Seas-NVE	Danish power company	Operator	Energy
Fondazione Politecnico di Milano	Developpement research Center	Expert	Energy
Tuv Rheinland	German businesses that provide inspection and product certification services	Expert	IT Certification
Gruppo Acea	Multi-Utility Company for develpment in the field of energy	Operator	Energy
TeleTrusT	Widespread competence network for IT security comprising members from industry, administration, consultancy and research as well as national and international partner organizations with similar objectives	Operator	Telecommunications
Rohde & Schwarz Cybersecurity	Award-winning IT security solutions	Producer	Telecommunications
TÜViT	IT tester	Expert	IT Security
Atsec information security GmbH	Independent, privately-owned company that focuses on providing laboratory and consulting services for information security	Operator	IT Security
CenterTools Software SE	IT Secure Solutions	Producer	IT Security
Detack GmbH	Independent supplier of quality IT security auditing and consulting services	Expert	IT Security
eco - Association of the Internet Industry e.V	Largest Internet industry association in Europe	Producer	IT Security
itWatch GmbH	Leading provider of secure device management	Producer	IT Security
NCP engineering GmbH	IT Security Solutions for Fintech	Producer	Finance
secunet Security Networks AG	Leading German providers of high-quality IT security.	Producer	Healthcare
RHEA Group	Highly specialized engineering international group of	Producer	Finance, Cloud

Recipient	Brief Description	Classification	Domain
	companies providing products		
World Security Report	Research Center and Publications	Expert	Transport
Dreger Group GmbH	Consulting Company for Fintech	Expert	Finance
Friedrich-Alexander-University	Research Center and Publications	Expert	Finance
Seconda Unviersità di Napoli	Research Center and Publications	Expert	Finance
Academia General Militar	Research Center and Publications	Expert	Energy
AVL List GmbH	Austrian-based automotive consulting firm as well as an independent research institute	Operator	Transport
IMDEA Software Institute	Madrid Institute for Advanced Studies in Software Development Technologies	Expert	Finance
ONRIX gcv	Company networked with various other consultants and professionals, each with specific core competences and capabilities	Operator	Finance
BNY Mellon Investment Management	Privately owned investment manager. The firm provides sub-advisory services to its client	Operator	Finance
Bit4id	IT Security Provider	Producer	Finance
Security Affairs	Major European Journal on IT Security	Expert	Finance

7.4 An overview of criticism related to Common Criteria

The Common Criteria evaluation and certification is one of the most commonly used process to improve the trust in the security of evaluated products. Nevertheless, this methodology has a lot of problems and side effects that lead to limitations of which the enduser should be aware[16].
For the manufacturer, the main goal of security evaluation is to obtain a degree (such as CC certificate) which validates the security level of his product. Despite the CC certification gives many advantages to the manufacturers, on the other side CC presents various limits.

Limit in perimeter
One very famous limit of the common criteria is that an initiator can voluntarily restrict the scope of the Target Of Evaluation (TOE) in order to exclude some part of the IT product that would be subjected to some flaws. Indeed, the initiator very often starts the security evaluation of the overall IT product and in the same time that the security evaluation is conducted, some flaws are found and he reduces the scope of the TOE. It is thus of the responsibility of the customer to verify the scope that the certificate covers. Two other limits of the common criteria are still focused on the scope of the TOE. First limit, the scope of the TOE is very static after the issuance of the certificate and each change in the scope of the product implies to evaluate again the product. To cope with this problem, a process of maintenance has been set up to follow each modification in an IT product. Second limit, even if the product is a software platform able to support several applications (like Java Card could be) and that this platform is certified, it is not allowed to make the composition of it with a new application that could have been already certified. However in the fictive example aforementioned both the platform (more precisely its scope) and the application (its scope too) have been certified. Since it is allowed to do such composition, the national body forbids evaluating an application alone independently of the platform on which it will run. We can summarize this problem as a lack of dynamicity of the scope and even if the common criteria security evaluation. It is a pity since it will be helpful to reduce the overall cost and time of the security evaluation. It would be nice to reach the time to market needs. This limit regarding the short lifecycle of the certificate is very close of the static aspect of the scope of the TOE. Indeed, the certificate is only valid at the time of its issuance. This short delay is explained by the possibility that new attacks could have been discovered just at the time of the issuance or just after.
Integrating flaws or new attacks
Even if the product could be finally not sensitive to theses new attacks, with a fixed context, some new attacks haven't taken into account in the product conception. To limit this delay, the conception and the evaluation must be scheduled in parallel way. But with this method, flaws must be corrected in time and all depending process must be re-evaluated. Moreover during this additive delay for evaluation, the market requirements can change. A new component can appear with more capacities, more security and with a lower price. Hence the delay between the product conception and the sale must be as short as possible.

Product distribution
When a product is certified, it is deployed on the market. However an analysis of what happens starting to the deployment time shows that any element enabling to ensure traceability and thus to maintain the chain of trust, have been set up. In the following, the problems can be raised and will be illustrated using as example the smart card products. The company considered here could be a bank, a mobile operator, in short a large company which has an important need of smart cards. In general this company will be directly provided by the chosen manufacturer and not by the retailers. Moreover this major company is very often the initiator of the evaluation (or at least the privileged target of the manufacturer for which it has funded itself the evaluation). At the time of the products reception phase, several types of problems can exist or even to coexist:

- problems due to a negligence: there is an error in the batches or in the production line and the company does not receive the good cards. Normally the procedures of delivery defined by the CC (ADO/DEL) and of audit of the production sites make it possible to be sure that such a trouble is not possible (in theory).

[16] Dusart Pierre, Sauveron Damien, Tai-Hoon Kim, Some limits of Common Criteria certification, *International Journal of Security and Its Applications*

- problems due to an ill will of economical type: to save money the manufacturer has used more powerful (hardware/software) components during the evaluation and lost-cost and less powerful components in production. Once again the procedures of delivery and audit make it possible to counter this trouble (in theory).
- problem due to an ill will of mischievous type: for example, modification by the manufacturer of a batch of cards for specific reasons (desire to mischief, backdoor to keep the possibility to correct possible security problems later). As for the previous case, there cannot theoretically occur.
- distribution problem: according to procedures of delivery defined by the CC, the company receives from the manufacturer the good ordered cards (same model that that evaluated) and it is perfect.

At end-user level, the same problem appears. How can he be sure that the proposed product is secure? It seems important since for example, in the case of the banking world, its own money depends on the card security. He should trust his service supplier whereas this one is perhaps not able itself to have a full trust in its product. Clearly the limits of trust in CC certification are related to the absence of proof attached to the product.

Conformity of penetration tests.
To verify the security of the product, some tests are achieved in the Vulnerability analysis part. Vulnerability analysis consists of the identification of flaws potentially introduced in the different refinement steps of the development. It results in the definition of penetration tests through the collection of the necessary information concerning: the completeness of the security functions, the dependencies between all security requirements and whether any of the security requirements can be undermined through unexpected behavior of the system. These potential vulnerabilities are assessed through penetration testing to determine whether they could, in practice, be exploitable to compromise the security of the system. The number and the complexity of theses tests depend on the assurance level indicated in the main document (Security Target document). One must verify that the security functions are efficient through these tests. Some attack paths use different kind of attack and knowledge. But the execution of theses tests is made in different ways by the ITSEF Centers. There is no homologated set of attack but what the evaluator wants to do or what he can do. The effective level of the vulnerability tests depend on the center quality and knowledge. Hence a same product can be evaluated as good by one center and as bad by another center. However theses differences are limited by the certification authority which asks for complementary tests if doubts on security level appear. This choice of management facilitates the mind of initiative to create / to invent new tests. If the list of attacks was fixed as for tests of validity, it would not correspond to the reality of the reel world.

Problems of interpretation
The problems of interpretation are split in two sorts:

- difficulties in the intrinsic comprehension of the criteria: it is exactly the same thing that the laws (a paper can understand differently according to the situation, the use, the past abuses, etc.): it is necessary to legislate. An international committee exists to limit this kind of difficulty (http://www.commoncriteriaportal.org/interpretations.html)
- difficulties in terms of translation in the language of the country. The used terms do not necessarily exist and can be understood or felt in a different way. (Ex: the term "freedom" will not be understood / felt in the same way into different countries)

Moreover, as shown in the study “Analyzing Common Criteria Shortcomings to Improve its Efficacy”, in the view of industry-related security researchers and various stakeholders identifies some main problems of CC. The most common problems identified within the study are:

- The whole process of the evaluation is costly to fulfil the CC requirements in a sense of expenditure, time and production.
- The EALs (i.e. 5, 6, and 7) are known as the higher assurance level for US and European member’s countries who signed the MRA agreement, which is a challenge for new member’s countries.

- Outsized IT systems evaluation is very complex because evaluation zoom-in to the system components and evaluate each unit. After the evaluation zoom-out and viewing the system as a whole, the task is very much complex and sometime impossible to recombine[17].
- The attempt and time required placing evaluation confirmation and certification is very hard job that by the time the work is finished, the artefact in evaluation is usually outdated.
- From industry point of view there is some input but have slight impact on the CC assessment.
- From the evaluation point of view CC is just paperwork the actual product is not properly evaluated. However, this point is for the lower level of EALs not for the higher level.
- CC discriminates against Free and Open Source Software because these are not dependent on any type of criteria for evaluation.
- Quick raise in extent, strength, rigor for TOE at high EALs, but not for PP, produce a generalization hole that is costly to overpass.

Another study entitled "*Common Criteria: Its Limitations and Advice on Improvement*"[18] confirms the shortcomings and limitations of CC shown above. In fact, some issues are related to evaluation process. Especially, CC is criticized as being costly and time consuming. Meanwhile, there are issues in general evaluation methodology. Particularly, its limitation on vulnerability analysis is eminent: CC is not good at addressing security flaws in product implementation. The methodology of vulnerability assessment in CC is too generic, not rigorous to identify vulnerability in implemetation, and does not take into account vulnerabilities specific to individual technology area.

As exposed within the article "*Symantec: Common Criteria is bad for you",* vendors have to pay hundreds of thousands of dollars to get their products evaluated, and the evaluations ' which are conducted by third-party testing firms ' can take up to a year.
As a result, agencies may have to install older, already-obsolete versions of software in order to comply with NSTISSP. With security products in particular, this is a dangerous practice, as updates are frequently added to these products in order to address recent vulnerabilities,
As a result, by the time most companies can assemble adequate information for a Security Target, they are already halfway through the development cycle.
After many years of development, there are still many limitations in Common Criteria. It shall have to continuously improve to be relevant to current development of security assurance. Adoption of security practices into the development life cycle (e.g., threat and risk analysis, misuse and abuse case generation, analysis of implementation representation to detect any implementation defects, risk-based security testing, vulnerability analysis, and penetration testing, etc.) can not only improve the security assurance but also facilitate the evaluation process. All in all, the goal of improving the security assurance cannot be achieved only through the third-party evaluation and certification;t it needs the developer to reasonably retrofit and introduce good security practices into its product development life cycle.

[17] Hunstad, A.; Hallberg, J.; Andersson, R., "Measuring IT security - a method based on common criteria's security functional requirements," Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC, pp. 226-233, 10-11 June 2004, URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1437821&isnumber=30958

[18] http://www.difesa.it/SMD_/Staff/Reparti/II/CeVa/Pubblicazioni/Estere/Documents/CommonCriteria_ISSA%20Journal_0411.pdf

7.5 Cyber Security market Insights

The European Commission has mandated PwC and LSEC for a Cyber Security Market Study that should be completed within 2017. On the 6th June 2017 in Brussels, European Cyber Security Organisation (ECSO) with PwC and LSEC have organised a "Fact Finding Workshop" in order to share the first preliminary results of the study "Cyber Security Industry Market Analysis (CIMA)"[19].
The purpose of the study is to assess how cybersecurity challenges can become an EU competitive advantage and propose a European industrial cybersecurity roadmap. In addition, it should also investigate how the cybersecurity industrial tissue in Europe needs to be developed to support the European organisations, governments, infrastructures, enterprises, services and manufacturing industries.
The value of Global Cyber Market has reached **640 billion euros** in 2016 increasing compared to 2015 (512 billion euros). The Value of EU Cyber Market increased by 17.4% compared to 2015 reaching **157 billion euros** of Sales. EU Cyber Market accounts for 26,3% of global market.

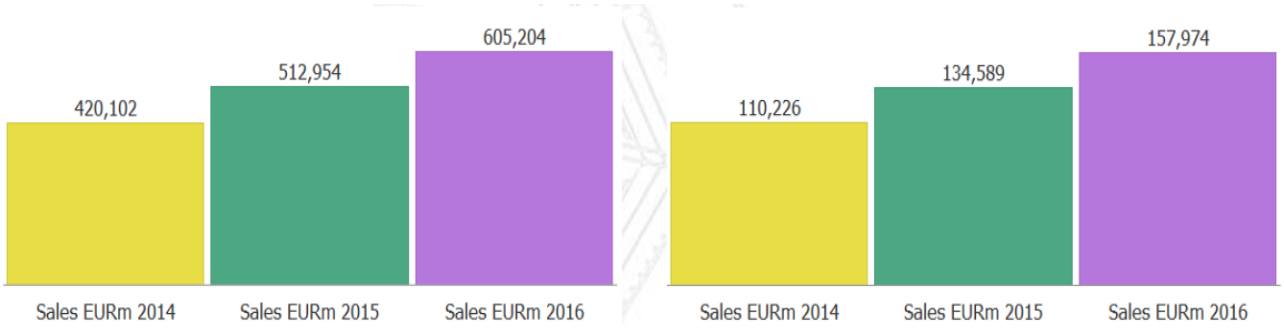


Figure- Global vs EU Cyber Market 2014 through 2016

Sales by EU country shows consistently strong growth for the past two years: growth to 2016 ranges between 14-20%. Moreover, the largest economy does not always equate to the largest growth.
Together with sales, the number of companies on the cyber market is growing: in 2016 the number of cyber companies in the world reached **222 thousands** increasing by 19% from 2015. In Europe, nearly **60 thousands companies** operated in 2016 increasing by 18,2% from 2015.

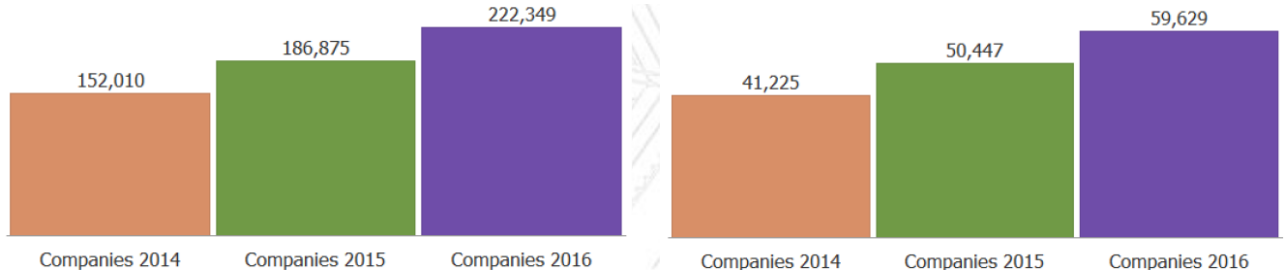


Figure - Global vs European number of Cyber security related companies

The number of Global Cyber employment is increasing according to the growth of the global cyber market: in 2016 the Global Cyber Employment reached 3,7 million increasing by 18% from 2015. In Europe, it is possible to note the same growth: 17,5% increase from 2015 reaching the number of 910 thousands employees.

To have a better overview on the global cyber security market, the demand for cybersecurity solutions from the sectors identified in the NIS Directive is analysed with a high-level segmentation to provide quantitative analysis of the market size and forecasts:

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

- "Government" – including any department, organisation or agency that is Security-specific and funded by government. For the UK, that would including Home Office, UKTI, Police and public security organisations.
- "Other Public" – including any public funded not listed above i.e. local government and those responsible for the security of public places (amongst other responsibilities).
- "Private Sector" – including a wide range of industries like Utilities, Manufacturing, Energy etc.

The range for each segment vary globally:

- Government = 18% to 26%,
- Other Public Agencies = 13% to 23% and
- Commercial = 51% to 70%

Growth forecasts for Europe are between 11% and 13% to 2021. This percentage is slightly less than global forecast growth. Both for Europe and globally, the forecast is lower than actual growth in last two years and is likely to be underestimating future shore-term growth.

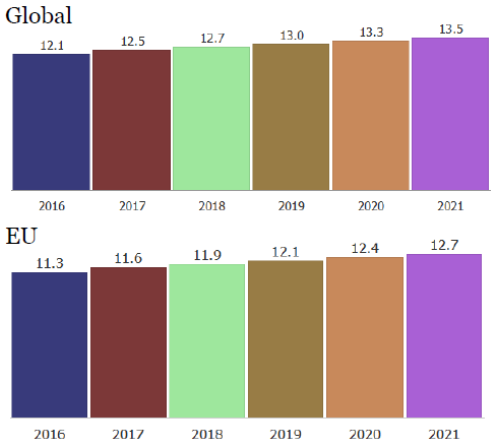


Figure - Analysts Growth Forecast

To measure the degree of innovation, the study has adopted market (demand for) innovation as an appropriate and quantifiable measure of performance. This is applied by country and by product / service. Standard metrics, taken from industry practice and collected from a wide variety of industry sources, include:

- Number new products/services per annum (pull)
- Value of new products/services per annum (pull)
- New product as % of total sales (pull)
- Average investment in R&D per annum (push)

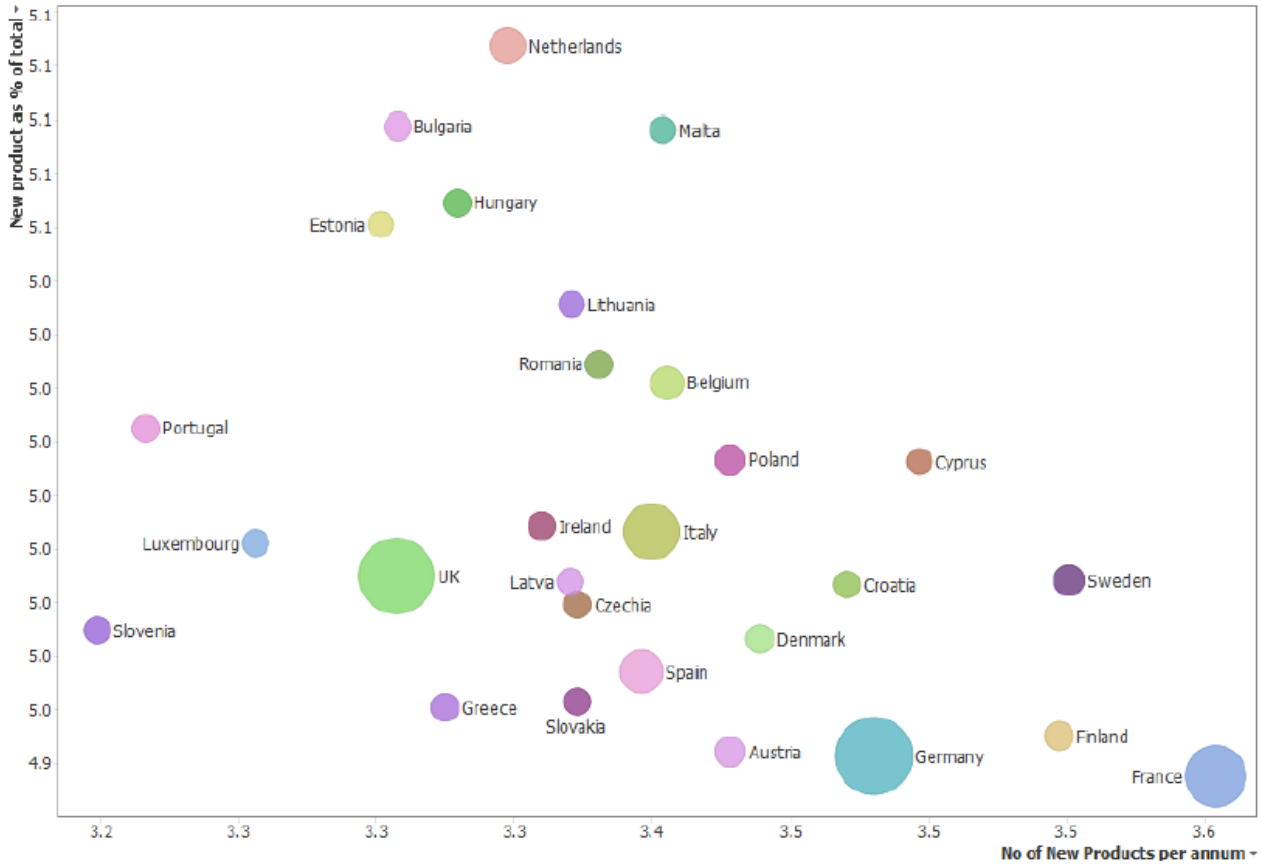


Figure - Country Cyber Innovations - Whole Sector

Graphic shows:

- Horizontal axis = new product as % of sales
- Vertical axis = new product per annum
- Bubble = value of new product sales

Axis ranges are narrow at this aggregated level but extend (and are more meaningful) at the sub sector level.

The cybersecurity market has also been analysed by looking at the import and export flows of cybersecurity products.
In 2016, the first country that exported the largest quantity of cybersecurity products is China. The analysis shows that four EU countries fall within the top 12 exporters of Cybersecurity products.

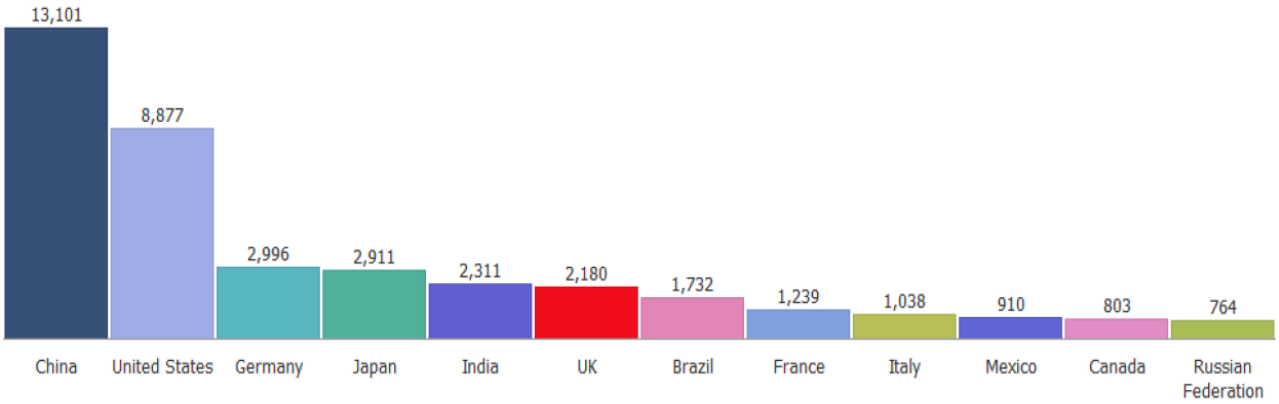


Figure - Top 12 Exporters (EURm)

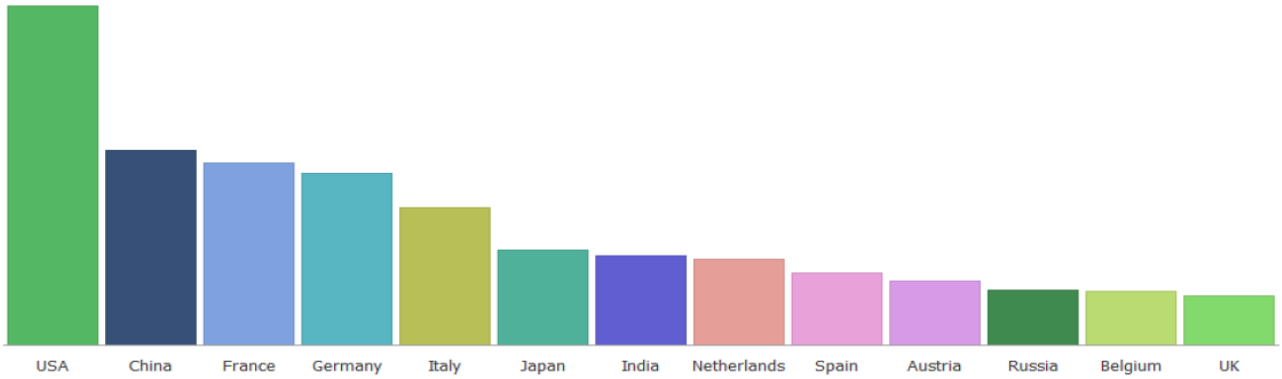


Figure - Export Destinations

In the end, looking at the market import side, the highest value importers are Germany, France and Italy.

Country	Total EUR	Total EU EUR	Total Non EU EUR
Austria	570.8	190.9	379.9
Belgium	485.8	161.0	324.8
Bulgaria	216.5	38.6	177.9
Croatia	25.8	5.1	20.7
Cyprus	8.1	1.6	6.5
Czech Republic	389.1	62.7	326.4
Denmark	439.3	68.5	370.8
Estonia	99.8	22.8	77.0
Finland	362.8	79.3	283.6
France	1,011.4	539.1	472.2
Germany	1,608.3	508.4	1,099.8
Greece	416.5	82.7	333.8
Hungary	433.5	79.0	354.4
Ireland	66.0	13.6	52.4
Italy	964.1	406.7	557.4
Latvia	129.5	26.7	102.8
Lithuania	86.1	23.1	63.0
Luxembourg	14.4	3.0	11.4
Malta	3.7	0.7	3.0
Netherlands	709.8	255.4	454.4
Poland	461.3	84.0	377.3
Portugal	379.1	102.8	276.3
Romania	360.2	80.8	279.5
Slovakia	41.2	8.2	33.0
Slovenia	20.5	4.2	16.3
Spain	553.7	213.1	340.6
Sweden	363.7	81.3	282.4
UK	870.7	150.0	720.7

Figura 1 - EU Cyber Imports

7.6 Case Study – "The impact of an EU wide Certification Scheme on Smart-Meter Industry"

A smart-meter company, which wants to sell its products in two Member States e.g. France and UK.

	Now	Future

Requirements	• *In order to sell in UK and France manufacturers have to certify against different schemes:*
	  ○ *CPA (Commercial Product Assurance) in UK,*
	  ○ *CSPN (Certification de Sécurité de Premier Niveau) in France*
		○ Manufacturers will need to undergo a single certification process, as envisaged in the future European certification scheme for smart meters. The resulting certificate will be accepted by all public authorities in Member States.

Cost	• The overall cost is at least 300 thousand euros for the two markets (about 150 thousand euro in UK and about 150 thousand euros in France).	• The estimation of costs saving ranges up **to 80% of current costs**

Time	• **6 to 18 months.** This estimate takes into account:
	  ○ Completion of multiple certifications processes and supporting documentation
	  ○ Identification of various requirements that a vendors needs to comply with.
	  ○ limited number of conformity assessment bodies able to certify against the requirements of different schemes.
		• **Faster process** that takes into account:
		  ○ Role of ENISA that provides information needed for compliance with the European scheme (e.g. specialised conformity assessment; documentation)
		Completion of single process : no multiple certifications are needed and capacities of existing CABs can be used more efficiently

Other	**Different methodologies** for risk assessment and definition of security requirements	**Standard methodologies** for risk assessment and definition of security requirements

Full Description:

Methodology: The research methodology of this case study is based on literature retrieved from desk research and on the analysis of multiple interviews with cybersecurity experts and professionals working in the Smart-Meter Industry.

Background: By May 2014, Member States committed to rolling out close to 200 million smart meters for electricity and 45 million for gas by 2020 at a total potential investment of €45 billion. By 2020, it is expected that almost 72% of European consumers will have a smart meter for electricity while 40% will have one for gas. Up to date, 80 million smart meters have been installed in the EU28 and Norway, which constitutes 30% of the overall European electricity metering points[20]. With potentially millions of networked end-points, there are significant cyber threats organizations and consumers will be exposed to.

Fragmentation of the Smart Meter Industry: Various and not fully coordinated certification initiatives across Europe are increasing fragmentation in the domain of ICT certification and therefore also for Smart-Meter Industry, resulting in duplication of efforts and waste of resources. The non-exhaustive list of certification schemes applicable to Smart Meters across Europe includes, among others:

- CPA (Commercial Product Assurance) is the certification scheme recognised in UK,
- CSPN (Certification de Sécurité de Premier Niveau) is the certification scheme recognised in France,
- A protection profile based on Common Criteria is the certification scheme recognised by BSI in Germany.

These three European Countries **do not recognise** each other their certification scheme.

The processes of certification are based on national requirements. In the UK, they are called security objectives. Based on these requirements and objectives, each MS has defined a security certification approach at a national level. There are also national communications infrastructure for devices connected to smart-meters including interfaces with the different stakeholders involved such as the German Smart Meter "**Gateway**" and in the UK the so-called "**Communication Hub**". Other national initiatives are emerging as the **Dutch Smart Meter Requirements** (DSMR) developed by the Dutch national organization of DSO's "Netbeheer Nederland". If Member States across Europe continue not to accept each other Certification schemes, each Member States will continue to improve its own Certification scheme and this could create a strong legacy making harmonisation more difficult. Another problem regards a European accordance on minimum requirements, on documentations and tests results for the same functionality and in the same language, ready and accepted by the different authorities of different countries. Furthermore, such fragmentation is also happening on the evaluation side; the three different Certification Schemes mentioned above require three different methodology of evaluation and it's not always sure that they give the same results. There are only limited number of Conformity Assessment Body (CAB) that are able to certify against the requirements of different schemes and the evaluation period for Smart meters products, as above mentioned, usually can last from **6 months to 18 months**. In this way, additional market entry barrier are created.

Cost for Certification: The proliferation of national certification scheme increases 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.

To provide concrete example, considering that the cost of certification depends on products, evaluation assurance level needed or components to be evaluated, the cost of certification can reach more than 1 million euros and the SMEs are out of this gain. For BSI "**Smart Meter Gateway**" certificate the cost is much more than **one million euros**. The cost for smart meters certification in UK is almost **150 thousand euro**. In France, the cost it is similar to the UK, about **150 thousand euros or more.** In Netherlands, the average

[20] USmartConsumer Project, European Smart Metering Landscape Report, "Utilities and consumers", 2016

costs of a certification under Baseline Security Product Assessment (BSPA) scheme are approximately **40 thousand euros**. The significant difference of costs for certification between Germany and other Member States have various reasons. France is for instance more focused on testing in a fixed time: given a fixed time the device has to pass all the security tests during that time. At the end of the fixed time, a finale report is sent on whether it is working fine or not. The German approach has a higher level of tests and assurance. On the other hand in UK and in France a security assessment is performed on one product, while in Germany the whole infrastructure need to be tested and certified. Considering that these National Certification schemes are not mutually recognised, smart meters companies should sustain additional costs in order to enter another Member State's market. In fact, the total cost for certification usually ranges **from 150 thousand euros to 1 million euros and more.** Only one of the biggest smart-metering companies is starting a certification to enter other markets and all the other companies are present only in the German market. In this context, one of the most important barrier to trade for the smart metering industry are the costs for certification. In the absence of an EU wide certification framework a Smart Meters company that wants to access the French market must certificate its products under the CSPN scheme and once again under the CPA scheme to enter the UK market, therefore it would pay **300 thousand euros**. With an EU wide framework, being the product certification of France deemed as equivalent to the one in the UK, the smart-meter company will have to certificate only once but will access the French and English market paying a cost of around 150 thousand euros and a **direct saving of 150 thousand euros**. More in general, it is estimated that the introduction of an EU wide certification framework could lead to smart meters companies **saving up to 80% on costs.**

Benefits for the Smart Meter Industry of an EU wide Certification Framework: For the Smart-Meters industry a European scheme would be a valuable policy option. It would make certification schemes mutually recognised across Europe, standardise a methodology on how risks are assessed and how security requirements are defined. Moreover, it would be very important to have flexibility in certification scheme, determine also on the risk connected to the product evaluated and the risk connected to the location of the product. The introduction of an EU wide Certification scheme will produce many benefits for the Smart Meters industry including:

- the reduction of fragmentation,
- the reduction of market barriers,
- the reduction of the costs for certification.

Conclusion: There is no common baseline set of security requirements that can be recognized by all participating EU Member States. At least three Member States have defined their own protection profiles. These requirements are different per country, based on different standards and adopted by technical committees. There is no scheme that includes all aspects and enables a pan European approach[21]. In order to improve the current situation and to reduce the market fragmentation and the costs for certification, the introduction of an EU wide Certification scheme could have a positive impact for the Smart Meter Industry. A European framework would reduce also the information asymmetry on security requirements of ICT products and make the European Market less fragmented.

[21] ENISA, Smart grid security certification in Europe, December 2014

7.7 Case Study – "The impact of an EU wide Certification Scheme on Alarm Systems Industry"

	Now	Future
Requirements	• A manufacturer of a security alarm systems seeking to supply their product throughout the EU will typically need to apply for 10-15 certificates requested in different Member States	• Manufacturer need to undergo a single certification process as envisaged in the future European certification scheme for alarm system. The resulting certificate will be accepted by all public authorities in Member States
Cost	• The costs of certifications of an alarm system are on average (with a large spread depending on the nature of the product) at the level of **200-300 thousand euros** for full access to Europe including all tests	• The estimated cost for obtaining a single European certificate would amount to **40-60 thousand euros** • A potential impact in terms of cost savings for intruder alarm systems amounts to a range of **4.7 million euros to 9.9 million euros per year**
Time	• **Long "time to market"** due to the multiple processes/test to obtain several certifications for a single product	• **Reduction** of the "time to market" thanks to a single certification process. ENISA would accelerate this process by providing all information and documentation needed for compliance with the European scheme
Other	• High costs and long duration of certifications are barriers to market for alarm systems. These will deteriorate the competitiveness of the EU industry on the global market.	• Enhanced competitiveness of European industry through: o Reduction of costs and time associated to multiple certification requirements o Improved transparency of EU-wide security requirements needed for this product o Enhanced competition among EU suppliers

Full Description:

Methodology: The research methodology of this case study is based on literature retrieved from desk research and on the analysis of the European landscape of Alarm-Systems and Security Industry.

Background: The security industry in the EU generates a turnover of close to € 200 billion, and creates employment for 4.7 million persons[22]. European companies are still among the world leaders in the majority of the segments of the security sector. One of these segments is represented by Alarm Systems Industry. According to a new research report by Berg Insight, the number of monitored alarm systems in Europe is forecasted **to grow from 8.7 million in 2016** at a compound annual growth rate (CAGR) of 4.0 percent **to reach 10.6 million in 2021**[23]. The growing international competition and recent market evolutions do however indicate that the global market shares of European companies could drop significantly over the next years if no action is launched to enhance the competitiveness of the EU security and alarm systems industry. The Security market has three distinctive features[24]:

(1) It is a highly fragmented market divided along national or even regional boundaries. Security, being one of the most sensitive policy fields, is one of the areas where Member States are hesitant to give up their national prerogatives.

(2) It is an institutional market. In large parts the security market is still an institutional market, i.e. the buyers are public authorities. Even in areas where it is a commercial market, the security requirements are still largely framed through legislation.

(3) It has a strong societal dimension. Whilst security is one of the most essential human needs, it is also a highly sensitive area. Security measures and technologies can have an impact on fundamental rights and often provoke fear of a possible undermining of privacy

Fragmentation of the Security Industry: Various and not fully coordinated certification initiatives across Europe are increasing fragmentation in the domain of ICT certification and therefore also for Security and Alarm Systems Industry which are becoming more and more dependent on the internet, resulting in duplication of efforts and waste of resources. 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[25]. The non-exhaustive list of certification schemes applicable to Alarm Systems and Security products across Europe, includes, among others:

- **CertAlarm:** 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. The CertAlarm Certification includes some standards on IP interoperability implementation based on Web services for each kind of alarm[26].
- **Alarm System Certificate[27]:** 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)[28]
- **ONVIF and PSIA**: 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

[22] https://ec.europa.eu/home-affairs/what-we-do/policies/industry-for-security_en
[23] http://www.berginsight.com/news.aspx
[24] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0417&from=EN
[25] ECORYS. (2011). Security Regulation, Conformity Assessment & Certification. Brussels: Report delivered by ECORYS for the European Commission.
[26] http://www.certalarm.org/ca/sites/default/files/Scheme%20Rules-2-Iss_5.pdf
[27] http://industries.ul.com/blog/alarm-system-certificate
[28] (http://industries.ul.com/wp-content/uploads/sites/2/2016/04/UL_CAP-Overview-Info.pdf)

and end users the necessary protections from today's cyber security threats, in addition to providing out-of-the-box interoperability[29].

- **EuroPriSe**: EuroPriSe is a European scheme providing privacy and data protection certification for IT products and IT-based services. The procedure consists of an evaluation of the product or service by admitted legal and IT experts and a validation of the evaluation report by an independent certification authority[30].

Cost for Certification: The costs of certification of an alarm system are on average (with a large spread depending on the nature of the product) at the level of **200-300 thousand euros** for full access to Europe including all tests. Stakeholders indicate that the estimated cost for obtaining a mutually recognised certificate for the same alarm system would amount to **40-60 thousand euros**[31]. Under an EU-wide system of conformity assessment and certification that provides for mutual recognition of certification throughout the EU, security products will have to be certified only once, instead of multiple times. This implies a reduction of costs associated to multiple conformity assessment (i.e. testing) and certification for those products, and in those markets, that are currently required to undergo national conformity assessment and certification. A global estimate of the potential impact in terms of cost savings for intruder alarm systems **amounts to a range of EUR 4.7 million to 9.9 million per year**. For other product categories for which national authorities require some form of approval, the evaluation of product performance is more often organised on an *ad hoc* basis involving a mixture of testing and operational trials.

Benefits for the Alarm-System Industry of an EU wide Certification Framework: Without (effective) action at the EU-level (baseline), the lack of an internal market for alarm systems products/components will deteriorate the position of the EU industry on the global market. The development of EU-wide harmonised standards and a common conformity assessment procedure is expected to significantly reduce the certification costs for suppliers of intruder alarm systems where they serve multiple national markets in the EU. Moreover, it should reduce costs incurred in developing variants of products that are adapted to comply with differing standards and conformity assessment procedures at national level, which industry stakeholders consider often have limited actual impact on product performance for final customers. Removing the need for multiple certifications would enable suppliers of alarm systems to more rapidly access different parts of the EU market which, in turn, could benefit the organisation and scale of production activities. Further, by reducing delays in 'time to market' caused through multiple certification requirements, an EU-wide scheme should reduce the risk of new product innovations being replicated by competitors. Thus, an EU wide scheme should increase the potential return and reduce the level of risk associated to investments in research and technology development[32].

The expected positive consequences of harmonised EU wide certification procedures are:

- reduction of costs associated to multiple testing;
- facilitated access to markets;
- reduction of the "time to market";
- improved transparency of performance requirements and standards;
- enhanced competition among EU suppliers;
- reduction of costs for conformity assessment and certification (CAC) services and the development of security technologies;
- lower prices for security technologies

Conclusion: In order to ensure the market leading position of EU companies over the years to come, the first priority will be to overcome the fragmentation of the EU security markets through the harmonisation of standards and certification procedures for security technologies. The societal acceptance of security technologies will be promoted through the introduction of the "privacy by design" and "privacy by default" concepts throughout the development of new security technologies. Although a handful of major players dominate both the EU (and US) market, there remain many niche markets that are very attractive for SMEs,

[29] https://www.ifsecglobal.com/onvif-introduces-profile-q-to-tackle-cyber-security-challenges/
[30] https://www.european-privacy-seal.eu/EPS-en/Product-and-Service-Privacy-Certification
[31] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0233&from=EN
[32] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0233&from=EN

either directly or through the supply of specialized products and components to major manufacturers and integrators, and to the installation service market. Conformity assessment and certification costs represent a proportionately higher share of total costs for SMEs and consequently a greater market access barrier. Accordingly, they are expected to benefit in particular from the cost savings resulting from EU-wide harmonised standards and certification procedures. In addition, an EU certification scheme should serve as a recognised mark of product performance and quality that can reduce the importance of 'reputation effects' of larger players and local companies, thus facilitating SMEs to trade across borders within the EU and even in global markets. Overall, an EU-wide scheme is expected to increase market efficiency in the EU by raising the level of competition – both between EU companies and from outside the EU – and stimulate improvements in industry performance levels (e.g. productivity). It is not expected, however, that the reduction in costs resulting from an EU-wide approach would have a significant impact on the price competitiveness of EU alarm products in international markets. Nonetheless, a less fragmented EU market should encourage investment in research, technology development and innovation, which would have an impact on 'dynamic' competitiveness. Further, to the extent that it obtains higher market recognition than existing national schemes, an EU-wide certification scheme (providing for a corresponding EU security 'performance mark' or 'quality label') should contribute to strengthening broader international market awareness and acceptance of EU products[33].

[33] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0233&from=EN

7.8 Case Study – "The impact of an EU wide Certification Scheme on Cloud Computing Industry"

	Now	Future
Requirements	• In order to sell Cloud Computing Products / Services in France and Germany providers have to certify against: *SecNumCloud* **and** *Compliance Controls Catalogue (C5)*	• Providers need to undergo a single certification process, as envisaged in the future European certification scheme for cloud computing. The resulting certificate will be accepted by all public authorities in Member States
Cost	• Costs associated to compliance with different technical rules and multiple testing is estimated around 1.2 billion euro, that accounts for **2% to 10%** of companies' annual expenditures.	• An increased level of competition, introducing an EU wide Certification Scheme, would result in a **yearly saving of € 1.1 billion in the EU public sector alone**
Time	• **Around 7-9 months** due to the multiple audit and testing processes to obtain several certifications	• **Reduced time**: duration of a single process is estimated to take around 4 to 6 months. ENISA would accelerate the process by providing the information needed for compliance with the European scheme
Other	• Faced with co-existence of multiple schemes and standards[34], end-users (esp. in the banking sector) are not able to compare and judge which scheme or standard would best satisfy their particular security requirements. This deteriorates the trust in cloud computing services.	• The existence of a security certification scheme for cloud computing agreed at EU level, increases the trust in this service • Competitive gain for cloud providers due to cost and time reduction

[34] ECSO has published a State-of-the-Art Syllabus listing 8 different schemes and standards to certify the security of cloud computing services. See here: www.upm.es/observatorio/vi/gestor_general/recuperar_archivo.jsp?idf=642&tipo=2

Full Description:

Methodology: This case study is based on information obtained from secondary sources (literature review), from the analysis of the European landscape of Cloud Computing Industry conducted on the basis of an online search and from interviews conducted with different impacted Stakeholders.

Background: The ongoing digital transformation is strategically affecting both private and public sector organisations also in terms of cybersecurity[35]. Cloud computing has the potential to reduce IT expenditure and boost organisational flexibility while at the same time improving the scope for delivering flexible high-quality new services. Some of the general benefits are reducing costs, increasing the storage capabilities and the chance to adapt in a flexible way to the changing business conditions[36]. These benefits can be applied in a lot of different domains and fields.

The increase in the use of Cloud globally is also visible from the Market, over the last two years[37]. In 2017, spending on public cloud Infrastructure as a Service hardware and software is forecast to reach **61 billion U.S. dollars worldwide**[38]. According to Gartner, Inc., the highest growth will come from cloud system infrastructure services (IaaS), which is projected to grow **36.8 percent in 2017 to reach $34.6 billion**. Cloud application services (SaaS) is expected to grow 20.1 percent to reach $46.3 billion[39].
Despite its growing influence, concerns regarding cloud computing still remain. There are in fact challenges that it still has to face, such as: **Data Protection, Data Recovery and Availability, Management Capabilities and Regulatory and Compliance Restrictions**[40].

Incidents related to Cloud Computing services worry the companies especially for sectors such as Finance where a data breach can cause huge economic and reputable damages. According to representatives from European Banks, they are not very sure if the data are stored in a secure way, especially according to the various jurisdictions of different Countries.

Cloud Computing is going to be fundamental for the future. For this reason, it is necessary that it as secure as possible.

Fragmentation of the Cloud Computing Industry: Cloud service providers offer their services internationally in several markets. Therefore, national approaches for certification and assurance are of limited use to them. National cyber security authorities can usually only set national standards, even if other countries use them too[41]. ANSSI (Agence national de la sécurité des systèmes d'information) and the BSI have been very intensively involved with the security of Cloud Computing in recent years. Both authorities arrived at a very similar understanding of the Cloud security standards that need to be met, and both initiated new ways of verifying secure Cloud Computing, since the existing certifications failed to adequately meet the needs in this area. However, both authorities pursued different paths[42].

- **Compliance Controls Catalogue (C5)** - The BSI developed the Cloud Computing Compliance Controls Catalogue (C5). This catalogue, which is closely oriented to tried and tested standards, defines the requirements for the secure provision of services critical to businesses, which the Cloud provider must meet. Additionally, the provider must make their offer transparent, such as the location of data processing and the subcontractor. The auditing process is conducted in line with the international recognised standard, the ISAE 3000. The audit report is based on standards such as the ISAE 3402 and SOC 2. Auditors and Cloud experts conduct this audit and issue an audit opinion, for which the auditor bears liability. The C5 also contains standards for greater protection needs and can be individually extended – for example for a specific industrial sector. The BSI sets the standards and specifies criteria for the audit, but has no further supervisory role with regard to specific procedures.
- **SecNumCloud** - The ANSSI takes a very different approach. The Référentiel SecNumCloud, which is strongly oriented to the ISO/IEC 27001 standard and which supplements it with several specifications of its own, defines the standards required for secure Cloud Computing. In the Référentiel, there are two levels: sécure and sécure plus, whereby the latter sets higher security standards and limits to France the

[35] https://www.enisa.europa.eu/publications/exploring-cloud-incidents
[36] http://picse.eu/sites/default/files/ProcuringCloudServicesToday_March2016_web.pdf
[37] https://www.forbes.com/sites/louiscolumbus/2016/03/13/roundup-of-cloud-computing-forecasts-and-market-estimates-2016/#51dfa21b2187
[38] https://www.statista.com/statistics/507952/worldwide-public-cloud-infrastructure-hardware-and-software-spending-by-segment/
[39] http://www.gartner.com/newsroom/id/3616417
[40] http://www.thbs.com/downloads/Cloud-Computing-Overview.pdf
[41] https://www.bsi.bund.de/EN/Topics/CloudComputing/ESCloudLabel/ESCloudLabel_node.html
[42] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2016-02.pdf?__blob=publicationFile&v=4

service provided. Taking this as a basis, the ANSSI has developed a completely new certification of its own, which it has established in France. Cloud providers receive a certificate which is issued by the ANSSI and on which an audit report produced by ANSSI certified auditors is based. For example, providers who want to be certified with SecNumCloud can be audited by AFNOR Certification[43].

While the security levels which the BSI and ANSSI would like to see in place are very similar, **the two very different approaches towards certification and attestation appear to contradict each other**.

Moreover, the list of applicable Standards and Certification Schemes for Cloud Computing across Europe includes, among others: ISO 27001/2, ISO 20000 (ITIL), CSA Open Certification Framework (OCF), Eurocloud, Star Audit, SOC 1-2-3, PCI – DSS, Europrise, FISMA, Cloud Industry Forum Code of Practice, ISACA COBIT, Security Rating (Leet security), TUV certififed.

Motivated by the German-French business consultations[44] and based on a high level of mutual trust, the idea therefore emerged of generating a **new Cloud Label**. It stands for the joint Cloud security standards and is suitable evidence that they have been met. The underlying principle on which the label is based is a joint short catalogue with security targets ("core rules"). Naturally, the attestation in accordance with the BSI's C5 and the ANSSI certification are sufficient to meet these standards. **A provider who already has one of the two certifications can receive this label and as such advertise the security level of their product very easily on both markets.** The Cloud Label is regarded by the ANSSI and BSI as being an explicitly European initiative, which can also incorporate the certifications of other countries. In this way, the expertise and independent nature of the BSI and ANSSI, as well as their cooperation based on trust, are of benefit to the whole of Europe.

Another European initiative towards a unique approach for ICT Security Certification Schemes comes from **Horizon 2020 Programme**: the project EU-SEC[45]. The EU-SEC, started at the beginning of 2017, will last until 2019 and aims to create a framework under which existing, certification and assurance approaches can co-exist. Furthermore, it will feature a tailored architecture and provide a set of tools to improve the efficiency and effectiveness of current assurance schemes targeting security, governance, risks management and compliance in the Cloud.

Cost Analysis: An economic paper by economists of DG ECFIN estimated that the cost associated to differences in technical rules and multiple testing/certification are between **2% to 10% of companies annual turn-over[46]**. According to this paper inadequate standards and insufficient mutual recognition, including in the ICT sector, is among the main barriers to the single market. For example, the costs of an ISAE 3000 implementation project, in order to be certified under the Cloud Computing Compliance Controls Catalogue (C5) Scheme, can vary from **ten thousand USD up to a million USD or even more**[47]. The costs for enterprises of product conformity assessment can be substantial and we there is lack of mutual recognition this implies the multiplication of such costs: for companies offering several product types on a national market of a receiving Member State the costs amount to approximately 2% of their entire annual turnover on that market, whereas they can reach up to 10% for companies specialized in one specific product type because they do not benefit from economies of scale[48]. Even applying the lower bound of 2% only to 60% of the cyber security market to be conservative (i.e. assuming 40% of the market concerns products for which certification is no require) **the costs of lack of mutual recognition reach a figure in the range of 1.2 billion euro**.
Moreover, many organizations are 'locked' into their ICT systems because detailed knowledge about how the system works is available only to the provider, so that when they need to buy new components or licenses only that provider can deliver. **This lack of competition leads to higher prices and some € 1.1 billion per year is lost unnecessarily in the public sector alone[49]**.

[43] http://www.afnor.org/en/news/cybersecurity-vigilance-required/
[44] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2016-02.pdf?__blob=publicationFile&v=4
[45] http://cordis.europa.eu/project/rcn/207439_en.html
[46] Ilzkovitz, F. Dierx, A. Kovacs, V. & Sousa (2007) Steps towards a deeper economic integration: the internal market in the 21st century", European Economy, Economic Papers, No. 271. European Commission.
[47] https://www.isae3000.com/controlreports
[48] Ibid. p. 61
[49] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013DC0455&from=EN

As mentioned in the SWD "A Single Market Strategy for Europe - Analysis and Evidence"[50] a large body of economic studies that show the impact that standard have on economic growth and GDP[51]. **For France the impact on growth is estimated at 0.8 %, for United Kingdom at 0.3 % and for Germany at 0.9 % of GDP**. To put this in monetary terms, DIN (the German Institute for Standardization) estimates that in Germany alone, standards generate up to EUR 17 billion a year. A more recent study from the UK 'The Economic Contribution of Standards to the UK Economy' also confirms that the use of standards benefits the national economy: standards contributed to around EUR 11 billion of the EUR 40 billion GDP growth in 2013 (2014 prices) and to around EUR 8.5 billion to UK exports52. The same study shows that standards help to enhance quality, with 70 % of respondents stating that standards had contributed improving the quality of supplier products and services. In the econometric models supporting such estimates standards are considered, together with R&D expenditure and patents, as fuelling the knowledge input in the classical production functions. One key hypothesis is that standards can, to some extent, counterbalance some well-known market failures and the possibility that investments in knowledge by private players are sub-optimal and not sufficient to produce social surplus (externalities).

Benefits for the Cloud Computing Industry of an EU wide Certification Framework: In a world that is increasingly interconnected, it does not make much sense for a State to tackle digital security issues on its own. The new French digital security strategy states France's will to engage a dialogue both within multilateral organizations and with long-term trustworthy partners following two objectives: contributing to the global stability of cyberspace as well as reinforcing the States' own cybersecurity.
The longstanding and close bilateral cooperation between ANSSI and BSI is based on trust and has been greatly facilitated by a shared vision on many strategic and political issues, a common positioning at the national level fulfilling only defensive missions and a comparable high level of technical expertise.
ANSSI and BSI have been working together in many fields, such as cloud-computing with the creation of a common label for secure cloud service providers, security certification though a very strong support of the international recognition schemes (CCRA and SOG-IS) and industrial synergies. An EU wide Certification Framework could guide these initiatives in order to avoid the fragmentation of Standards and Certification Schemes across Europe and the further development of National Approaches. The benefits of standardization through an EU wide Certification Scheme include, among others:

- **Competitive Advantage**. Companies are motivated to participate in standardization because they gain an edge over non-participating companies in terms of insider knowledge. Early access to information is valuable;
- **Cost Reduction**. Standardization lead to lower transaction costs in the economy as a whole, as well as to savings for individual businesses. transaction costs drop considerably as a result of standards, since they make information available and they are accessible to all interested parties;
- **Supplier/Client Relationship**. Standards can help businesses avoid dependence on a single supplier because the availability of standards opens up the market. The result is a broader choice for businesses and increased competition among suppliers;
- **Standards and R&D**. Businesses not only reduce the economic risk of their R&D activities by participating in standardization, but can also lower their R&D costs. When a company can influence the content of standards to its advantage, the economic risk is lower. The expense of R&D is potentially reduced when the participants in standards work make their results generally available, and research need not be duplicated

[50] Brussels, 8.10.2015 SWD (2015) 202 final, accompanying the document Upgrading the Single Market: more opportunities for people and business (COM (2015) 550 final) {SWD(2015) 203 final}).
[51] Among peer-reviewed journal articles see: Acemoglu, D., G. Gancia and F. Zilibotti (2012), 'Competing Engines of Growth: Innovation and Standardization,' Journal of Economic Theory, 147, 570–601;Blind, K. and A. Jungmittag (2008), 'The Impact of Patents and Standards on Macroeconomic Growth: A Panel Approach Covering Four Countries and 12 Sectors,' Journal of Productivity Analysis, 29, 51–60; Jungmittag, A., K. Blind and H. Grupp (1999), 'Innovation, Standardisation and the Long-term Production Function,' Zeitschrift für Wirtschafts- und Sozialwissenschaften, 119, 205–222; Wakke, P., Blind, K.; Ramel, F. (2016): The impact of participation within formal standardization on firm performance, Journal of Productivity Analysis 45 (Issue 3), 317–330; Wijen, F.H. (2014). Means versus ends in opaque institutional fields: Trading off compliance and achievement in sustainability standard adoption. Academy of Management Review, 39 (3), 302-323.Swann, P. (2010), International Standards and Trade: A Review of the Empirical Literature. Report for the UK Department of Business, Innovation and Skills (BIS). OECD Trade Policy Working Papers. Among reports commissioned by standardization bodies see: SCC (2007). Economic Value of standardisation; AFNOR (2009). The Economic Impact of standardisation; DIN (2011). The Economic Benefits of standardisation; Standards Australia (2012). The Economic Benefits of standardisation; Cebr (2015). The Economic Contribution of standards to the UK Economy; Cebr (2016). Economic Contribution of Standards in Ireland – A report for the National Standards Authority of Ireland.
[52] British Standards Institution (BSI), 'The Economic Contribution of Standards to the UK Economy', 2015

- **Raising Trust**. An annual report featured on eWeek[53] shows that 73% of survey respondents are worried about cloud computing security. An EU wide Certification Scheme could raise the trust level of companies in the Cloud Computing services, reducing insecurity due to the various jurisdictions of different Countries.

Conclusion: Even if States are primarily responsible for their national digital security, it is France and Germany's shared vision that many challenges can best be addressed **through a common and coordinated effort at European level.** This could be guaranteed introducing an EU wide Certification Framework, which avoids multiplication of National Approaches, duplication of efforts and waste of resources. Beyond the development of EU Member States' capacities and cooperation, the EU must as well recognize that European digital security is challenged on other fronts, requiring a collective ambition to guarantee Europe's digital sovereignty. Three challenges in particular are ahead of us[54]:

- the EU and the Member States' ability to protect and defend the EU institutions, the administrations, the critical infrastructures, the companies and the general public in cyberspace must be ensured;
- the EU must actively support the development of sustainable European industries in the field of digital security and guarantee Member States' ability to evaluate and approve the security of digital products and services;
- the EU must preserve its capacity to choose autonomously how data and related services should be protected in Europe.

Along with like-minded Member States, France and Germany will closely work together to promote the European digital strategic autonomy, a long-term guarantor of a cyberspace that is more secure and respectful of European values.

[53] http://www.eweek.com/cloud/companies-worry-about-security-implications-of-cloud-services

[54] Federal Office of Information Security, BSI, Security in focus, Europe and International Cooperation, BSI Magazine 2016/02

7.9 IoT Trust Label - Proposed Requirements as a Basis for Endpoint Trust Labels (from Stakeholder Support)

The IoT Trust Label requirements consist of a set of endpoint guiding principles that enable for an IoT solution to have an intelligent, automated and secure way to manage the device through its lifecycle. End users, including consumers, enterprises, and service providers, purchasing labeled equipment and services can have confidence as to the level of trustworthiness that vendors are building into their products. The basis of these requirements is that the system and its components should provide protection across the end to end solution – before, during, and after an attack.

In the context of the IoT, a "Thing" is an endpoint that has network connectivity and a well-designed purpose with constrained functionality as compared to general purpose IT devices. **A trust labeled Thing has additional capabilities that provide owners and operators the confidence that it is designed to be secure and simple to manage**. For the purpose of this trust label document, "Endpoint" and "Thing" are the same.

The IoT Trust Label requirements are intended to improve overall cyber resilience of IoT solutions by addressing common weaknesses with products and ecosystems that provide easy attack vectors. A second and equally important outcome is that the end user can have confidence in these products because manufacturers are accountable for what is "built in" to the product.

Labeling is a mechanism of informing interested parties of the capabilities or components of the labeled equipment. The following information should be delivered as part of the label definition:

- The actual assertions being made,
- Identification as to whether assertion is made by vendor or 3rd party testing/certification organization.

Additional information that could be considered for either part of the label definition or part of the assertions include:

- Is this assertion time limited?
- Is this assertion dependent on external services or facts that might change?

Where the assertions being made are direct facts, it is sometimes advantageous to simply list them. For example, the "grams of sugar" within a food serving is a factual statement. A conversion of this direct fact, using an external standard, can be used to help consumers make informed choices. For example, 25g of sugar is "50% daily value" and performing this lookup when printing the label is intended to help consumers understand the relevancy of their decision; it saves them a step of doing the lookup or memorizing the recommendations. While advantageous for communicating with homogenous user base with general agreement concerning the "daily value" metrics, this form of label is less helpful at communicating core information (# of grams) to consumers with custom use cases (for example a vet at zoo attempting to determine if the grams of sugar in a snack are appropriate for an orangutan with a different calorie diet, a different daily value for sugar).

Similarly, security labeling provides simple information to the end user for making purchasing decisions. The situation is complicated by the variety of use cases and associated disagreement about the "daily value" metrics. One use case might prioritize lots of confidentiality (sugar) and another might prioritize lots of availability (think "protein" in our nutrition metaphor).

The labeling method therefore must impart either:

- The use case labeling indicates the offer is appropriate for
- Or, discrete facts that allow the end user to judge appropriateness for arbitrary use cases

There is commonality among use cases in that, at least with respect to cyber security resilience, it may be useful to combine and generalize facts in a way that imparts high level information without also enforcing a specific use case. This hybrid approach may be more tractable.

Endpoint capabilities will vary greatly depending upon intended application(s), deployment environment, and cost considerations (memory size, computing power, battery life, etc.). As such, the requirements have been aligned to three Trust Label categories that aim to provide purchasing guidance based on the expected usage of the device and the environment where it operates.

- **Bronze**: The bronze level of IoT device provides the lowest level of assurance and cyber resilience to the end user and does not require any technical changes to the product itself. Vendors provide one-time information describing the device and expected behavior to achieve this level of compliance. Bronze devices rely on their implicit identities to provide the underlying network infrastructure to provide essential "Before" capabilities in the security, data protection, and privacy areas.

  Devices in the Bronze tier are targeted at buyers that are price sensitive and NOT concerned about the overall security or resilience of the individual device due to the level of management that can be provided through existing network and security capabilities that exist within the organization to provide before, during, and after protections. If the device is compromised by an attacker, the buyer accepts the fact that the device would have to be replaced with a new unit.

- **Silver:** In addition to meeting the Bronze level requirements, the Silver level IoT device implements more trustworthy identity and authentication mechanisms, standalone cyber security functionality, and assists the network in enhancing the device's cyber resilience in the "Before" and "During" attack continuum stages by providing some visibility into the devices security state. The cybersecurity functionality of the device compliance tested by vendor and the results MAY be shared with customers. Vendors must also provide or contract for any ongoing cloud services that are required to maintain the cyber resilience of the device.

  Devices in the Silver tier are targeted at buyers that are concerned about the overall cyber security and resilience of the individual devices being deployed, but do not have the need or capability to provide ongoing network and security management for their devices. Unlike the Bronze device, if this class of device is vulnerable to exploit or compromised by an attacker, the vendor provides software updates to mitigate security vulnerabilities for a period of time that is made known to the buyer via the trust label.

- **Gold:** In addition to meeting the Silver level requirements, the Gold level IoT device and its vendor provide visibility into the security, data, and privacy assertions that are made as well as coverage across the Before, During, and After stages of to the attack continuum. Secure development lifecycle compliance, independent security testing results, information on data usage and protection controls, and the ability to control the personal or customer data usage MUST be readily available for customers.

  Devices in the Gold tier are targeted at buyers that are extremely sensitive to risks associated with security, data, and privacy. As a result of the increased visibility into the device's security state, Gold devices are best suited for tight network integration and enable maximum cyber resilience across the attack continuum.

Bronze Devices Appropriate use cases for Bronze devices include areas where the things are deployed within a managed environment that provides appropriate security and safety controls to compensate for the lack of resilience of the actual Thing.

An example of a bronze device would be connected lights deployed within a traditional enterprise network environment where an IT organization is able to layer in appropriate controls based on the Thing manufacturer's device usage information in order to compensate for the device's lack of cyber resilience capabilities.

Silver Devices

Silver devices are well suited for deployment within consumer use cases where an IT organization is not present and/or the consumer in not able to provide sufficient management and control of the devices to protect them against a cyber-attack.

An example of a silver device would be a connected baby monitor that allows the consumer to trust that the device is operating securely and protecting the privacy of the owners.

Gold Devices
Gold devices are best suited for deployments that require a higher level of assurance that the device is operating in a known to be good state of security due to either the criticality of the use case or sensitivity of the data being processed.

An example of a gold device would be an autonomous vehicle being used by a taxi service where the passengers of the vehicle would ideally be able to be aware of the security state of the vehicle prior to departure.

Endpoint Capabilities
Each requirement is specified with an associated compliance level. Where applicable, a normative reference and/or open source reference implementation is provided. For areas where a standard does not exist, or the requirement may be more difficult to measure, we have provided non-normative references.

Secure Manufacturer-based Identity and Certificate Storage (Silver)
Endpoints that communicate via IEEE 802 networking MUST contain a certificate (IDevID) along with the MUD-URL, and associated private key for the certificate. [IEEE802.1AR]

Secure Local Identity (Silver)
Endpoints that implement IEEE 802 networking MUST support installation of at least one local certificate (LDevIDs) and associated private keying material.

Certificate Management (Silver)
An Endpoint that communicates via IEEE 802 networking MUST support [RFC7030], Section 3 on TLS Layer, for certificate management of secure transport.

Key and Certificate Storage Requirements (Silver)
The Endpoint MUST contain the certificate chain used to validate BRSKI vouchers, as well as any trust chains necessary to validate signatures on firmware or software updates.

Secure Storage (Gold)
Endpoints MUST store private keying material and certificates in tamperproof storage.

Random Number Generation (Silver)
Quality random number generation is required by several of the security protocols implemented by an Endpoint.

An Endpoint MUST provide random number generation either through hardware or as compliant with FIPS 140-2 Sections 4.7.1 and 4.9.2 or equivalent standards.

Cryptographic Protocol Support
Hash Algorithms (Silver)
An Endpoint MUST minimally support the SHA-256 hash algorithm. Endpoints MAY support stronger suites and algorithms.

Asymmetric Cryptography: LDevIDs (Silver)
An Endpoint MUST provide support for Elliptic Curve Cryptography described in [RFC6090] and [IEEE802.1AR] for use as LDevIDs.

Asymmetric Cryptography (IDevIDs) (Silver)
An Endpoint MUST support either 2048-bit RSA certificates or ECC certificates as described in [RFC6090] and [IEEE802.1AR] for IDevIDs .

(D)TLS Cipher Suite Support (Silver)
Endpoints MUST minimally support the TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 cipher suite which is detailed within [RFC 7251] for EAP-TLS. This cipher suite will be used for the authentication operations used for both network layer and application layer authentication processes.

Endpoint Hardening (Silver)
Endpoints MUST only run services that are described in the MUD profile. Extraneous code MUST be removed prior to Endpoint production.

Authentication
The focus of this section is Endpoint-2-Network authentication. This includes during initial establishment of secure network connectivity (aka onboarding) and subsequent management activities.

EAP-TLS (Gold)
Endpoints using IEEE 802.3 (wired Ethernet) MUST support [IEEE 802.1x] using the EAP-TLS [RFC5216] EAP method. Endpoints that have IEEE 802.11 transceivers MUST make use of [IEEE802.11] security in conjunction with [IEEE802.1X] (WPA Enterprise) to exchange [IEEE802.1AR] certificates.

IEEE 802.1x (Silver)
Prior to completing onboarding (e.g. obtaining a local trust anchor and LDevID) Endpoints communicating on IEEE 802 networks MUST authenticate using their IDevID and MUST accept the local 802.1X network credentials without validation purely for the purposes of onboarding.
[[NOTE: the change-of-authorization for the 802.1X session after onboarding is complete is not clearly defined]].

After LDevID enrollment via onboarding subsequent 802.1X sessions are authenticated using the LDevID. The Endpoint MAY make full use of the connection for management and thing-to-thing and thing-to-vendor communications.

The reference implementation for IEEE 802.1X can be found here and is available in most Linux distributions.

Onboarding (Silver)
Endpoints MUST initiate BRSKI onboarding, including support for the BRSKI-optional integrated EST enrollment for an LDevID. Network infrastructure MUST only allow BRSKI onboarding for Endpoints that authenticate using their IDevID credential. See [BRSKI] for details.

The Endpoint MUST fail gracefully, if attempted connections are rejected.

Ongoing Key Management (Silver)
EST supports key renewal. IoT Trust Label Endpoints that use IEEE 802 networking to communicate MUST renew their LDevIDs via EST no later than 30 days prior to expiration of the current key, and must log any renewal failures with increasing urgency.

Transmission and processing of MUD-URLs (Silver)
A MUD-URL is transmitted as part of a certificate. If the endpoint cannot find a local registrar for 802.1X or BRSKI, it MUST transmit the MUD-URL found in the certificate or otherwise configured via LLDP or DHCP.

A reference implementation for a DHCP client that supports MUD is dhcpcd, which is distributed with most major distributions. A second reference implementation is dhclient, which is distributed by ISC.

A MUD File generator is available at https://www.ofcourseimright.com/mudmaker/.

Secure Firmware/Software Update (Silver)
Endpoints MUST have the ability to securely receive and apply a software and/or firmware update. All Updates MUST be signed by the manufacturer and Endpoints MUST validate signatures. The endpoint MUST be configured to check for an HMAC signature whose key strength is determined by deployment environment. Careful key management processes SHOULD be implemented during code development and release.

System Event Logging (Silver)
Endpoints MUST implement SYSLOG to report all anomalous behavior and any supervisory access to provide the necessary visibility for incident monitoring and defense.

Examples of supervisory access include:

- Reading the Endpoint state.
- Configuration change to the Endpoint.
- Updating Endpoint software or firmware.

Anomalous behavior includes excessive unauthorized access attempts or excessive or inappropriate use of the Endpoint. An example would be door lock that is repeatedly activated in a very brief period of time.

A normative reference for logging can be found at:
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf.

Secure Event Logging (Silver)
Event logging MUST be made using syslog over DTLS [RFC6012]. The certificate used to authenticate to the syslog server SHOULD be the same one established during onboarding operations.

A reference implementation for syslog over DTLS can be found at
http://www.rsyslog.com/doc/tls_cert_client.html

Time Distribution (Silver)*
During onboarding, the BRSKI protocol is designed to support devices that do not have a real-time clock. The full details are described in the BRSKI document but are summarized as: The network administrator decides if BRSKI vouchers are permanent (timeless) or if they are required to have a cryptographic nonce ensuring freshness for the particular bootstrapping attempt. Certificate validity periods are ignored until BRSKI completes. At this point the device enters a mode in which the certificate authority root certificate validity period is used to assume a current time window until Network Time Protocol (NTP) time updates narrow the window further.

A trusted time source is necessary for the process of certificate validation and reliable system event logging and correlation. Endpoints MUST use either Simple NTP version 4 [RFC4330] or time provided by a trusted and authenticated server as described in Section 5.5.

Endpoints MUST periodically write the current time to non-volatile storage, and use that as a base prior to being configured with accurate time. The purpose of doing so is simply to prevent attackers from using expired certificate to gain unauthorized access to an Endpoint.

Privacy
Endpoints may collect, store, or transmit a variety of information based on the intended usage of the device and the market vertical. Endpoint manufacturers MUST use [PRENG] or [PbD] principles during the product development cycle.

Limited Collection (Bronze)*
Endpoints MUST only collect the information that is necessary for the stated purpose of the device and that has been communicated to the end user via a standard Privacy Policy that is available from the manufacturer's website.

A normative reference for this requirement is the EU General Data Protection Regulation (GDPR) Article 5(1c).

Controlled User Access to Personally Identifiable Information (Gold)*
Endpoints MUST protect personally identifiable information from disclosure and modification. The actual implementation will depend on the nature of the Endpoint and associated service, but an example would be to encrypt information on the device such that only authorized users may access it.

A normative reference for this requirement is GDPR Article 5(1f).

End User Data Removal (Bronze)

During the lifecycle of an endpoint, it may be necessary to ensure complete erasure of all end user (personal or customer) data from the device. This could through a factory reset option or data removal option. One use-case for data removal would be the event of an endpoint passing from one owner to another legally or illegally.

Endpoints MUST provide a means to remove/erase all end personal and/or customer data. This includes any data that may be stored on the cloud server.

A set of normative references for this requirement are GDPR Article 20 - Portability and Article 17 – Erasure.

Service Requirements
These requirements relate to those necessary procedures and mechanisms that manufacturers must support in order for devices to properly function on an ongoing basis.

MASA Server (Silver)
An IoT Trust Label Manufacturer MUST provide a Manufacturer Authorized Signing Authority (MASA) service in accordance with [BRSKI]. In addition, this service MUST be secure, fault tolerant and available at all times, in order for a new device and operational network to establish trust in one another.

BRSKI supports the issuance of nonce-less vouchers that enable onboarding or recovery operations when the MASA service is not available. This does not impact the requirement that a MASA service be available when the local network administrator wishes to obtain either nonce-less or nonced onboarding vouchers.

A third-party MAY initially offer as a trusted service a MASA Server. However, the manufacturer is under no obligation to use that site.
MASA Server Logging (Silver)
The MASA server MUST maintain logging of all transactions (success and failure) for analytical purposes, such as enabling for the legitimate transfer of ownership with minimal requirements upon the device vendors. The log is made available as defined in BRSKI.

MUD Server (Bronze)
An IoT Trust Label Manufacturer MUST provide a file server that distributes Manufacturer Usage Description (MUD) files in accordance with [MUD]. This service MUST be fault tolerant and available at all times, as it is required to establish appropriate network access controls for IoT Trust Label devices.

A third-party MAY initially offer as a trusted service a site that an Endpoint manufacturer may use to distribute MUD files. However, the manufacturer is under no obligation to use that site. The service provider will validate signatures of MUD files and vet them for risks prior to them being used in local deployments.

Cloud-Based Management Functionality (Gold)
IoT Trust Label Endpoints will often establish cloud-based communications in order to satisfy various operational requirements (e.g., firmware upgrade). Such services may not be reachable by other devices in an IoT Labelled Network unless all specifically allowed by local network administrator or automatically authorized based on identity and posture of the devices. Manufacturers meeting IOT Trust Label “Silver” requirements MUST clearly label and advertise, in a MUD file or other well-known place, whether Internet access is required for a given device.

All communications to the cloud service MUST make use of TLS 1.2 or higher with the TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 cryptographic suite.

Furthermore, any information provided to the manufacturer (logging or customer related) must be explained clearly to customers prior to collections and transport. See Privacy requirement about Limited Collection of Data in 0.

Identification by Heuristics (Bronze)
Manufacturers MUST provide a description of device behavior that may be used by the network to infer identities and apply policies. This includes MAC address ranges used, services, and any cloud-based addresses. Note: devices that provide certificates as described in Section 3.1 are exempt from this requirement.

Process Requirements
Product Vulnerabilities, Incident Reporting and Remediation (Silver)
Product vulnerabilities will arise from time to time, either through some flaw in coding practices or through a vulnerable third party library or entity. Endpoint manufacturers MUST have an active product incident response team (PSIRT), with documented processes and service level agreements that customers and others can easily locate and call to report product vulnerabilities.

The European Union Agency for Network and Information Security has published a Good Practice Guide on Vulnerability Disclosure.

Secure Development Lifecycle (Gold)
IoT Trust Label Endpoints are intended to be "trusted" by our customers and our partners. This includes the confidence and assurance that secure (and good) development lifecycle practices are followed in the development and maintenance of the product. IoT Ready vendors MUST have SDLC Process in place that includes the following elements at a minimum:

- Training for software developers which includes secure coding techniques and requirements standard C libraries.
- Threat modeling that includes a summary report of findings and a diagram.
- Software security testing thru either dynamic or static analysis tools and a report that demonstrates testing was completed and output of testing.

A way to document and track third party and open source components used in product.

A summary of the vendor's specific SDLC process MUST be available on their public facing webserver.

While this requirement is listed as Gold, it is highly recommended for all IoT Label certification levels.

Normative Reference: NIST Security Considerations in the System Development Lifecycle

Data Privacy – Right to Erasure (Bronze)
The manufacturer MUST support the capability for the erasure of end user data at either a point in time when the data no longer provides value for the purpose for which it was collected or the end user withdraws consent for the processing of the data.

A set of normative references for this requirement are GDPR and Article 17 – Erasure.

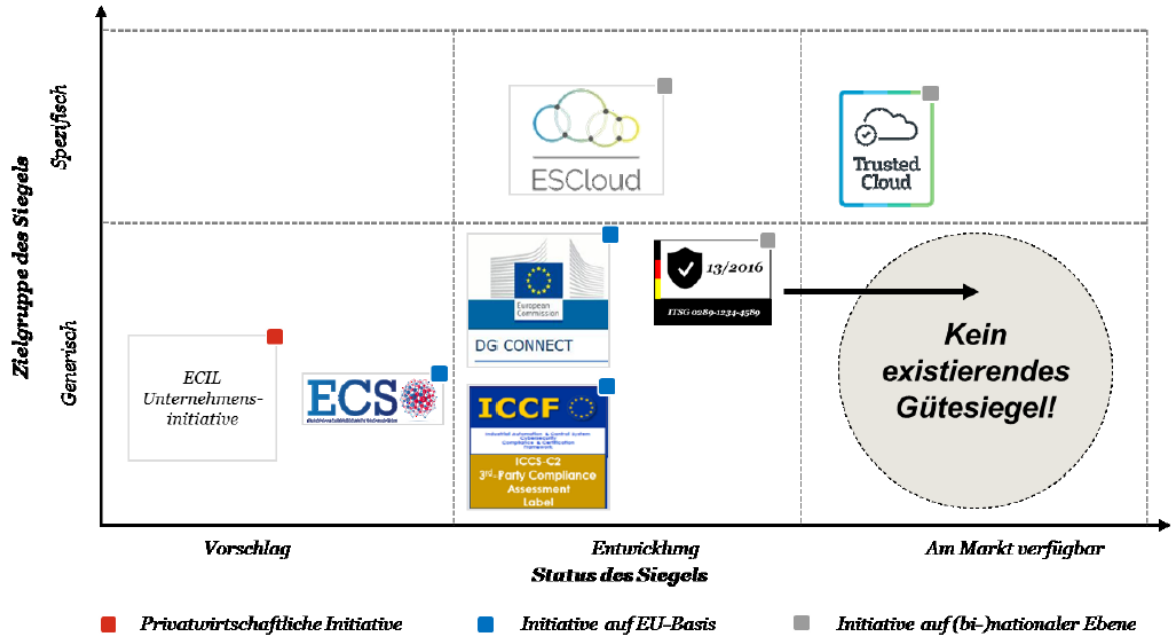
Data Privacy – Pseudonymization (Gold)
The manufacturer MUST support the use of pseudonymization as a process for protecting end user data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.

A set of normative references for this requirement are GDPR and Article 6 – Lawfulness of Processing.

7.10 German Ministry of Interior – Study on "Introduction of a label of quality for IT security features of Internet-enabled products"

Right after the cyber-attacks of on hundreds of thousands Router of a German telecommunication group and the "Mirai"-Botnet Attack, IT security has become more and more important for the citizens. In order to face these threats, the Cyber security strategy of the Federal Government included the introduction of a quality label for IT Security in 2016. To do so, the Federal Ministry of the Interior asked PwC Strategy& to do a research on this topic. In their study, PwC Strategy& organized a representative survey specifically designed for consumer side and set direct interviews with IT manufacturers, in order to understand their interest and potential necessity for an IT Security Certification.

The necessity of this Certification also comes from the fact that the EU suggested the Member States to increase Cyber Security levels and at the moment the only label initiatives at European level are still at a launch stage (see Trusted Cloud label "and "label ESCloud). Therefore, the IT Security label could function as a pioneer for a European solution.



Customer's Survey

PwC Strategy& collected information from the consumer's side through a survey to which 1.022 interviewees answered in the period from the 2nd to the 8th February, 2017. Their age ranged from the age of 18 to 69 years old.

Through the survey PwC Strategy& discovered that:

- On security information: 90% of the interviewees would like to receive more information about the security of their IT devices
- On the buying decision:
  - 91% of the interviewees considered the Security of the Device important at the moment of purchase
  - 70% of the customers is influenced positively by the presence of a security label.

- More than 65% of the customers would be in favor of paying a higher price for security labelled product

As a consequence of these results, PwC Strategy& found out that an IT security label would be a demarcation characteristic feature from the "less protected" products.

According to consumer's priority, the products that should be labelled for their Security are computer and laptop (> 83%), followed by Smartphones and Tablets (82%), while smart Home and electrical appliances and wearables are less
relevant.

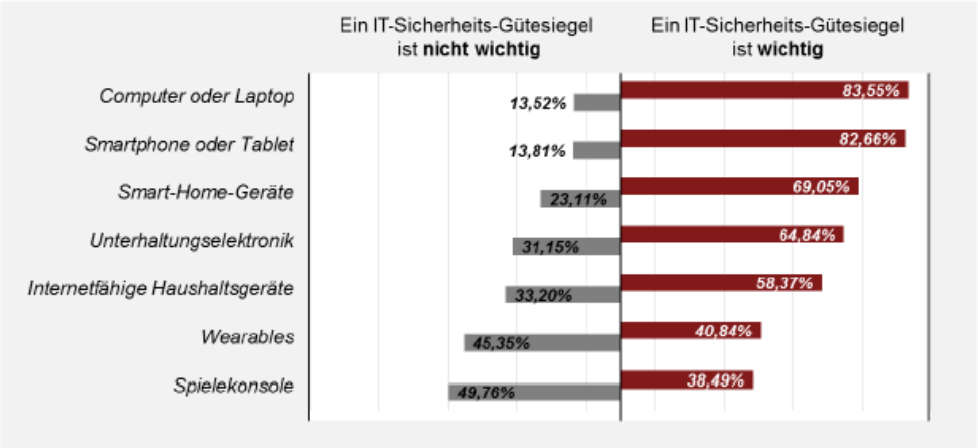


Abbildung 4: Interesse an einem IT-Sicherheits-Gütesiegel nach Produktgruppen

According to the responsibility of who should assure the security of the products, it was discovered that:

- Nearly 90% of the interviewees believe that the responsibility for IT security depends on the manufacturers.
- Only 61% see the government (state) as the responsible authority with the obligation for IT security.
- More than 82% of the interviewees think that the IT Security Label should come from Stately promoted institute
- Only 44% believes that the label should be a responsibility of a private test institute
- A majority of the interviewees considers that the assignment of the security label should not depend from private-economic institutions (57%).

Manufacturer's interviews

PwC Strategy& asked the opinion of 18 relevant manufacturer's enterprises and five groups of the IKT branch on the IT security label, in the period from the 1st February to the 7th April, 2017.

What they found was:

On the importance of IT Security label for the company

- IT security is a central factor in the product development
- Manufacturer with higher prices don't want to endanger their brand by a possible security gap in their IT devices
- Only very much few enterprises know or use existing security labels in the area of IT security with end user's focus
- If the IT security label would guarantee a uniformed standard at European levels, manufacturer interest would increase remarkably

- Enterprises have a bigger interest in an IT Security label in the middle price segment of the marker

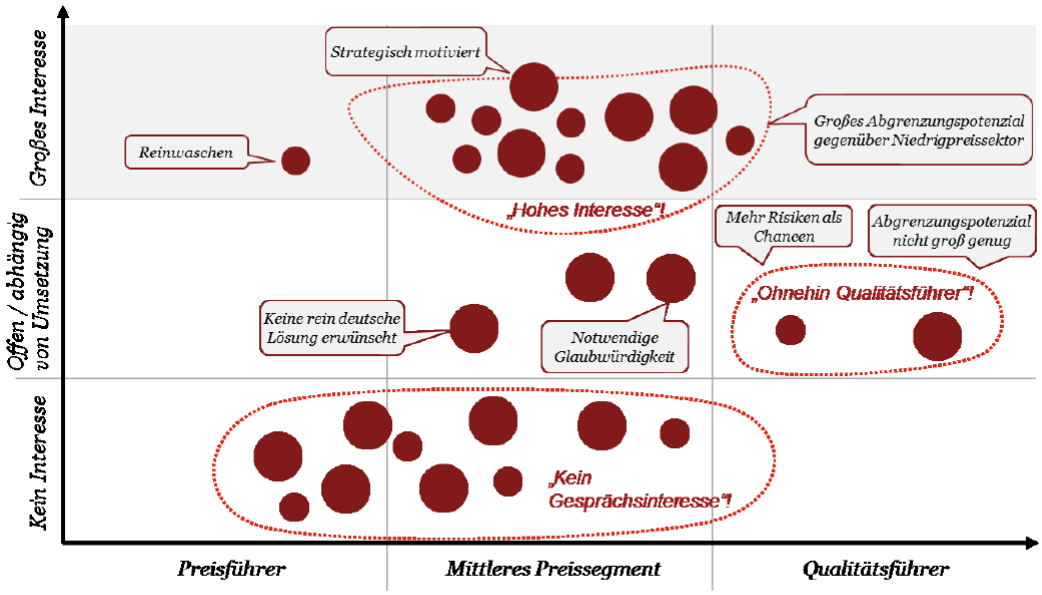


Abbildung 5: Einordnung der Hersteller hinsichtlich Interesse und Preissegment

Challenges for the certification:

- The certification would guaranty IT security only for a limited period of time, since there always newer security threats.
- The security label would be only an indication, not a proof. In some cases, the
- Enterprises can guarantee no IT security for a certain period in this frame, but minimize only risks or conclude (close) recognized security gaps. The consumer has in fact partial responsibility on the security of the IT device.
- IT devices have multiple components such as hardware, software and apps. It is important to clarify where the security label applies.

Patronage of the certification

Since the BSI would be the responsible for the definition of the criteria, they will have to cooperate with the manufacturers and the consumers' protectors. The responsible ministries can also cooperate. Even though the BSI is the distributor of the label, the security tests can be done in other external structures.

7.11 Cyber Risks and Cyber Resilience of Critical Infrastructures

European Critical Infrastructures constitute those designated critical infrastructures which are of the highest importance for the Community and which if disrupted or destroyed would affect two or more MS, or a single Member State if the critical infrastructure is located in another Member State. This includes transboundary effects resulting from interdependencies between interconnected infrastructures across various sectors[55].

In the last years, the dependence of critical infrastructures from cyber space has become increasingly important. Europe and the entire world is experiencing a massive growth in connected cyber-physical infrastructures – ranging from IoT-based smart environments to critical infrastructures such as power grids, energy, water and manufacturing systems.

The number of connected devices is expected to grow to tens of billions by the year 2020. Very large cyber-physical infrastructures are envisioned which will integrate multiple applications run by a variety of stakeholders within a shared fabric. Examples include future industrial environments, infrastructure monitoring technologies and intelligent transportation systems. In such contexts, thousands of nodes will be deployed and used by a large number of stakeholders to provide a multitude of services. Such shared fabrics will remain in operation for a long time (potentially decades) and the physical composition, the services provided and the stakeholders involved will change with time.

In a survey of critical infrastructure organisations in the United States (US), the United Kingdom (UK), France, and Germany, 48% of respondents expressed that it would be likely for a cyber-attack to take down critical infrastructure with the potential loss of life[56]. The scale of future cyber-physical infrastructures and their dynamic nature in terms of stakeholders, services and physical properties over long time periods poses unique security and resilience challenges[57].

In the following paragraphs, four critical infrastructures sectors will be analysed to underline problems, risks and resilience due to the depence from cyber space.

Energy Sector

New energy technologies such as renewable generation, electricity storage and electric vehicles will have far-reaching social and economic benefits. These transformations, however, depend upon the employment of 'smart' technology, which underpins other digitalisation strategies to deliver the benefits associated with smart cities, health, transport and logistics.

The smart energy system is therefore created through the significantly greater use of ICT in the digitalisation of energy production and distribution. The resulting energy transformation will see increasing decentralization of the energy system and greater inclusion of the consumer across the energy value chain.[58] It is essential to maintain equilibrium in critical infrastructure such as energy, which supports and sustains other critical infrastructure. A power outage often has serious consequences due to the cascade effect, inevitably affecting other sectors and their infrastructure[59]. The Ukraine power grid attack[60] in 2015 demonstrated the potential impact of cyber-attacks to the electricity subsector. This well-planned hack on 3 power-distribution companies caused outages to 80,000 energy customers.

The focus of cyber security in the energy sector is to support the reliability and resilience even in the event of a cyber-attack. Unlike IT systems, a control system in the energy sector that is under attack cannot be easily disconnected from the network as this could potentially result in safety issues, brownouts or even blackouts.[61] The scale of the threat to energy cyber security is massively increasing as energy systems develop ubiquitous intelligence and communications capabilities throughout their operations. In addition, development of a cost effective low carbon energy system across the EU will require a more distributed energy system, whilst also employing increased inter-connection and cooperation across national

[55] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN
[56] The Aspen Institute and Intel Security, 2015: Critical Infrastructure Readiness Report: Holding the Line Against Cyber threats
[57] Awais Rashid, Wouter Joosen, Simon Foley, *Security and Resilience of Cyber-Physical Infrastructures,* Lancaster University Technical Report No: SCC-2016-01
[58] http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf
[59] http://www.osce.org/secretariat/103500?download=true
[60] Analysis of the Cyber Attack on the Ukrainian Power Grid, Defense Use Case, March 18, 2016, SANS ICS and E-ISAC.
[61] https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

boundaries.[62] At the same time, demand for energy is always on the rise. As the German government put it, "New solutions must be found that support the transition to liberalized markets, decentralized and volatile power generation structures, and electro mobility – while also ensuring the maximum possible level of cost-effectiveness, security of supply, and environmental compatibility." In this context, the security of critical infrastructure is a core issue in national, international, and corporate security dialogue and policies.[63] Energy reliability at the European level relies on trans-European connectivity. A failure in one energy system can have a potential cascading effect across regions as shown in a major European blackout in 2006 caused by a planned disconnection of a transmission line.

Despite cyber security being a recent subject, a number of initiatives have already been conducted by Member States in order to enhance the country's ability to face any attack. Member States need to learn about best practice from other sectors or other world regions that deal with highly sensitive information or are subject to cyberattacks on a regular basis. For example[64]:

- In **Denmark**, there is a close exchange of data between the transmission system operator (TSO), DSOs, generators and retailers via a data hub. Energinet.dk (TSO) is responsible for data security in relation to information exchange in the electricity market, but it has outsourced the security service to a third party;
- In **Norway**, companies are obliged to report major incidents (including cyber security incidents) to the national authority NVE. Apart from that, in 2014 Norway has set up "KraftCERT" (see https://www.kraftcert.no/english/index.html);
- In **Austria**, there is a public-private cooperation in order to set up (voluntary) national security and safety standards for the power industry, carry out a risk assessment and develop an action plan to tackle these risks;
- In **France**, companies are about to be obliged 12to report large cyber security incidents to the national cyber authority, ANSSI. There is also a CSPN certification for black box testing of product security level. However, there is a lack of mutual recognition with other Member States: no market for suppliers, therefore no incentive for certification. That is why it has been mainly used only by Small and Medium Enterprises (SMEs) so far;
- In **Sweden**, there is a long tradition of cooperation between the energy sector and the responsible authorities regarding all security matters. A common security website for the energy sector (www.energisakerhetsportalen.se) has been developed where all relevant information is gathered;
- In **Portugal**, the National Cyber security Center (CNCS), part of the National Security Authority, ensures effective crisis management, coordinates the operational response to cyberattacks, develops national synergies and enhance international cooperation in this field. It has been developing a number of initiatives closely related to the energy sector;
- In **Germany**, the national IT-Security Act came into force in June 2015. Since May 2016, operators of critical infrastructures in the energy sector are obliged to report network and information security incidents that may have a disruptive effect on the provision of their service. In addition to that, all DSOs and TSOs need to fulfill a catalogue of IT-security measures and implement an Information Security Management System (ISMS) compliant with ISO/IEC 27001. Electricity generation plants that have been identified as critical infrastructures will need to fulfill a different catalogue of IT-security measures that is currently being drafted by the national regulatory authority."

Ensuring resilience of the energy supply systems against cyber risks and threats are becoming increasingly important as widespread use of ICT and data communication is becoming the foundation for the functioning of infrastructures underlying the energy systems. The increased efficiency in supply services comes with a price: increased exposure to cyber incidents and attacks. In a cross-sector manner, these threats apply to all generation, transmission, distribution and process technologies, and to energy market services.

[62] http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf

[63] http://www.osce.org/secretariat/103500?download=true

[64] http://www.eemg-mediators.eu/downloads/Report_on_smart_grid_cyber_security_20.12.2017.pdf

The digitalization of the energy sector also raises the question of how to face the risks and threats of cyber incidents and attacks affecting personal data and strategic energy infrastructure data, which are sometimes crucial for the security of the energy supply.[65]

Transportation Sector

The integration of several ICT systems for water transport, railways, airports and intelligent public transport, where cyber-physical devices, communication networks and central servers optimise the transport service up to a certain degree of automation, it also has the effect of introducing cyber security risks into transport networks that have not historically been susceptible to such risks. A total of 81% of large businesses and 60% of small businesses suffered a cyber security breach in the past year. €700,000 – € 1,30 million is the averaged cost to a large organisation[66].

Some examples of cyber risks for the transportation sectors are related to: Physical asset damage and associated loss of use, unavailability of IT systems and networks, loss or deletion of data, data breach leading to the compromise of third-party confidential information including personal data, cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information[67]. Risks for railway comes for example when informational systems are attacked leading to unavailability of services for the passenger, like being unable to buy a ticket or digitally check a ticket into the system[68].

For Smart airports, the introduction of new components and functionalities to facilitate the infrastructure-to-passenger interaction and vice-versa paves the way for new attack vectors or pathways and exposes airport assets to a larger attack surface. These risks include vulnerabilities in ICT and electronic systems as well as the information and data held and processed by such systems. Vulnerabilities can be exploited by malicious actions, but also human errors, system or third party failures and natural phenomena.

Therefore, it is imperative to put in place a collaborative model to set goals and define an appropriate cyber security approach to strengthen the aviation system's resilience against attacks. To this aim, significant effort is being invested across the aviation community at different levels, including standardization, security working groups, research and education. Identification of challenges posed by cyber threats, risk assessment approaches and guidelines to enhance cyber security, either in terms of high-level governance strategies or in terms of specific technological supports, are priorities currently tackled.[69]

Finance Sector

For the Finance Sector, a complex set of interconnected networks allows real-time data exchange thus increasing the efficiency of communications, but, on the other side, it increases the risk of accessibility to confidential information and to critical systems able to control physical assets.[70]

Financial IT systems are exposed to a number of hazards which require consistent efforts to operate securely. In recent years, NIS risks have become more complex and their impact can range from low to very high, including domino effects. Such impacts will not be confined to the "virtual" world; a major attack outreach would most certainly impact the assets in safekeeping or in transit.[71]

Online financial services and lending companies are increasingly being targeted by fraudsters and costing consumers millions of euros around the world, according to research. Cyber-attacks against online lending companies and alternative payment systems increased 122% in 2016, according to ThreatMetrix, a security company that monitors more than 20 billion online transactions a year. The fraud is estimated to have cost consumers as much as 9 billion euros in 2016, the company said[72].

ICT operators, intended as operators who directly manage Internet connections (such as Internet Service Providers and telecom operators), are directly involved in the cybersecurity issues and considered the most

[65] https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf
[66] 2014 Information Security Breaches Survey: http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf.
[67] http://www.oliverwyman.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Risk%20in%20the%20Transportation%20Industry-03-2015.pdf
[68] https://www.enisa.europa.eu/publications/challenges-of-security-certification-in-emerging-ict-environments/
[69] https://www.enisa.europa.eu/publications/securing-smart-airports
[70] Fabio Bisogni, Simona Cavallini, Sara Di Trocchio, Cybersecurity at European level: The Role of Information Availability, Fondazione FORMIT, 2011
[71] https://www.enisa.europa.eu/publications/network-and-information-security-in-the-finance-sector
[72] http://www.telegraph.co.uk/technology/2017/02/27/cyber-attacks-against-financial-services-cost-consumers-8bn/

liable actors. Due to the fact that they manage ICT infrastructures and connected services, in the case of a successful cyber-attack, they would suffer the most direct consequences, but wide damages would also affect the rest of society.[73] A survey of 1,000 companies who have been victims of a ransomware attack, when cyber criminals lock all the files in a system and demand payment, revealed such breaches on average knock systems down for a full week, costing up to €2,300 a day in lost revenue. Of the affected businesses, more than 250 paid over €5,700 for the safe return of their data. One third could not access their information for a month after the attack, while 15% said it was never recoverable[74].

Moreover, Criminals have moved away from cracking metal safes and bank vaults. The money is now in their digital equivalents and these are proving vulnerable to the hackers and crackers of the codes of the digital world. The cryptographic codes of the digital world are extremely hard to break, but however hard these may be, they can be vulnerable to being bypassed. In the case of Bitcoin, the 'wallets' that hold the currency have proved vulnerable to theft — but the ledger itself has remained resilient, though in principle it would be vulnerable if over 50% of the computer processing power for the Bitcoin ledger fell into the hands of a single malevolent individual or organisation. Indeed, a great strength of distributed ledgers is that they should be highly resilient to attack.[75]

Against this background and according to the "SANS Financial Services Security" Survey[76], most organizations operating in the finance sector need to be compliant with multiple mandates, which could also explain why so much of their budgets are being spent on compliance. Maintaining these compliance requirements requires automated tools to help identify overlaps in compliance reporting requirements as they monitor against multiple frameworks. Payment Card Industry Data Security Standard (PCI DSS), a requirement for processing credit cards, was cited by 50% of respondents as a mandate they adhered to. Other key mandates included Sarbanes-Oxley Act of 2002 (SOX, P.L. 107-204), a requirement for publicly traded companies (49%), and Gramm-Leach-Bliley Act, the Financial Services Modernization Act of 1999 (GLBA, P.L. 106-102; 47%), a requirement for financial institutions. In addition, approximately 37% adhere to the Bank Secrecy Act and 35% to Federal Financial Institutions Examination Council (FFIEC). Almost 45% of the respondents answered that their organization must be compliant also with State/Regional laws or rules governing financial services systems. Survey respondents also use a range of security frameworks and standards. The top two (49% each) were the ISO 27000 Series and PCI DSS for securing card payments. Credit card processors require card issuers and merchant banks to be compliant with PCI DSS as well as to use only service providers that also demonstrate compliance. In November 2013, the PCI Security Standards Council released PCI DSS version 3.0. Another common security framework is COBIT. Published by the Information Systems Audit and Control Association (ISACA), it is a business framework for the governance and management of enterprise IT.

Growing numbers of regulations are attempting to control the potential losses in the financial services industry. The amount organizations spend on meeting regulatory requirements is huge and is getting bigger. But, for every euro spent on completing a regulatory form, there is one less euro available for actually making systems more secure. There is room for legislative reform to move mature organizations away from being compliance driven to focusing on reducing attack surfaces, minimizing vulnerabilities and defending against threats.

Healthcare Sector

Devices, system components and networks are becoming autonomous, ubiquitous and interconnected. When this technological advancement applies to the healthcare sectors, one of the most traditional critical sectors, the results are remarkable. Connected medical devices transform the way the healthcare industry works, both within hospitals and between different actors of the healthcare industry.[77]

In most countries an eHealth strategy exists, following the recommendation of the first EU eHealth Action Plan requesting the Member States to setup such policy documents to describe eHealth specificities, bodies involved and their responsibilities at a national level. Overall, eHealth infrastructures protection falls under the generic umbrella of CIIP.

[73] Fabio Bisogni, Simona Cavallini, Sara Di Trocchio, Cybersecurity at European level: The Role of Information Availability, Fondazione FORMIT, 2011
[74] http://www.telegraph.co.uk/technology/2017/02/27/cyber-attacks-against-financial-services-cost-consumers-8bn/
[75] http://www.ameda.org.eg/files/gs-16-1-distributed-ledger-technology.pdf
[76] https://www.sans.org/reading-room/whitepapers/analyst/risk-loss-security-spending-financial-sector-survey-34690
[77] https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

Currently, there is no specific regulatory framework on critical eHealth infrastructure protection.[78] Not all MS consider eHealth as a critical sector; in some cases eHealth services formulate a different category of emergency services and are not classified as critical, in other cases healthcare ICT services are not considered critical as the environment is considered so isolated that any incident would have small impact. Instead, the complexity of eHealth systems is very high, which renders information quality (completeness, integrity), accessibility and availability a very challenging task. Emerging healthcare data sharing schemes like EHR (Electronic Health Records) or PHR (Patient Health Records) as well as cross-border scenarios further complicate the technological challenges and respective protection requirements.[79]

Another major issue affecting cyber security in the case of healthcare is the lifespan of medical devices and equipment. Medical devices like CAT scanners, MRI machines etc. can stay as part of a hospital for more than a decade. This means that new vulnerabilities arise as attackers become more sophisticated. Moreover, this shows that intensive focus should be given in the patching and updating management of these devices. The very thin line between usability and security is becoming now more transparent as patching comes second (or even lower) in priority especially as the machines might need to be available at any given moment.[80]

To provide some quantitative data, according to "Health care and Cyber Security: Increasing Threats Require Increased Capabilities"[81] report, the greatest vulnerabilities for the health sector come from: 65% External Attackers, 48% Sharing Data with Third-Parties, 35% Employee Breaches/Theft, 35% Wireless Computing, 27% Inadequate firewalls. Mature incident and vulnerability management processes are lacking in most organizations, and thus, daily threats are not even reported or managed effectively by many organizations. In fact, there were more than 700,000 hacking attacks in any given minute against healthcare organizations in the fourth quarter of 2016, according to a study of 450 providers around the world by the threat intelligence arm of cybersecurity vendor Fortinet[82].

There is no getting around the huge financial results of a data breach[83]. According to Ponemon Institute's 2016 Cost of Data Breach Study, the average total cost of losing sensitive corporate or personal information is approximately 3,51 billion euros. Per stolen record, businesses and associations can spend anywhere between €130 and $140, with health card information costing the most to lose, at $311 per record.

The majority of data breach costs are associated with resolving the matter, as organizations must pay compliance fines and court fees, invest in forensic and investigation processes, and spend revenue on identity theft prevention services for customers or employees. Additionally, Ponemon's report noted that turnover of consumers directly impacts business costs, and from then on out, these organizations must spend more on customer acquisition as the reputational losses of a data breach last a long time.

Healthcare actors including hospitals need to anticipate, prepare for, and respond and adapt not only to incremental change but also to sudden disruption. In smart hospitals, achieving this is more challenging than in traditional hospitals because the number of components that could lead to and be affected by service unavailability is much higher. Moreover, with the constant increase in the use of ICT components/products applied to the healthcare sector, to make sure that security-related requirements from users as well as regulators are met, it is important to involve them into test design and execution at an early stage. In the healthcare context, hospitals should play a key role in the testing activities. For instance, cross-testing could be performed in a larger number of hospitals before products are released. Moreover, regular penetration testing and mock by through security companies are advisable to assess security levels. Mock attacks could also be useful for hospitals as they allow determining response times.[84]

[78] https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services
[79] https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services
[80] https://www.enisa.europa.eu/publications/challenges-of-security-certification-in-emerging-ict-environments/
[81] https://assets.kpmg.com/content/dam/kpmg/pdf/2015/09/cyber-health-care-survey-kpmg-2015.pdf
[82] http://www.healthcareitnews.com/news/how-many-hacks-happen-every-minute-against-healthcare-more-700000-fortinet-says
[83] https://www.cloudmask.com/blog/the-cost-of-data-security-are-cybersecurity-investments-worth-it
[84] https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

7.12 The Lack of Appropriate Standards and the Need for a Common International Approach

Standards and other standardisation publications are **voluntary** guidelines providing **technical specifications** for products, services and processes. Standards are developed by private standardisation organisations usually on the initiative of stakeholders who see a need to apply a standard. Although standards as such are voluntary, using them proves that your products and services reach a certain level of quality, safety and reliability. In some cases, standards are referenced in legislation as a **preferred way** or even as a **mandatory requirement** to comply with specific laws (i.e. safety legislation or interoperability requirements).

Nations are using standards to meet a variety of objectives, in some cases imposing standards that are competing and contradictory, or excessively restrictive and not interoperable. Standardizing processes and procedures is an essential part of achieving successful cooperation in a cross-border or cross-community environment. In the absence of standardization, both processes and communication can be rendered ineffective.

Standards play a key role in ensuring that security products can be put together into systems capable of detecting and responding to real events. In particular, standard interfaces and protocols make systems integration much simpler and allow products to interoperate in heterogeneous environments. Standardization of testing methods also makes it possible to compare security products in a meaningful manner ('benchmarking') and provides a means for the end user to assess new products or services.[85]

The rapid evolution of the IoT market has caused an explosion in the number and variety of IoT solutions. Additionally, large amounts of funding are being deployed at IoT startups. Consequently, the focus of the industry has been on manufacturing and producing the right types of hardware to enable those solutions. In the current model, most IoT solution providers have been building all components of the stack, from the hardware devices to the relevant cloud services or as they would like to name it as "IoT solutions", as a result, there is a **lack of consistency and standards** across the cloud services used by the different IoT solutions.

The increasing dependence on ICT goods and services in today's society emphasizes the need to ensure their security. ICT is responsible for economic growth in Europe and is at the core of daily life. With these positive developments also come with an increasing risk of ICT dependencies, disruption and failure as well. The question arises on who is responsible for ensuring cyber security and cyber resilience. This is not an easy question to answer as government, consumers, ICT providers, companies all have an equal stake in this field.

Within the study "Challenges of security certification in emerging ICT environments"[86], five sectors have been selected to investigate in more detail and to consider a broad spectrum of different requirements and cases that could lead to certification drivers concerning these devices. The five sectors are Energy, ICT, Health Care, Rail Transport and Water Transport. The key finding is that every sector has its own functional and security challenges which makes the target of a common certification framework a challenge. The energy sector, for example, largely depends on real-time interfaces on process automation level to provide a stable and reliable electrical power supply. The need for more real-time data exchange is increasing due to the decentralization of the power grid, increasing penetration of renewables and further integration of markets. On the other hand, the health care sector largely depends on informational systems and interfaces, like centralized patient databases that are used by companies that provide healthcare. Automation takes place on small scale, for example at hospitals to provide health monitoring. Transportation is mostly about logistics and safety. Finally, trains on a track need to be able to communicate with the generic infrastructure, while for the water transportation a vessel contains automation systems from office automation to process automation concerning electric power supply and vessel control. At the same time, ICT becomes the common processing platform which supports all these different functional and security requirements. **This underlines the (increasing) need for a common approach on standards and frameworks for certification.**

When the EU launched the strategy for the Digital Single Market, which included cyber security, it also produced Directives on General Data Protection Regulation (GDPR) and Network and Information Security (NIS), to strengthen the protection of consumers. However, the general legal framework in the EU that

[85] https://www.enisa.europa.eu/publications/articles/standards-for-cyber-security
[86] https://www.enisa.europa.eu/publications/challenges-of-security-certification-in-emerging-ict-environments/

applies to the sale of goods and services from ICT providers to consumers was not covered properly. Fragmentation is still a major issue. **A single market following international standardization is necessary to ensure a consistent approach to the IoT and cybersecurity**. The development of national efforts that would lead to further fragmentation should be avoided, as it could hinder IoT technologies to unfold its economic and social positive impact[87].

Energy sector

In the progression to smart energy networks the IT and OT environments within energy utilities have become more interconnected and reliant upon one another. In addition, communication technologies and system heterogeneity are increasing the technological complexity of the energy networks. The security challenges of sub-systems, combined with an increasingly distributed and multi-functional environment, therefore only increases the energy system vulnerability and potential level of cyber threats. Smart grids are a relatively new concept and therefore experience or relevant information regarding security threats or incidents is minimal. As a result, many application-level protocols have been designed without adequate levels of intrinsic security mechanisms which fully address the impacts of a fully integrated smart energy network. A few examples[88] of resulting issues that have been identified include:

1. In 2014, a team of university researchers from Portugal, found a flaw in an encryption standard developed by the Open Smart Grid Protocol (OSGP) Alliance, intended to secure smart grid networks in the EU and adopted by the European Telecommunications Standards Institute (ETSI).
2. The UK' Government Communications Headquarters (GCHQ) in 2014, intervened in the UK's smart meter roll-out plans due to the proposed use of a single decryption key for all communications between smart meters and energy service providers. This approach created the potential for chaos across the network, as a single hacker could conceivably disable the entire population's electricity meters.
3. Similar concerns were raised from a study conducted by security researchers in Spain in 2014, where millions of network-connected electricity smart meters were deemed susceptible to cyber-attack due to lack of proper security controls.

Typically, protection concepts are prepared at the time of procurement of a system which may take under consideration the risks and threats known at this point in time. Threat and risks are evolving and those legacy systems and devices used in the network do not necessarily comply with up-to-date operational and/or security standards. This reflects one key challenge in energy systems today. Additionally, cyber security in a multi-vendor environment requires interoperability where components should rely on the same set of security standards and requirements used, but these requirements of course vary depending on the operational context.[89]

The harmonization of security implementation across the European Union is not sufficiently addressed as mainly the common base to rely on international standards and specifications is requested. Consequently, the **level of implementation is expected to be unequal** across European Union.[90]

As instance, the architecture of the smart metering infrastructure varies from country to country with the use of different applications (i.e. DLMS, Meters and More or OSGP), different communication technologies and different regulatory requirements[91].

Protection of the energy grid is a collective responsibility of the respective operators and the Member States. However, the criticality and the interdependency of the grid require a harmonization of the protection of respective systems across the European Union. An appropriate tool to define and develop the protection level of an energy grid is the usage of a cyber security maturity framework, which should be defined at EU level and best based on international standards (e.g. ISO/IEC 27000 series). This would allow a flat assessment scheme against to which Member States and the EU can evaluate the maturity of security within the Member State and the EU and on which the overall resilience of the energy grid within the EU can be measured and assessed while avoiding a scattered view of the EU landscape. Examples of a maturity framework for the

87 https://www.cybersecurityraad.nl/binaries/Report%20European%20Foresight%20Cyber%20Security%202016_tcm56-102235.pdf

88 http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf

89 https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

90 https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

91 https://www.enisa.europa.eu/publications/challenges-of-security-certification-in-emerging-ict-environments/

energy grid exist for example by the ES-C2M241 framework for electricity subsector or the ONG-C2M2 framework for the oil and gas subsector from the United States Department of Energy (DoE). An additional advantage of a maturity framework would be to enable and foster use of cyber insurance as one mechanism to cover potential damages by cyber-attacks and by the achievement of a higher maturity level that may result in a lower insurance cost.[92]

The current lack of standards for smart energy communication system design and integration increases the vulnerability of communications networks to cyber-attacks. Such standards and guidelines should in turn provide a basis for the development of a European certification scheme. These communication standards should include:

- a common reference architecture,
- technical and operational requirements for smart energy / grid applications and systems,
- remote updates and reconfiguration – providing for smart energy / grid communications systems that utilise updatable devices to dynamically and remotely update security applications,
- a reference risk assessment framework and methodology[93]

Another concrete example of lack of standards and common approach for the Energy sector regards the Virtual Power Plants. A Virtual Power Plant consists of a central IT control system and distributed energy resources (often renewable energy resources like solar, wind, hydropower, and biomass units) as well as flexible power consumers. By networking all participating units through a remote control unit, it establishes a data transfer between the central control system and the participating units. The central control system is then able to monitor, forecast, and dispatch the networked units.
Currently for the security of Virtual Power Plants, the VHPready standard is not mature and finalized yet, therefore there is currently no compliance scheme available. It is currently focusing on security rules and best practices imposed by other standards like IEC 62351[94].

Looking at the nuclear energy sector, As no regulation for cyber security currently exist at EU level, **Member States often simply follow in their national approaches** on computer security principles and methods developed by the IAEA, which offers a set of cyber security standards supplemented by the voluntary possibility of an advisory service (IPPAS66) of IAEA on State's request. However, not all EU Member States have already an effective legislation and regulation developed or implemented, as can, for example, be seen from the detailed evaluation of the Nuclear Threat Initiative (NTI) on security conditions.[95]

Transportation Sector

There is currently no common EU approach specific to either intelligent or standard public transport, or related framework that specifically address IPT cyber security needs. Potentially the proposed NIS Directive might have an impact on addressing elements of this gap, above all in relation to cyber threat reporting, but may need to be expanded to encompass requirements for IPT cyber security within both urban transport networks and national/international rail networks.

There is a lack of specific security standards for IPT that can address the specific context and security threats faced by IPT assets. Generic standards, such as the ISO27000 series, are not sufficiently useful for the complex reality of IPT and are poorly related to the security environment within which transport organisations interact and operate today. It is important that standards are able to accommodate new IPT functionalities and concepts as they become relevant, while being able to remain dynamic, extensible and flexible.

The lack of a dedicated cyber security standard for IPT is an obstacle to the adoption of good security principles by IPT operators, manufacturers and solution vendors. With the support of the EC and MS, the industry (private and public sector) should ensure the development and adoption of harmonised standards adapted to the particularities. One or several completing standards could be developed to cover cyber security from various points of views as it has been proposed in other domains (*e.g.* Smart Grids)[96].

[92] https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf
[93] http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf
[94] https://www.enisa.europa.eu/publications/challenges-of-security-certification-in-emerging-ict-environments/
[95] https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf
[96] https://www.enisa.europa.eu/publications/good-practices-recommendations

Many of the component technologies that can deliver intelligent and resource-efficient mobility and energy production and use have already been developed. Now industry players from different sectors need to jointly develop and apply solutions that meet, for example, the demand for energy efficiency, alternative fuels and ICT in urban energy efficient applications. At the same time, risks related to the scale-up and integration of these solutions remain. They originate from and are related to regulatory uncertainties, risk averseness of public procurement concerning innovative solutions, the current absence of standards and the immature market for truly integrated energy, transport and ICT solutions, among other things[97].

A concrete example where the lack of standards affect the Water Transport sector are the IMO mandatory requirements. IMO mandatory requirements for the electronic exchange of information on cargo, crew and passengers have been adopted by the International Maritime Organization (IMO) on 11/04/2016. These include standardized forms for the maximum information required for the general declaration, cargo declaration, crew list and passenger list; and agreed essential minimum information requirements for the ship's stores declaration and crew's effects declaration. Although standards and recommended practices relating to stowaways are updated to include references to relevant sections of the International Ship and Port Facilities' Security (ISPS) Code, the ISPS audits **do not currently address the cyber security aspect** of the electronic passenger lists[98].

Given the highly interconnected and complex nature of transportation networks, there is the need for more sophisticated analysis tools that can capture asset interdependence and cascade-effects among all the involved assets and different stakeholders. These tools will help capture how interdependencies operate and will heighten impacts in order to develop procedures and policies to improve recovery.

Risk assessment methodologies that can deal with multiple networked stakeholders working in collaboration need to be developed. This requires a different mind-set for existing risk management approaches, which often begin by scoping a system (*i.e.* defining its borders) prior to a risk assessment based on the individual elements. However, in interconnected systems this clear border does not exist. To address this gap we need to redesign risk management systems/approaches so that they operate from a *stakeholder* perspective rather than *border* perspective[99].

[97] https://ec.europa.eu/digital-single-market/en/news/smart-cities-and-communities-european-innovation-partnership-communication-commission-c2012

[98] ENISA, *Challenges of security certification in emerging ICT environments,* December 2016

[99] https://www.enisa.europa.eu/publications/good-practices-recommendations

Financial Sector

The financial industry is more regulated and has more oversight than any other industry on the planet. However, fintech's do not face the same level of regulation, because they may not fall under FDIC, SEC, or any other number of federal and state agencies. Therein lies one of the major hurdles to regulation. The sheer volume of oversight agencies creates more complexity in trying to build a singular regulatory policy or framework for the industry. Financial institutions are more regulated, because of the calamitous disruption and financial instability that will ensue when not properly regulated. Fintech's create the same types of disruption and instability with data breaches and exposing customer data, because they are creating a larger attack vector for the organization utilizing their service offering.[100]

Sensor data analytics and, in general, big data technologies, are changing the provision of insurance and other financial services as new sources of data, alternative data, can be taken into account for risk scoring, pricing and for the provision of tailor-made products.

The lack of security standardization in the Internet of Things (IoT) and sensor data analytics is an example of a real challenge we are seeing nowadays and on which the EC and other regulators are beginning to be concerned. IoT manufacturers should increase security measures to protect data. There is also a lack of consensus on the security standards to be used among manufacturers or among countries like China, USA and Europe.[101]

Organizations in the industry also use fewer processes to analyse compromised systems, eliminate the causes of security incidents, and restore affected systems. The lack of security maturity, limited funds, and the low priority placed on security may be major factors for this trend. [102]

Healthcare Sector

Mobile medical applications or wearable devices allow patient data to be collected. Health events can be captured or monitored and data connected to a private or public cloud. However, as more healthcare devices become network-aware, it becomes challenging for IoT companies to agree on common interoperability protocols and standards for sharing and protecting data, and for the hardware sensors that collect that data.

Many implantable medical devices have already wireless capabilities. Patients and care providers are becoming more and more security aware. Lack of standardization have triggered concerns and raised questions whether products fulfills safety and security standards like the ISO80001. The once seemingly futuristic exploit of implanted medical devices has been made present with the demonstration of successful attacks against devices such as the insulin pump and pacemakers. Research from the Archimedes, Ann Arbor Research Center for Medical Device Security at the University of Michigan has demonstrated the potential compromise to implanted devices. The lack of device embedded security controls is of greater concern than the incidents they result in. Research has demonstrated that issues such as web interfaces to infusion pumps, default hard coded administration passwords, access to the Internet through devices connected to internal networks, are just a few of the common vulnerabilities found in devices used in the hospital environment. Embedded web services, with unauthenticated and unencrypted communication are one of the biggest vulnerabilities, as an attacker can potentially affect these devices remotely from anywhere in the world.[103]

Security experts compare **the lack of standards to the wild days of the web of the '90s**. Today competing standards, vendor lock-in, proprietary devices and private networks make it hard for devices to share a common security protocol.

To that end, healthcare is a microcosm of the larger security challenges that face IoT. A lack of loyalty to one IoT common standard for connected devices in other business environments is one of a number of barriers that is holding back mass adoption broad IoT security protection, say security experts.

Gartner argues it's the sheer number of IoT use cases that contribute to a wildly divergent number of approaches to solve IoT problems, which creates interoperability challenges and, ultimately, security gaps[104].

Recognition of the increasing vulnerability of medical networks, as well as medical devices connected to these networks, is reflected in the revisions to the international standard International Organization for

[100] https://tokenex.com/fintech-solving-problems-finance-introducing-risk-part-2-3/
[101] http://www.ebf.eu/wp-content/uploads/2017/06/EBF_026943-Fintech-consultation_EBF-response_15.06.2017.pdf
[102] http://www.cisco.com/c/dam/assets/docs/transportation-security.pdf
[103] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/
[104] https://www.nsslabs.com/company/news/media-resources/iot-insecurity-pinpointing-the-problems/

Standardization (ISO)/IEC 27000-series "Information security management systems" and ISO/IEC 80001 "Application of risk management for IT networks incorporating medical devices". However, consideration of the threat to the devices themselves and subsequently the resulting patient safety concerns are of greater concern when the connections are to wireless networks.

What complicates the security risks with medical devices is that these devices expose both data/information and potentially the control of the device itself. In addition, the cybersecurity discipline tends to take a risk approach to any problem. Traditionally security has been viewed as a technological solution space, and subsequently the change in the operating environment driven by technology such as wireless, has been focused on controlling the risk with technology. This perspective has gradually altered over time with acknowledgment that those practical security solutions in health care need to take a socio-technical approach. Further, for practical security solutions to be effective, research shows that they must, at the very least, consider clinical workflow, if not seamless integration with this workflow.

While there are a number of international standards that are pre-requisites for the certification of medical devices, these are limited to the development and design risk assessment process. **These standards do not focus on the specificity required for cybersecurity within the complex deployment setting**. However, since many security flaws and subsequent vulnerabilities are a consequence of poor software design, which may include medical device software.[105]

Considering the very sensitive nature of health data and the vulnerability and easy dissemination of information on electronic format, special attention should be paid to the security of data from EHRs. The Study[106] shows, however, that half of the countries covered have not set specific rules for institutions hosting and managing EHRs, relying instead on the general rules setting security requirements for all types of data controllers. In addition, almost all the countries covered have not gone beyond Directive 95/46/EC in what relates to authorisation requirements. The authorization procedure to host and process EHRs is, in the vast majority of countries, the same as to host and process other data. Also, only a minority of the countries has set specific auditing requirements for institutions hosting and managing EHRs.

A binding European legal framework on basic user and access management that should also include operational rules on other security aspects such as end-to-end encryption (currently not possible because of the lack of a common encryption standard) and audit trails (who will be in charge of recovering data events in case of an incident) should be adopted. Agreement is also recommended on a model service level agreement for cloud services with regard to EHRs. The eHealth Network should closely follow up the progress made in this context and stimulate the development of European model provisions for cloud SLAs dedicated for eHealth services and EHRs in particular.

Belgium has developed and uses a standard for the exchange of minimal medical transaction information, called SumEHR. The SumEHR standard was introduced in 2005 and an EHR software package used by a physician should be capable of exporting a SumEHR message for any given patient. Currently more than 80% of all GPs across Belgium use certified EHR systems with this capability. In Slovakia, health care providers are required to use certified information systems which comply with connectivity and security standards, as well as with rules on identification and authentication of health professionals. In Italy, the draft implementing decree and an annex thereto lay down specific provisions on interoperability.

[105] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/
[106] http://ec.europa.eu/health//sites/health/files/ehealth/docs/laws_report_recommendations_en.pdf

7.13 Economics of Standards

Lack of mutual recognition in cybersecurity certification can be equated to an absence of common technical standards; by the same token having common certification criteria for cybersecurity in EU28 would amount to introducing new technical standards. The economics of standardisation in general[107], and of ICT standards in particular[108], show that technical standards have positive impacts on R&D and on economic growth. ICT standards embed knowledge that becomes accessible to all and firms can invest the resources released from having to go through multiple certification to R&D. ICT standardisation reduce costs (transaction costs and cost reduction), improve competition (using standards to organize markets) or communication and coordination (organizing the development of technology around agreed technical specifications) and in the long run creates selection efficiencies by pruning the tree of available technical solutions for any given problem and channelling R&D efforts in the most efficient directions. Not surprisingly, as mentioned in the SWD "A Single Market Strategy for Europe - Analysis and Evidence"[109] a large body of economic studies that show the impact that standards have on economic growth and GDP For France the impact on growth is estimated at 0.8 %, for United Kingdom at 0.3 % and for Germany at 0.9 % of GDP. Furthermore, an economic paper by economists of DG ECFIN estimated that the cost associated to differences in technical rules and multiple testing/certification are between 2% to 10% of companies' annual turnover[110]. According to this paper inadequate standards and insufficient mutual recognition, including in the ICT sector, is among the main barriers to the single market. The costs for enterprises of product conformity assessment can be substantial and we there is lack of mutual recognition this implies the multiplication of such costs: for companies offering several product types on a national market of a receiving Member State the costs amount to approximately 2% of their entire annual turnover on that market, whereas they can reach up to 10% for companies specialised in one specific product type because they do not benefit from economies of scale[111]. Even applying the lower bound of 2% only to 60% of the cyber security market to be conservative (i.e. assuming 40% of the market concerns products for which certification is no require) the costs of lack of mutual recognition reach a figure in the range of 1.2 billion euro.

[107] Among peer-reviewed journal articles see: Acemoglu, D., G. Gancia and F. Zilibotti (2012), 'Competing Engines of Growth: Innovation and Standardization,' Journal of Economic Theory, 147, 570–601;Blind, K. and A. Jungmittag (2008), 'The Impact of Patents and Standards on Macroeconomic Growth: A Panel Approach Covering Four Countries and 12 Sectors,' Journal of Productivity Analysis, 29, 51–60; Jungmittag, A., K. Blind and H. Grupp (1999), 'Innovation, Standardisation and the Long-term Production Function,' Zeitschrift für Wirtschafts- und Sozialwissenschaften, 119, 205–222; Wakke, P., Blind, K.; Ramel, F. (2016): The impact of participation within formal standardization on firm performance, Journal of Productivity Analysis 45 (Issue 3), 317–330; Wijen, F.H. (2014). Means versus ends in opaque institutional fields: Trading off compliance and achievement in sustainability standard adoption. Academy of Management Review, 39 (3), 302-323.Swann, P. (2010), International Standards and Trade: A Review of the Empirical Literature. Report for the UK Department of Business, Innovation and Skills (BIS). OECD Trade Policy Working Papers. Among reports commissioned by standardization bodies see: SCC (2007). Economic Value of standardisation; AFNOR (2009). The Economic Impact of standardisation; DIN (2011). The Economic Benefits of standardisation; Standards Australia (2012). The Economic Benefits of standardisation; Cebr (2015). The Economic Contribution of standards to the UK Economy; Cebr (2016). Economic Contribution of Standards in Ireland – A report for the National Standards Authority of Ireland.

[108] Blind, K., Gauch, S. and Hawkins, R. (2010), 'How stakeholders view the impacts of international ICT standards', Telecommunications Policy, Elsevier, vol. 34(3)

[109] Brussels, 8.10.2015 SWD (2015) 202 final, accompanying the document Upgrading the Single Market: more opportunities for people and business (COM (2015) 550 final) {SWD(2015) 203 final}).

[110] Ilzkovitz, F. Dierx, A. Kovacs, V. & Sousa (2007) Steps towards a deeper economic integration: the internal market in the 21st century", European Economy, Economic Papers, No. 271. European Commission.

[111] *Ibid.* p. 61

7.14 References

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.

Akerlof, G. (1970). The Market for Lemons: Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics, 84*(3), 488-500.

ANSSI. (2015). Introduction A La Certification De La Sécurité Des Technologies De L'information Paris: Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI).

ANSSI, & BSI. (2017). Towards a European certification scheme: Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI) & German Federal Office for Information Security (BSI).

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

Business Insider. (2017). The Internet of Things 2017 Report.

Codagnone, C., Bogliacino, F., & Veltri, G. (2013). Testing CO2/Car labelling options and consumer information. Final Report. Brussels: European Commission (available at: http://ec.europa.eu/clima/policies/transport/vehicles/labelling/docs/report_car_labelling_en.pdf).

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.

CSIS. (2014). Net Losses: Estimating the Global Cost of Cybercrime. Washington, D.C.: Center for Strategic and International Study (CSIS).

Dusart Pierre, Sauveron Damien, Tai-Hoon Kim, Some limits of Common Criteria certification, International Journal of Security and Its Applications

DIGITALEUROPE. (2017). DIGITALEUROPE'S views on Cybersecurity Certification and Labelling Schemes. Brussels: DIGITALEUROPE.

ECORYS. (2011). Security Regulation, Conformity Assessment & Certification. Brussels: Report delivered by ECORYS for the European Commission.

Enisa. (2014). Smart grid security certification in Europe. Challenges and recommendations: European Union Agency for Network and Information Security (ENISA).

Enisa. (2016a). Results of ENISA workshop on a common European ICT product security certification framework (February 2016): European Union Agency for Network and Information Security (ENISA).

Enisa. (2016b). A European ICT Security Certification Framework - Workshop Summary (17 October 2016): European Union Agency for Network and Information Security (ENISA).

ERNCIP. (2014). Proposals from the ERNCIP Thematic Group, "Case Studies for the Cyber-security of Industrial Automation and Control Systems", for a European IACS Components Cyber-security Compliance and Certification Scheme.

European Commission. (2006). Labelling: competitiveness, consumer information and better regulation for the EU. Brussels: DG Sanco, European Commission.

European Commission. (2009). Impact Assessment Guidelines. SEC(2009) 92, Brussels: European Commission, available at: http://ec.europa.eu/governance/impact/commission_guidelines/docs/iag_2009_en.pdf.

European Commission. (2012a). Security Industrial Policy. COM(2012) 417 final, Brussels: European Commission.

European Commission. (2012b). Commission Staff Working Document Accompanying the Communication on Security Industrial Policy. SWD(2012) 233 final, Brussels: European Commission.

European Commission. (2015a). Commission Staff Working Document, Better Regulation Guidelines. Brussels, COM(2015) 215 final, SWD (2015) 110 final.

European Commission. (2015b). A Digital Single Market Strategy for Europe. COM(2015) 192 final, Brussels: European Commission.

European Commission. (2016a). Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry. COM(2016) 410 final, Brussels: European Commission.

European Commission. (2016b). Staff Working Document. Contractual Public Private Partnership on Cybersecurity & Accompanying Measures. SWD(2016) 216 final, Brussels: European Commission.

European Commission. (2016c). Staff Working Document. Report on the public consultation and other consultation activities of the European Commission for the preparation of the EU Cybersecurity contractual Public-Private Partnership and Accompanying Measures. SWD(2016) 215 final, Brussels: European Commission.

European Commission. (2016d). Commission Decision on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation. C(2016) 4400 final, Brussels: European Commission.

European Commission, SWD(2016) 216 final, Communication: Strenghtening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry

European Commission. (2017). Building a European Data Economy. COM(2017) 9 final, Brussels: European Commission.

Friedman, C. (2015). Cybersecurity workforce shortage: Millions of experts needed, http://www.ksat.com/news/cybersecurity-workforce-shortage-millions-of-experts-needed.

Hunstad, A.; Hallberg, J.; Andersson, R., "Measuring IT security - a method based on common criteria's security functional requirements," Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC, pp. 226-233, 10-11 June 2004, URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1437821&isnumber=30958

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

Ilzkovitz, F., Dierx,A., Kovacs, V., & Sousa,N. (2007). Steps towards a deeper economic integration: the internal market in the 21st century. Brussels: . European Commission, European Economy, Economic Papers, No. 271.

ISACA. (2015). 2015 Global Cybersecurity Status Report: ISACA.

Lunn, P. (2015). Are Consumer Decision-Making Phenomena a Fourth Market Failure? *Journal of Consumer Policy, 38*(3), 315-331. doi: 10.1007/s10603-014-9281-1

OECD. (2013). Exploring Data-Driven Innovation as a New Source of Growth. Paris: OECD.

OECD. (2015). OECD Digital Economy Outlook 2015. Paris: OECD.

NIST. (2010). Guide for Applying the Risk Management Framework to Federal Information Systems. Washington DC: National Institute of Standards and Technology (NIST), US Department of Commerce

Norton. (2016). Cyber Security Insights Report: Symantec.

Optimity Advisors. (2015). Study on Synergies between the civilian and the defence cybersecurity markets Brussels: Report delivered by Optimity Advisors for the European Commission.

PwC. (2015). Cyber Security M&A Decoding deals in the global Cyber Security Industry: https://www.pwc.com/gx/en/aerospace-defence/pdf/cyber-security-mergers-acquisitions.pdf.

Schierholz, R., & McGrath, K. (2010). *Security Certification – A critical review*. ABB by DHS.

Symantec. (2017). Internet Security Threat Report: Volume 22, Symantec.

Thales, P. (2016). Introduction to the European IACS components Cybersecurity Certification Framework (ICCF). JRC Science for Policy Report. Luxembourg: Publications Office of the European Union.

Yeung, K. (2017). 'Hypernudge': Big Data as a mode of regulation by design. *Information, Communication & Society, 20*(1), 118-136. doi: 10.1080/1369118X.2016.1186713

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