Considerations on ICT security certification in EU

Survey Report

FINAL

AUGUST 2017

www.enisa.europa.eu

European Union Agency For Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use isdp@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN: 978-92-9204-225-7, DOI: 10.2824/090677

Table of Contents

Executive Summary

Quite often implementing European legislative initiatives relies on the availability of trustworthy information technology which means that the technology options used must be duly scrutinised and standardised prior to being put in good use.Over the last years, ENISA has engaged in a number of activities in pursuit of supporting the Commission and the Member States in identifying a way forward on the certification of ICT security products and services, which on the one hand seeks to boost competition and on the other to promote mutual recognition or harmonisation of certification practices up to a certain level. This online EU-wide survey on the topic of ICT Security Certification has been singled out as a suitable instrument to consult with stakeholders and seek structured feedback against the currently envisaged policy options. On the background, in April 2017 the Commission presented a set of tentative policy approaches as follows:

- Option 0 - Do nothing: No EU policy initiative or action – baseline scenario
- Option 1 - Soft law approach: Commission to encourage and support national or industry initiatives
- Option 2 - Extension of SOGIS agreement: Legislative proposal making MS participation to the SOG-IS agreement mandatory
- Option 3 - European certification framework: EU-wide framework with its own scope, functioning and governance rules

This survey has been broadly publicised, albeit within the confined boundaries of the certification stakeholders' community, along with a number of prospective respondents from competent Member State agencies, vendors, manufacturers and consumer associations that were all invited to participate. The survey was structured across five main thematic pillars, namely i) current situation and open issues, ii) future evolution, iii) sectors and technologies, iv) policy options and envisioned features and v) roles and competencies for the policy stakeholders.

Survey respondents reflected and responded on the need to design and deploy ICT security certification at the EU level as the current ICT security certification landscape incommodes mutual recognition across Member States. The aspects of costs, duration, transparency and support during the lifecycle of a product's certification were also highlighted as present barriers featured in the current landscape, along with different security baselines and levels of assurance concerning the criticality or the impact of each sector, such as Internet of Things and Industrial Control Systems. To meet the expectation of reducing internal market fragmentation and improving trust in the security of ICT products and services in the EU, the respondents were mostly in favour of a general European certification general framework.

Following the analysis of the responses it has become clear that there is no one-size-fits-all approach to certification and labelling. The respondents agreed that the processes and tools used for security certification should be improved to ensure the required flexibility to adapt to different market situations, particularly by allowing different level of assurances according to market needs. For high assurance sectors SOG-IS MRA was perceived as a suitable paradigm to build upon and create a platform to consult further among participants while for lower assurance sectors, self-certification could complement the overall framework.

Overall, any procedures implemented need to mitigate risk and allow for forthcoming technologies to take root in the EU ; the prevailing approach should be supported by an adequate amount of resources, in order to ensure appropriate coordination and support, at the level of EU Institutions and Bodies, notably at the level of the EUROPEAN Commission with support from an EU Agency such as ENISA.

1. Background

Trustworthiness and security of information technology products can be enhanced by putting in place a certification framework. In the EU, a common scheme would support the recognition of security certification across Member States, an essential pillar towards achieving trust and security required to promote the Digital Single Market. The European Commission, has emphasized on the need to develop a proposal for a European ICT security certification framework as stated in Commissions' COM(2016) 410[1].

ENISA, within the scope of its Programming Document 2017-2019[2], has continued supporting the European Commission and the Member States in their efforts to identify a way forward on ICT security products certification, which on one hand seeks to boost competition and on the other to promote mutual recognition or harmonisation of certification practices up to a certain level. The Agency, has engaged in a number of activities in pursuit of this goal. This online EU-wide survey on the topic of ICT Security Certification has been deemed being a suitable instrument to consult with stakeholders and seek structured feedback against set policy options. On the background, in April 2017[3] the Commission presented a set of tentative policy approaches as follows:

- Option 0 - Do nothing: No EU policy initiative or action – baseline scenario
- Option 1 - Soft law approach: Commission to encourage and support national or industry initiatives
- Option 2 - Extension of SOGIS agreement: Legislative proposal making MS participation to the SOG-IS agreement mandatory
- Option 3 - European certification framework: EU-wide framework with its own scope, functioning and governance rules

These four options have been reflected in the survey.

With this survey ENISA and the European Commission have aimed to actively consult with industry representatives and experts from Member States on the subject-matter area, complementing the outcomes and findings of studies and consultation workshops organized. This survey serves the purpose of consulting with stakeholders to come up with an approach that serves the interests of the bulk of stakeholders across the EU.

While quantitative research aims to quantifying attitudes, opinions or other defined variables in order to generalize input from a sample population, while qualitative research is focused on explaining the reasons, the opinions, and the options ofa sample population 's behavior. This report relies on a combination of both research strategies was followed and a self-completion questionnaire was used to support the survey outcomes.

The survey comprises 14 closed questions, the majority of which are based on multiple choice questions; the participants were also asked to provide comments and feedback in relation to ICT security certification on open-ended subquestions. This survey was carried outin Q2 2017.

[1] https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-410-EN-F1-1.PDF
[2] https://www.enisa.europa.eu/publications/corporate/enisa-programming-document-2017-2019
[3] https://www.enisa.europa.eu/events/ict-security-certification-april-2017/workshop-on-a-european-ict-security-certification-framework

2. Analysis of results

This survey has been broadly publicised, albeit within the boundaries of the certification stakeholders' community, and a number of prospective respondents was invited to join and respond; specifically invitations to respond were sent to 28 agencies from Member States, 24 vendors and manufacturers from the private sector, and 4 consumer associations.

The questions presented to the respondents are available under Annex A. To facilitate the presentation of the results the survey questions have been grouped across five thematic areas, namely:

- Current Situation and open issues are covered by questions 2, 3 and 4
- Future evolution are covered by questions 5 and 6
- Sectors and technologies are covered by questions 7 and 8
- Policy Options and envisioned features are covered by questions 9 through to 13
- Roles and competencies for the policy stakeholders are covered by question 14

The full set of questions can be found in Annex A and the question with the responses given in Annex B. In total 33 participants provided full responses; the following tables display the survey results that derived from the number of responses collected for each answer option per question. A concise overview of the respondents' composition is presented hereinafter:

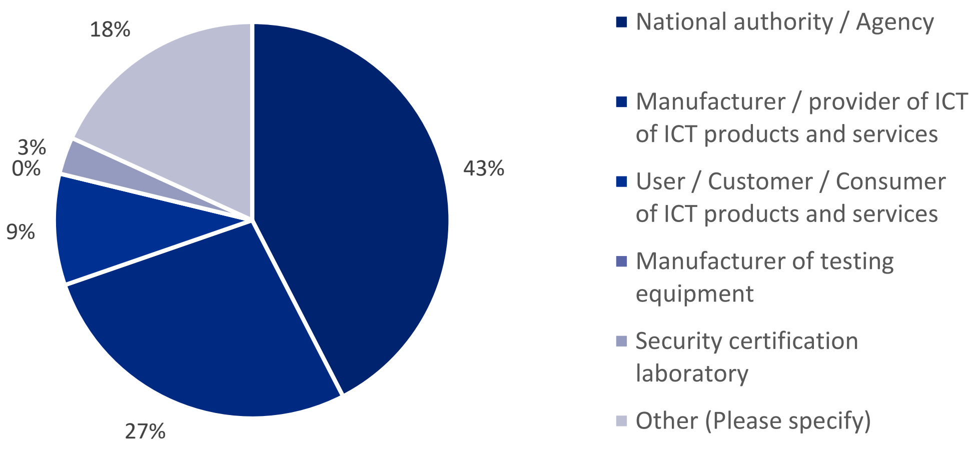

Figure 1: Respondents' composition

TYPE OF ORGANISATION	RESPONSES
National authority / Agency	14
Manufacturer / provider of ICT of ICT products (both hardware and software) and services	9
User / Customer / Consumer of ICT products (both hardware and software) and services	3
Manufacturer of testing equipment	0
Security certification laboratory	1
Other (Please specify)	6

Table 1: Type of organisation

2.1 Current Situation in ICT Security Certification

All survey participants agreed on the need to design and deploy ICT security certification, although some suggested that it should be limited to the Member States' or to the industry sectorial level concerned. All respondents agreed on the need to leverage on certification to mitigate cybersecurity risks. The majority of the participants (57,5%) is aware of multiple existing ICT security certification schemes across EU Member States for the same product or service and they provided examples thereto.

AWARENESS OF THE EXISTENCE OF MULTIPLE ICT SECURITY CERTIFICATION SCHEMES ACROSS EU MEMBER STATES FOR THE SAME PRODUCT/SERVICE	RESPONSES
Yes	19
No	12
Don't know	2

Table 2: Multiple ICT security certification schemes across EU Member States for the same product/service

Some of the examples provided by the respondents include the following:

- National ICT Security Certification Schemes,
- SOG-IS MRA
- Certification against International Standards
- Sector specific certification schemes
- Market driven certification schemes

A smaller percentage (36,3%) of the respondents suggest that they were not aware of multiple ICT security schemes across EU, but they expressed their preparedness to accept one; at least, the survey reveals, these respondents have acknowledged the need to have ICT security certification schemes at large.

Examples provided by the respondents include:

- Privacy and Personal Data protection

- IoT
- Industrial Control Systems
- Telecom,
- Health
- Aerospace
- Cloud security
- ICT products and services

When dealing with ICT security certification procedures, the respondents indicated that the main problems they encounter are the following:

- Costs (mentioned by 72,7% of respondents)
- Duration of the process (supported by 57,5% of respondents)
- Lack of mutual recognition of certificates across Member States (supported by 51,5% of respondents)
- Lack of a dedicated scheme to cyber -certify a specific product/service (supported by 45,4% of respondents)
- Lack of certification support for the lifecycle of the product (e.g., incremental certification for software and hardware changes/updates) (supported by 39,3% of respondents)
- Lack of transparency in the certification process (supported by 36,3% of respondents)

PROBLEMS WHEN DEALING WITH ICT SECURITY CERTIFICATION PROCEDURES	TOTAL RESPONSES
Lack of mutual recognition of certificates across Member States	17
Cost	24
Duration of the process	19
Lack of transparency	12
Lack of a dedicated scheme to cyber-certify a specific product/service	15
Lack of certification support for the lifecycle of the product	13

Table 3 : Problems when dealing with ICT security certification procedures

2.2 Future Evolution of ICT security certification across EU

Almost all respondents, 90,9%, agreed that mutual recognition of ICT security certification schemes is desirable at European level. There was 81,8% of the respondents who agreed also that certification and labelling can be effective tools to increase transparency about the level of security assurances of ICT products/services, and enhance trust across the Digital Single Market. However, it was noted that a ranking of assurance levels with clear information is required as oversimplifying could introduce additional risks. In addition, certification and labelling should denote only baseline security requirements and should not deferment innovation or increase complexity.

NEED FOR A MUTUAL ICT SECURITY RECOGNITION MECHANISM OF CERTIFICATES ACROSS ALL MS	RESPONSES
The current situation is satisfactory	1
Mutual recognition is desirable at European level	30
The current situation is satisfactory; mutual recognition is desirable at European level	2
Don't know	0

Table 4 : Need for a mutual ICT recognition mechanism of certificates across all Member Statess

CERTIFICATION AND LABELLING CAN BE EFFECTIVE TOOLS TO INCREASE TRANSPARENCY ABOUT THE LEVEL OF SECURITY ASSURANCES OF ICT PRODUCTS/SERVICES, AND ENHANCE TRUST ACROSS THE DIGITAL SINGLE MARKET.	RESPONSES
Agree	27
Disagree	6
Don’t know	0

Table 5 : Certification and labeling ars effective tools to increase transparency

The need for greater efforts to promote ICT security certification was highlighted by 66,6% of the respondents who made specific reference to industry sectors while 21,2% stated that ICT security certification is a pure market issue and there is no need for additional support.

RECOURSES TO CERTIFICATION AND LABELLING IN THE ICT SECTOR ARE SUFFICIENTLY WIDESPREAD OR GREATER EFFORT IS NEEDED TO PROMOTE ICT SECURITY CERTIFICATION IN SPECIFIC SECTORS	RESPONSES
This is a pure market issue and there is no need for additional support	7
No, greater efforts are required in specific sector	22
Don’t know	4

Table 6: Promotion of ICT security certification in specific sectors

2.3 Sectors and Technologies

The majority of the respondents (75,7%) identified the need for ICT security and labelling in the Internet of Things-domain, due to the imminent ubiquity of IoT, issues of vulnerabilities and the required interoperability across different platforms.

NEED FOR ICT SECURITY CERTIFICATION AND LABELLING IN THE INTERNET OF THINGS DOMAIN	RESPONSES
Yes	25
No	6
Don't know	2

Table 7: Need for ICT security and labelling in the Internet of Things domain

Similarly, 66,6% of the respondents, identified the need for ICT security certification in the Industrial Control System (ICS)-domain, due to the criticality of processes they support and the level of cyber threats they are exposed to.

NEED FOR ICT SECURITY CERTIFICATION IN THE INDUSTRIAL CONTROL SYSTEM (ICS)-DOMAIN	RESPONSES
Yes	22
No	7
Don't know	4

Table 8: Need for ICT security and labelling in the Industrial Control System (ICS) domain

2.4 Policy Options and Envisioned Features

To reach the objective of reducing internal market fragmentation and improving trust in the security of ICT products and services in the EU, 33,3% of the respondents opted for creating a European certification general framework, laying down the essential rules for mutual recognition of certificates issued in accordance with the framework. The "Soft law approach", encouraging, supporting and to the extent possible coordinating the adoption and use of certification initiatives at European level was supported only by 18,1% while 12,1% of the respondents were in favour of extending the SOG-IS MRA to all Member States and make it mandatory. Lastly, 12,1% opted for regulating the security of I CT products and services and specify essential security requirements for such products to be placed on the market. The remaining respondents indicated that a mixed approach, from all the aforementioned options, should be the preferred path of action instead. They argued that mutual recognition of existing certification schemes and labelling programs can promote a robust Digital Single Market and support EU digital economy while an entirely new certification framework would not scale with the dynamicsecurity landscape.

ACTIONS FOR REDUCING INTERNAL MARKET FRAGMENTATION AND IMPROVING TRUST IN THE SECURITY OF ICT PRODUCTS AND SERVICES IN THE EU	RESPONSES

"Soft law approach", encouraging, supporting and to the extent possible coordinating the adoption and use of certification initiatives at European level	6
Extending the SOG-IS MRA to all Member States: legislative proposal making MS participation to the SOGIS agreement mandatory	4
Creating a European certification general framework, laying down the essential rules for mutual recognition of certificates issued in accordance with the framework	11
Regulating the security of ICT products and services, specifying essential security requirements for such products to be placed on the market	4
None of the above	8

Table 9: Possible options for reducing internal market fragmentation and improving trust

In all, 45,4% of the respondents were in favour of exploiting the current SOG-IS MRA as the basis to build an EU-wide certification framework, while 21,2% stated otherwise and 33,3% did not answer either positive or negative on the role of SOG-IS MRA.

SOG-IS MRA COULD BE A BASIS TO BUILD AN EU-WIDE CERTIFICATION FRAMEWORK	RESPONSES
Yes	15
No	7
Don’t know	11

Table 10: SOG-IS MRA role within an EU-wide certification framework

On self-certification schemes, 66,6% of the respondents agreed that these schemes could present a viable option to boost the level of cyber-security for selected product’ domains, especially for low assurance level products and should be considered as an integral part of the future EU certification framework, drawing also experience from existing market driven initiatives. Nevertheless, 24,2% of the respondents disagree that self-certification should be considered, as it does not provide for any assurance, there is no control and it is not sufficient unless there is a third party validating conformance.

SELF-CERTIFICATION SCHEMES COULD BE CONSIDERED A VIABLE OPTION TO BOOST THE LEVEL OF CYBER-SECURITY FOR SELECTED PRODUCT’ DOMAINS	RESPONSES
Yes	22
No	8
Don’t know	3

Table 11: Self-certification schemes

The overwhelming majority of the respondents, i.e. 90,9%, indicated that the processes and tools used for security certification should be improved to ensure the required flexibility by allowing different level of assurance.

PROCESSES AND TOOLS USED FOR SECURITY CERTIFICATION SHOULD BE IMPROVED TO ENSURE THE REQUIRED FLEXIBILITY TO ADAPT TO DIFFERENT MARKET SITUATIONS, PARTICULARLY BY ALLOWING DIFFERENT LEVEL OF ASSURANCES ACCORDING TO MARKET NEEDS	RESPONSES
Yes	30
No	1
Don’t know	2

Table 12: Flexibility to allow different assurance levels

Introducing a common label across the EU was accepted by 66,6% of the respondents. Such a label would indicate that the products have been certified within a certification scheme in accordance with EU rules and provide visual notice that product’s features comply with specific requirements. Nevertheless, the respondents who were not in favour of a common label, proposed a specific sectoral labelling (e.g. SOGIS) or consider that it could be difficult for complex systems and/or it could also result in a false sense of security.

INTRODUCTION OF A COMMON LABEL SIGNALLING CERTIFIED PRODUCTS	RESPONSES
Yes	22
No	8
Don’t know	3

Table 13: Introduction of a common label signalling certified products

2.5 Roles and Competencies of Policy Stakeholders

The majority of the respondents, 78,7%, envisage a role for existing European Commission bodies and agencies (e.g. JRC, ENISA, ACER) in a possible future EU certification and labelling security framework. Among the respondents who did not see a role for existing EU Commission's bodies and agencies, supporting actions such as determining a minimum level of security per category of technology, issuing voluntary guidelines for both industry and consumers, were envisioned, without identifying key EU bodies or agencies.

ACTIVE ROLES FOR EXISTING EU COMMISSION'S BODIES AND AGENCIES (E.G. JRC, ENISA, ACER) IN A POSSIBLE FUTURE CERTIFICATION AND LABELLING FRAMEWORK.	RESPONSES
Yes	26

No	4
Don’t know	3

Table 14: Roles and Competencies for existing EU Commission's bodies and agencies

Respondents envisaging a role for existing EU Commission's bodies and agencies indicated that:

- A central organization at EU level is needed to warrant that a robust system is in place with defined rules, references and tools. Such a referencecentral organization could also induce recognition by Member States.
- CEN/CENELEC should be involved in a future scheme with the contribution of ENISA to support technical, organisational and stakeholders’ management tasks.
- EU agencies, with respective competences such as ACER and ENISA, could participate in the development of guidelines, criteria, etc., to be applied in a certification and labelling system, and promote its adoption across various stakeholders.
- JRC and ENISA could serve as a monitoring body to guarantee compliance with the proposed way forward. ENISA could mandate expert groups with the definition of flexible certification approaches in respective sectors.
- EU bodies could provide administrative support while supporting definition of the scheme, interacting with EU standardization bodies.

3. Conclusions

ICT security certification plays an important role in increasing trust and security in products and services and all survey participants reflected on the necessity to design and deploy ICT security certification at a European Level. This broad consensus was also prevalent in the consultation workshops organized by ENISA and the Europen Commission during 2016 as ICT security certification has been regarded as one of the means to enhance trust across the digital single market. This survey confirms that doing nothing is no policy option for the EU; pro-activity at the policy level is favoured by respondents who see the European Commisison as a driver for change and a greater role of the EU in the area of certification of products meets stakeholder's expectations.

Currently, the ICT security certification landscape comprises of SOG-IS MRA, national and sectorial schemes along to internal standards, which incommodes a wide-ranging recognition of certificates across Member States. Respondents also highlighted the aspects of costs, duration, transparency and support during the lifecycle as existing barriers to current setting while highlighting that depending on the criticality or the impact of each sector, such as Internet of Things and Industrial Control Systems, more attentive efforts are needed.

To meet the expectation of reducing internal market fragmentation and improving trust in the security of ICT products and services in the EU, the respondents were mostly in favour of creating a European certification general framework. Notably a number of respondents were also in favour of extending the SOG-IS MRA to all Member States or encouraging, and supporting the adoption and use of certification initiatives at European level.

The respondents agreed that the processes and tools used for security certification should be improved to ensure the required flexibility to adapt to different market situations, particularly by allowing different level of assurances according to market needs. There is no one-size-fits-all approach to certification and a scheme based on labelling, and flexibility is likely to be more permitting of greater transparency in this area. Any certification scheme needs to appropriately mitigate risk and be commercially oriented to allow for market forces shape benefit from forthcoming technologies i.e. the security for a handset used for emergency services should be at a higher standard than consumer devices, and therefore at a higher cost. For high assurance sectors SOG-IS MRA was perceived as a suitable framework to build upon and set up a framework to consult further among participants while for lower assurance sectors, self-certification could complement the overall framework.

Lastly, respondents underlined the importance to allocate adequate resources in order to ensure due maintenance of such a framework while coordination and support roles were suggested or existing EU Institutions and Bodies, including the European Commission and an agency like ENISA.

Annex A: Questionnaire Responses

Q.1 TYPE OF ORGANISATION:	RESPONSES
National authority / Agency	14
Manufacturer / provider of ICT of ICT products (both hardware and software) and services	9
User / Customer / Consumer of ICT products (both hardware and software) and services	3
Manufacturer of testing equipment	0
Security certification laboratory	1
Other (Please specify)[4]	6

Q.2 ARE YOU AWARE OF THE EXISTENCE OF MULTIPLE ICT SECURITY CERTIFICATION SCHEMES ACROSS EU MEMBER STATES FOR THE SAME PRODUCT/SERVICE?	RESPONSES
Yes (Please answer question 2a)	19
No (Please answer question 2b)	12
Don't know	2

Q.2A IF YES, PLEASE ADD FURTHER DETAILS CONCERNING PRODUCT/SCHEME/COUNTRY/MANDATORY-VOLUNTARY NATURE, ETC.:	RESPONSES

Q.2B IF NOT, 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?	RESPONSES
Yes (please answer question 2c)	12
No	2
Don't know	2

[4] While most respondents did not splify their background some of the respondents, according to information they submitted themselves, include the following: an ISO/IEC17065 accredited body, a National standardization body, CERT.LV, Eurosmart, ZVEI, DIGITALEUROPE, Manufacturer IACS equipment and software, NXP Semiconductors.

Q.2C IF YES, PLEASE ADD DETAIL ON TYPE OF PRODUCT/SERVICE/SECTOR.	RESPONSES

Q.3 HAVE YOU ENCOUNTERED ANY OF THE FOLLOWING PROBLEMS WHEN DEALING WITH ICT SECURITY CERTIFICATION PROCEDURES? PLEASE THICK BOX(ES) AS APPROPRIATE (MORE CHOICES POSSIBLE):	TOTAL RESPONSES
Lack of mutual recognition of certificates across Member States	17
Cost	24
Duration of the process	19
Lack of transparency	12
Lack of a dedicated scheme to cyber-certify a specific product/service	15
Lack of certification support for the lifecycle of the product (e.g., incremental certification for software and hardware changes/updates)	13

Q.4 CURRENTLY, THERE IS NO EU-WIDE ICT CERTIFICATION FRAMEWORK ALLOWING FOR MUTUAL/CROSS RECOGNITION OF NATIONAL SCHEMES. DO YOU SEE THE NEED FOR A MUTUAL RECOGNITION MECHANISM OF CERTIFICATES ACROSS ALL MS? PLEASE THICK BOX(ES) AS APPROPRIATE (MORE CHOICES POSSIBLE):	RESPONSES
The current situation is satisfactory	1
Mutual recognition is desirable at European level	30
The current situation is satisfactory; mutual recognition is desirable at European level	2
Don't know	0

Q.5 DO YOU THINK THAT CERTIFICATION AND LABELLING CAN BE EFFECTIVE TOOLS TO INCREASE TRANSPARENCY ABOUT THE LEVEL OF SECURITY ASSURANCES OF ICT PRODUCTS/SERVICES, AND ENHANCE TRUST ACROSS THE DIGITAL SINGLE MARKET?	RESPONSES
Yes	27
No	6
Don't know	0

Q.6 DO YOU CONSIDER THAT RECOURSE TO CERTIFICATION AND LABELLING IN THE ICT SECTOR ARE SUFFICIENTLY WIDESPREAD OR RATHER THAT IT SHOULD BE FURTHER ENCOURAGED OR SUPPORTED? DO YOU BELIEVE THAT GREATER EFFORT TO PROMOTE ICT SECURITY CERTIFICATION IS NEEDED IN SPECIFIC SECTORS?	RESPONSES
This is a pure market issue and there is no need for additional support	7
No, greater efforts are required in specific sector	22
Don't know	4

Q.7 DO YOU SEE A SPECIFIC ROLE FOR CERTIFICATION AND LABELLING IN THE INTERNET OF THINGS-DOMAIN?	RESPONSES
Yes	25
No	6
Don't know	2

Q.8 DO YOU SEE A SPECIFIC ROLE FOR CERTIFICATION AND LABELLING IN INDUSTRIAL CONTROL SYSTEM (ICS)-DOMAIN?	RESPONSES
Yes	22
No	7
Don't know	4

Q.9 WHICH OF THE FOLLOWING ACTIONS DO YOU CONSIDER APPROPRIATE AND PROPORTIONATE TO ACHIEVE THE OBJECTIVE OF REDUCING INTERNAL MARKET FRAGMENTATION AND IMPROVING TRUST IN THE SECURITY OF ICT PRODUCTS AND SERVICES IN THE EU?	RESPONSES
"Soft law approach", encouraging, supporting and to the extent possible coordinating the adoption and use of certification initiatives at European level	6
Extending the SOG-IS MRA to all Member States: legislative proposal making MS participation to the SOGIS agreement mandatory	4
Creating a European certification general framework, laying down the essential rules for mutual recognition of certificates issued in accordance with the framework	11
Regulating the security of ICT products and services, specifying essential security requirements for such products to be placed on the market	4
None of the above (Please explain)	8

Q10. DO YOU THINK THAT THE CURRENT SOG-IS MRA COULD BE A BASIS TO BUILD AN EU-WIDE CERTIFICATION FRAMEWORK?	RESPONSES
Yes	15
No	7
Don't Know	11

Q.11 DO YOU THINK THAT SELF-CERTIFICATION SCHEMES COULD BE CONSIDERED A VIABLE OPTION TO BOOST THE LEVEL OF CYBER-SECURITY FOR SELECTED PRODUCT' DOMAINS?	RESPONSES
Yes	22
No	8
Don't Know	3

Q.12 DO YOU THINK THAT THE PROCESSES AND TOOLS USED FOR SECURITY CERTIFICATION SHOULD BE IMPROVED TO ENSURE THE REQUIRED FLEXIBILITY TO ADAPT TO DIFFERENT MARKET SITUATIONS, PARTICULARLY BY ALLOWING DIFFERENT LEVEL 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)?	RESPONSES
Yes	30
No	1
Don't Know	2

Q.13 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?	RESPONSES
Yes	22
No	8
Don't Know	3

Q.14 DO YOU SEE A ROLE FOR EXISTING EU COMMISSION'S BODIES AND AGENCIES (E.G. JRC, ENISA, ACER) IN A POSSIBLE FUTURE CERTIFICATION AND LABELLING FRAMEWORK?	RESPONSES
Yes	26
No	4

Q.14 DO YOU SEE A ROLE FOR EXISTING EU COMMISSION'S BODIES AND AGENCIES (E.G. JRC, ENISA, ACER) IN A POSSIBLE FUTURE CERTIFICATION AND LABELLING FRAMEWORK?	RESPONSES
Don’t Know	3

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

TP-01-17-890-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-225-7
DOI: 10.2824/090677