EUROPEAN UNION AGENCY
FOR CYBERSECURITY

PUBLIC CONSULTATION ON THE DRAFT CANDIDATE EUCC SCHEME

Report on Public Consultation

MAY 2021

ABOUT ENISA

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

CONTACT

For contacting the authors please use certification@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHOR

European Union Agency for Cybersecurity (ENISA)

ACKNOWLEDGEMENTS

ENISA thanks the entities and individuals who took part to the public consultation on the first draft candidate cybersecurity certification scheme, the European Common Criteria Scheme (EUCC). ENISA also thanks all experts, groups and other participants that have been providing input and contributing to their best efforts to the design of the EUCC scheme and provided their comments.

More information related to the launch of the Public Consultation on July 2nd, 2020 can be found on this webpage: https://www.enisa.europa.eu/topics/standards/Public-Consultations

LEGAL NOTICE

Notice must be taken that this report is generated by the processing of feedback that was provided by the respondents that participated in the draft candidate EUCC scheme consultation. The results are presented "as is" and reflect a total overview of the opinions and suggestions made by the respondents. The text represents the outcome of the total overview and contains recommendations made by ENISA. The Public Consultation is performed in line with Article 49 (3) of the Regulation (EU) No 2019/881[1], hereinafter referred to as the Cybersecurity Act (CSA).

This publication should not be construed to be a legal action of ENISA or of the ENISA bodies, unless adopted pursuant to the CSA. The document is only reflecting the views and suggestions of the participants that were provided in the Month of July 2020 and therefore does not reflect the opinion of the individual respondents. No rights can or may be derived from this report.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&qid=1599479391322&from=EN

for the use that might be made of the information contained in this document. It must be accessible free of charge. If Third-party sources are used, they are quoted as appropriate. ENISA is not responsible for the content of the external sources, including external websites, if referenced, in this publication.

DISCLAIMER RELATED TO THE INTERPRETATIONS OF ARTICLES RELATED TO THE CYBERSECURITY ACT:

The interpretations of the articles of the Cybersecurity Act in this publication have no official nor legal power, nor do they constitute an authoritative interpretation of EU law, which is a prerogative of the Court of Justice of the European Union. The explanations provided in this report are for explanatory purposes only; no rights can or may be derived from any interpretative information provided in this report.

COPYRIGHT NOTICE

EXECUTIVE SUMMARY

Following the request from the European Commission in accordance with Article 48.2 of the Cybersecurity Act[2] (hereinafter referred to as CSA as indicated in the glossary), ENISA has set up an Ad Hoc Working Group (AHWG) to support the preparation of a candidate EU cybersecurity certification scheme to serve as a successor to the existing ICT products certification schemes operating under the SOG-IS MRA (Senior Officials Group Information Systems Security Mutual Recognition Agreement).

As stipulated by Article 49.3 of the Cybersecurity Act, "*When preparing a candidate scheme, ENISA shall consult all relevant stakeholders by means of a formal, open, transparent and inclusive consultation process.*" ENISA has therefore organised a public consultation from July,2 to July, 31 2020.

This report presents the outcome of this consultation. It contains 3 chapters. Under Chapter 1 the approach and process of the public consultation are explained. Under Chapter 2 the actual analysis of the results is presented of which the main outcomes are outlined below:

The survey was designed in seven different sections with questions related to:

- **The contributors**
  - Important fact is that the contributors represent a broad spectrum of actors involved in ICT products certification ensuring that input is received from all different angles.
  - Manufacturers/developers represented 37 % and the conformity assessment bodies (certification bodies and ITSEFs/testing laboratories) 24 % of the total number of respondents.
  - 77% of the participants indicated EU/EEA as their country of establishment and 20% as non-EU/EEA. Further to that, 32% indicated that their country of establishment participates in the SOG-IS MRA and 33% that their country of establishment is a member of the Common Criteria Recognition Arrangement (CCRA).

- The **intend to use the draft candidate EUCC scheme:** 33% of the respondents indicated to envisage having ICT products certified under the EUCC scheme (manufacturers/producers/developers and trade organisations) and 25% indicated to have their products certified; generating a demand side that is more or less in balance with the activity of contributors.

- The **transition from current scheme** (SOG-IS or national schemes) **to EUCC scheme**; 64% of the survey participants agreed that the choices made in the EUCC scheme will have a positive impact on the transition from current activities. 32% were neutral and only 4% were of the opinion that the impact will not be positive. The need of guidance to support transition was noted.

[2] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

- The **opinion on the new elements** that were developed in the EUCC scheme, such as:
    - Conditions for issuing, maintenance, renewal and continuation of certifications
    - Monitoring & handling of non-compliances and non-conformities
    - Vulnerability handling procedures
    - Patch management procedures to support vulnerability handling

  is the following: 70% of the survey participants agreed that these improvements will have a positive impact on the certification of ICT products. 24% were neutral and only 6% were of the opinion that the impact will not be positive. Additional comments led to some adjustments in the scheme.

- The **guidance** that is needed for stakeholders related to the implementation of the scheme: respondents preferred written guidance (33%), webinars (19%) and training (19%). Some comments resulted in an extension of the topics that needed further guidance, respondents also brought up new concepts to improve implementation that may need further attention.

- The **opinion on the impact** of the EUCC scheme **on market conditions:** the use of a harmonised label and a QR code to easily upload certification information and the possibility to establish generic specifications for products through certified Protection Profiles, was welcomed by 75% of the participants who agreed that these provisions will have a positive impact on EU market conditions while 16% were neutral and only 10% were of the opinion that the impact will not be positive.

- The **opinion on the maintenance** of the EUCC scheme: comments were collected and analysed.

- Any **additional comments** of the stakeholders are listed under section 2.9 of this report.

In addition, Chapter 3 provides an insight in the main transformations to the initial version 1.0 of the candidate EUCC scheme, according to comments made. The revised version 1.1 will be submitted to the ECCG for its opinion.

TABLE OF CONTENTS

1. INTRODUCTION

Following the request from the European Commission in accordance with Article 48.2 of the Cybersecurity Act[3] (hereinafter referred to as CSA as indicated in the glossary), ENISA has set up an Ad Hoc Working Group (AHWG) to support the preparation of a candidate EU cybersecurity certification scheme to serve as a successor to the existing schemes operating under the SOG-IS MRA (Senior Officials Group Information Systems Security Mutual Recognition Agreement).

Based on the outcomes from this AHWG, launched on November 27th, 2019 and composed of twenty (20) selected members representing industry (e.g., developers, evaluators), as well as around twelve (12) participants from accreditation bodies and EU Members States, regular discussions within the ECCG and after an internal review, ENISA has consolidated in the very beginning of July 2020 a candidate scheme, the EUCC scheme.

As required by Article 49.3 of the Cybersecurity Act, "*When preparing a candidate scheme, ENISA shall consult all relevant stakeholders by means of a formal, open, transparent and inclusive consultation process.*" ENISA has therefore launched a public consultation from July,2nd to July, 31st 2020.

A cybersecurity certification scheme is developed in collaboration with all stakeholders involved, taking into consideration all aspects and angles of the certification process.

1.1 WHY A PUBLIC CONSULTATION

The 20 experts composing the AHWG established to support ENISA for the development of the EUCC candidate scheme do represent a very good selection of the relevant stakeholders that may be involved into the use of such of scheme, if and when adopted through EU legislation.

With their support, ENISA could therefore successfully establish a first version 1.0 of this scheme in accordance with the time constrains given to this project. However, the improvements to the existing SOG-IS schemes proposed as to cover the requirements of the CSA will have a significant impact on current activities.

In addition, as the EUCC is the first candidate scheme, and therefore its draft establishes a first set of "interpretations" of the CSA. The understanding on what these are and how they should be reflected in a clear and unambiguous way in this scheme is important. Therefore, the feedback of the external readers is also crucial. Finally, ENISA is engaged into the development of another candidate scheme, related to Cloud services, which targets a potentially different audience than the Common Criteria community, but will benefit from the outcome of the EUCC.

As a result, ENISA decided to establish the necessary consultation required by Article 49.3 of the CSA by means of a public consultation, open to any party, directly accessible on its website, and without any limitation of participation.

As such, the public consultation was expected to give the chance to the Agency to collect the opinions, feedback on technical, procedural, practical and explanatory fields of stakeholders in order to align and improve the current draft of the scheme and bring it into the final stage.

[3] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

1.2 CONSULTATION PROCESS

For the public consultation the EU Survey[4] tool was used that enables parties to participate online at any given moment and save and/or print their input in PDF version. To encourage the public to provide feedback, the announcement of the public consultation was presented on the ENISA website with a news item and was also pushed through social media enabling interested parties to participate not only within, but also outside the European Union.

The public consultation was opened from July 2nd until July 31st 2020. Besides the public, the European Cybersecurity Certification Group (ECCG- consisting of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities and invited stakeholders and relevant third parties that participate in the work)[5] and the Stakeholder Cybersecurity certification Group (SCCG- composed of members selected from among recognised experts representing the relevant stakeholders)[6] were invited to participate in the consultation. The results of the ECCG are published in a separate report, as they reflect the opinions of the Member States, as such. The public collection of feedback from different stakeholders, together with the feedback from the ECCG, will help to consolidate the draft scheme with the opinions of all relevant stakeholders.

The public consultation report includes recommendations proposed by the Agency in terms of proposed changes and/or action points that are listed for uptake.

ENISA reconvened the AHWG that had been put in a "dormant" phase, as to analyse and review the comments made, and to establish the necessary updates of the scheme. The elements provided by ENISA to the AHWG were sanitized prior to the analysis and review (removal of any indication on which individual or company/entity would have made the comments).

The AHWG received separately the comments provided by the Member States that accepted to share them with the group.

Upon presentation to the ECCG, SCCG and the Commission, the consultation results included in this report with the identified necessary changes and defined action points, are now made public.

1.3 PROCESSING THE RECEIVED DATA

The survey was designed in seven different sections with questions related to:

- **The contributors**
- The **intend to use the draft EUCC candidate scheme**
- The **transition from current schemes** (SOG-IS or national scheme)
- The **opinion on the new elements** that were developed in the EUCC scheme
    - Conditions for issuing, maintenance, renewal and continuation of certifications
    - Monitoring & handling of non-compliances and non-conformities
    - Vulnerability handling procedures
    - Patch management procedures to support vulnerability handling
- The **guidance** that is needed for stakeholders related to the implementation of the scheme
- The **opinion on the impact** of the EUCC scheme **on market conditions**

[4] https://ec.europa.eu/eusurvey/
[5] See Art. 62 CSA.
[6] See Art. 22 CSA.

- The **opinion on the maintenance** of the EUCC scheme
- Any **additional comments** of the stakeholders.

This report formulates the opinions received as well as the questions and concerns raised.

The outcome of the survey is processed in a way that it is providing insights for all respondents as well as for the Agency, the Commission and the ECCG and SCCG. Upon each graphic, diagram ENISA presents and provides explanatory text and remarks to assist the reader in the clarification of the outcome. For some outcomes it is of relevance to analyse the feedback provided and relate it to the background of the participants providing insights into the different interests respondents may have depending on their activity.

None of the questions in this consultation were presented as mandatory to answer. In order to provide a clear insight the percentages in each question were adjusted according to the replies submitted, the non-answered questions are also indicated.

Lastly, for some questions participants could select more than one responses, as to better depict their background, interest and/or expectation(s).

2. ANALYSIS OF RESULTS

2.1 THE CONTRIBUTORS

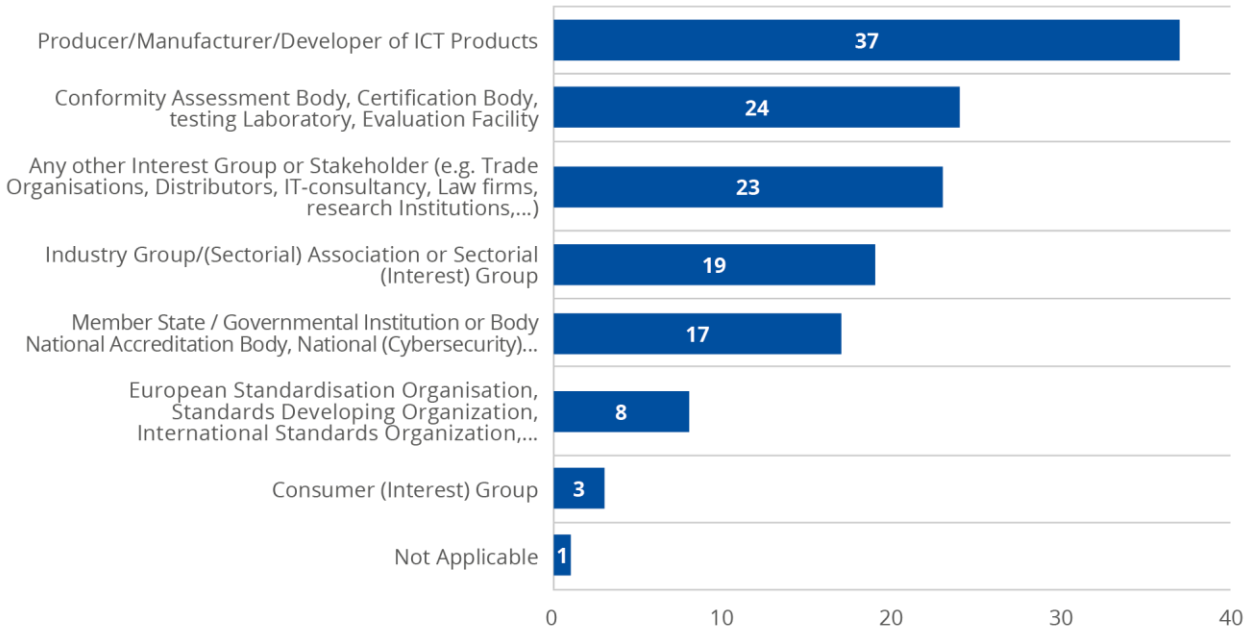
In total 114 respondents participated in the survey. ENISA indeed welcomed the balanced contributions from 37 producers, manufacturers and developers, 24 bodies that issue certificates or perform conformity assessment, 19 interest groups from industry or sectorial associations, 23 stakeholder interest groups such as trade organisations, distributors, consultancy firms, research institutions and Academia. 17 Member States and governmental institutions/bodies and National Cybersecurity Certification Authorities (NCCA's) and Accreditation bodies. Lastly, 8 participants indicated that they are affiliated with standards developing organizations.

It should be noted that participants were able to select more than one option for this topic.

Important fact is that the contributors represent a brought spectrum of actors involved in certification ensuring that input is received from all different angles.

The limited representation of consumer groups is to be noted, and gives indication to ENISA for the development of a communication plan, for the implementation phase of this scheme, that will make sure consumers are well informed of what cybersecurity certification of ICT products entails, and can find cybersecurity support related to the certified product.

Figure 1: Survey Participants' Composition



Recommendation #1: During the implementation phase of the EUCC scheme, a communication plan will be established. The plan will include communication with consumers to ensure they are well informed in what cybersecurity certification of ICT products entails.

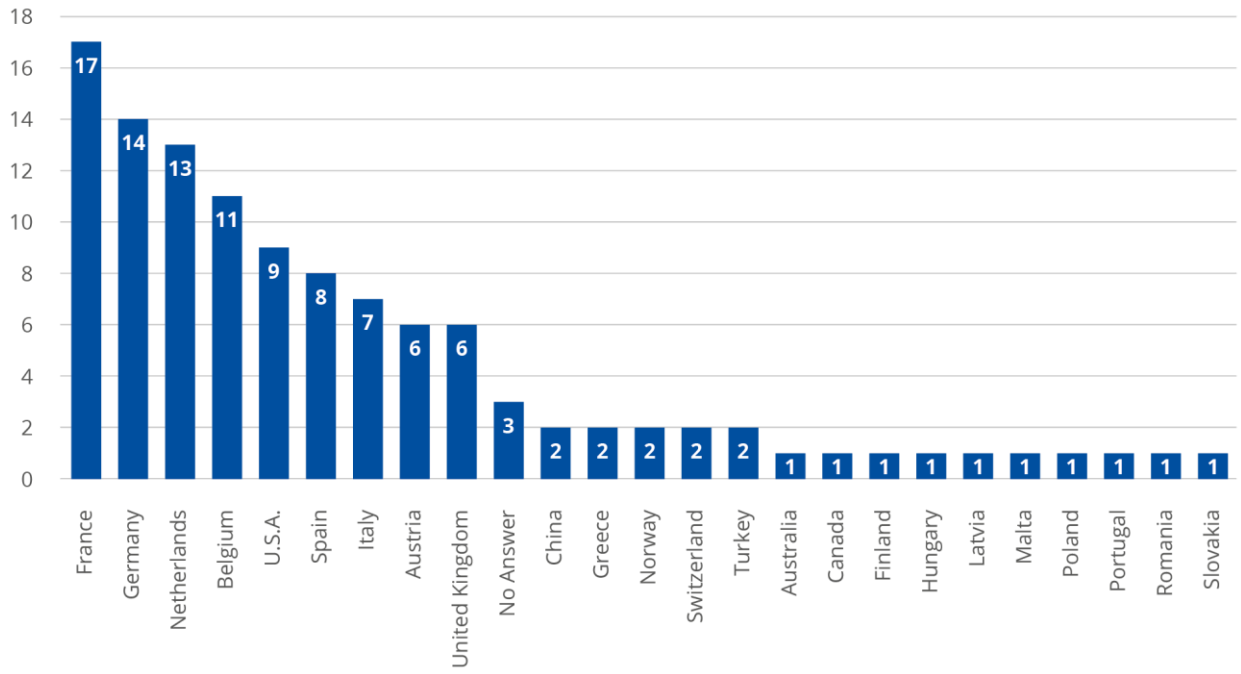
2.2 GEOGRAPHIC COMPOSITION OF PARTICIPANTS

Figure 2 reveals a broad spectrum of participating countries, but looking at the number of participants per country, France, Germany, the Netherlands and Belgium showed the largest percentage of participants in the consultation.

77% of the participants indicated EU/EEA as their country of establishment and 20% as non-EU/EEA. Further to that, 32% indicated that their country of establishment participates in the SOG-IS MRA and 33% that their country of establishment is a member of the Common Criteria Recognition Arrangement (CCRA). As this first scheme is built upon the current SOG-IS MRA certification mechanism, it is understandable that the SOG-IS MRA participants and the CCRA members in particular are participating in the feedback of the EUCC scheme. 28% indicated that their country of establishment has experience in relevant national certification schemes and only 2% indicated that their country does not has relevant experience, indicating that most parties that responded have experience with cybersecurity certification.

The relative high number of participants from the USA is also to be noted.

Figure 2: Geographic Composition of Participants



For the EU Cybersecurity Certification Framework to become effective, it is important that Member States and countries in the European Economic Area who are currently not involved or engaged in the SOG-IS certification and have the intention to participate in the EUCC scheme, are supported and enabled in the setting up of the certification mechanism. The Commission and experienced SOG-IS Member States could consider to set up a programme to provide the opportunity to set up and gain experience in cybersecurity certification issuance to enhance and increase the certification capability and participation.

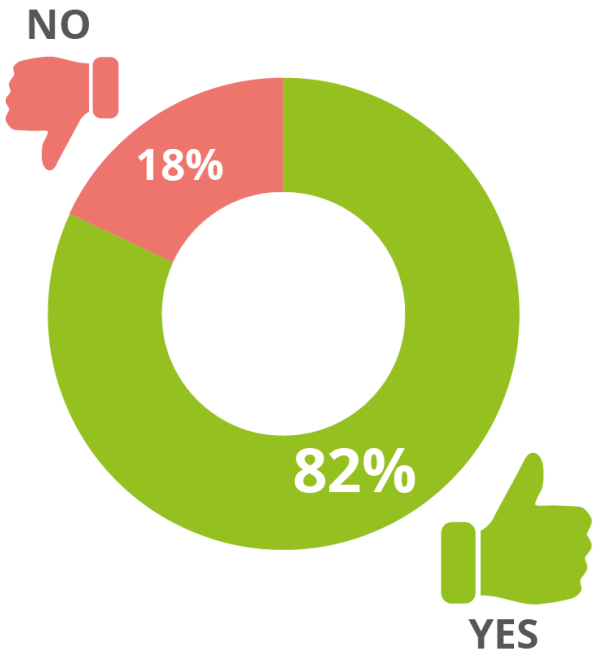
Recommendation #2: Ease the participation of interested EU Member States newcomers to cybersecurity certification to participate to the EUCC scheme by a dedicated training programme

2.3 INTENTION TO USE THE EUCC SCHEME

82% of the participants indicated their intention to use the EUCC scheme. 18% (13 participants) indicated not to intend to use the EUCC scheme. From EU /EEA perspective 80% of the participants from EU/EEA countries indicated that they intend to use the EUCC scheme, even if it is voluntary, while 61% of the participants outside EU/EEA indicated that they also intend to use the EUCC scheme.

Some EU/EEA countries that currently are not involved in the SOG-IS certification and participated in the survey indicated that they intend to start using the EUCC scheme, this is why we recommend to support these countries in their intent to participate.

Figure 3: Intention to use the EUCC scheme



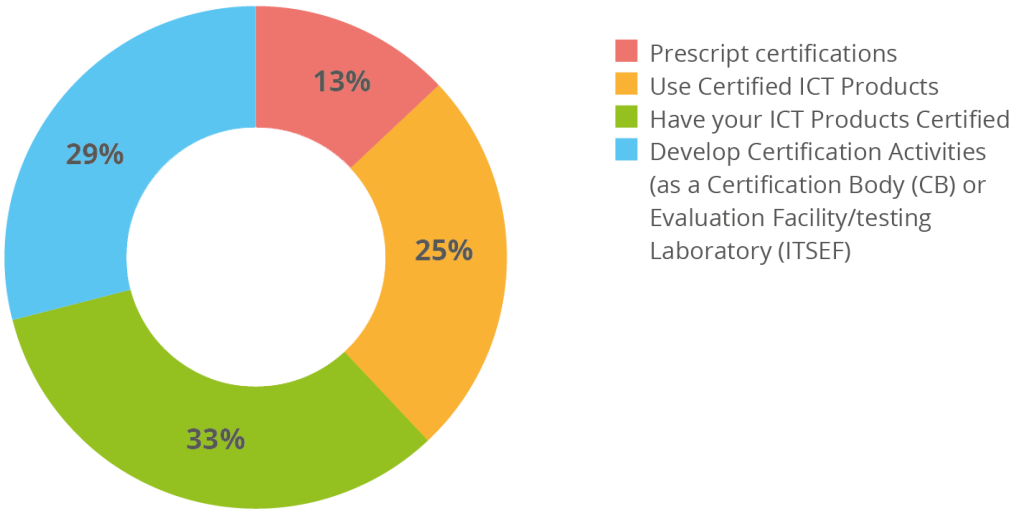
2.4 ENVISIONED PURPOSES OF USING THE EUCC SCHEME

33% of the respondents indicated to envisage having their ICT products certified under the EUCC scheme (manufacturers/producers/developers and trade organisations), 25% indicated they intended to use certified products, and 29% they intended to develop certification related activities (as a CB or ITSEF), showing a purpose to use the EUCC scheme very much in line with the profile of the respondents.

Many of the manufacturers/producers/developers and trade organisations indicated that they currently certify their products under the SOG-IS scheme and have every intention to extend their certificate to the EU level:

"*For our products in the verticals of telecommunication, identity, payment and transit Common Criteria security certification on a high level is a key selling proposition. The high level of assurance needs to be highly visible to our customers.*"

Figure 4: Envisioned use of the EUCC scheme



Others indicated the market perspective as reason:

"As we wish to assess the security quality of our ICT products against a uniform and consensus-based certification scheme which is recognized by all relevant parties, including telecom operators, suppliers and regulators, to jointly enhance cybersecurity for ICT industry."

"As a private business aiming to make organisations more secure and resilient to cyber threats, we will certify our products to indicate even further their trustworthiness. Likewise, we intend to make the forthcoming certification a major requirement for our supply chain"

"As an IT-consultancy enterprise, we intend to primarily develop certification activities as an Evaluation Facility/Testing Laboratory (ITSEF), not as a Certification Body (CB). Secondly, we intend to prescribe certifications at the partners we collaborate with, to take the responsibilities we have on the area of security."

Other participants indicate the certification intentions, depending on market considerations:

"We are committed to considering certification activities using the EUCC scheme, although any decision would depend on market demand, product development cycle, evaluation lead time, among other considerations."

Parties that indicate not to intend using the EUCC scheme provided their reasons to do so:

"*We operate our own global certification programme with a methodology developed on best security evaluation principles to deliver cybersecurity products at a high assurance level. Our scheme already provides similar benefits and there is not a need to duplicate these efforts."*

Others indicate the non-applicability*:*

"Our organization does not currently produce ICT products that would benefit from certification against 'substantial' or 'high ratings'. However, we may use ICT products from other manufacturers/providers in the assembly of our products."

Some SMEs provided a different reason:

"The approach is not SME-friendly. The CC (and ISO/IEC 15408) has generally proved to be difficult to apply and unaffordable to SMEs. We advise to tailor a scheme to the levels of risks and size of organizations (and their roles in a value chain)."

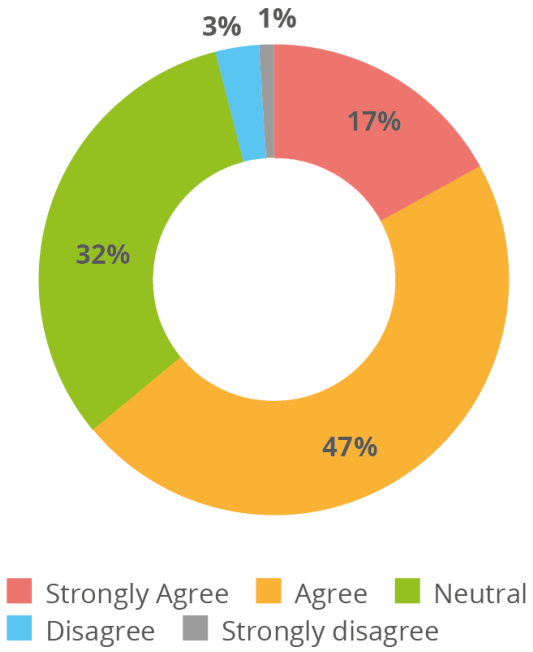
2.5 TRANSITION FROM THE SOG-IS MRA TO THE EUCC SCHEME

The draft candidate EUCC scheme included a number of transitional measures and recommendations to support a transition from the SOG-IS MRA to the EUCC scheme. These transitional measures relate to:

- The extensive reuse of the Joint Interpretation Library (JIL) mandatory supporting documents:
- The continuation of the Technical Domains of Smart Cards and similar devices and of Hardware Devices with Security Boxes:
- Governance of the scheme by the European Cybersecurity Certification Group (ECCG) and relevant subgroups.

64% of the survey participants agreed that these choices will have a positive impact on the transition. 32% were neutral and only 4% were of the opinion that the impact will not be positive.

Figure 5: Positive impact of transitional measures from the SOG-IS MRA to the EUCC



In addition to these responses, 63% of the participants foresaw possible issues related to the transition that they may run into. The relative large percentage of neutral scores deserves more attention in order to learn what the related issues are.

The responses to the question as to what should be considered to be necessary in order to successfully implement the transition from SOG-IS MRA schemes to the EUCC scheme differed:

- some participants pointed to the fact that this is the first scheme that is designed to be applied horizontally to all industry domains and products;

- others indicated that they like to have additional information as to how the transition in practice will be organised, as they were in need of support in their certification migration process;
- or pointed towards the uncertainty in processing time as certification is considered complex and time critical;
- indicated that it might be useful to design a requirement mapping to get better insights into what is needed to make the transfer successful for them;
- emphasized the importance of mutual recognition on a worldwide basis;
- brought up that self-declaration and the assurance level "basic" is not addressed by the scheme;
- expressed their concerns to the fact that the review of the NIS directive and the Radio Equipment Directive might impact the security requirements in their sectors and subsequently also have impact on the cybersecurity certification framework;
- asked for clear communication to avoid confusion between existing & future schemes.

This information provides valuable insights and helps ENISA to design guidance that provides clarification in the process and support in how to approach the migration effectively and efficiently. It is clear that the EUCC scheme will be subject to maintenance and will adapt to either legal, economical changes and/or technological innovations and improvements. The EUCC scheme will be subject to continuous contributions to the evaluation of the certification processes and the regular analysis of the main trends in the cybersecurity market both to the demand and supply side as indicated under article 8 of the CSA.[7]

The estimated timeline indicated by participants for efficient transition varies between 1-3 years with a slight majority for 2 years.

2.6 IMPROVEMENTS FROM THE SOG-IS MRA TO THE EUCC SCHEME

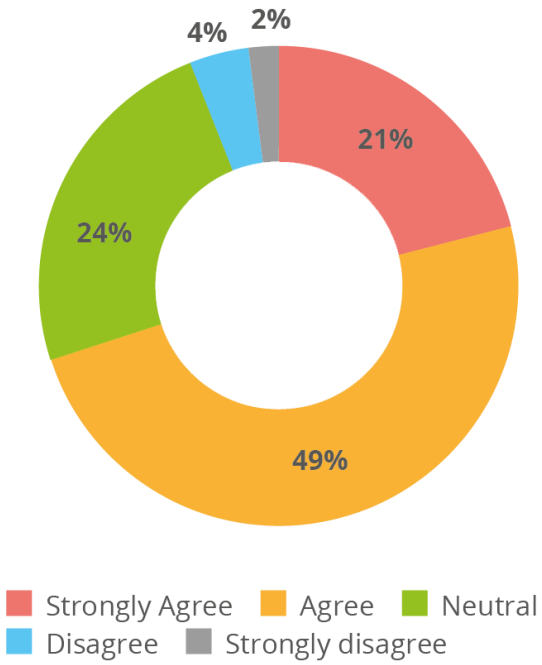
Based on the relevant CSA provisions, the draft candidate EUCC scheme included a number of improvements to further advance the current SOG-IS MRA and to ensure assurance continuity of the certificates. These improvements cover:

- the maintenance of the certificates,
- harmonised activities related to the monitoring and handling of non-compliances and non-conformities,
- harmonised conditions for vulnerability handling and disclosure
- the introduction of a patch management mechanism to support vulnerability handling.

70% of the survey participants agreed that these improvements will have a positive impact on the certification scheme. 24% were neutral and only 6% were of the opinion that the impact will not be positive. Out of the participants that indicated their country of establishment, 69% (57 responses) from EU/EEA countries indicated that they agree and strongly agree that impact will be positive, 28% (23 responses) were neutral and 3% (3 responses) disagreed or strongly disagreed.

[7] Article 8 (4) and 8 (7) CSA.

Figure 6: Positive impact of improvements from the SOG-IS MRA to the EUCC

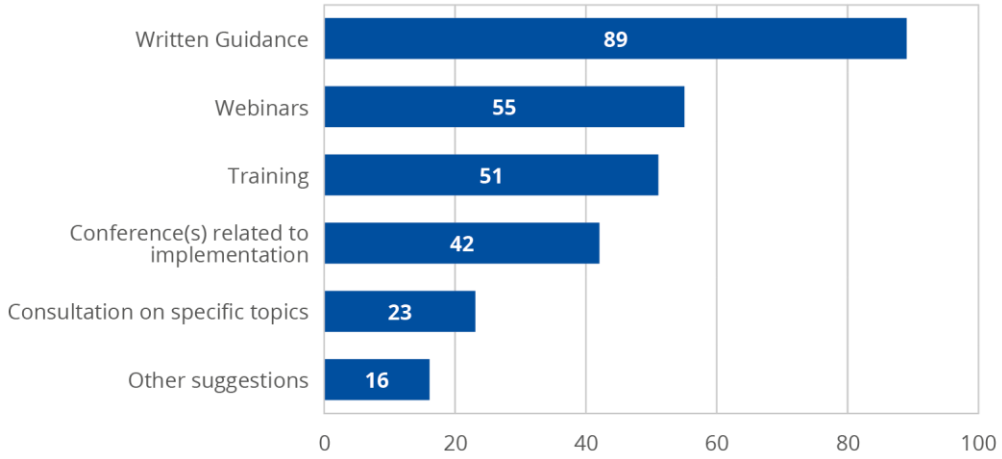


Looking at the 24 % of neutrality towards the indicated improvements, comments relate in particular to:

- a call for more flexibility on possible delays, suspensions periods, embargo and communication to customers, associated with concerns about some indicated timelines that seem 'ambitious' and not based yet upon best practice;
- standards for vulnerability management already under development for some industries;
- questions about the maintenance of these new elements and the cooperation amongst stakeholders in these new processes and compliance to these processes, with the call for the use of a public forum instead of a closed working group under NDA;
- the need for periodic feedback on the implementation of the scheme from relevant types of actors e.g. by means of setting out a request for consultation (such as this one);
- for future maintenance and reviews of the EUCC scheme, the request to get reasonable time in advance (e.g. 6 months in advance) to ensure providing high quality responses and eventually contribute to continuous improvement of the certification program as such.
- the proposal to adjust these new processes upon a risk based approach, meaning that for lower risk products the effort should be accordingly limited.

2.7 FORM OF GUIDANCE TO BE DEVELOPED

Figure 7: Form of guidance



Looking at the indicated preferences for guidance, most participants indicated the importance of written guidance as this provides reproducible material. These guidance supports may either be combined with trainings, webinars or conferences and consultation rounds. The different types of guidance should be adjusted in line with the maintenance of the scheme.

A selection of ideas that were brought forward as 'other ideas' are listed below:

- Set up a community slack channel or similar chat-like environment. Similar to OWASP where one can issue questions and discuss with others working on the same topic;
- Develop tooling for evaluation (preparation);
- Developing a common virtual laboratory to prepare efficiently for evaluations/pentests
- Mutual virtual visits or learning exercises and field trips for stakeholders to share experiences, observe functioning certification system in place;
- A platform where adopted methodologies and workflows can be shared and demonstrated.

2.8 IMPACT OF THE EUCC SCHEME ON EU MARKET CONDITIONS

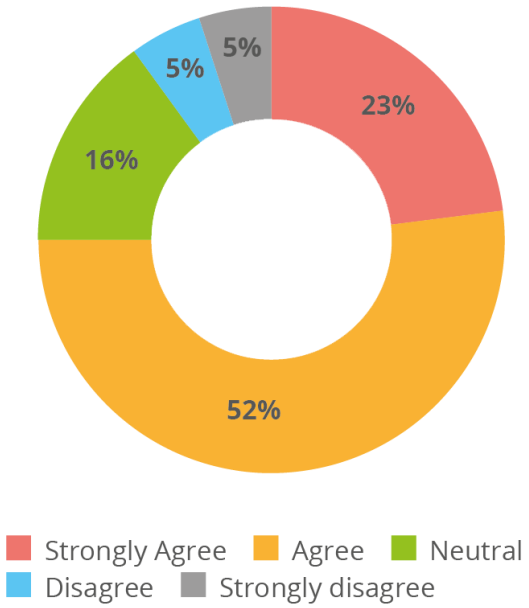
Based on the relevant CSA provisions, the candidate EUCC includes a number of aspects to enhance the market conditions for the certified ICT products (both under the EUCC scheme and future schemes). These aspects include:

- An EU certificate will be valid throughout the entire European Union;
- The certificates issued will also include a label that is associated to the EUCC scheme;
- The label will be designed in a harmonised and clearly recognisable way across all EU cybersecurity certification schemes;
- The label will have a QR code associated to the certificate;
- The QR code will provide access to the relevant publicly available certification information and other related information regarding the Cybersecurity Certification Framework under the Website on European cybersecurity certification schemes;
- Stakeholder communities will have the possibility to establish generic specifications for their products through certified Protection Profiles.

75% of the participants agreed that these provisions will have a positive impact on EU market conditions while 16% were neutral and only 10% were of the opinion that the impact will not be positive. Out of the participants that indicated their country of establishment, 76% (64

responses) from EU/EEA countries indicated that they agree and strongly agree that impact will be positive, 14% (12 responses) were neutral and 10% (8 responses) disagreed or strongly disagreed. From non EU/EEA countries, 70% (14 responses) indicated that they agree and strongly agree that impact will be positive, 20% (4 responses) were neutral and 10% (2 responses) disagreed or strongly disagreed.

Figure 8: Positive impact of the EUCC scheme on EU market conditions



The participants that indicated a 'neutral' impact on market conditions, indicated remarks related to the maintenance and transition, recognition and guidance with some of them already presented in the previous sections of this report.

2.9 IMPORTANT ASPECTS RELATED TO THE EUCC SCHEME

Upon the question to the participants on what additional important aspects the Agency should take into consideration, the following is a selection of the points that were addressed multiple times:

- Reusability of evidence, protection profiles, continuation of existing certificates, and a lightweight way to migrate protection profiles and certificates from existing schemes into the EUCC should be possible. The approach towards reuse of evidence of CBs in different countries should be harmonised as harmonisation of acceptance of evidence is crucial for composition;
- Composition of certificates is very important to accommodate products based on certified building blocks; such composition should not only be possible within the EUCC scheme but also reusing existing evidence, PPs and certificates from legacy schemes for a suitable transition period;
- "The mapping of VAN.3 to "high" will weaken the significance of "high resistance" and open the door to marketing campaign promoting "high" whereas the resistance is not;
- Discussion on cryptographic analysis is missing in the EUCC proposal. However, this is an important topic to be clarified in EUCC scheme as currently one SOG-IS governmental agency performs a cryptographic analysis for the evaluation of a product, while other EU SOG-IS agencies do not. It is important that harmonization on this aspect is considered in the EUCC scheme;

- The workflows and roles have to be described clearly and have to be published;
- The decision structure for the maintenance of the scheme has to be described clearly and has to be published;
- The derogation of Art. 56. 6b of the CSA offers to provide for a chance for private schemes to get involved in the EUCC, but should be described more clearly;
- Monitoring and metrics of performance of the NCCAs and CABs should be introduced so the required agile management of security issues are ensured;
- The scheme is intended to be voluntary, however some are also considering a possible future in which certification becomes required as result of regulatory mandate, market pressure, or both. This can only be done at a moment the certification processes are mature, cost efficient and have proven to be effective;
- Next to a principle-based security and privacy framework, there is a need for dynamic assurance and continuous certification. Autonomous cars already foresee the need for continuous monitoring of the security and safety of the vehicle and trustworthiness of the whole digital ecosystem of self-driving-cars. For the EUCC scheme to be effective, it is imperative that it takes into account the whole ecosystem and not just one component;
- Certification schemes operated by industry or other private organisations are not mentioned, and fall outside the CSA. The CSA public bodies operating such schemes should be able to propose that the Commission consider such schemes as a basis for approving them as a European Cybersecurity Certification scheme. As an example, private schemes would be recognised if requested to mitigate any duplication impact to vendors supporting the cards payments industry and digital single market;
- The EUCC scheme would benefit from greater use of principles and process based approaches which are much more scalable and hence effective than evaluation. Approaches (such as those proposed for high) that mainly focus on vulnerability searches are particularly costly and ineffective since vulnerabilities are almost always found in real use;
- For products in the verticals of telecommunication, identity, payment and transit Common Criteria security certification on a high level is a key selling proposition. “The high level of assurance needs to be highly visible to our customers.”; the security quality of ICT products needs a uniform and consensus-based certification scheme which is recognized by all relevant parties, including telecom operators, suppliers and regulators, to jointly enhance cybersecurity for ICT industry.

3. CONCLUSIONS & ACTIONS TAKEN

3.1 CONCLUSIONS

The EUCC candidate scheme received in majority a positive feedback.

Points that were brought up by stakeholders, experts, groups and participants, encourage ENISA to further improve the EUCC scheme whether in current adjustments or amendments or in a later maintenance phase. The feedback that ENISA received also helps to extend the Cybersecurity Certification Framework upon the lessons learned

Some of the comments received are not addressed, as they were already discussed under the AHWG. ENISA therefore considered sufficient background had been given into the current version of the scheme.

In addition, the ECCG[8] also proceeded to the review of version 1.0 of the candidate scheme. Their comments, are not included in this report and processed in a separate report. Their feedback also contributes to the revisions made within the candidate scheme.

Proposals for adjustments or amendments related to this public survey are described in the next section. They will be processed into the updated versions of the EUCC candidate scheme, either through direct changes, or in the form of recommendations for future activities or guidance.

3.2 ACTIONS TAKEN/ TO BE TAKEN

The main changes to the initial version 1.0 of the candidate EUCC scheme that are processed into the updated version 1.1 are the following:

- addition and clarification of definitions;
- systematic cooperation with the ECCG for the development of guidance documents supporting the scheme;
- clarification of activities related to the maintenance of certificates;
- clarification of deadlines associated to the handling of non-conformities, non-compliances and vulnerabilities;
- modification of the status of the new patch management process, now in annex and for trial use;
- modification of the logo associated to the certificates, allowing to establish an additional specific logo for the scheme and to mention the evaluation level (AVA_VAN) achieved in addition to the CSA level;
- clarification of the peer assessment requirements and simplification of the associated annex;
- update of annexes 7 and 9 based on their recent evolution within the SOG-IS, and the addition of one annex related to ST sanitization.

In addition, ENISA considers to launch several actions to improve the capacity to promote and explain the importance of the use of the EUCC scheme to the EU community and to provide potential newcomers to EUCC certification with additional information and assistance on associated deadlines that need to be met and the required conditions, such as engaging into guidance development or into a dedicated project to develop a communication plan. Moreover, a transition project should be established in order to provide and ensure the best conditions for a smooth transfer from the current SOG-IS activities to the EUCC.

[8] Article 62 CSA.

ANNEX A: PUBLIC CONSULTATION QUESTIONNAIRE

Consultation questionnaire of the draft EUCC candidate scheme, in accordance with Article 49(3) of the Cybersecurity Act.

1. INTRODUCTION

Upon request of the European Commission, based on Article 48 (2) of the Cybersecurity Act[9] (hereinafter referred to as CSA), ENISA has set up an Ad Hoc Working Group, hereinafter referred to as EUCC AHWG, to support the preparation of a candidate cybersecurity certification scheme that will serve as a successor to the SOG-IS Mutual Recognition Agreement, hereinafter referred to as SOG-IS MRA[10] .

The EUCC AHWG is chaired by ENISA and is composed of 20 appointed members representing industry (developers, evaluators), as well as around 12 participants from accreditation bodies and Members States.

This EUCC AHWG worked in close collaboration with the European Commission and with the European Cybersecurity Certification Group (ECCG: composed of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities of the EU Member States).

The current consultation aims to collect your opinion(s), view(s) and suggestion(s) on the draft version of the candidate EUCC scheme, the deployment and its future implementation, in line with Article 49 (3) of the CSA. The consultation will remain open for contributions until July 31st, 12:00 CET.

Before going through the questions below, you can download the draft EUCC candidate Cybersecurity Certification Scheme under the relevant section of the ENISA website. Please note that within the questions below, there are references to specific sections/chapters/annexes of the draft scheme.

For any query/problem related to the consultation on the draft EUCC candidate scheme, please contact ENISA at certification at enisa.europa.eu

Following the conclusion of the consultation, the Agency will make available a consolidated report on the ENISA website.

1.1. As it is important to have an understanding on the type of actor/stakeholder you belong to and the interaction, you may have with the EUCC scheme, please indicate the type of actor you represent:

You can select more than one

- ○ Member State / Governmental Institution or Body

[9] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[10] https://www.sogis.eu/

- National Accreditation Body, National (Cybersecurity) Certification Authority
- Conformity Assessment Body, Certification Body, Testing laboratory, Evaluation facility
- European Standardisation Organisation, Standards Developing Organization, International Standards
- Organization, Standardisation Alliance or Group
- National Regulatory Authority (such as Data Protection, Telecommunication, NIS, etc), Market Surveillance
- Authority, Consumer Surveillance Authority or any other Authority
- Producer / Manufacturer / Developer of ICT Products
- Industry Group / (Sectorial) Association or Sectorial (Interest) Group
- Consumer (Interest) Group
- Any other Interest Group or Stakeholder (e.g Trade Organisations, Distributors, IT-consultancy, Law firms, Research Institutions, Academia, etc)

1.2 If indicated Other, can you please specify:
50 character(s) maximum

1.3 Please indicate if your country of establishment:
You can select more than one

- Participates in the SOG-IS MRA
- Is a member of the Common Criteria Recognition Arrangement (CCRA)
- Has no prior experience in the use of Common Criteria or participation in the SOG-IS MRA
- Has experience in relevant national certification schemes

1.4 Can you please indicate your country of establishment?

1.5 If your country of establishment has experience with a National Scheme related to (cyber)security certification, could you please indicate this scheme?
50 character(s) maximum

2. YOUR OPINION ON THE DRAFT EUCC CANDIDATE SCHEME

2.1 The implementation of this draft EUCC candidate scheme will be voluntary of nature. Do you intend to use the EUCC scheme?

- Yes
- No

2.2 If indicated Yes, would you consider using the draft EUCC candidate scheme to:
You can select more than one

- Prescript Certifications
- Use Certified ICT Products
- Have your ICT Products Certified
- Develop Certification Activities (as a Certification Body (CB) or Evaluation Facility/Testing Laboratory (ITSEF))

2.3 Can you please elaborate on your selections above?
500 character(s) maximum

3. TRANSITION FROM THE SOG-IS MRA TO THE EUCC SCHEME

3.1 In the draft EUCC candidate scheme, the following transitional measures and recommendations are included to support a transition from the SOG-IS MRA to the EUCC scheme:

- The extensive reuse of the Joint Interpretation Library (JIL) mandatory supporting documents integrated into the scheme as annexes (Annexes 2-10);
- The continuation of the Technical Domains of Smart Cards and similar devices and of Hardware Devices with Security Boxes (Chapter 8 and Annexes 1-10);
- Governance of the scheme by the European Cybersecurity Certification Group (ECCG) and relevant subgroups (Chapter 26).

Do you believe that the aforementioned choices will have a positive impact on the transition from the SOGIS MRA to the EUCC scheme?

- ○ Strongly agree
- ○ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly disagree

3.2 Which are the important transition conditions that you consider necessary, in order to successfully implement the transition from the SOG-IS MRA schemes to the EUCC scheme?
500 character(s) maximum

3.3 Do you foresee (possible) issues, related to the transition that you may run into?

○ Yes ○ No

3.4 If indicated Yes, can you please elaborate on your concerns or issues?
500 character(s) maximum

3.5 What timelines could be taken into consideration in order to make the transition period short, but effective and successful?
500 character(s) maximum

4. ADDITIONAL ELEMENTS OF THE EUCC SCHEME

4.1 In the draft EUCC candidate scheme, a number of improvements have been included to further advance the current SOG-IS MRA, to ensure assurance continuity of the certificates, covering:

- Their maintenance (Chapter 12);
- Harmonised activities related to the monitoring and handling of non-compliances and nonconformities (Chapters 11 and 13);
- Harmonised conditions for vulnerability handling and disclosure (Chapter 14);
- Introduction of a patch management mechanism to support vulnerability handling (Chapter 15).

Do you believe these improvements will have a positive impact on the transition from the SOG-IS MRA to the EUCC scheme?

- ○ Strongly agree
- ○ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly disagree

4.2 Do you have any comments/concerns on the introduced aspects presented above?
500 character(s) maximum

4.3 Are there any additional aspects that you think are important and should be considered by the EUCC scheme?
500 character(s) maximum

4.4 In the process of drafting the candidate EUCC scheme, guidance elements have been identified by the EUCC AHWG as prominent for the uptake of the scheme, in addition to existing guidance supporting documents established under the current SOG-IS MRA, including among others:

- A harmonised methodology for the mapping between risk assessments and the choice of the relevant assurance levels.
- Guidance for mutually approved interpretation of the accreditation standards for certification and testing laboratory activities.
- Guidance on the commitments and compliance requirements that may be part of a certification request.
- Guidance on the transformation of SOG-IS MRA certificates and schemes (CB, ITSEF) into the EUCC scheme.
- Guidance on the taxonomy of ICT products as to offer a harmonised list of types of ICT products across the EU.
- Guidance on the delivery and publication of the certificates and their updates.

Would you have further suggestions for additional guidance?

○ Yes ○ No

4.5 If indicated Yes, what additional guidance would you require (please indicate the relevant chapter/section of the draft EUCC candidate scheme)?
500 character(s) maximum

4.6 Please indicate what form of guidance you prefer:
You can select more than one

- ○ Training
- ○ Webinars
- ○ Written Guidance
- ○ Consultation on specific topics (Which topics? Please indicate in open text field)
- ○ Conference related to implementation
- ○ Other ideas (Please indicate in the open text field below)

Can you please indicate the specific topics that would require consultation?
500 character(s) maximum

5. IMPACT OF THE EUCC SCHEME ON EU MARKET CONDITIONS

5.1 The draft EUCC candidate presents the following proposals to enhance the market conditions for the certified ICT products (both under the EUCC scheme and under future schemes):

- An EU certificate will be valid throughout the entire European Union;
- The certificates issued will also include a label that is associated to the EUCC scheme;
    - The label will be designed in a harmonised and clearly recognisable way across all EU cybersecurity certification schemes;
    - The label will have a QR code associated to the certificate. The QR code will provide access to the relevant publicly available certification information and other related information regarding the Cybersecurity Certification Framework under the Website on European cybersecurity certification schemes;
- Stakeholder communities will have the possibility to establish generic specifications for their products through certified Protection Profiles.

Do you believe that the aforementioned proposals will have a positive impact on market conditions for the certified ICT products (both under the EUCC and under future schemes)?

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

6. MAINTENANCE OF THE EUCC SCHEME

The EUCC scheme will be subject to continuous maintenance and review to improve the certification conditions, to align with the state-of-the-art technology and security and to broaden, where possible, its impact on the EU market. Several recommendations have been included in the draft EUCC candidate scheme under Chapter 26.

6.1 What additional suggestions related to the organisation, process or other aspects of future maintenance and review would you like to bring forward?
500 character(s) maximum

7. ADDITIONAL COMMENTS

Please provide any further comments you might have on the draft EUCC candidate scheme and/or indicate any information that you think would be necessary.
500 character(s) maximum

ABOUT ENISA

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

ENISA
European Union Agency for Cybersecurity

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

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

enisa.europa.eu