Evaluation ENISA (European Union Agency for Cybersecurity) and the European Cybersecurity Certification Framework

Table of Contents:

Introduction and summary

This is the response of the Online Trust Coalition to the European Commission's (DG CNECT) call for evidence for an evaluation / fitness check of ENISA (European Union Agency for Cybersecurity) and the Cybersecurity framework. The current mandate of ENISA is to contribute to achieving a "high common level of cybersecurity across the Union", "act as a reference point for advice and expertise on cybersecurity" and "contribute to reducing the fragmentation of the internal market". For these goals ENISA performs a number of tasks. Since the Online Trust Coalition's primary focus is on the trustworthiness of cloud services, this response focusses on ENISA's efforts to create a cybersecurity certification scheme for cloud services based on the framework provided in the EU Cybersecurity Act (Regulation (EU) 2019/881), further referred to as the EUCS. Where reference is made to the EUCS this relates to version V1.0.319 dated May 2023.

The Online Trust Coalition acknowledges the need for a common high level of cybersecurity and resilience throughout the European Union and supports the efforts taken by the European Commission to this end. Critical comments and observations made in this evaluation are therefore intended to further improve the processes and operations in place to reach these goals in the context of a single European digital market.

In summary, our comments and observations relate to:

- **General**

We identify a lack of transparency in the communication by ENISA and between the European Commission and ENISA. The EUCS draft scheme was changed several times without consulting the Ad-hoc working group, it is not clear who decides on changes made to the scheme, what steps are taken and how final decisions are made. One major result is that the draft scheme contains elements that are political by nature. Political decisions should be made in accordance with democratic political decision making procedures by authorized bodies under control by the European Parliament and not by an EU Agency or Ad Hoc working group. We strongly urge to have a public consultation on the final draft of the EUCS since the draft was changed considerably since the 2020 consultation. Also we strongly recommend to include a mandatory acceptance by SCCG and ECCG before including the draft scheme into an implementing Act.

In addition to the lack of transparency, we identify a lack of stakeholder involvement. The mandate of the Stakeholder Cybersecurity Certification Group (SCCG) in the Cybersecurity Act is too limited. Furthermore based upon the feedback we received from the SCCG we identify that their involvement is currently in practice absent. The role and functionality of the Ad-Hoc working group should be evaluated, as it is not accessible by all relevant experts, thereby not inclusive.

- **Cybersecurity Certification Framework**

The framework as laid down in the Cybersecurity Act is based on the Common Criteria / SOG-IS approach for product certification. Existing substantial differences in laboratory testing of products and the audit of services make the framework not suitable for certification of services.

According to Article 56 (2) of the Cybersecurity Act: "The cybersecurity certification shall be voluntary, unless otherwise specified by Union law or Member State law". Recent developments in other regulations and directives however show a tendency to mandate cybersecurity certification. Therefore in our opinion the requirements and processes in the scheme should be treated as if they are mandatory and a mandatory impact assessment prior to implementation of the scheme should be part of the framework.

Given the important role of the cybersecurity certification in other legal acts like among others NIS2 Directive, Cyber Resilience Act, e-IDAS2 and DORA, it is important to safeguard the consistency between these legal acts. Also opportunities for synergy and efficiency like harmonization of criteria across sectors and scope of legal acts and re-use of audit reports should be considered to reduce the compliance cost of CSPs and consequently reduce the price of cloud services.

- **EUCS scheme development**

Annex J of the draft scheme contains requirements that aim to safeguard the sovereignty of European cloud services (PUA: Protection against Unlawful Access). These requirements were included without a prior proper economic impact assessment. In the opinion of the Online Trust Coalition this faces the risk of disrupting the EU single internal cloud market. Furthermore the risk that the PUA requirements conflict with other international treaties and agreements like the General Agreement on Trade in Services (GATS) by the WTO, should be assessed.

The use of (European or international) standards is essential for the mutual recognition of the cybersecurity certificates and also for the effectiveness of all legal acts affected. Article 54 (1.c) of the EU Cybersecurity Act requires that the schemes shall at least include references to international, European or national standards applied. Recital 69 of that same act states that the European cybersecurity certification schemes should be based on European or international standards. Requirements of certification schemes therefore should be based on existing standards. The draft EUCS scheme however contains important elements that are not standardized (e.g. Annex J) or are submitted for standardisation to CEN-CENELEC (the security requirements in Annex A and the Meta-approach). The Online Trust Coalition supports the role of CEN-CENELEC as it has a well established reputation and transparent governance structure.

There is a need to invest in the development of supporting tools and expertise. In accordance with the EU Cybersecurity Act the scheme currently requires Conformity Assessment Bodies to be accredited against ISO 17065 which is an obstacle for auditors that work in accordance with International Standards on Assurance Engagements (ISAE, issued by IAASB) to act as Conformity Assessment Bodies.

Overall the development of the EUCS is taking too long. Development by the Ad Hoc working group started in March 2020 and preparatory work was done by the CSPCert stakeholder group. An important factor in the delay was caused by the inclusion of sovereignty criteria. A discussion that started in October 2020 and still goes on until today. We recommend to separate the discussion on sovereignty from the completion of the scheme and give priority to completing the EUCS without Annex J.

About the Online Trust Coalition

The Online Trust Coalition is a public and private partnership at the initiative of the Dutch Ministry of Economic Affairs and Climate Policy. Its objective is to increase public confidence in cloud services by stimulating the development of harmonized tools that prove the trustworthiness of cloud services to stakeholders. To this end the Online Trust Coalition defined three basic concepts: 1 clear and transparent criteria, 2 independent proof that the criteria are met and 3 clear and understandable communication. In the vision of the Online Trust Coalition transparency, harmonization and re-use of proof are essential elements for installing trust in cloud services.

The Online Trust Coalition is a collaboration of over 30 parties in Government, business and the science sector.

One of the working groups of the Online Trust Coalition is the EU Scheme development group in which members of the Online Trust Coalition participate that are involved in the development and deployment of EU cybersecurity certification schemes. Members of this group meet frequently to monitor the development process and exchanges views and information. The purpose of this group is to align the Dutch contribution to EU scheme development. The information presented in this document is gathered by this group.

General remarks

Transparency

Article 26 of the EU Cybersecurity Act states that ENISA shall carry out its activities with a high level of transparency. In the opinion of the Online Trust Coalition lack of transparency is the major issue in scheme development. We identify a lack of transparency in the communication by ENISA and between the European Commission and ENISA. Overall our concerns relate to:

- The way the Ad-Hoc working groups are composed by ENISA
- Lack of stakeholder (SCCG) involvement during the development process of the schemes
- Changes made to the draft scheme without consulting the Ad-Hoc working group
- Unclarity on how decisions regarding changes to the scheme are made, what steps are taken and how final decisions are made

The Online Trust Coalition calls upon ENISA to evaluate these concerns.

Members of the Ad Hoc working groups are forced to sign a non-disclosure agreement and since the introduction of the sovereignty requirements the EUCS scheme was treated confidential by both ENISA and the European Commission. Even members of the EUCS Ad Hoc working group were not given access to the draft scheme in its (complete) final version. The reason given for this, is that the European Commission did not want discussions on the INL/PUA requirements “in the press”.

Discussions on the INL/PUA requirements were initially based upon the position paper issued by the Online Trust Coalition to ENISA, the European Commission, the European Parliament and the Dutch Ministry of Economic Affairs and Climate Policy in November

2021. Later our concerns were used as input for a non-paper by the Dutch Ministry of Economic Affairs and Climate Policy that was shared among the member states.

Introduction of the INL/PUA requirements is a political decision and should never have been part of the technical development of the EUCS scheme by ENISA and the Ad Hoc working group. This kind of decisions should be made in accordance with rules and procedures for democratic political decision making in de European Union.

In order to prevent politicization of the schemes we call upon ENISA and the European Commission to:

- Make versions of draft schemes easily accessible for the public, especially versions that will be submitted to the ECCG
- Hold public consultations of final drafts, containing fundamental changes other than implementation of European standards
- Strengthen the position of the ECCG in approval of the schemes by simple majority
- Give the SCCG a role in the process of scheme development
- Offer the ECCG the possibility to declare elements of a scheme politically controversial by a simple majority and introduce an escalation procedure in the CSA involving potentially the European Parliament, the Horizontal Working Group for Cyberissues or the Telecom Working Group

Stakeholder involvement

Stakeholder involvement is crucial for the development and acceptance of certification schemes. In addition to the lack of transparency, we also identify a lack of stakeholder involvement.

The mandate of the Stakeholder Cybersecurity Certification Group (SCCG) is described in article 22 under 3 of the Cybersecurity Act and is limited on strategic advisory of the Commission and ENISA (upon request) and assistance regarding the Union Rolling Work Programme. The feedback we received from the SCCG is that their involvement in these topics is currently in practice absent. Furthermore the Cybersecurity Act does not define any involvement of the SCCG in the development or approval of certification schemes. In our opinion the mandate of the SCCG should be extended and their involvement increased.

Stakeholder involvement in the Ad-Hoc working group in our opinion should be improved. In particular the role and functionality of the Ad-Hoc working group should be evaluated, as it is not accessible by all relevant experts, thereby not inclusive.

We strongly recommend to evaluate stakeholder involvement in both the Ad-Hoc working group and the SCCG (mandate and involvement).

Evaluation of the Cybersecurity Certification Framework

Cybersecurity Act as basis for certification of cloud services

The certification framework presented in the Cybersecurity Act is intended to provide cybersecurity certification for ICT products, ICT services and ICT processes. The mutual recognition of certificates between the member states is an important condition. Preambles 68 and 69 of the Act name Senior Officials Group – Information Systems Security (SOG-IS) Mutual Recognition Agreement (MRA) as the most important model for cooperation and mutual recognition in the field of security certification. And therefore SOG-IS is considered an important building stone for the certification framework presented in the Cybersecurity Act. The impact of this decision however is that elements of SOG-IS, especially terminology, are used throughout the Act that are derived from SOG-IS.

SOG-IS is a product certification, performed by laboratories on products that have fixed specifications, behave consistently and in general do not change. If a product changes, a new product appears. Cloud services are volatile, are dependent on human behavior and adherence to procedures. They are tested by auditors for operating effectiveness. This is a different approach from the testing of products in laboratories.

Nevertheless the terminologies used in SOG-IS show a lot of resemblance with terminologies used in the audit of services. As an example the "assurance levels" defined in SOG-IS and used in the Cybersecurity Act have a completely different meaning in the audit of services. This leads to communication gaps that need to be bridged in the schemes.

Voluntary or mandatory?

According to Article 56 (2) of the Cybersecurity Act: "The cybersecurity certification shall be voluntary, unless otherwise specified by Union law or Member State law". Recent developments in other regulations and directives however show a tendency to mandate cybersecurity certification. The EUCS is foreseen to play an important role in the implementation of the NIS2 Directive and also contribute to oversight and enforcement of, among others, the Cyber Resilience Act, e-IDAS2, AI-Act and DORA.

During discussions with ENISA and the European Commission on the proposed sovereignty requirements, the argument that certification is voluntary, is used to waive the need for an impact assessment. Given the importance of cybersecurity certification in the entire regulatory context however, it is our opinion that cybersecurity certification should be treated as mandatory and therefore a thorough impact assessment on the schemes is needed prior to implementation.

Consistency with other legal acts

Over the years the European commission is launching a substantial number of Regulations, Act and Directives that each involve oversight of cloud service providers. As an example: apart from the oversight already in place, providers will now be faced with direct oversight by (or on behalf of) the European Supervisory Authorities (ESA's: EBA, EIOPA and ESMA). The Online Trust Coalition recognizes the importance of regulations and oversight. Equally important however in our opinion is the harmonization of requirements (criteria) and re-use of proof (audit) to reduce the administrative burden it imposes.

We call upon the European Commission to safeguard consistency among legal acts and improve harmonization and opportunities for synergy to keep use of cloud services competitive.

Evaluation of EUCS scheme development

Introduction of PUA requirements

Annex J of the draft scheme contains requirements that aim to safeguard the sovereignty of European cloud services (PUA: Protection against Unlawful Access). These requirements were included without a prior proper economic impact assessment. The Online Trust Coalition conducted a survey on the potential impact of these requirements among providers and users of cloud schemes. The conclusion from this survey is that the potential impact for both providers and users of cloud services is expected to be high. We therefore call upon the European Commission:

- To perform an EU wide assessment of the impact of PUA/INL-criteria on both the level of the cloud market and individual enterprises, taking into account the effects of new regulations;
- To define potential scenarios based on this assessment and validate these scenarios against individual assessments by stakeholders and the objectives of EU's Digital Agenda;
- To detach the implementation of PUA/INL-criteria from finalization of the EUCS scheme, in order to allow sufficient time for the market to prepare and no longer delay implementation of the EUCS

The full report is available at https://onlinetrustcoalitie.nl/wp-content/uploads/2023/07/23.06.15_OTC_PUA-INLrapport.pdf

Furthermore the risk that the PUA requirements conflict with other international treaties and agreements should be assessed. As an example some organizations and legal experts claim that the PUA requirements conflict with the General Agreement on Trade in Services (GATS) by the WTO,

Use of standards

The use of (European or international) standards is essential for the mutual recognition of the cybersecurity certificates and also for the effectiveness of all legal acts affected. Article 54 (1.c) of the EU Cybersecurity Act requires that the schemes shall at least include references to international, European or national standards applied. Reference is made to Regulation (EU) 1025/2012. Recital 69 of that same act states that the European

cybersecurity certification schemes should be based on European or international standards. Requirements of certification schemes therefore should be based on existing standards. The framework does however not indicate for which elements of the scheme the use of (European or international) standards is mandatory.

At the beginning of the scheme development, an assessment is made by ENISA on what European standards can be used and for which parts of the scheme no suitable standards are available. This assessment is an important starting point for the development of the scheme, however the gap assessment was not made public. In the case of the EUCS, ENISA started the scheme development by defining the criteria and the meta-approach which were afterwards submitted for review to CEN-CENELEC. In our opinion this was an important reason for the delay in the development of the scheme. For future scheme developments we recommend to perform the gap assessment together with industry experts from the Ad-Hoc working group or the SCCG and if gaps are defined, first explore the development of European standards before developing taylor made solutions by ENISA.

The draft EUCS scheme contains important elements that are not standardized (e.g. Annex J) or are submitted for review to CEN-CENELEC but are not standards (the security requirements in Annex A and the Meta-approach).

The Online Trust Coalition recommends to specifically define which elements of a scheme require mandatory use of acknowledged standards as well as the procedure to be used when standards are not available.

Supporting tools and expertise

Cybersecurity is a very volatile topic and threats and controls change almost on a daily basis. Currently the scheme contains a very detailed set of criteria that are generally considered to be state of the art. These criteria must also provide guidance both for parties responsible for cybersecurity of cloud services and auditors acting as Conformity Assessment Bodies for the cybersecurity certification. For an effective common level of cybersecurity and resilience throughout the European Union, the challenge is to reflect the volatility of the topic in the scheme's criteria and conformity assessment. We are concerned that for the execution of the scheme in the European Union insufficient tooling and expertise is available. We therefore strongly recommend to invest in the development of supporting automation, including AI and the training of auditors and monitoring of the work performed by CAB's.

The draft scheme in accordance with the EU Cybersecurity Act requires Conformity Assessment Bodies to be accredited against ISO 17065. This is an obstacle for auditors that work in accordance with International Standards on Assurance Engagements (ISAE, issued by IAASB) to act as Conformity Assessment Bodies. Allowing ISAE auditors to act as Conformity Assessment Bodies will not only increase the pool of expertise for EU cybersecurity certification, it will also lead to synergy with financial audits.

Finalization of the EUCS

The objectives of EU cybersecurity certification are too important to get delayed by political discussions. Development of the EUCS started in March 2020 and currently the implementation act has not been finalized. It is expected that when the Cybersecurity Act

will celebrate its 5th anniversary in June 2024, not a single certificate will be delivered. It is simply taking too long.

The Online Trust Coalition calls upon the European Commission to detach the discussion on the PUA requirements from the finalization of the EUCS and implement the scheme for the time being without Annex J.