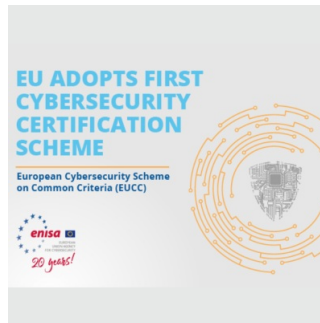

An EU Prime! EU adopts first Cybersecurity Certification Scheme



The European Cybersecurity Scheme on Common Criteria (EUCC) drafted by the European Union Agency for Cybersecurity (ENISA) has been adopted as the first scheme within the EU cybersecurity certification framework.

The European Commission adopted the implementing regulation concerning the EU cybersecurity certification scheme on Common Criteria (EUCC). The outcome is fully in line with the candidate cybersecurity certification scheme on EUCC that ENISA drafted in response to a request issued by the European Commission. In drafting the candidate scheme, ENISA was supported by an Ad-hoc working group (AHWG) composed by area experts from across the industry and EU Member States National Cybersecurity Certification Authorities (NCCAs).

ENISA is grateful for the guidance and support received by Member States via the European Cybersecurity Certification Group (ECCG), as well as for the contributions of the Stakeholder Cybersecurity Certification Group (SCCG).

As the first EU cybersecurity certification scheme to be adopted, it is expected that the EUCC paves the way for the next schemes that are currently in preparation. While an implementing act is part of the “acquis communautaire”, the EU Law, the cybersecurity certification framework is voluntary. In time, EUCC will replace national certification schemes previously under the SOG-IS agreement.

EU Agency for Cybersecurity Executive Director, Juhan Lepassaar underscored that “The adoption of the first cybersecurity certification scheme marks a milestone towards a trusted EU digital single market and it is a piece of the puzzle of the EU cybersecurity certification framework that is currently in the making.”

What is EUCC?

As provided for by the 2019 Cybersecurity Act, the new scheme falls under the EU cybersecurity certification framework. The objective of this framework was to raise the level of cybersecurity of ICT products, services and processes in the EU Market. It does so by setting a comprehensive set of rules, of technical standards requirements, standards and procedures to be applied across the Union.

Voluntary-based, the new EUCC scheme allows ICT suppliers who wish to showcase proof of assurance to go through an EU commonly understood assessment process to certify ICT products such as technological components (chips, smartcards), hardware and software.

The scheme is based on the time-proven SOG-IS Common Criteria evaluation framework already used across 17 EU Member States. It proposes two levels of assurance based on the level of risk associated with the intended use of the product, service or process, in terms of probability and impact of an accident.

Based on extensive research and consultation, the comprehensive scheme has been tailored to the needs of the EU Member States. The Union-wide mechanisms of certification therefore allow European businesses to compete at national, Union and global level.

In other words, EU certification schemes such as EUCC are expected to also stand as an incentive for suppliers to adhere to cybersecurity certification requirements. The EUCC enters the vibrant market of cyber certifications studied in the new report published by ENISA carrying on the evolution of the number of assessment methodologies and bodies dedicated to ICT products and services.

Adoption process and next steps

Together with the ad-hoc working group, ENISA compiled the candidate scheme with the security requirements and commonly accepted

assessment methods defined and agreed to.

ENISA transmitted the drafted scheme to the European Commission after the ECCG issued its opinion. The implementing act issued by the European Commission as a result was subsequently adopted under the relevant procedure known as the comitology procedure.

The adopted act foresees a transition period during which organisations will still be able to benefit from existing certifications under national schemes across selected Member States. Conformity Assessment Bodies (CABs) interested in assessing against EUCC can be accredited and notified. Vendors will be able to convert their existing SOG-IS certificates into EUCC ones after assessing their solutions against added or updated requirements as specified in the EUCC.

Certificates issued under EUCC will be published by ENISA. ENISA also publishes the Implementing Act and supporting documents such as annexes, state of the art documents and guidance on the dedicated certification website. The European Union Agency for Cybersecurity is also proposing support material including a video on the latest developments of the scheme and in support of its implementation.

Other EU Cybersecurity Certification Schemes

ENISA is currently working on two more cybersecurity certification schemes, EUCS on cloud services and EU5G on 5G security. The Agency has also undertaken a feasibility study on an EU cybersecurity certification requirements on AI and is supporting the European Commission and Member States to establish a certification strategy for the eIDAS/wallet. More recently the [European Commission proposed an amendment to the Cybersecurity Act](#) that foresees a scheme for managed security services (MSSPs).

Source & Image Credit: [ENISA](#)

Published on : Wed, 31 Jan 2024