

The EU cybersecurity certification framework

The EU cybersecurity certification framework for ICT products enables the creation of tailored and risk-based EU certification schemes.



© iStock by Getty Images -1159281243 Wojtek Skora

Certification plays a crucial role in increasing trust and security in important products and services for the digital world. At the moment, a number of different security certification schemes for ICT products exist in the EU. But, without a common framework for EU-wide valid cybersecurity certificates, there is an increasing risk of fragmentation and barriers between Member States.

The certification framework will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. The framework will be based on agreement at EU level on the evaluation of the security properties of a specific ICT-based product or service. It will attest that ICT products and services that have been certified in accordance with such a scheme comply with specified requirements.

In particular, each European scheme should specify:

- the categories of products and services covered;
- the cybersecurity requirements, such as standards or technical specifications;
- the type of evaluation, such as self-assessment or third party;
- the intended level of assurance.

The assurance levels are used to inform users of the cybersecurity risk of a product, and can be basic,

substantial, and/or high. They are commensurate with the level of risk associated with the intended use of the product, service or process, in terms of probability and impact of an accident. A high assurance level would mean that the certified product passed the highest security tests.

The resulting certificate will be recognised in all EU Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product or service.

As for the implementation of the certification framework, Member State authorities, gathered in the European Cybersecurity Certification Group (ECCG) have already met several times.

Stakeholder Cybersecurity Certification Group

Following the entry into force of the Cybersecurity Act in 2019, the European Commission launched a call for applications to select members of the Stakeholder Cybersecurity Certification Group (SCCG).

The SCCG will be responsible for advising the Commission and ENISA on strategic issues regarding cybersecurity certification, and assisting the Commission in the preparation of the Union rolling work programme. This is the first stakeholder expert group for cybersecurity certification launched by the European Commission.

Follow the work of the Group

Follow the latest progress and learn more about getting involved.

Follow the Commission's work on cybersecurity @CyberSec_EU

Latest

PRESS RELEASE | 30 September 2021

Trade and Technology Council: Inaugural meeting
agrees on important deliverables and outlines
areas for future EU-US cooperation

At the first meeting of the Trade and Technology
Council (TTC) in Pittsburgh, the EU and the US
agreed on concrete deliverables and outlined the

future scope of work. Notably, the EU and the US committed to cooperating closely on shared priorities such as export controls, foreign investment screening, critical and emerging technology standards including Artificial Intelligence, and secure supply chains including on semiconductors. They also agreed to work together on important global trade issues, such as the challenges posed by non-market economies and trade-related climate and environment

PRESS RELEASE | 30 September 2021

The European Cybersecurity Month is kicking off: 'Think Before U Click'

The ninth edition of the European Cybersecurity Month has kicked off and will run for the entire month of October under the motto 'Think Before U Click'. This is an annual awareness campaign organised by the Commission, the European Union Agency for Cybersecurity (ENISA) and over 300 partners in the Member States, including local authorities, governments, universities, think tanks, NGOs and professional associations.

PRESS RELEASE | 28 June 2021

The European Cybersecurity Competence Centre and Network is now ready to take off

The regulation establishing a new Cybersecurity Competence Centre and a Network of National Coordination Centres has entered into force this week. The Cybersecurity Competence Centre, which will be located in Bucharest, will contribute to strengthening European cybersecurity capacities and to boosting research excellence and the competitiveness of the Union's industry in the cybersecurity field.

PRESS RELEASE | 23 June 2021

EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents

The Commission has laid out a vision to build a new Joint Cyber Unit to tackle the rising number of serious cyber incidents impacting public services, as well as the life of businesses and citizens across the European Union. Advanced and coordinated responses in the field of cybersecurity have become increasingly necessary, as cyberattacks grow in number, scale and consequences, impacting heavily our security. All relevant actors in the EU need to be prepared to respond collectively and exchange relevant information on a 'need to share', rather than only 'need to know', basis.

[Browse Cybersecurity](#)

Related Content

Big Picture

Cybersecurity Policies

The European Union works on various fronts to promote cyber resilience, safeguarding our communication and data and keeping online society and economy secure.

See Also

European Cybersecurity Competence Network and Centre

The European Cybersecurity Network and Cybersecurity Competence Centre help the EU retain and develop cybersecurity technological and industrial capacities.

Stakeholder Cybersecurity Certification Group

The Stakeholder Cybersecurity Certification Group was established to provide advice on strategic issues regarding cybersecurity certification.

The EU Cybersecurity Act

The Cybersecurity Act strengthens the EU Agency for cybersecurity (ENISA) and establishes a cybersecurity certification framework for products and services.

NIS Directive

The NIS Directive is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.

Source URL: <https://digital-strategy.ec.europa.eu/policies/cybersecurity-certification-framework>