The European Cybersecurity Act

EUROSMART

The Voice of the Digital Security Industry

THE CYBERSECU

- **Permanent mandat cybersecurity certif**
- **ENISA is tasked w schemes, acting on**
- **There are three lev substantial and hig**
- **The possibility to p assurance level;**
- **A triple role for nat**
  - **Accredi**
  - **Supervi in acco Regulat**
  - **Issuing for the**
- **Voluntary certifica latest, a list of pr certification schem**
- **Creation of a Stak stakeholders to ad**

Towards the Cybersecurity Act

On 13 September 2017, Jean-Claude Juncker announced in his annual State of the Union address that protection of Europeans in the digital era is one of the European Union's key priorities. He recalled that 4000 ransomware attacks were recorded in 2016. He explained that the Union needs new tools to combat cyberattacks and notably a European Agency for Cybersecurity.

RITY ACT AT A GLANCE

te for ENISA and broader expertise, notably in terms of fication;

vith drawing up European cybersecurity certification a proposal from the Commission;

vels of assurance level with various requirements: basic, h;

perform a self-assessment of compliance with the basic

ional cybersecurity certification authorities;

tation of conformity assessment bodies;

sion of certificates or statements of conformity issued rdance with the requirements of the scheme and the ion;

of certificates for assurance level high and in some cases lower levels;

tion but the Commission will establish by 2023, at the oducts, services and processes covered by an existing e which should be covered by a mandatory scheme;

eholder Cybersecurity Certification Group composed of vise ENISA on certification.

The same day, the European Commission published its "cybersecurity package", a set of initiatives aimed at strengthening resilience, deterrence and the defence of the Union in the face of cyberattacks. These measures include a proposal for a regulation on ENISA and certification of cybersecurity information technologies and communications (Cybersecurity Act – COM (2017) 477). The Regulation gives ENISA a permanent mandate and strengthens its role in prevention, advice and cooperation. The Cybersecurity Act has a second component which is to create a European cybersecurity certification framework in which ENISA will play an essential role.

In spring 2019 the Regulation was finally adopted by the European Parliament and by the Council of the EU. It should enter into force in mid-2019.

The Cybersecurity Act contains provisions which will have a major impact on the field of cybersecurity in Europe, particularly with the creation of European cybersecurity certification schemes. These schemes may contribute to the consolidation of the single market solving current problems related to the fragmentation of European certification schemes.

Forewords

Cybersecurity - acting local

Prof. Dr. Angelika NIEBLER
Member of the European
Rapporteur of the Cyberse

Many people still think of cyber-attacks as science fiction and a story that makes for a good Hollywood movie. But that's not the case anymore! One of the major attacks already happened in 1999 followed by a high number of attacks including "WannaCry" in 2017 that infected 300.000 computers in 150 countries demanding users to hand over money in exchange for keys to de-encrypt files. In the last year, 80% of European companies fell victim to at least one cybersecurity incident. These developments threaten our society and industry and called for the EU to react. And we did react!

With the recently adopted Cybersecurity Act, European Parliament wanted to tackle in particular two issues: The first issue relates to the increasing number of attacks on our critical infrastructure, which means on all aspects of our daily lives - electricity, communication, water etc. The second issue relates to the increasing number of internet of things-devices and the user's mistrust in the safety and privacy of their devices.

The European Parliament worked hard to ensure a strong European response to the increasing number of threats. The result is the establishment of a European cybersecurity certification fra which will be voluntary at first, but the Commission is obliged to assess whether certification schemes shall be made m in particular in view of critical infras We have also strengthened the st involvement in the certification process the European Commission to come up wi programme on upcoming certification sch more transparency and strengthened E European cybersecurity agency.

My other mission as rapporteur of the Cybe Act was to make sure that all users of in things-devices could place trust in the s security of their products. With more a devices and services connected to the users are increasingly put at risk of cybe By 2020 the vast majority of our digital int will be machine to machine with tens of internet of things-devices. As we all know are often the biggest security risk. We do n our passwords regularly, protect our hom and smart home appliances and most p not patch often enough. However, the

thinking global,

R
Parliament
ecurity Act

amework, European particular mandatory, tructures. akeholder s; obliged ith a work hemes for NISA, the

ersecurity nternet of afety and and more internet, er-attacks. teractions billions of w, humans ot change he routers people do user can

help create a safe environment and therefore, he has to play an active role. In order to support the user,

product information for smart devices must now be provided, so that users are given guidance and learn about secure configurations and maintenance of their devices, availability and duration of updates and known vulnerabilities. If users follow these recommendations, it will provide for more cybersecurity and resilience.

Europe needs a cyberspace that is safe and secure and the Cybersecurity Act contributes to this target.

ENISA
The European Cybersecurity Agency

MANDATE AND OBJECTIVES OF ENISA

ENISA's current mandate ends in 2020 but the Cybersecurity Act gives the Agency a permanent mandate ensuring its longevity (Article 68).

The Regulation stipulates that the objective of ENISA is to increase the common level of cybersecurity across the Union, including by actively supporting the activities of Member States, Union institutions, bodies, offices and agencies. Furthermore, ENISA must contribute to reducing fragmentation of the internal market (Article 3). ENISA is therefore tasked with drawing up European cybersecurity certification schemes as detailed in Title III of the Regulation with a view to reducing this fragmentation.

ENISA TASKS

DEVELOPMENT AND IMPLEMENTATION OF UNION LAW (ARTICLE 5)

ENISA shall:

- provide independent analysis and preparatory work on the development and review of Union policy and law in the field of cybersecurity. It will do the same on sector-specific policies involving cybersecurity matters.
- assist Member States to implement consistently the Union policy and law regarding cybersecurity, in particular in relation to NIS Directive (EU) 2016/1148;
- facilitate the exchange of best practices between competent authorities.

CAPACITY-BUILDING (ARTICLE 6)

ENISA shall:

- provide Member States and Union institutions the knowledge and expertise necessary to improve the prevention, detection and analysis of cyber threats and incidents, together with the ability to react;
- support the strengthening of national and Union CSIRTs notably by promoting dialogue and the exchange of information;
- organise at least twice a year cybersecurity exercises at the Union level;
- assist Member States in the exchange of best practices especially with regard to identifying operators of essential services.

OPERATIONAL COOPERATION AT UNION LEVEL (ARTICLE 7)

ENISA shall:

- cooperate at the operational level and establish synergies with Union institutions, bodies, offices and agencies, including the CERT-EU, with the services dealing with cybercrime and with supervisory authorities dealing with the protection of privacy and personal data, with a view to addressing issues of common concern;
- provide the Secretariat for the network of CSIRTs;
- contribute to cooperation on the operational level within the CSIRT network through the support it offers Member States;
- organise regular cybersecurity exercises at the Union level and following a request to do so support Member States and Union institutions, bodies, offices and agencies in organising cybersecurity exercises. A large-scale comprehensive exercise should be organised every two years;
- contribute to sectoral cybersecurity exercises;
- prepare in close cooperation with the Member States, a regular report on the technical situation of cybersecurity incidents and threats in the EU;
- contribute to the development of a cooperative response at Union and Member States level to large-scale cross-border incidents or crises related to cybersecurity.

MARKET, CYBERSECURITY CERTIFICATION, AND STANDARDISATION (ARTICLE 8)

ENISA shall:

- support and promote the development and implementation of Union policy on cybersecurity certification of ICT products and services as established in Title III of the Regulation;
- facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products, services and processes.
- draw up, in collaboration with Member States and industry, advice and guidelines regarding the technical areas related to the security requirements for operators of essential services and digital service providers, as well as regarding already existing standards, including Member States' national standards, pursuant to Article 19(2) of NIS Directive (EU) 2016/1148;
- perform and disseminate regular analyses of the main trends in the cybersecurity market on both the demand and supply sides, with a view to fostering the cybersecurity market in the Union.

KNOWLEDGE AND INFORMATION (ARTICLE 9)

ENISA shall:

- perform analyses of emerging technologies and provide topic-specific assessments on the expected societal, legal, economic and regulatory impact of technological innovations on cybersecurity;
- perform long-term strategic analyses of cybersecurity threats and incidents;
- provide advice, guidance and best practices for the security of network and information systems, in cooperation with experts from Member States and stakeholders;
- pool, organise and make available to the public through a dedicated portal information on cybersecurity;
- collect and analyse publicly available information regarding significant incidents and compile reports with a view to providing guidance to businesses and private individuals across the Union.

AWARENESS-RAISING AND EDUCATION (ARTICLE 10)

ENISA shall:

- raise public awareness of cybersecurity risks, and provide guidance on best practices for users aimed at private individuals and organisations;
- organise regular outreach campaigns in cooperation with the Member States, Union institutions, bodies, offices and agencies to increase cybersecurity and its visibility in the Union and encourage public debate;
- assist Member States in their efforts to raise cybersecurity awareness and promote cybersecurity education;
- facilitate closer coordination and exchange of best practices amongst Member States on cybersecurity education and awareness.

RESEARCH AND INNOVATION (ARTICLE 11)

ENISA shall:

- advise the Union and Member States on research needs and priorities in the field of cybersecurity;
- participate, where the Commission has conferred the relevant powers, in the implementation phase of research and innovation funding programmes or as a beneficiary;
- contribute to the strategic research and innovation agenda at Union level in the field of cybersecurity.

INTERNATIONAL COOPERATION (ARTICLE 12)

ENISA shall contribute to the Union's efforts to cooperate with third countries and international organisations as well as within relevant international cooperation frameworks by:

- engaging, where appropriate, as an observer in the organisation of international exercises;
- facilitating, at the request of the Commission, the exchange of best practices;
- providing, at the request of the Commission, its expertise;
- providing recommendations and assistance to the Commission on matters concerning agreements for the mutual recognition of cybersecurity certificates with third countries, in collaboration with the Member States certification group established under Article 53.

GOVERNANCE OF ENISA (ART.13)

Body	Composition / Appointment	Tasks	Members' term of office
MANAGEMENT BOARD (Art. 14-18)	One representative from each Member State Two representatives appointed by the Commission	Establish the general direction of the functioning of ENISA; Adopt, taking into account the Commission's opinion, ENISA's single programming document; Adopt ENISA's annual budget; Adopt the rules on the internal functioning of ENISA; Appoint the Executive Director and where relevant extend his or her term of office or remove him or her from office.	4 years, renewable
EXECUTIVE BOARD (Art. 19)	Five members appointed from amongst the members of the Management Board, including its Chairperson and one of the representatives of the Commission.	Prepare decisions to be adopted by the Management Board; Ensure, together with the Management Board, the adequate follow-up to the findings and recommendations stemming from investigations of OLAF and the various internal or external audit reports and evaluations; Assist and advise the Executive Director in implementing the decisions of the Management Board on administrative and budgetary matters.	4 years, renewable
EXECUTIVE DIRECTOR (Art. 20 and Art. 36)	Appointed by the Management Board from a list of candidates proposed by the Commission. The Executive Director may be removed from office only by decision of the Management Board, acting on a proposal from the Commission.	Ensure the day-to-day administration of ENISA; Implement the decisions adopted by the Management Board; Prepare and implement once approved the single programming document; Develop and maintain contact with the business community and consumer organisations to ensure regular dialogue with relevant stakeholders;	5 years, renewable once

Body	Composition / Appointment	Tasks	Members' term of office
		Liaise regularly with Union institutions, bodies, offices and agencies regarding their activities in the field of cybersecurity to ensure coherence in the development and implementation of European policies; If necessary, set up ad hoc working groups composed of experts, including experts from the Member States' competent authorities. The Management Board having been previously informed.	
ENISA ADVISORY GROUP (Art. 21)	Set up by the Management Board acting on a proposal from the Executive Director. Composed of recognised experts representing the relevant stakeholders, such as the ICT industry, providers of electronic communications networks or services available to the public, SMEs, operators of essential services, consumer groups, academic experts in the field of cybersecurity, and representatives of competent authorities notified in accordance with Directive 2016/0288**,** European standardisation organisations, as well as of law enforcement and data protection supervisory authorities. The Group is chaired by the Executive Director or by the person the Executive Director appoints. Members of the Management Board cannot be members of this Group.	Advise ENISA on the performance of its activities except on the implementation of Title III (certification) of the Regulation; Advise the Executive Director during the preparation of a proposal for ENISA's annual work plan; Advise the Executive Director on communication with the relevant stakeholders on issues relating to the annual work programme;	2.5 years

Body	Composition / Appointment	Tasks	Members' term of office
NATIONAL LIAISON OFFICERS NETWORK (Art. 23)	The National Liaison Officers Network is set up by the Management Board acting on a proposal from the Executive Director. The Network is composed of representatives of the Member States. Each Member State appoints one representative.	Facilitate the exchange of information between ENISA and Member States; Support ENISA in disseminating its activities, findings and recommendations; Facilitate cooperation between ENISA and national experts in the context of the implementation of the annual work programme;	Not specified in the Regulation

STAKEHOLDER CYBERSECURITY CERTIFICATION GROUP (ARTICLE 22)

The Stakeholder Cybersecurity Certification Group (Article 22)

The Stakeholder Cybersecurity Certification Group was not in the Commission's initial proposal. It is a new element introduced by the European Parliament during the legislative procedure.

The Group is composed of members selected from amongst recognised experts representing the relevant stakeholders. The European Commission chooses the members acting on a proposal from ENISA, through a transparent and open call for applicants.

Stakeholder Cybersecurity Certification Group:

- advises the Commission on strategic issues regarding the European cybersecurity certification framework;

- upon request, advises ENISA on general and strategic matters concerning ENISA's tasks relating to the market, cybersecurity certification, and standardisation;

- assists the Commission in the preparation of the Union rolling work programme;

- issues an opinion on the programme;

- in urgent cases, provides advice to the Commission and the ECCG on the need for additional certification schemes not included in the Union work programme.

The Group is co-chaired by the Commission and ENISA.

The European Cybersecurity Certification Framework

Title III of the Cybersecurity Act establishes a European cybersecurity certification framework. The framework aims to improve the functioning of the internal market by increasing cybersecurity within the Union and offering a harmonised approach to certification schemes. It defines a mechanism to establish European certification schemes and confirm that ICT products, services and processes certified in accordance with these schemes satisfy the specified security requirements.

The Cybersecurity Act details the objectives of the European cybersecurity certification schemes (Article 51) as well as the elements of a European certification schemes (Article 54).

NATIONAL CYBERSECURITY CERTIFICATIONS AUTHORITIES (ARTICLE 58)

Each Member State designates one or more national cybersecurity certification authorities in its territory or with mutual agreement, in the territory of another Member State (Article 58). These authorities have a key role in accrediting the conformity assessment bodies (Article 60) but also in issuing certificates, particularly for the high assurance level (Article 56(6)). These two points will be developed later.

Furthermore, the national authorities ensure that in their respective territories the certified ITC products, processes and services effectively satisfy the requirements associated with the certificates issued. They are also in charge of monitoring manufacturers or providers who perform a conformity self-assessment to make sure that they effectively respect the obligations mentioned in the Regulation. The national authorities are required to cooperate amongst themselves by sharing information on the possible non-compliance of processes, products or services with the requirements of the Regulation or scheme.

The final version of the text establishes in Article 59 a peer review mechanism amongst national certification authorities. The objective is to ensure that the certifications and statements of conformity effectively correspond to the same requirements from one Member State to another. The peer review is notably aimed at guaranteeing that national authorities have put in place a strict separation of the roles and responsibilities of their certificate issuing and their supervision activities.

EUROPEAN CYBERSECURITY CERTIFICATION GROUP ECCG (ARTICLE 62)

National cybersecurity certification authorities take part in the European Cybersecurity Certification Group (ECCG) or the European Cybersecurity Certification Group. Other relevant national authorities may also take part in the ECCG.

The Group notably has the task of:

- advising and assisting the Commission in its work to ensure the consistent implementation and application of the provisions of the Regulation, in particular regarding the Union rolling work programme;
- assisting, advising and cooperating with ENISA in relation to the preparation of a candidate scheme;
- adopting an opinion on candidate schemes;
- requesting ENISA to prepare European candidate cybersecurity certification schemes pursuant to Article 48(2) of the Regulation;
- adopting opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes;
- facilitating the cooperation between national cybersecurity certification authorities through capacity-building and the exchange of information;
- facilitating the alignment of European cybersecurity certification schemes with internationally recognised standards, including by reviewing existing European cybersecurity schemes and, where appropriate, making recommendations to ENISA to engage with relevant international standardisation organisations to address insufficiencies or gaps in internationally recognised standards.

The Commission shall chair the Group and provide the secretariat with the assistance of ENISA. Interested stakeholders may be invited to attend meetings of the Group and to participate in its work.

DEVELOPMENT OF A EUROPEAN CERTIFICATION SCHEME

WORK PROGRAMME (ARTICLE 47)

It identifies strategic priorities for future European cybersecurity certification schemes. The programme

shall in particular include a list of ICT products, services and processes or categories that are capable of benefiting from being included in the scope of a European cybersecurity certification scheme. During the development of its programme, the Commission can take into account the opinions of the ECCG and the Stakeholder Certification Group.

The first programme will be published at the latest one year after the entry into force of the Regulation. It should be updated as often as necessary but, in any case, at least once every three years.

INITIATIVE (ARTICLE 48)

European cybersecurity certification schemes are prepared by ENISA at the request of the Commission (for the most part) or by the ECCG.

The Commission may request ENISA to prepare a candidate cybersecurity certification scheme or to review an existing scheme on the basis of the work programme. In duly justified cases, the Commission may also ask ENISA to prepare a candidate scheme or to review an existing scheme which is not included in the work programme (Article 48).

The ECCG also has a power of initiative but it is more limited. In duly justified cases, it can ask ENISA to prepare a candidate scheme or to review an existing scheme which is not included in the work programme (Article 48).

A difference is therefore observed between the initiative of the Commission and the initiative of the ECCG. If the Commission issues a request to prepare a scheme, ENISA is obliged to prepare it. If, on the other hand the request comes from the ECCG, ENISA's Management Board may reject the request but ENISA must justify its decision (Article 49).

PREPARATION OF SCHEMES (ARTICLE 49)

When preparing a candidate scheme, ENISA consults all relevant stakeholders by means of a formal, open, transparent and inclusive consultation process. For each candidate scheme, ENISA establishes an ad hoc working group in accordance with Article 20(4) of the Regulation which provides ENISA with its expertise and recommendations.

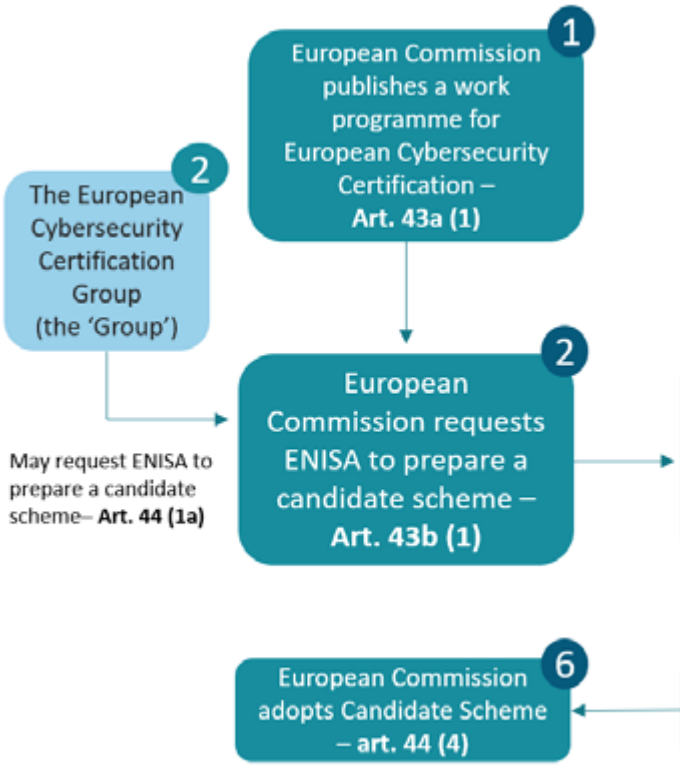
ENISA works in close collaboration with the ECCG which provides ENISA with assistance and an expert opinion on the preparation of a candidate scheme. ENISA is required to take into account the opinion of the ECCG before transmitting the candidate scheme to the Commission. However, the ECCG's opinion is not legally binding.

IMPLEMENTING ACTS (ARTICLE 49(7))

The Commission, based on the candidate scheme prepared by ENISA, may adopt implementing acts providing for European cybersecurity certification schemes for ICT products, services and processes.

EVALUATION AND REVIEW OF SCHEMES (ARTICLE 49(8))

At least every 5 years, ENISA evaluates each adopted European cybersecurity certification scheme, taking into account the feedback received from relevant stakeholders. If necessary, the Commission or the ECCG may request ENISA to begin the preparation process for a revised candidate scheme.



ASSURANCE LEVELS (ARTICLE 52)

A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, services and processes certified within the framework of the scheme: basic, substantial or high. The assurance level is proportional to the level of risk in terms of the probability of an incident and its impact. The level also depends on the intended use of the product, service or process.

The levels of assurance basic, substantial and high refer to a certificate or statement of conformity issued within the framework of a European certification scheme. Every assurance level has a set of security requirements, notably relating to security functionalities and the amount of effort needed to assess the product, process or service. The certificate or statement of conformity shall refer to technical specifications, standards and procedures, including technical controls, the purpose of which is to decrease the risk of cybersecurity incidents.

Basic, substantial and high assurance levels respectively satisfy the following criteria:

BASIC

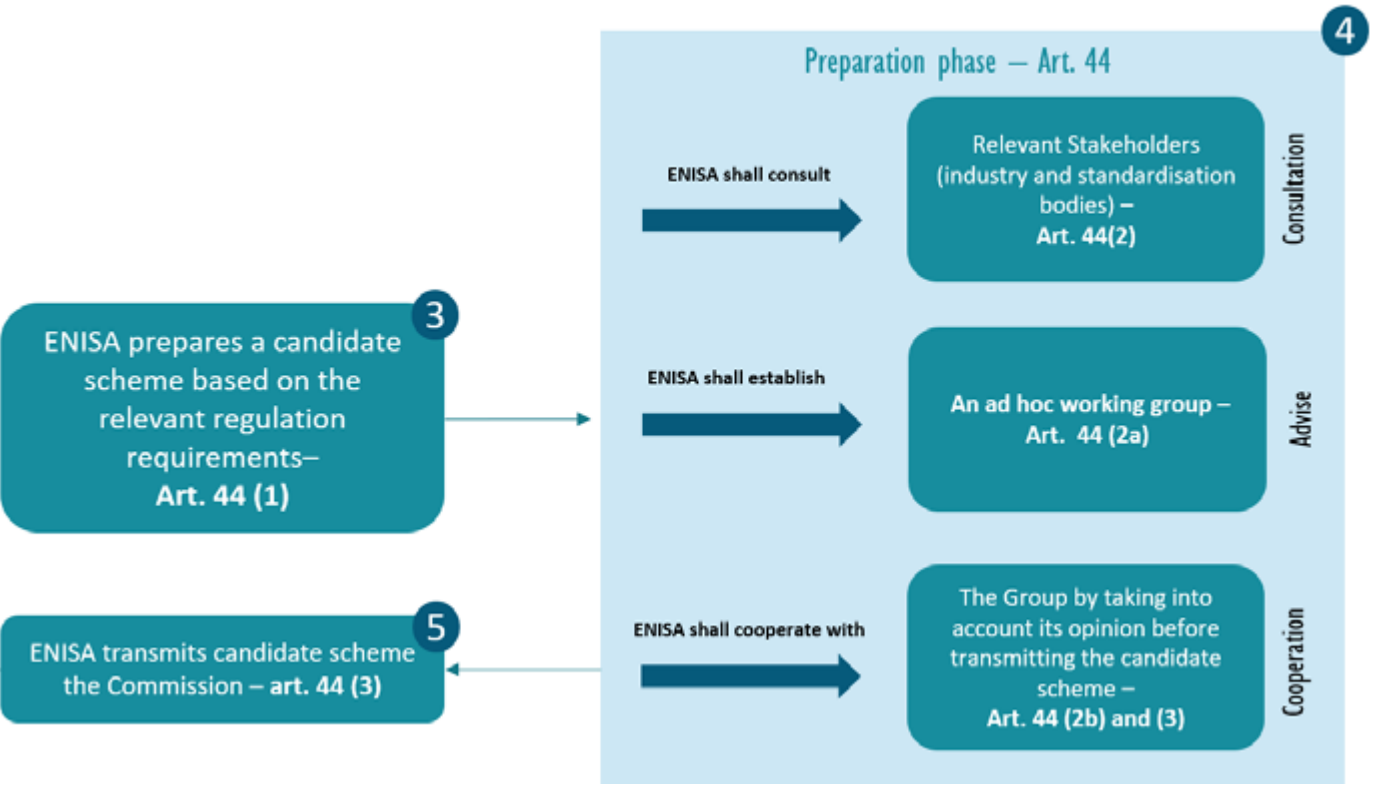
A European cybersecurity certificate or an EU statement of conformity referring to assurance level 'basic' provides assurance that the ITC products, services and processes meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known basic risks of cyberincidents and cyberattacks.

- The evaluation activities should include at least a review of the technical documentation or, failing that, substitute evaluation activities with equivalent effect.

SUBSTANTIAL

A European cybersecurity certificate referring to assurance level 'substantial' provides assurance that the ITC products, services and processes

reparation and adoption: articles 43a, 43b, 44



meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise cybersecurity risks, cyberincidents and cyberattacks carried out by actors with limited skills and resources.

- The evaluation activities should include at least:
  a review to demonstrate the absence of known vulnerabilities;
  testing to demonstrate that the products, service or processes correctly implement the security functionalities;
  failing that, substitute evaluation activities with equivalent effect.

HIGH

A European cybersecurity certificate referring to assurance level 'high' provides assurance that the ITC products, services and processes meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources.

- The evaluation activities should include at least:
  a review to demonstrate the absence of known vulnerabilities;
  testing to demonstrate that the products, service or processes correctly implement the security functionalities;
  an assessment of their resistance to skilled attackers using penetration testing;
  failing that, substitute activities.

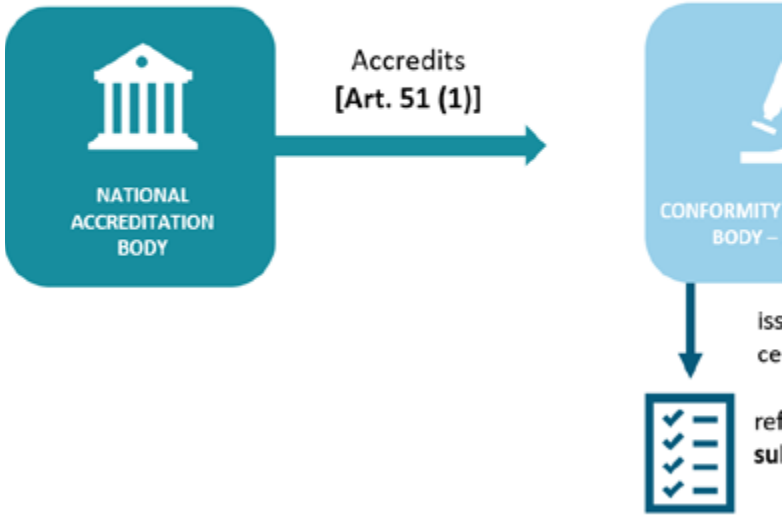
Regardless of the assurance level, the certificate holder is required to inform the certificate issuing body of any subsequently detected vulnerabilities or irregularities concerning the security of the certified processes, products or services that may have an impact on its compliance with the requirements related to the certification.

FROM VOLUNTARY TO MANDATORY CERTIFICATION (ARTICLE 56(3))

The Regulation explicitly states that certification is voluntary unless European or national law provides otherwise.

However, the Commission must regularly assess, starting at the latest by 31 December 2023 and every two years thereafter, the efficiency and use of the adopted certification schemes. The Commission must notably assess if a specific scheme is to be made compulsory through relevant Union law to ensure an adequate level of cybersecurity of products, services and processes and improve the functioning of the internal market. Based on its assessment, the Commission will identify the products, services and processes covered by an existing certification scheme which should be covered by a mandatory scheme.

Conformity



As a priority, the Commission must focus on the sectors listed in Annex II of NIS Directive (EU) 2016/1148, which will be assessed at the latest two years after the adoption of the first scheme.

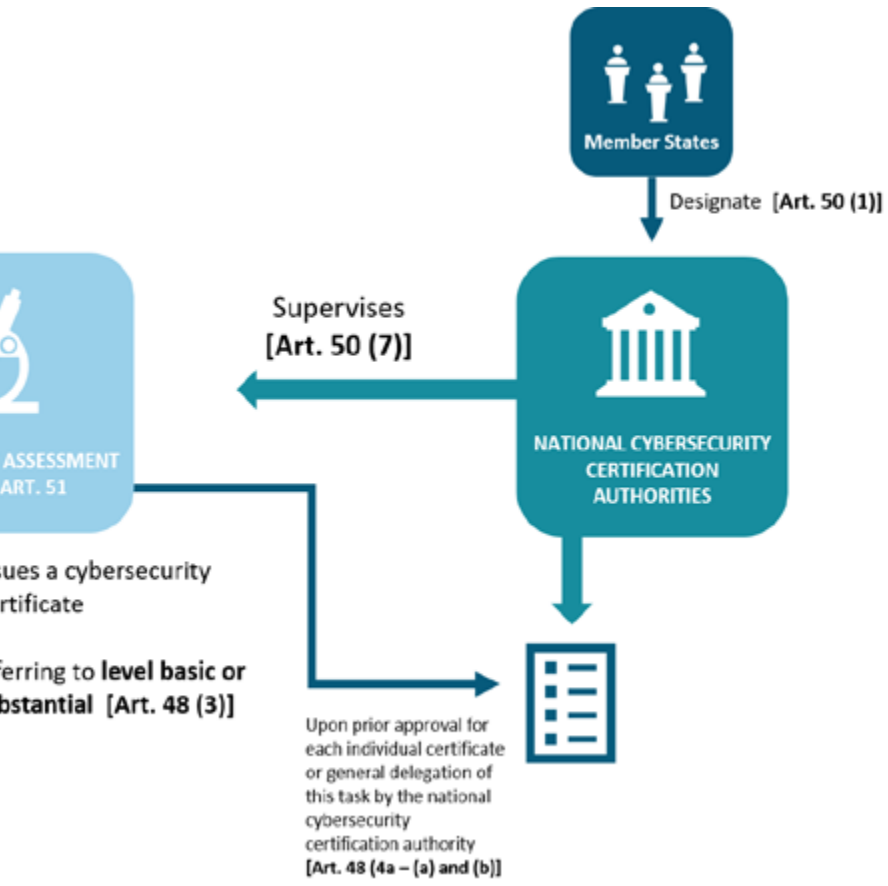
CONFORMITY ASSESSMENT BODIES (ARTICLE 60)

For each European cybersecurity certification scheme, the national cybersecurity certification authorities are required to notify the Commission of the conformity assessment bodies that have been accredited to issue certificates at specified assurance levels. One year after the entry into force of a European cybersecurity certification scheme, the Commission will publish in the Official Journal of the European Union a list of the notified conformity assessment bodies. National authorities must inform the Commission, without undue delay of any subsequent changes to the list.

A national cybersecurity certification authority may submit to the Commission a request to remove a conformity assessment body notified by that authority from the list. The Commission will publish the corresponding amendments to that list in the Official Journal within one month of the date of receipt of the national authority's request.

The requirements that conformity assessment bodies must satisfy in order to be accredited are detailed in the Annex to the Regulation. Conformity assessment bodies are independent of the organisation or the ICT products, services or processes that they asses. Nevertheless, a body that belongs to an association or professional federation representing businesses involved in the design, manufacturing, provision, assembly, use or maintenance of ICT products, services or processes may be considered to be a conformity assessment body, provided that its independence and the absence of any conflict of interest are demonstrated.

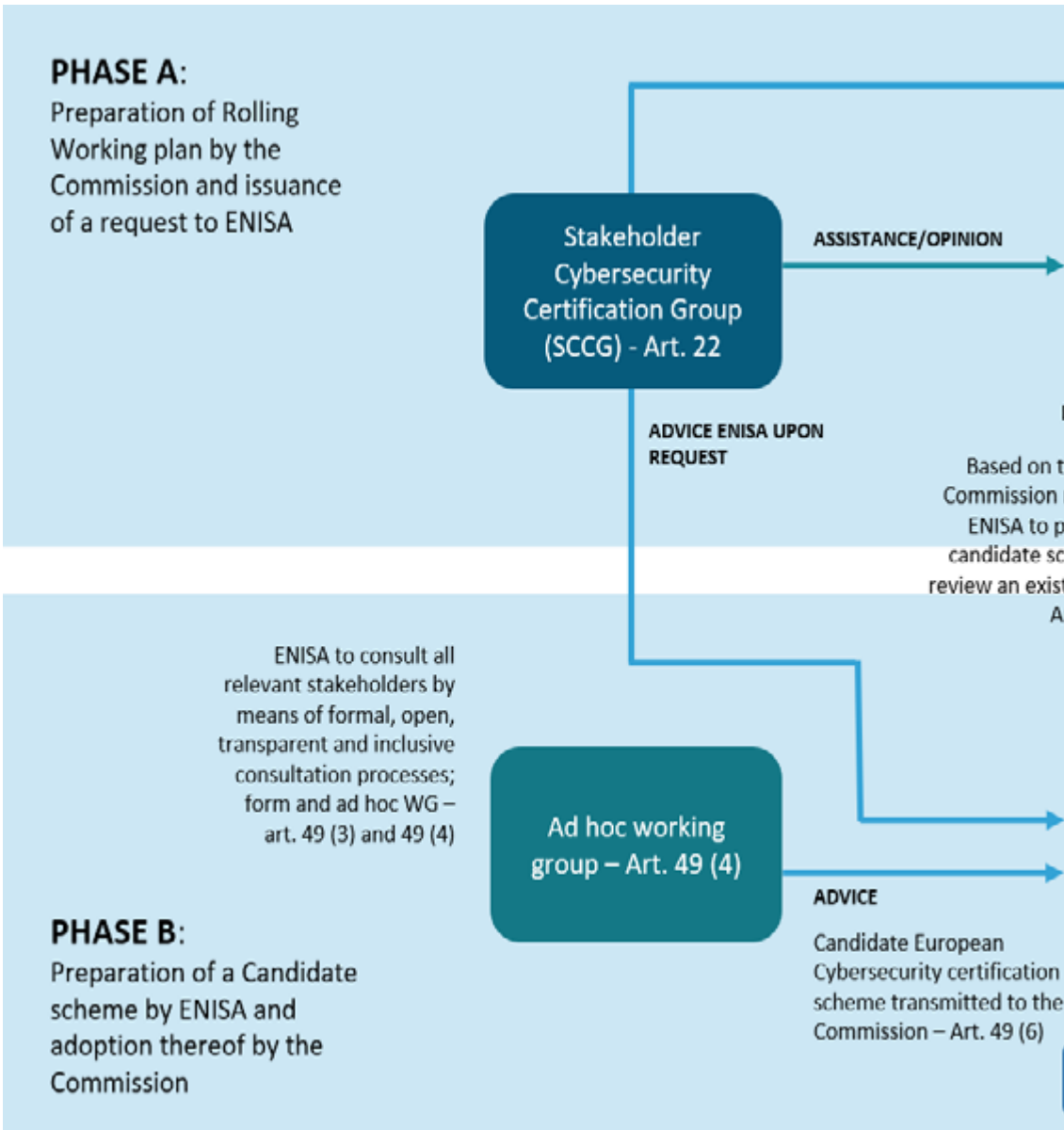
y assessment bodies



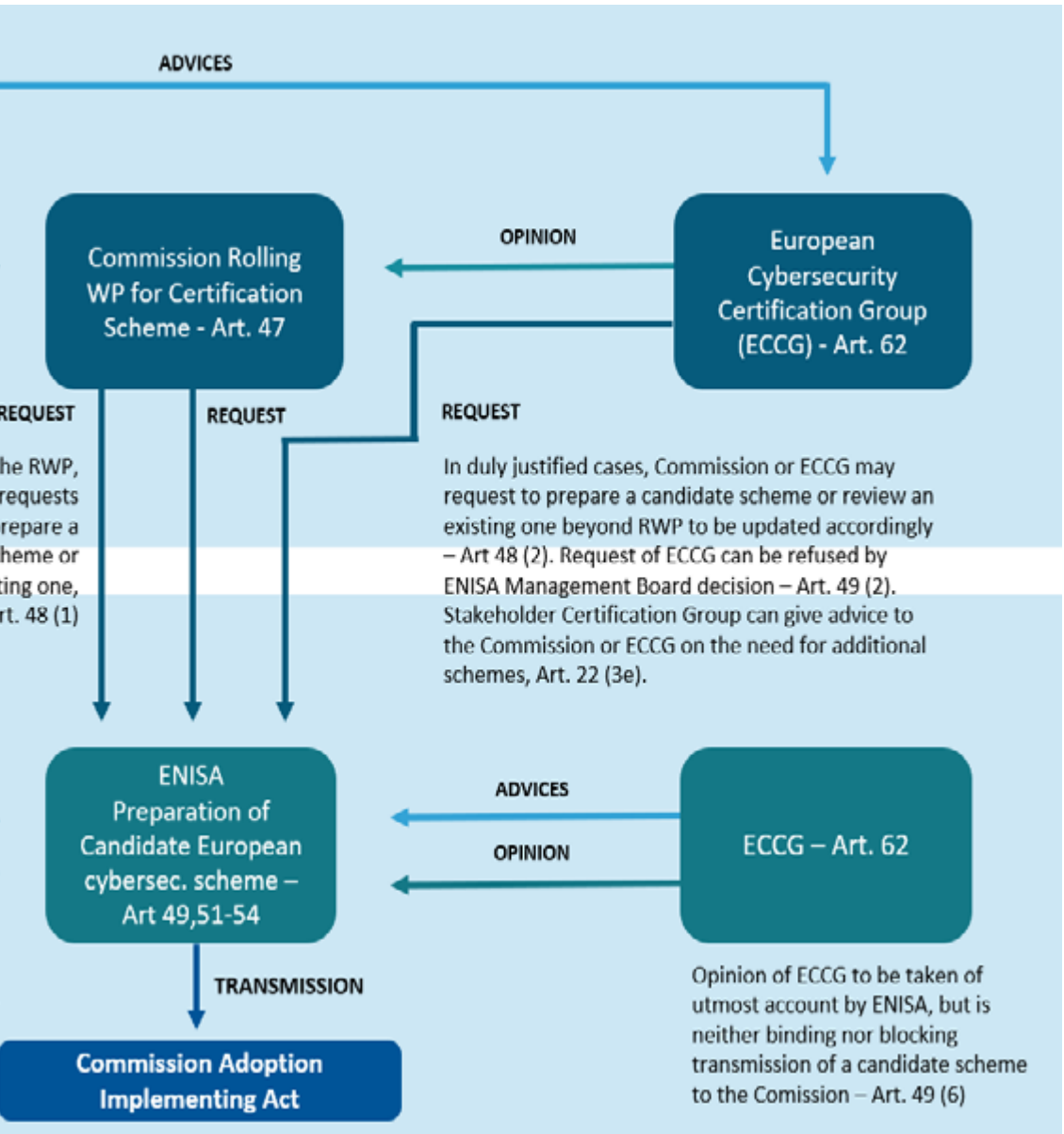
ENTRY INTO FORCE AND IMPLEMENTATION OF THE REGULATION (ARTICLE 69)

The Cybersecurity Act will enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. It will be applied from [date to be decided] except for Articles 58, 60, 61, 63, 64 and 65, which deal with national cybersecurity certification authorities and conformity assessment bodies. These Articles will apply 24 months after the publication date of the Regulation in the Official Journal of the European Union.

Interaction among sta



Annex
keholders



Eurosmart, the Voice of the Digital Security Industry,is an international non-profit association located in Brussels, representing the Digital Security Industryfor multisector applications. Founded in 1995, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications. Our membersMembers are manufacturers of secure element, semiconductors,smart cards, secure software, High Security Hardware and terminals, biometric technology providers, system integrators, application developers and issuers.

EUROSMART members are companies (BCA, Fingerprint Cards, Gemalto, Giesecke+Devrient, GS TAG, IDEMIA, IN GROUPE, Infineon Technologies, Inside Secure, Internet of Trust, Linxens, Nedcard, NXP Semiconductors, +ID, Prove & Run, Qualcomm, Real Casa de la Moneda, Samsung, Sanoïa, Sarapis, SGS, STMicroelectronics, Tiempo Secure,Toshiba, Trusted Objects, Trust CB, WISekey, Winbond), laboratories (Keolabs, Serma, Brightsight, Red Alert Labs, Cabinet Louis Renaud), research organisations (FraunhoferAISEC, Institut Mines-Telecom -IMT, ISEN -Institut Supérieur de l'Électronique et du NumériqueToulon), associations (SCS Innovationcluster, SmartPaymentAssociation, SPAC, Mobismart, DanishBiometrics).

EUROSMART and its members are also active in many other security initiatives and umbrella organisations on EU-level, like CEN, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART

Rue de la Science 14b
1040 Brussels BELGIUM

+ 32 2 880 36 35

contact@eurosmart.com

www.eurosmart.com