DECISION

NO.813, DATE 30/12/2025
ON THE APPROVAL OF THE NATIONAL CYBERSECURITY CERTIFICATION SCHEME AS WELL AS THE SECURITY LEVELS OF THE SCHEME[1]

In accordance with Article 100 of the Constitution and Article 42(1) of Law No. 25/2024 "On cybersecurity", upon the proposal of the Prime Minister,

DECIDED:

CHAPTER I
GENERAL PROVISIONS

Article 1
Object and scope

1. The object of this Decision is to approve a cybersecurity certification scheme based on European Common Criteria as well as the security levels of the scheme.
2. This Decision applies to all information and communication technology (ICT) products, including the documentation submitted for certification under the scheme, as well as all protection profiles submitted for certification as part of the ICT process up to the certification of ICT products.

Article 2
Definitions

For the purposes of this Decision, the following terms shall have the following meanings:

1. "Market surveillance authority" means the structure responsible for market surveillance, according to the provisions of the legislation in force and the relevant Decision of the Council of Ministers on the establishment, organization and functioning of the state inspectorate responsible for market surveillance.
2. "Certificate" is a cybersecurity certificate issued under the cybersecurity certification scheme for ICT products or for protection profiles that can be used exclusively in the ICT and ICT product certification process;

3. "Statement of conformity", a statement issued by the manufacturer or provider of an ICT product, service or process, by which he declares under his own responsibility that this product, service or process complies with the security requirements and criteria set out in the cybersecurity certification scheme.

[1] This Decision is fully aligned with the Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC), CELEX no.: EUR-Lex- 32024R0482, Natural no .: 2024/482/BE, Journal Official : Series L, date 7.2.2024, page 6-45, which is amended by the Regulation Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024, No. CELEX: EUR-Lex-32024R3144, No. Natural : 2024/3144 /EU , Official Journal Official : Series L, date 19.12.2024, pages 3-7.
https://eur-lex.europa.eu/legal-conte nt/EN/TXT/?uri=celex%3A32024R0482

4. "State-of-the-art document" means a document specifying evaluation methods, techniques and tools applied for the certification of ICT products, or the security requirements of a general category of ICT products, or any other requirements necessary for certification, with the aim to harmonise the evaluation, in particular of technical domains or protection profiles;

5. "Technical domain" means a common technical framework related to a particular technology for harmonized certification with a set of security requirements;

6. "Common Criteria" means the Common Criteria for information technology security evaluation, as set out in the standards ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022 or ISO/IEC 15408-5:2022, or in the Common Criteria for information technology (IT) security evaluation[2], Common Criteria version 2022, Parts 1 to 5, which have been adopted and published at the national level by the General Directorate of Standardization;

7. "Common Evaluation Methodology" means the common methodology for information technology security evaluation, as set out in standard ISO/IEC 18045:2022, which have been adopted and published at the national level by the General Directorate of Standardization, or the common methodology for information technology security evaluation[3], version "Common Evaluation Methodology 2022";

8. "AVA_VAN Level" means the assurance vulnerability analysis level that indicates the extent of cybersecurity evaluation activities carried out to determine the level of resistance to potential exploitability of flaws or weaknesses in the target of evaluation in its operational environment, as set out in the scheme;

9. "Target of evaluation" means an ICT product or part thereof, or a protection profile as part of an ICT process, which is subjected to cybersecurity evaluation to receive certification under the scheme;

10. "Security target" means a description of security requirements that are expected to be met and depend on the implementation for a specific ICT product.

11. "Certification body" means a legal person, national or international, accredited by the institution responsible for accreditation and authorized by the authority responsible for cybersecurity, responsible for carrying out conformity assessment activities based on evaluation reports prepared by ITSEF, including certification and inspection;

12. "Conformity assessment bodies" means bodies that carry out conformity assessment activities, including certification bodies and ITSEF, as defined in this scheme.

13. "National cybersecurity certification authority" means the National Cybersecurity Authority responsible for cybersecurity certification under this Decision;

14. "Information technology security assessment body (ITSEF)" means a legal person, national or international, accredited by the institution responsible for accreditation and authorized by the authority responsible for cybersecurity to carry out technical conformity assessment activities including calibration and testing.

---

[2] Common Criteria for Information Technology Security Evaluation: https://commoncriteriaportal.org/files/ccfiles/CC2022PART1R1.pdf

[3] Common Methodology for Information Technology Security Evaluation: https://www.commoncriteriaportal.org/files/ccfiles/CEM2022R1.pdf

15."Composite product" means an ICT product that is evaluated together with another ICT product that has already received a certificate, on whose security functionality the composite ICT product depends;

16. “Protection profile” means an ICT process that defines security requirements for a specific category of ICT products, addressing implementation-independent security needs, which can be used to evaluate ICT products belonging to that specific category for the purpose of their certification;

17. "Evaluation technical report" means a document produced by an ITSEF to present the findings, verdicts and justifications obtained during the evaluation of an ICT product or a protection profile in accordance with the rules and obligations set out in this Decision;

Article 3
Evaluation standards

1. The standards that apply to evaluations carried out under the scheme are:
   1) the Common Criteria;
   2) the Common Evaluation Methodology.

2. A certificate meeting the standards referred to in point 1 of this Article may also be issued under the scheme, declaring conformity with a protection profile, provided that the use of such a protection profile is required under the legislation in force for tachographs or under the legislation in force for electronic identification and trust services, which has met one of the following standards:

   a) Common Criteria for information technology security evaluation, version 3.1, revisions 1 to 4;
   b) Common methodology for information technology security evaluation, version 3.1, revisions 1 to 4.

Article 4
Assurance levels for which certification is required

1. Certification bodies shall issue certificates under the scheme at assurance level “substantial” or “high”.
2. Certificates at the assurance level “substantial” shall correspond to certificates covering AVA_VAN level 1 or 2.
3. Certificates at the assurance level “high” shall correspond to certificates covering AVA_VAN level 3, 4 or 5.
4. The assurance level confirmed in a certificate under the scheme shall distinguish between the conformant and augmented use of assurance components as defined in the Common Criteria in accordance with Annex VIII to this Decision.

5. Conformity assessment bodies shall apply those assurance components on which the selected AVA_VAN level depends in accordance with the standards referred to in Article 3 of this Decision.

Article 5
Methods for certifying ICT products

1. Certification of an ICT product shall be carried out against its security target:
   a) as defined by the applicant; or
   b) incorporating a certified protection profile as part of the ICT process, where the ICT product falls within the ICT product category covered by that protection profile.

2. Protection profiles shall be certified for the sole purpose of the certification of ICT products falling in the specific category of ICT products covered by the protection profile.

Article 6
Conformity self-assessment

A conformity self-assessment by the manufacturer or provider of ICT products, services or processes shall not be permitted.

CHAPTER II
CERTIFICATION OF ICT PRODUCTS

SECTION I
SPECIFIC STANDARDS AND REQUIREMENTS FOR EVALUATION

Article 7
Evaluation criteria and methods for ICT products

1. An ICT product submitted for certification shall, as a minimum, be evaluated in accordance with the following:

   a) the applicable elements of the standards referred to in Article 3 of this Decision;
   b) the security assurance requirements classes for vulnerability assessment and independent functional testing, as set out in the evaluation standards referred to in Article 3 of this Decision;
   c) the level of risk associated with the intended use of ICT products, as defined in Article 8 of this Decision and in Article 40 of Law No 25/2024 “On cybersecurity”;

   ç) the applicable state-of-the-art documents as defined in Annex I of this Decision;

   d) the applicable certified protection profiles in accordance with provisions in Annex II of this Decision.

2. In exceptional and justified cases, a conformity assessment body may request to refrain from the application of the state-of-the-art document. In such cases, the conformity assessment body

shall inform the national cybersecurity certification authority, with a justification for its request. The national cybersecurity certification authority shall assess the justification for an exception and, where justified, approve it. Pending the decision of the national cybersecurity certification authority, the conformity assessment body shall not issue any certificate. Upon the accession of the Republic of Albania to the European Union, the national cybersecurity certification authority shall notify the approved exception to the European Cybersecurity Certification Group, which may issue an opinion. The opinion of the European Cybersecurity Certification Group shall be taken into account by the national cybersecurity certification authority.
3. Certification of ICT products at AVA_VAN level 4 or 5 shall only be possible for the following scenarios:

a) where the ICT product is covered by any technical domain in accordance with provisions in Annex I of this Decision, it is evaluated in accordance with the applicable state-of-the-art documents for technical domains;
b) where the ICT product falls into a category of ICT products covered by a certified protection profile that includes AVA_VAN levels 4 or 5 and has been listed as a protection profile as defined in Annex II of this Decision, it shall be evaluated in accordance with the evaluation methodology specified for that protection profile;
c) where the provisions in points (a) and (b) are not applicable and where the inclusion of a technical domain as defined in Annex I of this Decision or of a certified protection profile as defined in Annex II of this Decision is unlikely in the foreseeable future, only in exceptional and justified cases subject to the conditions set out in point 4 of this Article.

4. Where a conformity assessment body considers to be in an exceptional and duly justified case referred to in point (c) of paragraph 3 of this Article, it shall notify the intended certification to the national cybersecurity certification authority, with a justification and a proposed evaluation methodology. The national cybersecurity certification authority shall assess the justification for an exception and, where justified, approve or amend the evaluation methodology to be applied by the conformity assessment body. Pending the decision of the national cybersecurity certification authority, the conformity assessment body shall not issue certificates. Upon the accession of the Republic of Albania to the European Union, the national cybersecurity certification authority shall report the intended certification to the European Cybersecurity Certification Group, which may issue an opinion. The opinion of the European Cybersecurity Certification Group shall be taken into account by the national cybersecurity certification authority.
5. In the case of an ICT product undergoing a composite product evaluation in accordance with the relevant state-of-the-art documents, the ITSEF that carried out the evaluation of the underlying ICT product shall share the relevant information with the ITSEF performing the evaluation of the composite ICT product.

Article 8
Assurance levels of the cybersecurity certification scheme

1. The cybersecurity certification scheme shall specify one or more of the assurance levels for ICT products, services and processes, 'basic', 'substantial' or 'high'. The assurance level is proportional to the level of risk associated with the intended use of the ICT product, service and process, in

terms of the probability and impact of a cybersecurity incident.
2. The cybersecurity certificate shall refer to any assurance level specified in the cybersecurity certification scheme under which the cybersecurity certificate is issued.
3. The security requirements corresponding to each assurance level shall be defined in the cybersecurity certification scheme, including the relevant security functionalities and the appropriate severity and depth of the evaluation to which the ICT product, service, or process shall be subjected.
4. The certificate shall refer to technical specifications, standards, and procedures related thereto, including technical controls, the purpose of which is to reduce risks or prevent cybersecurity incidents.
5. A cybersecurity certificate or statement of conformity referring to the assurance level 'basic' shall provide assurance that ICT products, services and processes for which a certificate or statement of conformity has been issued meet the relevant security requirements, including security functionalities, as well as the evaluation at the level intended to minimise the known basic risks of cyber incidents and attacks. The evaluation activities undertaken must include at least a review of the technical documentation. Where such a review is not appropriate, alternative assessment activities with the equivalent effect shall be undertaken.
6. A cybersecurity certificate referring to the assurance level 'substantial' shall provide assurance that the ICT products, services and processes for which the certificate has been issued meet the relevant security requirements, including security functionalities, as well as the evaluation at a level intended to minimise known cybersecurity risks and the risk of incidents and cyber-attacks carried out by actors with limited capabilities and resources. The evaluation activities to be undertaken shall include at least a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, services or processes correctly implement the necessary security functionalities, and where the evaluation activity is not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.
7. A cybersecurity certificate referring to the assurance level "high" shall provide the assurance that the ICT products, services and processes for which the certificate has been issued meet the relevant security requirements, including security functionalities, as well as the evaluation at a level intended to minimise the risk of modern cyber-attacks carried out by actors with significant capabilities and resources. The assessment activities undertaken shall include at least a review to demonstrate the absence of publicly known vulnerabilities, testing to demonstrate that the ICT products, services or processes correctly implement the necessary security functionalities at the technology state as well as an assessment of their resistance to attackers, using penetration testing, and when any such evaluation activity is not appropriate, substitute evaluation activities with the same effect shall be undertaken.
8. A cybersecurity certification scheme may specify several evaluation levels depending on the severity and depth of the evaluation methodology used. Each of the evaluation levels corresponds to one of the assurance levels and shall be defined by an appropriate combination of assurance components.

SECTION II
ISSUANCE, RENEWAL AND WITHDRAWAL OF CERTIFICATES

Article 9

Information necessary for certification and evaluation

1. An applicant for certification under the scheme shall provide or make available to the certification body and ITSEF the information necessary for evaluation and certification activities.

2. The information referred to in point 1 of this Article shall include all relevant evidence in accordance with developer action elements in the appropriate format as defined in the content and presentation of the evidence element of the Common Criteria and Common Evaluation Methodology for the selected assurance level and the associated security assurance requirements. The evidence shall include, where necessary, details of the ICT product and its source code as defined in this Decision, subject to safeguards against unauthorised disclosure.

3. Applicants for certification may provide to the certification body and ITSEF appropriate evaluation results from prior certification pursuant to:

a) provisions of this Decision;
b) a European cybersecurity certification scheme.

4. Where the evaluation results are pertinent to its tasks, the ITSEF may reuse the evaluation results provided that such results conform to the applicable requirements and its authenticity is confirmed.

5. Where the certification body allows the product to undergo a composite-product certification, the applicant for certification shall make available to the certification body and the ITSEF all necessary elements, where applicable, in accordance with the state-of-the-art documents.

6. Applicants for certification shall also make available to the certification body and the ITSEF the following information:

a) the link to their website containing the supplementary cybersecurity information referred to in Article 10 of this Decision;
b) a description of the applicant's procedures for vulnerability management and disclosure.

7. The relevant documentation referred to in this Article shall be retained by the certification body, the ITSEF and the applicant for a period of five years after the expiry of the certificate.

Article 10
Supplementary cybersecurity information for certified ICT products, ICT services, and ICT processes

1. The manufacturer or provider of certified ICT products, ICT services, or ICT processes, or of ICT products, ICT services, and ICT processes for which a statement of conformity has been issued, shall make publicly available the following additional cybersecurity information:

a) guidelines and recommendations to assist end users with the secure configuration, installation, deployment, operation, and maintenance of the ICT products or services;

b) the period during which cybersecurity support is offered to end users, in particular regarding the availability of cybersecurity-related updates;
c) the manufacturer's or provider's contact information and the accepted methods for receiving vulnerability information from end users and security researchers;
ç) a reference to the list of weaknesses published online related to the ICT product, ICT service, or ICT process, as well as any relevant cybersecurity advisories.

2. The information referred to in point 1 of this Article shall be made available in electronic form and shall remain accessible and updated as necessary at least until the expiry of the corresponding cybersecurity certificate or the statement of conformity.

Article 11
Conditions for issuance of a certificate

1. Certification bodies shall issue a certificate under the scheme where all of the following conditions are met:

a) the category of ICT product falls within the scope of the accreditation, and where applicable of the authorisation, of the certification body and the ITSEF involved in the certification;
b) the applicant for certification has signed a statement undertaking all the commitments listed in point 2 of this Article;
c) the ITSEF has concluded the evaluation without objections, in accordance with the evaluation standards, criteria and methods referred to in Articles 3 and 7 of this Decision;
d) the certification body has concluded the review of the evaluation results without objections;
e) the certification body has verified that the evaluation technical reports provided by the ITSEF are consistent with the provided evidence and that the evaluation standards, criteria and methods referred to in Articles 3 and 7 of this Decision have been correctly applied.

2. The applicant for certification shall undertake the following commitments:

a) to provide the certification body and the ITSEF with all necessary, complete and correct information, and to provide additional information if requested;
b) not to promote the ICT product as being certified under the scheme before the certificate has been issued;
c) to promote the ICT product as being certified only with respect to the scope set out in the issued certificate;

ç) to cease immediately the promotion of the ICT product as being certified in the event of the suspension, withdrawal or expiry of the certificate;

d) to ensure that ICT products sold with reference to the certificate are strictly identical to the ICT product that undergoes certification;

dh) to respect the rules of use of the mark and label established for the certificate in accordance with Article 13 of this Decision.

3. In the case of an ICT product undergoing composite product certification, in accordance with the state-of-the-art documents, the certification body that carried out the certification of the underlying ICT product shall share the relevant information with the certification body that

performs the certification of the composite ICT product.

Article 12
Content and format of a certificate

1. A certificate shall include the relevant information specified in Annex VII of this Decision.
2. The scope and boundaries of the certified ICT product shall be specified in the certificate or in the certification report, indicating whether the entire ICT product is certified or only parts thereof.
3. The certification body shall provide the certificate to the applicant at least in electronic form.
4. The certification body shall produce a certification report in accordance with the provisions in the Annex V of this Decision for every issued certificate. The certification report shall be based on the evaluation technical report issued by the ITSEF. The evaluation technical report and the certification report shall indicate the specific evaluation criteria and methods referred to in Article 7 of this Decision used for the evaluation.
5. The certification body shall provide the national cybersecurity certification authority and, upon the accession of the Republic of Albania to the European Union, ENISA, with every certificate and every certification report in electronic form.

Article 13
Mark and label

1. The holder of a certificate may affix a mark and label to a certified ICT product. The mark and label indicate that the ICT product has been certified in accordance with this Decision. Mark and label shall be affixed in accordance with this Article and in Annex IX of this Decision.
2. The mark and label shall be affixed in a visible, legible and indelible manner on the certified ICT product or on its data plate. Where this is impossible or not warranted on account of the nature of the product, the mark shall be affixed to the packaging and to the accompanying documents. Where the certified ICT product is delivered in software form, the mark and label shall appear in a visible, legible and indelible manner in the accompanying documentation, or that documentation shall be made easily and directly accessible to users on a website.
3. The mark and label shall be set out in accordance with provisions in Annex IX of this Decision and shall contain:
   a) the assurance level and the AVA_VAN level of the certified ICT product;
   b) the unique identification of the certificate, consisting of:
      i. the name of the scheme;
      ii. the name and accreditation reference number of the certification body that has issued the certificate;
      iii. year and month of issuance;
      iv. identification number assigned by the certification body that has issued the certificate.
4. The mark and label shall be accompanied by a QR code with a link to a website that contains at least:
   a) the information on the validity of the certificate;
   b) the necessary certification information required as set out in Annexes V and VII of this Decision;

c) the information to be made publicly available by the holder of the certificate in accordance with Article of this Decision;

ç) where applicable, the historic information related to the specific certification or certifications of the ICT product to enable traceability.

Article 14
Period of validity of a certificate

1. The certification body shall set a period of validity for each certificate it issues, taking into account the characteristics of the certified ICT product.

2. The period of validity of the certificate shall not exceed 5 years.

3. By derogation from paragraph of this Article, that period may exceed five years, subject to the prior approval of the national cybersecurity certification authority. Upon the accession of the Republic of Albania to the European Union, the national cybersecurity certification authority shall immediately notify the European Cybersecurity Certification Group.

Article 15
Review of a certificate

1. Upon request of the holder of the certificate or for justified reasons, the certification body may decide to review the certificate for an ICT product. The review shall be carried out in accordance with Annex IV of this Decision. The certification body shall determine the extent of the review and, where necessary for the review, shall require the ITSEF to perform a re-evaluation of the certified ICT product.
2. Following the results of the review and according to the applicable re-evaluation case, the certification body shall:

a) confirm the certificate;
b) withdraw the certificate in accordance with Article 16 of this Decision;
c) withdraw the certificate in accordance with Article 16 of this Decision and issue a new certificate with identical scope and an extended validity period;
d) withdraw the certificate in accordance with Article 16 of this Decision and issue a new certificate with a different scope.

3. The certification body may decide to suspend the certificate, without undue delay, in accordance with Article 32 of this Decision, until remedial actions are taken by the holder of the certificate.

Article 16
Withdrawal of a certificate

1. The certification body that issued the certificate shall withdraw it when the certificate does not comply with the requirements set out in Articles 11, 12, 15 and point 3 of Article 31 of this Decision.

2. The certification body referred to in point 1 of this Article shall notify the national cybersecurity certification authority of the withdrawal of the certificate and, upon the accession of the Republic of Albania to the European Union, shall also notify ENISA. The national cybersecurity certification authority shall inform the market surveillance authority.
3. The certificate holder may request the withdrawal of the certificate.

CHAPTER III
CERTIFICATION OF PROTECTION PROFILES

SECTION I
SPECIFIC STANDARDS AND REQUIREMENTS FOR EVALUATION

Article 17
Evaluation criteria and methods

1. A protection profile shall be evaluated, as a minimum, in accordance with the following:

a) the applicable elements of the standards referred to in Article 3 of this Decision;
b) the level of risk associated with the intended use of ICT products as defined in Article 8 of this Decision and in Article 40 of Law No 25/2024 “On cybersecurity”;
c) the state-of-the-art documents specified in the Annex I of this Decision. A protection profile covered by a technical domain shall be certified against the requirements set out in that technical domain.

2. In exceptional and justified cases, a conformity assessment body may certify a protection profile without applying the state-of-the-art documents. In such cases, the certification body shall inform the national cybersecurity certification authority and provide a justification for the intended certification without applying the state-of-the-art documents as well as the proposed evaluation methodology. The national cybersecurity certification authority shall assess the justification and, where justified, approve the non-application of the state-of-the-art documents as well as shall approve or, where appropriate, amend the evaluation methodology to be applied by the conformity assessment body. Pending the decision of the national cybersecurity certification authority, the conformity assessment body shall not issue a certificate for the protection profile. Upon the accession of the Republic of Albania to the European Union, the national cybersecurity certification authority shall notify, without undue delay, the authorisation for the non-application of the state-of-the-art documents to the European Cybersecurity Certification Group, which may issue an opinion. The national cybersecurity certification authority shall take the opinion of European Cybersecurity Certification Group into account.

SECTION II
ISSUANCE, RENEWAL AND WITHDRAWAL OF CERTIFICATES FOR PROTECTION PROFILES

Article 18
Information necessary for certification and evaluation of protection profiles

An applicant for certification of a protection profile shall provide or make available to the certification body and ITSEF the information necessary for the certification and evaluation activities. Points 2, 3, 4 and 7 of Article 9 of this Decision shall apply mutatis mutandis.

Article 19
Issuance of certificates for protection profiles

1. For the issuance of certificates for protection profiles, the provisions of Articles 11 and 12 of this Decision shall apply mutatis mutandis.
2. The ITSEF shall evaluate whether a protection profile is complete, consistent, technically correct, and effective for the intended use and the security objectives of the ICT product category covered by that protection profile.
3. A protection profile shall be certified solely by:

a) a national cybersecurity certification authority;

b) a certification body, upon prior approval by the national cybersecurity certification authority for each individual protection profile.

Article 20
Period of validity of a certificate for protection profiles

1. The certification body shall set a period of validity for each certificate.
2. The period of validity may be up to the lifetime of the protection profile concerned.

Article 21
Review of a certificate for protection profiles

1. Upon request of the holder of the certificate or for other justified reasons , the certification body may decide to review a certificate for a protection profile. The review shall be carried out by applying the conditions laid down in Article 17 of this Decision. The certification body shall determine the duration of the review and, where necessary for the review, shall request the ITSEF to carry out a re-evaluation of the certified protection profile.
2. Following the results of the review and, according to the applicable re-evaluation case, the certification body shall do one of the following:

a) confirm the certificate;
b) withdraw the certificate in accordance with Article 22 of this Decision;
c) withdraw the certificate in accordance with Article 22 of this Decision and issue a new certificate with identical scope and an extended validity period;
ç) withdraw the certificate in accordance with Article 22 of this Decision and issue a new certificate with a different scope.

Article 22
Withdrawal of a certificate for a protection profile

1. The certification body that issued the certificate shall withdraw it when the certificate does not comply with the provisions of this Decision. The provisions of Article 16 of this Decision shall apply mutatis mutandis for the withdrawal of a certificate for a protection profile.

2. A certificate for a protection profile issued in accordance with Article 19(4)(b) of this Decision shall be withdrawn by the national cybersecurity certification authority that approved that certificate.

Article 23
Specification of requirements for accreditation of conformity assessment bodies

The accreditation of conformity assessment bodies shall take into account the specification of accreditation requirements for certification bodies and ITSEFs, as defined in the relevant state-of-the-art documents listed in point 2 of Annex I of this Decision.

CHAPTER IV
CONFORMITY ASSESSMENT BODIES

Article 24
Additional or specific requirements for a certification body and recognition of their assessments and reports

1. A certification body shall be authorised by the national cybersecurity certification authority to issue certificates at assurance level 'high' where that body is accredited by the institution responsible for accreditation in the Republic of Albania, according to the legislation in force on accreditation, and meets the following requirements:
   a) it has the appropriate expertise and competences to issue the certification decision at assurance level 'high';
   b) it conducts its certification activities in cooperation with an ITSEF authorised in accordance with Article 25 of this Decision;
   c) it has the requisite competences and implements appropriate technical and operational measures to effectively protect confidential and sensitive information for assurance level 'high', in addition to the requirements defined in Article 44 of this Decision.
2. The national cybersecurity certification authority shall assess whether the certification body meets all the requirements set out in point 1 of this Article. The assessment shall include at least structured interviews and a review of at least one pilot certification carried out by the certification body in accordance with this Decision. In its assessment, the national cybersecurity certification authority may reuse any appropriate evidence from prior authorisation or similar activities pursuant to:
   a) this Decision;
   b) a European cybersecurity certification scheme.
3. The national cybersecurity certification authority shall produce an authorisation report in accordance with the procedures for monitoring, authorising and supervising the activities of conformity assessment bodies.
4. The national cybersecurity certification authority shall specify the ICT product categories and

protection profiles to which the authorisation extends. The authorisation shall be valid for a period no longer than the validity of the accreditation. The authorisation may be renewed upon request, provided that the certification body still meets the requirements set out in this Article. Pilot assessments shall not be required for renewal of the authorization.
5. The national cybersecurity certification authority shall withdraw the authorisation of the certification body where it no longer meets the conditions in accordance with the provisions of this Article. Upon withdrawal of the authorisation, the certification body shall immediately cease its activity as an authorised certification body.
6. Evaluations carried out, certification reports and certificates issued by certification bodies that are accredited and authorised in a Member State of the European Union shall have the same validity as evaluations carried out, certification reports and certificates issued by certification bodies that are accredited and authorised in the Republic of Albania.

Article 25

Additional or specific requirements for an ITSEF and recognition of their assessments and reports

1. An ITSEF shall be authorised by the national cybersecurity certification authority to carry out the evaluation of ICT products that are subject to certification at assurance level 'high', where the ITSEF is a body accredited by the institution responsible for accreditation in the Republic of Albania, according to the legislation in force on accreditation, and meets the following requirements:

a) it has the necessary expertise for performing the evaluation activities to determine the resistance to state-of-the-art cyberattacks carried out by actors with significant skills and resources;
b) for the technical domains and protection profiles, which are part of the ICT process for those ICT products, it has:
   i. the expertise to perform the specific evaluation activities necessary to methodically determine a target of evaluation's resistance against skilled attackers in its operational environment assuming an attack potential of 'moderate' or 'high' as set out in the standards referred to in Article 3 of this Decision;
   ii. the appropriate technical competences as specified in the relevant state-of-the-art documents listed in Annex I of this Decision;
a) it has the requisite competence and puts in place the necessary technical and operational measures to effectively protect confidential and sensitive information for assurance level 'high', in addition to the requirements set out in Article 44 of this Decision.

2. The national cybersecurity certification authority shall assess whether an ITSEF meets all the requirements set out in point 1 of this Article. This assessment shall include at least structured interviews and a review of at least one pilot evaluation performed by the ITSEF in accordance with this Decision.
3. In its assessment, the national cybersecurity certification authority may reuse any appropriate evidence from prior authorisation or similar activities according to provisions of:

a) this Decision;
b) a European cybersecurity certification scheme.

4. The national cybersecurity certification authority shall produce an authorisation report in accordance with the procedures for monitoring, authorising and supervising the activities of conformity assessment bodies.
5. The national cybersecurity certification authority shall specify the ICT-product categories and protection profiles to which the authorisation extends. The authorisation shall be valid for a period no longer than the validity of the accreditation. The authorisation may be renewed upon request, provided that the ITSEF meets the requirements set out in this Article. Pilot evaluations shall not be required for renewal of the authorisation.

6. The national cybersecurity certification authority shall withdraw the authorisation of the ITSEF when it no longer meets the conditions in accordance with the provisions in this article. Upon withdrawal of the authorisation, the ITSEF shall immediately cease to operate as an authorised ITSEF.
7. Evaluations performed and evaluation technical reports issued by ITSEFs that are accredited and authorised in a Member State of the European Union shall have the same validity as evaluations performed and evaluation technical reports issued by ITSEFs that are accredited and authorised in the Republic of Albania.

CHAPTER V
MONITORING, NON-CONFORMITY AND NON-COMPLIANCE

SECTION I
COMPLIANCE MONITORING

Article 26
National Cybersecurity Certification Authority

1. In the Republic of Albania, the National Cybersecurity Authority shall exercise the competences of the national cybersecurity certification authority.
2. The national cybersecurity certification authority shall be independent from the entities it supervises, including with regard to its organization, financial aspect, legal structure, and decision-making process.
3. The national cybersecurity certification authority shall have sufficient resources to exercise its powers and carry out its duties effectively.
4. The national cybersecurity certification authority shall exercise the following powers:

a) supervises and enforces the rules defined in this decision for monitoring the compliance of ICT products, services, and processes with the requirements of cybersecurity certificates that have been issued;
b) monitor compliance and the obligations of manufacturers or providers of ICT products, services, or processes;
c) supports the institution responsible for accreditation in monitoring and supervising the activities of conformity assessment bodies for the purposes of this Decision;
ç) monitors and supervises the activities according to the provisions in this Article as well as the conformity assessment bodies accredited by the institution responsible for accreditation;
d) where applicable, restricts, suspends, or withdraws existing authorizations when conformity assessment bodies infringe the requirements of this Decision;
dh) handles complaints from natural or legal persons regarding cybersecurity certificates issued by conformity assessment bodies as well as addresses such complaints and informs the complainant of the progress and outcome of the investigation within a reasonable timeframe;
e) ensures the preparation of an annual summary report on the activities carried out under this Article;
ë) cooperates with other public authorities, including the exchange of information on the potential non-conformity of ICT products, services, and processes with the requirements of this Decision;
f) monitors relevant developments in the field of cybersecurity certification.

Article 27
Monitoring activities by the national cybersecurity certification authority

1. Without prejudice to Article 26 of this Decision, the national cybersecurity certification authority shall monitor the compliance of:

a) the certification body and the ITSEF with the obligations according to the provisions of this Decision;
b) the holder of the certificate with the obligations according to the provisions of this decision;
c) certified ICT products with the requirements defined in this Decision;
ç) the assurance expressed in the certificate that addresses the emerging threats.

2. The national cybersecurity certification authority shall carry out its monitoring activities, in particular based on:

a) information coming from certification bodies, the authority responsible for accreditation, and the authority responsible for market surveillance;
b) information resulting from its own or another authority's audits and verifications;
c) sampling in accordance with provisions of Article 27(3);
ç) received complaints.

3. The national cybersecurity certification authority, in cooperation with the authority responsible for market surveillance, shall sample at least 4% of certificates each year as determined by a risk assessment conducted by the national cybersecurity certification authority. At the request of and acting on behalf of the national cybersecurity certification authority, certification body and, if necessary, ITSEF shall assist the authority in monitoring compliance.

4. The national cybersecurity certification authority shall select the sample of certified ICT products to be checked based on the following criteria:

a) the product category;
b) the assurance levels of the products;
c) the holder of the certificate;
ç) the certification body and, as applicable, the subcontracted ITSEF;
d) and shall take into account any other relevant information.

5. The national cybersecurity certification authority shall inform the holder of the certificate of the selected ICT products and of the selection criteria.

6. The certification body that certified the sampled ICT product, at the request of the national cybersecurity certification authority and with the assistance of the relevant ITSEF, shall carry out reviews in accordance with the procedure set out in Section 2 of Annex IV of this decision and shall inform on the results the national cybersecurity certification authority.

7. Where the national cybersecurity certification authority has sufficient reason to believe that a certified ICT product is no longer in conformity with this Decision, it may carry out verifications or make use of any other monitoring power set out in Article 26 of this Decision.

8. The national cybersecurity certification authority shall subsequently inform the certification body and the relevant ITSEF of the verifications and the selected ICT products.

9. When the national cybersecurity certification authority identifies that an ongoing verification relates to ICT products certified by certification bodies established in European Union Member States, shall inform the national cybersecurity certification authorities of those states in order to cooperate in the verifications where relevant. Upon the accession of the Republic of Albania to the European Union, the national cybersecurity certification authority shall also notify the European Cybersecurity Certification Group of the cross-border investigations and the resulting outcomes.

Article 28

Monitoring activities by the certification body

1. The certification body shall monitor:

a) the compliance of the holder of the certificate with their obligations as defined in this decision

according to the provisions of this decision towards the certificate issued by the certification body;
b) the compliance of ICT products which are certified with their respective security requirements;
c) the security expressed in the certified protection profiles.

2. The certification body shall undertake monitoring activities based on:
a) the information provided, of the commitments of the applicant for certification as referred to in Article 11(2) of this Decision;
b) information resulting from the activities of the authority responsible for market surveillance;
c) received complaints;
ç) information regarding vulnerabilities that affect ICT products which are certified.
3. The national cybersecurity certification authority may establish a communication protocol for information exchange between certification bodies and the holder of the certificate, to verify and report compliance with the commitments made in accordance with Article 11(2) of this Decision, without prejudice to the activities falling under the authority responsible for market surveillance.

Article 29
Monitoring activities by the holder of the certificate

1.The holder of the certificate, to monitor the conformity of the certified ICT product with its security requirements, shall carry out the following tasks:
a) monitors vulnerability information related to the certified ICT product with their own tools, while also taking into consideration:
i. a publication or submission regarding the vulnerability information by a user or a security researcher, as referred to in Article 10(1) of this Decision;
ii. a submission from any other source.
b) monitors the security as expressed in the certificate.
2.The holder of the certificate shall cooperate with the certification body, the ITSEF, and, where applicable, the national cybersecurity certification authority to support their monitoring activities.

SECTION II
CONFORMITY AND COMPLIANCE

Article 30

Consequences of the non-conformity of a certified ICT product or protection profile

1. When a certified ICT product or protection profile does not conform with the requirements set out in this decision, the certification body shall inform the holder of the certificate about the identified non-conformity and request remedial actions.

2. When a case of non-conformity with the provisions of this decision may affect compliance with the particular legislation in force, which provides for the possibility of demonstrating a presumption of conformity with the requirements of that legal act by using a certificate issued under the scheme, the certification body shall immediately inform the national cybersecurity certification authority. The national cybersecurity certification authority shall, in turn,

immediately notify the authority responsible for market surveillance under the other relevant legislation regarding the identified case of non-conformity.

3. Following the receipt of the information referred to in Article 30(1), the holder of the certificate shall propose to the certification body the necessary remedial actions to address the non-conformity within the deadline set by the certification body, which shall not exceed 30 days.

4. In emergency cases, the certification body may suspend immediately the certificate in accordance with Article 32 of this decision or in case when the holder of the certificate does not properly cooperate with the certification body.

5. The certification body shall carry out reviews in accordance with Articles 15 and 21 of this Decision, to assess whether the remedial action addresses the non-conformity.

6. When the holder of the certificate does not propose appropriate remedial actions during the period referred to in Article 30(3), the certificate shall be suspended in accordance with Article 32 or withdrawn in accordance with Articles 16 or 22 of this Decision.

7. This Article shall not apply in cases of vulnerabilities affecting a certified ICT product, which shall be handled in accordance with Chapter VI of this Decision.

Article 31
Consequences of non-compliance by the holder of the certificate

1.The certification body shall set a deadline of 30 days for the holder of the certificate to undertake remedial actions, when it finds that:

a) the holder of the certificate or the applicant for certification does not comply with the obligations set out in point Article 11(2), Article 19(2), Articles 29 and Article 43 of this Decision;

b) the holder of the certificate fails to inform the authority or the certification body of any discovered vulnerability or irregularity concerning the security of the certified ICT product, service or process that may impact compliance with the certification-related requirements.

2.If the holder of the certificate does not undertake remedial actions within the time period referred to in Article 31(1), the certificate shall be suspended in accordance with Article 32 or withdrawn in accordance with Article 16 or Article 22 of this Decision.

3. Recurring or continuous infringement by the holder of the certificate of the obligations referred to in Article 31(1) shall lead to the withdrawal of the certificate in accordance with Article 16 or Article 22 of this Decision.

4. The certification body shall inform the national cybersecurity certification authority of the findings referred to in Article 31(1). Where the non-compliance falls in contradictions to the applicable legal provisions, the national cybersecurity certification authority shall immediately notify the market surveillance authority.

Article 32
Suspension of the certificate

1. In the case of a suspension of a certificate in accordance with the provisions of this Decision, the certification body shall suspend the certificate for a period appropriate to the circumstances that led to the suspension, which shall not exceed 42 days. The suspension period shall begin on the day following the date of the Decision of the certification body and shall not affect the validity of the certificate.

2. The certification body shall immediately notify the holder of the certificate and the national cybersecurity certification authority of the suspension and shall provide the reasons for the suspension, the necessary remedial actions to be taken, and the suspension period.
3. The holder of the certificate shall notify the purchasers of the ICT products of the suspension and the reasons given by the certification body for the suspension, except for reasons whose disclosure would pose a security risk or involve sensitive information. This information shall also be made publicly available by the holder of the certificate.
4. Where the legislation in force provides for a presumption of conformity, based on certificates issued under the provisions of this decision, the national cybersecurity certification authority shall inform the authority responsible for market surveillance of the specific legislation in force regarding the suspension.
5. In duly justified cases, the national cybersecurity certification authority may authorize an extension of the suspension period of a certificate, where the total suspension period may not exceed one year.

Article 33
Consequences of non-compliance by the conformity assessment body

1. In the event of non-compliance by a certification body with its obligations, or upon identification of non-compliance by an ITSEF, the national cybersecurity certification authority shall immediately take the following actions:

a) identify potentially affected certificates, with the support of the relevant ITSEF;
b) when it is necessary, request evaluation activities to be carried out on one or more ICT products or protection profiles by the ITSEF that performed the evaluation, or by any other accredited ITSEF, and, where applicable, by an ITSEF with the technical capabilities to support identification;
c) analyze the impact of the non-compliance;

ç) notify the holder of the certificate affected by the non-compliance.

2. Based on the provisions of Article 33(1), the certification body shall take one of the following decisions regarding each affected certificate:
a) maintain the certificate unchanged;
b) withdraw the certificate in accordance with Article 16 or Article 22 of this Decision, and, where appropriate, issue a new certificate.
3. Based on the provisions of Article 33(1), the national cybersecurity certification authority shall, where applicable, take the following actions:
a) where necessary, report the non-compliance of the certification body or the relevant ITSEF to the competent authority for accreditation;
b) where applicable, assess the potential impact on the authorization.

CHAPTER VI
VULNERABILITY MANAGEMENT AND DISCLOSURE

Article 34
Scope of vulnerability management

This Chapter shall apply to ICT products for which a certificate has been issued.

SECTION I
VULNERABILITY MANAGEMENT

Article 35
Vulnerability management procedures

1.The holder of the certificate shall establish and maintain all necessary vulnerability management procedures in accordance with the rules set out in this section and, where necessary, complemented by the procedures defined in ISO/IEC 30111 for information technology, security techniques, and vulnerability handling processes.

2. Based on this Decision, the holder the certificate shall maintain and publish appropriate methods for receiving information on vulnerabilities related to their products from external sources, including users, certification bodies, and security researchers.

3. When the holder of the certificate, under the provisions of this Decision, discovers or receives information about a potential vulnerability affecting a certified ICT product, they shall register it and carry out an analysis of the vulnerability's impact.

4. When a potential vulnerability affects a composite product, the holder of the certificate, based on the provisions of this Decision, shall inform the holders of the dependent certificates about the potential vulnerabilities.

5. In response to a reasonable request from the certification body that issued the certificate, the holder of the certificate, based on the provisions of this Decision, shall transmit relevant information about potential vulnerabilities to that certification body.

Article 36
Vulnerability impact analysis

1. The vulnerability impact analysis shall refer to the target of evaluation and the assurance statements included in the certificate. The analysis shall be conducted within a time frame appropriate to the exploitability and criticality of the potential vulnerability affecting the certified ICT product.

2. When applicable, an attack potential calculation shall be carried out in accordance with the relevant methodology set out in the standards referenced in Article 3 of this Decision and the state-of-the-art documents as specified in Annex I of this Decision, in order to determine the exploitability of the vulnerability. The AVA_VAN level of the certificate under this Decision

shall be taken into account.

Article 37
Vulnerability impact analysis report

1. The holder of the certificate shall prepare a vulnerability impact analysis report where the impact analysis shows that the vulnerability has a potential impact on the conformity of the ICT product with its certificate.
2. The vulnerability impact analysis report shall contain an assessment of the following elements:
   a) the impact of the vulnerability on the certified ICT product;
   b) the potential risks related to the availability or likelihood of an attack occurring;
   c) whether the vulnerability may be remedied;
   ç) where the vulnerability may be remedied, the possible vulnerability resolutions.
3. The vulnerability impact analysis report, shall where applicable, contain details about possible tools used to exploit the vulnerability. Information regarding possible exploitation tools shall be handled in accordance with appropriate security measures to protect its confidentiality and, where necessary, ensure restricted distribution.
4. The holder of the certificate, in accordance with this decision, shall immediately transmit the vulnerability impact analysis report to the certification body or the national cybersecurity certification authority.
5. Where the vulnerability impact analysis report determines that the vulnerability is not residual within the meaning of the standards referred to in Article 3 of this Decision and can be remedied, Article 38 of this decision shall apply.
6. Where the vulnerability impact analysis report determines that the vulnerability is not residual and cannot be remedied, the certificate shall be withdrawn in accordance with Article 16 of this Decision.
7. The holder of the certificate, pursuant to this decision, shall monitor any residual vulnerabilities to ensure that it cannot be exploited in case of changes in the operational environment.

Article 38
Vulnerability remediation

The holder of the certificate, based on the provisions of this Decision, shall submit a proposal to the certification body for a remediation action. The certification body shall review the certificate in accordance with the provisions of Article 15 of this Decision. The scope of the review shall be determined by the proposed remediation of the vulnerability.

SECTION II
VULNERABILITY DISCLOSURE

Article 39
Information shared with the national cybersecurity certification authority

1. The information provided by the certification body to the national cybersecurity certification authority shall include all elements necessary for the national cybersecurity certification authority to understand the impact of the vulnerability, the changes required to the ICT product, and, where

available, any information from the certification body regarding the implications of the vulnerability for other certified ICT products.
2. The information provided in accordance with Article 39(1) shall not contain details of the means of exploitation of the vulnerability . This provision shall not affect the verification competences of the national cybersecurity certification authority.

Article 40
Cooperation with other national cybersecurity certification authorities

1. The national cybersecurity certification authority shall share the relevant information received pursuant to Article 39 of this Decision with the cybersecurity certification authorities of the Member States of the European Union and with ENISA, upon the accession of the Republic of Albania to the European Union.
2. Other cybersecurity certification authorities, upon the accession of the Republic of Albania to the European Union, may decide to further analyze the vulnerability or, after informing the holder of a certificate based in the European common criteria, may request certification bodies to assess whether the vulnerability may affect other certified ICT products.

Article 41
Publication of the vulnerability

Following the withdrawal of a certificate, the holder of the certificate, pursuant to the provisions of this Decision, shall disclose and report any publicly known and remediated vulnerability in the ICT product, which shall subsequently be recorded in the vulnerability registry as defined in the applicable cybersecurity legislation, and shall share information in accordance with the provisions of Article 10 of this Decision.

CHAPTER VII
RETENTION, DISCLOSURE AND PROTECTION OF INFORMATION

Article 42
Retention of records by certification bodies and ITSEF

1. The ITSEF and the certification body shall maintain a record-keeping system, which shall contain all documents produced in connection with each evaluation and certification they carry out.
2. The certification body and the ITSEF shall securely store the data and keep the records for the purposes of this Decision for at least 5 years after the withdrawal of the relevant certificate, in accordance with the provisions of this Decision. When the certification body has issued a new certificate pursuant to Article 15(2) point (c) of this Decision, the body shall retain the documentation of the withdrawn certificate together with, and for as long as, the new certificate is retained.

Article 43

Information made available by the holder of the certificate

1. The information referred to in Article 10 of this decision is available in Albanian and in another appropriate language that can be easily accessible to users.

2. The holder of the certificate shall securely retain, for the purposes of this Decision and for at least 5 years after the withdrawal of the certificate, the following:

a) the documentation of the information provided to the certification body and the ITSEF during the certification process;

b) a specimen of the certified ICT product.

3. Where the certification body has issued a new certificate pursuant to Article 15(2) point (c) of this Decision, the holder of the certificate shall retain the documentation related to the withdrawn certificate together with the new certificate, and for as long as the new certificate is retained.

4. Upon request of the certification body or the national cybersecurity certification authority, the holder of a certificate shall make available the data and copies referred to in Article 43(2).

Article 44
Protection of information

The national cybersecurity certification authority, the conformity assessment bodies, and all other parties shall ensure the security and protection of business secrets and other confidential information, including trade secrets, as well as the preservation of intellectual property rights, by taking the necessary and appropriate technical and organizational measures.

CHAPTER VIII
MUTUAL RECOGNITION AGREEMENTS

Article 45
Conditions

1. In order for the Republic of Albania to certify products in accordance with European Union regulations, and for such certification to be recognized within the European Union, shall conclude a mutual recognition agreement with the European Union.
2. The mutual recognition agreement shall cover the applicable assurance levels for certified ICT products and, where applicable, also protection profiles.
3. Republic of Albania, for the conclusion of the mutual recognition agreement with the European Union, in accordance with the provisions in Article 45(1), shall fulfill the following conditions:

a) have an authority that:
   i. is public and independent from the entities it supervises and monitors, in terms of

organizational and legal structure, financial source, and decision-making;

ii. have the appropriate supervisory and monitoring powers to perform verifications and is authorized to take suitable corrective measures to ensure compliance;

iii. have an effective, proportionate, and dissuasive penalty system to ensure compliance;

iv. agrees to cooperate with the European Cybersecurity Certification Group and ENISA to exchange best practices and relevant developments in the field of cybersecurity certification and to work towards a uniform interpretation of the currently applicable evaluation criteria and methods, including by applying harmonized documentation that is equivalent to the state-of-the-art documents, as specified in Annex I of this Decision;

b) have an independent authority responsible for accreditation that performs accreditations in line with EU regulations;

c) commit that the evaluation and certification processes and procedures are carried out professionally, taking into account compliance with international standards as defined in Article 3 of this Decision;

ç) have the capability to report previously undetected vulnerabilities and an established, adequate vulnerability disclosure and management procedure;

d) have procedures in place for the effective submission and handling of complaints and for providing effective legal remedies to complainants;

dh) establish a mechanism for cooperation with European Union bodies and Member States in the field of cybersecurity certification, including sharing information about possible non-compliance of certificates, monitoring developments in the field of certification, and ensuring a coordinated approach to maintaining and reviewing certification.

4. Republic of Albania, in addition to the conditions set out in Article 45(3), for the conclusion of a mutual recognition agreement with the European Union covering the assurance level "high", in accordance with provisions in Article 45(1), shall also meet the following conditions:

a) have an independent and public cybersecurity certification authority that performs or delegates evaluation activities to allow certification at the assurance level "high", which are equivalent to the requirements and procedures set out for national cybersecurity authorities pursuant to the EU regulation on cybersecurity certification scheme based on the common criteria and EU regulation on the cybersecurity of the information and communication technology;

b) the mutual recognition agreement shall establish a joint mechanism equivalent to peer assessment for cybersecurity certification based on the common criteria, to improve the exchange of practices and jointly resolve issues in the field of evaluation and certification.

CHAPTER IX
PEER ASSESSMENT OF CERTIFICATION BODIES

Article 46
Peer assessment procedure

1. A certification body that issues certificates based on the European Common Criteria at the assurance level "high" shall undergo a peer assessment regularly and at least every 5 years. The various types of peer assessments are listed in Annex VI of this Decision.
2. The European Cybersecurity Certification Group shall draft and maintain a peer assessment plan, ensuring that this periodicity is respected. Except in duly justified cases, peer assessments shall be performed onsite.
3. The peer assessment may rely on evidence collected during previous peer assessments or equivalent peer assessment procedures of the certification body or the national cybersecurity certification authority, provided that:

a) the results are not older than 5 years;
b) the results are accompanied by a description of the peer assessment procedures established for that scheme, which relate to a peer assessment conducted under another certification scheme;
c) the peer assessment report referred to in Article 48 of this Decision specifies which results are reused with or without further assessment.

4. Where a peer assessment covers a technical domain, the relevant ITSEF shall also be evaluated.
5. The peer-assessed certification body and, where applicable, the national cybersecurity certification authority shall ensure that relevant information is made available to the peer assessment team.
6. The peer assessment shall be conducted by a peer assessment team established in accordance with the provisions of Annex VI of this Decision.

Article 47
Peer assessment phases

1. During the preparatory phase, the members of the peer assessment team shall review the documentation of the certification body, covering its policies and procedures, including the use of state-of-the-art documents.
2. During the on-site visit phase, the peer assessment team evaluates the technical competence of the certification body and, where applicable, the competence of the ITSEF that has conducted at least one evaluation of an ICT product covered by the peer assessment.
3. The duration of the on-site visit phase may be extended or reduced depending on factors such as the possibility of reusing existing evidence and results from previous peer assessments, or the number of ITSEFs and technical domains for which the certification body issues certificates.
4. If applicable, the peer assessment team shall determine the technical competence of each ITSEF by visiting its technical laboratory or laboratories and interviewing its evaluators concerning the technical domain and specific attack methods.
5. In the reporting phase, the peer assessment team documents its conclusions in a peer assessment report, including a Decision and, where applicable, a list of identified non-conformities, each assessed according to a level of criticality.
6. The peer assessment report is first discussed with the assessed certification body by the peer assessment team. Following these discussions, the certification body assessed by the peer assessment team prepares a plan of measures to address the findings.

Article 48
Peer assessment report

1. The peer assessment team provides the certification body with a draft peer assessment report.
2. The certification body assessed by the peer assessment team submits to the peer assessment group its comments regarding the findings, along with a list of commitments to address the

shortcomings identified in the draft peer assessment report.
3. The peer assessment team shall submit to the European Cybersecurity Certification Group a final peer assessment report, which also shall include the comments and commitments made by the peer- assessed certification body. The peer assessment team also includes its position regarding the comments and whether the commitments are sufficient to address the identified shortcomings.
4. Where non-conformities are identified in the peer assessment report, the European Cybersecurity Certification Group may set an appropriate deadline for the assessed certification body to address the non-conformities.
5. The European Cybersecurity Certification Group approves an opinion on the peer assessment report when:

a) the peer assessment report does not identify any non-conformities or the non-conformities have been properly addressed by the peer-assessed certification body, the European Cybersecurity Certification Group may issue a positive opinion, and all relevant documents are published on ENISA's certification website;
b) the peer-assessed certification body fails to address the non-conformities properly within the set deadline, the European Cybersecurity Certification Group may issue a negative opinion, which is published on ENISA's certification website, including the peer assessment report and all relevant documents.

6. Prior to the publication of the opinion, all sensitive, personal, or proprietary information shall be removed from the published documents.

CHAPTER X
FINAL PROVISIONS

Article 49

Repeals on the date of accession of the Republic of Albania to the European Union

On the date of accession of the Republic of Albania to the European Union, all provisions of this Decision shall be repealed, with the exception of Article 26 of this Decision.

Article 50
Final provisions

1. The National Cybersecurity Authority, the institution responsible for market surveillance, the institution responsible for accreditation, and the conformity assessment bodies shall be responsible for the implementation of this Decision.
2. Until 31 December 2027, a certificate may be issued under Article 3(1) of this Decision, applying one of the following standards:
   a) ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 or ISO/IEC 15408-3:2008;
   b) the Common Criteria for Information Technology Security Evaluation, version 3.1, revision 5;
   c) ISO/IEC 18045:2008;
   ç) the Common Methodology for Information Technology Security Evaluation, version 3.1, revision 5.
3. Until 31 December 2027, a certificate issued in accordance with the standards referred to in Article 3(1) of this Decision may be issued under the scheme, with the presumption of conformity with a protection profile that meets the standards listed in Article 50(2).

4. Articles 46, 47 and 48 of this Decision shall start to be implemented upon the entrance into force of the mutual recognition agreement signed between the Republic of Albania and the European Union according to the provisions of Article 45 of this Decision or upon the accession of the Republic of Albania to the European Union.
5. This Decision shall enter into force upon publication in the Official Journal.

PRIME MINISTER
Edi RAMA

ANNEX I: Technical domains and state-of-the-art documents

State-of-the-art documents supporting technical domains and other state-of-the-art documents.

1. State-of-the-art documents supporting technical domains at AVA_VAN level 4 or 5:

a. the documents related to the harmonized evaluation of technical domain "Smart Cards and Similar Devices" are as follows:

i. Minimum ITSEF requirements for security evaluations of Smart Cards and Similar Devices, version 1.1;

ii. Minimum Site Security Requirements, version 1.1;

iii. Application of Common Criteria to integrated circuits, version 1.1;

iv. Security Architecture requirements (ADV_ARC) for Smart Cards and Similar Devices, version 1.1;

v. Certification of 'open' Smart Card products, version 1.1;

vi. Composite product evaluation for Smart Cards and Similar Devices, version 1.1;

vii. Application of Attack Potential to Smartcards and Similar Devices, version 1.2;

b. the documents related to the harmonized evaluation of technical domain "hardware devices with security boxes are as follows:

i. Minimum ITSEF Requirements for security evaluations of hardware devices with security boxes, version 1.1;

ii. Minimum Site Security Requirements, version 1.1;

iii. Application of Attack Potential to hardware devices with security boxes, version 1.2.

2. State-of-the-art documents related to the harmonized accreditation of conformity assessment

bodies are as follows:

a. Accreditation of ITSEFs pursuant to the provisions of the decisions, version 1.1;

b. Accreditation of ITSEFs pursuant to the provisions of the decisions", version 1.6c;

c. Accreditation of CBs pursuant to the provisions of the decisions, version 1.6b.

ANNEX II
Protection profiles certified at AVA_VAN level 4 or 5

1. For the category of remote qualified signature and seal creation devices:
   a) EN 419241-2:2019 – Trustworthy systems supporting server signing - Part 2: Protection profile for qualified signature creation devices for Server Signing;
   b) EN 419221-5:2018 - Protection profiles for cryptographic modules of Trust Service Providers - Part 5: Cryptographic Module for Trust Services.
2. Protection profiles approved as state-of-the-art documents.

ANNEX III –
Recommended protection profiles according to provisions in Annex I

1. For the category of Travel Documents Readable by Travel Document Reading Devices:

   a) Protection profile for machine-readable travel documents using standard inspection procedure with PACE (password authenticated connection creation), BSI-CC-PP-0068-V2-2011-MA-01;

   b) Protection profile for machine-readable travel documents with the "ICAO" application, extended access control, BSI-CC-PP-0056-2009;

   c) Protection profile for machine-readable travel documents with the "ICAO" application, extended access control with PACE (creation of password- authenticated connection), BSI-CC-PP-0056-V2-2012-MA-02;

   ç) Protection profile for machine-readable travel documents with the "ICAO" application, Basic Access Control BSI-CC-PP-0055-2009.

2. For the category of secure signature creation devices:

   a) EN 419211-1:2014 – Protection profiles for secure signature creation devices - Part 1: Overview;

   b) EN 419211-2:2013 - Protection profiles for secure signature creation devices - Part 2: Device with key generation;

   c) EN 419211-3:2013 - Protection profiles for secure signature creation devices - Part 3: Device with key import;

   ç) EN 419211-4:2013 - Protection profiles for secure signature creation devices - Part 4: Extension for device with key generation and trusted channel to certificate generation application;

   d) EN 419211-5:2013 - Protection profiles for secure signature creation devices - Part 5: Extension for device with key generation and trusted channel to signature creation application;

   dh) EN 419211-6:2014 - Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application;

3. for the category of digital tachographs:

   a) digital tachograph - Tachograph card , as defined in the legislation in force;

   b) digital tachograph - Vehicle unit as defined in the legislation in force;

   c) digital tachograph – External Global Navigation Satellite System GNSS (EGF PP) device;

   ç) digital tachograph - Motion sensor (MS PP) according to the definitions in the legislation in force.

4. For the category of secure integrated circuits, smart cards and related devices:

   a) Security IC Platform Protection Profile for Integrated Circuits, BSI-CC-PP-0084-2014;

   b) Java Card System - Open Configuration, V3.0.5 BSI-CC-PP-0099-2017;

   c) Java Card System - Closed Configuration, BSI-CC-PP-0101-2017;

ç) Protection profiles for a specific trusted platform module of a personal computer (PC client) , family 2.0 level 0 revision 1.16, ANSSI-CC-PP-2015/07;

d) Universal SIM card, PU-2009-RT-79, ANSSI-CC-PP-2010/04;

dh) Embedded universal integrated circuit card integrated in machine-to-machine devices, BSI-CC-PP-0089-2015.

5. For the category of interaction (payment) points and payment terminals:

a) Point of Interaction "POI-CHIP-ONLY", ANSSI-CC-PP-2015/01;

b) Point of Interaction "POI-CHIP-ONLY and Open Protocol Package", ANSSI-CC-PP-2015/02;

c) Point of Interaction "POI-COMPREHENSIVE", ANSSI-CC-PP- 2015/03;

ç) Point of Interaction "POI-COMPREHENSIVE and Open Protocol Package", ANSSI-CC-PP-2015/04;

d) Point of Interaction "POI-PED-ONLY", ANSSI-CC-PP-2015/05;

dh) Point of Interaction "POI-PED-ONLY and Open Protocol Package", ANSSI-CC-PP-2015/06.

6. For the category of hardware devices with security boxes:

a) Cryptographic module for cryptographic service-CSP provider signing operations with backup) – CMCSOB protection profile, PP HSM CMCSOB 14167-2, ANSSI-CC-PP-2015/08;

b) Cryptographic module for cryptographic service provider-CSP key generation services – CMCKG protection profile, PP HSM CMCKG 14167-3, ANSSI-CC-PP-2015/09;

c) Cryptographic module for cryptographic service provider-CSP signing operations without backup - PP CMCSO, PP HSM CMCKG 14167-4, ANSSI-CC-PP-2015/10

ANNEX IV: Assurance continuity and certificate review

IV.1 Assurance continuity: scope

1. The following requirements for assurance continuity apply to maintenance activities related to the following:

   a) a re-assessment if an unchanged certified ICT product meets its security requirements;

   b) an evaluation of the impacts of changes to a certified ICT product on its certification;

   c) if included in the certification, the application of patches in accordance with an assessed patch management process;

   ç) if included, the review of the holder of the certificate's lifecycle management or production processes.

2. The holder of a certificate may request a review of the certificate in the following cases:

   a) the certificate is due to expire within nine months;

   b) there has been a change either in the certified ICT product or in another factor that may affect its security functionality;

   c) The holder of the certificate demands that the vulnerability assessment is carried out again in order to reconfirm the assurance of the certificate associated with the ICT product's resistance to cyberattacks.

IV.2 Re-assessment

1. When it is necessary to assess the impact of changes in the threat environment of an unchanged certified ICT product, a re-assessment request shall be submitted to the certification body.

2. The re-assessment shall be carried out by the same ITSEF that was involved in the previous evaluation by reusing all its results that still apply. The evaluation focuses on the assurance activities that are potentially impacted by the changed threat environment of the certified ICT product, in particular the relevant AVA_VAN family and in addition to the assurance lifecycle (ALC) family, where sufficient evidence about the maintenance of the development environment shall be collected again.

3. The ITSEF shall describe the changes and detail the results of the re-assessment with an update of the previous evaluation technical report.

4. The certification body shall review the updated evaluation technical report and establish a re-assessment report. The status of the initial certificate shall then be modified in accordance with the provisions of Article 15 of the Decision.

5. The re-assessment report and updated certificate shall be provided to the national cybersecurity certification authority and ENISA for publication on its cybersecurity certification website.

IV.3 Changes to a certified ICT product

1. When a certified ICT product has been subject to changes, the holder of the certificate wishing

to maintain the certificate shall provide the certification body with an impact analysis report.

2. The impact analysis report shall provide the following elements:

a) an introduction containing the information necessary to identify the impact analysis report and the target of evaluation subject to the changes;

b) a description of the changes to the product;

c) identification of affected developer evidence;

ç) a description of the developer evidence modifications;

d) the findings and the conclusions on the impact on assurance for each change.

3. The certification body shall examine the changes described in the impact analysis report in order to validate their impact upon the assurance of the certified target of evaluation, as proposed in the conclusions of the impact analysis report.

4. Following the examination, the certification body determines the scale of a change as minor or major in correspondence to its impact.

5. Where the changes are confirmed by the certification body as minor, no new certificate shall be issued for the modified ICT product, but a maintenance report to the initial certification report shall be established. The maintenance report shall be included in the impact analysis report, containing following sections:
(a) introduction;
(b) description of changes;
(c) affected developer evidence.

6.Where the changes are confirmed to be major, a re-evaluation shall be carried out in the context of the previous evaluation and reusing any results from the previous evaluation that still apply.

7.After completion the evaluation of the changed target of evaluation, ITSEF shall create a new technical evaluation report. The certification body shall review the updated evaluation technical report and, where applicable, create a new certificate with a new certification report.

IV.4 Patch management

1. A patch management procedure provides a structured process for updating a certified ICT product. The patch management procedure, including the mechanism implemented in the ICT product by the applicant for certification, can be used after the certification of the ICT product under the responsibility of the conformity assessment body.

2. The applicant for certification may include in the certification of the ICT product a patch mechanism as part of a certified management procedure implemented in the ICT product under one of the following conditions:

a) the functionalities affected by the patch reside outside the target of evaluation of the certified ICT product;

b) The patch relates to a predetermined minor change to the certified ICT product;

c) The patch relates to a confirmed vulnerability with critical effects on the security of the certified ICT product.

3. If the patch relates to a major change to the target of evaluation of the certified ICT product in relation to a previously undetected vulnerability having no critical effects to the security of the ICT product, the provisions of Article 15 of the Decision apply .

4. The patch management procedure for an ICT product will be composed of the following elements:

a) the process for the development and release of the patch for the ICT product;

b) the technical mechanism and functions for the adoption of the patch in the ICT product;

c) a set of evaluation activities related to the effectiveness and performance of the technical mechanism.

5. During the certification of the ICT product:

a) the applicant for certification of the ICT product shall provide a description of the patch management procedure;

b) The ITSEF shall verify the following elements if:

i. the developer implemented the patch mechanisms in the ICT product in accordance with the patch management procedure submitted for certification;

ii. the target of evaluation boundaries are separated in a way that changes made to the separated processes do not affect the security of the target of evaluation;

iii. the technical patch mechanism performs in accordance with the provisions of the annex IV.4. and the applicant 's claims;

c) the certification body shall include in the certification report the outcome of the assessed patch management procedure.

6. The holder of the certificate may proceed to apply the patch produced in accordance with the certified patch management procedure to the certified ICT product and shall take the following steps within 5 working days in the following cases:

a) in the case referred to in point 2(a) of Annex IV.4, report the patch to the certification body that shall not change the corresponding certificate;

b) in the case referred to in point 2(b) of Annex IV.4, submit the patch to ITSEF for review. ITSEF shall inform the certification body after the reception of the patch, which the certification body takes the appropriate action on the issuance of a new version of the corresponding certificate according to the scheme and update the certification report;

c) in the case referred to in point 2(c) of Annex IV.4, submits the patch to ITSEF for the necessary re-evaluation, but may deploy the patch in parallel. ITSEF shall inform the certification body after which the certification body starts the relevant certification activities.

ANNEX V: Content of a certification report

V.1 Certification report

1. On the basis of the evaluation technical reports provided by ITSEF, the certification body establishes a certification report to be published together with the corresponding certificate.

2. The certification report is the source of detailed and practical information regarding the ICT product or category of ICT products and about the ICT product's secure deployment and therefore includes publicly available and sharable information of relevance to users and interested parties. This information can be referenced by the certification report.

3. The certification report shall contain at least the following points:

a) executive summary;

b) identification of the ICT product or the ICT product category for protection profiles;

c) security services;

ç) assumptions and clarification of the scope;

d) architectural information;

dh) supplementary cybersecurity information, if applicable;

e) ICT product testing, if it was performed;

ë) where applicable, an identification of the certificate holder's lifecycle management processes and production facilities;

f) results of the evaluation and information regarding the certificate;

g) summary of the security target of the ICT product submitted for certification;

gj) where available, the mark or label associated with the scheme;

h) bibliography.

4. The executive summary shall be a brief summary of the entire certification report. The executive summary provides a clear and concise overview of the evaluation results and includes the following information:

a) the name of the evaluated ICT product, enumeration of the product's components that are part of the evaluation and the ICT product version;

b) name of the ITSEF that performed out the evaluation and, where applicable, the list of subcontractors ;

c) completion date of evaluation;

ç) reference to the evaluation technical report created by ITSEF;

d) brief description of the certification report results, including:

i. the version and if applicable, the release of the Common Criteria applied to the evaluation;

ii. the Common Criteria assurance package and the security assurance components including the AVA_VAN level applied during the evaluation and the corresponding assurance level as set out in Article 8 of the Decision to which the certificate refers;

iii. the security functionality of the evaluated ICT product;

iv. a summary of the threats and organizational security policies addressed by the evaluated ICT product;

v. special configuration requirements;

vi. assumptions about the operating environment;

vii. where applicable, the presence of an approved patch management procedure in accordance with Annex IV.4;

viii. disclaimer(s).

5. The evaluated ICT product shall be clearly identified, including the following information:

a) the name of the evaluated ICT product;

b) an enumeration of the ICT product components that are part of the evaluation;

c) the version number of ICT product's components;

ç) identification of additional requirements to the operating environment of the certified ICT product;

d) name and contact information of the holder of certificate;

dh) where applicable, the patch management procedure included into the certificate;

e) link to the website of the holder where supplementary cybersecurity information for the certified ICT product in accordance with Article 10 of the Decision is provided.

6. The information included in this Section shall be accurate to ensure a complete and accurate representation of the ICT product that can be re-used in future evaluations.

7. The security policy section contains the description of the ICT product's security policy and the policies or rules that the evaluated ICT product shall enforce or comply with. It shall include a description of the policies as follows:

a) the vulnerability handling policy of the holder of the certificate;

b) the assurance continuity policy of the holder of the certificate.

8. Where applicable, the policy may include the conditions regarding the use of a patch management procedure during the validity of the certificate.

9. The section for the assumptions and clarification of scope contains exhaustive information regarding the circumstances and objectives related to the intended use of the product, as referred to in Article 7(1), point (c) of the Decision. The information shall include the following:

a) assumptions on the ICT product usage and deployment in the form of minimum requirements, such as proper installation and configuration and hardware requirements being satisfied;

b) assumptions on the environment for the compliant operation of the ICT product.

10. The information listed in point 9 of Annex V.1 shall be understandable to allow users of the certified ICT product to make informed decisions about the risks associated with its use.

11. The architectural information section shall include a high-level description of the ICT product and its main components in accordance with the Common Criteria ADV_TDS subsystem design.

12. A complete listing of the ICT product supplementary cybersecurity information shall be provided as defined in Article 10 of the Decision. All relevant documentation shall denoted by the version numbers.

13. The ICT product testing section shall include the following information:

a) the name and point of contact of the authority that issued the certificate, including the national cybersecurity certification authority;

b) the name of the ITSEF that performed the evaluation, when different from the certification body;

c) an identification of the used assurance components from the standards referred by Article 3 of the Decision;

ç) the version of the state-of-the-art document and further security evaluation criteria used in the evaluation;

d) the complete and precise settings and configuration of the ICT product during the evaluation, including operational notes and observations if available;

dh) any protection profile used, including the following information:

i. the author of the protection profile;

ii. the name and identifier of the protection profile;

iii. the identifier of the protection profile's certificate;

iv. the name and contact details of the certification body and of the ITSEF involved in the evaluation of the protection profile;

v. the assurance package(s) required for a product conforming to the protection profile.

14. The results of the evaluation and information regarding the certificate section shall include the following information:

a) confirmation of the attained assurance level as referred in Articles 4 and 8 of the Decision;

b) the assurance requirements from the standards as referred in Article 3 of the Decision that the ICT product or protection profile meets, including the AVA_VAN level;

c) detailed description of the assurance requirements, as well as details of how the product meets each of them;

ç) date of issuance and the period of validity of the certificate;

d) unique identifier of the certificate.

15. The security target shall be included in the certification report or referenced and summarized in the certification report and provided with the certification report associated with it for the purposes of publication.

16. The security target may be sanitized in accordance with Annex VI.2.

17. The mark or label associated with the scheme may be inserted in the certification report in accordance with the rules and procedures laid down in Article 13 of the Decision.

18. The bibliography section shall include references to documents used in the compilation of the

certification report. This information shall include at least the following:

a) the security evaluation criteria, state-of-the-art documents and relevant specifications used and their version;

b) the evaluation technical report;

c) the evaluation technical report for composite evaluation, when applicable;

ç) technical reference documentation;

d) developer documentation used in the evaluation efforts.

19. In order to guarantee the reproducibility of the evaluation, the documentation referred to has to be uniquely identified with the appropriate release date and version number.

V.2 Sanitization of a security target for publication

1. The security target to be included in the certification report pursuant to point 1 of Annex VI.1, may be sanitized by the removal or paraphrasing of proprietary technical information.

2. The resulting sanitised security target shall be a real representation of its complete original version. The sanitised security target does not remove information that is necessary to understand the security features of the target of evaluation and the scope of the evaluation.

3. The content of the sanitised security target shall conform minimum requirements as follows:

a) its introduction shall not sanitised and it includes no proprietary information in general;

b) the sanitised security target has to have a unique identifier that is different from its original complete version;

c) the target of evaluation description may be reduced as it may include proprietary and detailed information about the target of evaluation design, which should not published;

ç) target of evaluation security environment description (assumptions, threats, organisational security policies) shall not be reduced, in so far as that information is necessary to understand the scope of the evaluation;

d) security objectives shall not be reduced as all information is to be made public to understand the intention of the security target and target of evaluation;

dh) all security requirements shall be made public. Application notes may give information on how the functional requirements of the Common Criteria as referred to in Article 3 of the Decision were used to understand the security target;

e) the target of evaluation summary specification includes all target of evaluation security functions, but additional proprietary information may be sanitised;

ë) references to protection profiles applied to the to target of evaluation shall be included;

f) the rationale may be sanitised to remove proprietary information.

4. Even if the sanitised security target is not formally evaluated in accordance with the evaluation standards referred to in Article 3, the certification body shall ensure that it complies with the complete and evaluated security target, and reference both the complete and the sanitised security target in the certification report.

ANNEX VI: Scope and team composition for peer assessments

VI.1 Scope of the peer assessment

1. The types of peer assessments are as follows:

   a) Type 1: when a certification body performs certification activities at the AVA_VAN.3 level;

   b) Type 2: when a certification body performs certification activities in relation to a technical domain listed as the state-of-the-art documents as defined in Annex I;

   c) Type 3: when a certification body performs certification activities above AVA_VAN.3 level making use of a protection profile listed as the state-of-the-art documents in Annex II or III.

2. The peer-assessed certification body presents the list of certified ICT products that may be candidate to the review by the peer assessment team, in accordance with the following rules:

   a) The candidate products shall cover the technical scope of the certification body authorization, of which at least two different product evaluations at the assurance level 'high' will be analyzed through the peer assessment, and one protection profile if the certification body has issued the certificate at the assurance level 'high'.

   b) for a type 2 peer assessment, the certification body shall submit at least one product per technical domain and for the concerned ITSEF;

   c) For a Type 3 peer assessment, at least one candidate product shall be evaluated in accordance with an applicable and relevant protection profiles.

VI.2 Peer assessment team

1. The peer assessment team shall consist of at least two experts, each selected from a different certification body from different Member States that issues certificates at the assurance level 'high'. The experts should demonstrate relevant expertise in the standards as referred in Article 3 of the Decision and the state-of-the-art documents that are in scope of the peer assessment.

2. For a type 2 peer assessment, team members shall be selected from the certification bodies authorized for the relevant technical domain.

3. Each member of the peer assessment team shall have at least two years of experience in carrying out certification activities in a certification body;

4. For a type 2 or 3 peer assessment, each member of the peer assessment team must have at least two years of experience in performing certification activities in that technical domain or protection profile and proven expertise as well as participation in the authorization of an ITSEF.

5. The national cybersecurity certification authority which monitors and supervises the peer-assessed certification body and at least one national cybersecurity certification authority whose certification body is not subject to peer assessment shall participate in the peer assessment as an observer. ENISA may also participate in the peer assessment as an observer.

6. The peer-assessed certification body is presented with the composition of the peer assessment team. In justified cases, it may challenge the composition of the peer assessment team and ask for

its review.

ANNEX VII: Content of a certificate pursuant to the scheme

A certificate contains at least:

a) a unique identifier established by the certification body issuing the certificate;

b) information related to the certified ICT product or protection profile and the holder of the certificate, including:

   i. the name of the ICT product or protection profile and, where applicable, of the target of evaluation;

   ii. the type of ICT product or protection profile and, where applicable, of the target of evaluation;

   iii. version of the ICT product or protection profile;

   iv. name, address and contact information of the holder of the certificate;

   v. link to the website of the holder of the certificate containing the supplementary cybersecurity information referred to in Article 10 of the Decision;

c) information related to the evaluation and certification of the ICT product or protection profile, including:

   i. name, address and contact information of the certification body that issued the certificate;

   ii. where different from the certification body, the name of the ITSEF that performed the evaluation;

   iii. name of the national authority responsible for cybersecurity certification;

   iv. a reference to this Decision;

   v. a reference to the certification report associated to the certificate referred to in Annex V;

   vi. the applicable assurance level in accordance with Article 4 of the decision;

   vii. a reference to the version of the standards used for the evaluation, as defined in Article 3 of the Decision;

   viii. identification of the assurance level or package specified in the standards referred to in Article 3 of the Decision and in conformity with Annex VIII, including the security components used and the AVA_VAN level covered;

   ix. where applicable, reference to one or more protection profiles with which the ICT product or protection profile complies;

   x. date of issuance;

   xi. period of validity of the certificate.

d) the mark and label associated with the certificate in accordance with Article 13.

ANNEX VIII: Assurance package declaration

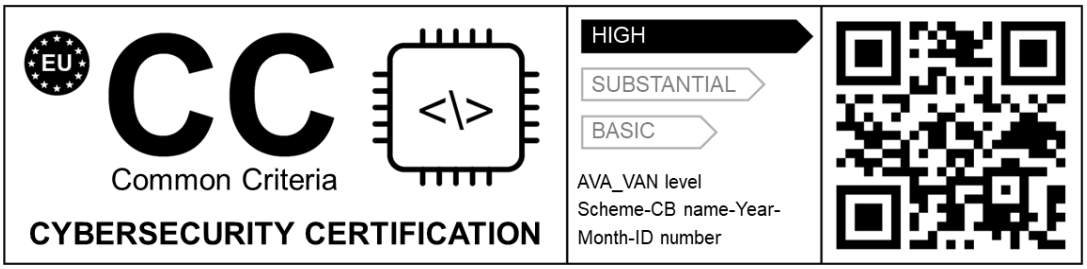
1. Contrary to the definitions in the Common Criteria, an augmentation:
   a) shall not be denoted with '+';
   b) shall not be detailed by a list of all concerned components;
   c) shall not be outlined in detail in the certification report.

2. The assurance level confirmed in a certificate may be complemented by the assurance level of the evaluation as specified in Article 3 of the Decision.

3. If the assurance level confirmed in a certificate does not refer to an augmentation, the certificate indicates one of the following packages:
   a) "the specific assurance package;
   b) "the assurance package conformant to a protection profile" in case it refers to a protection profile without an evaluation assurance level.

ANNEX IX: Mark and label

1. The form of mark and label:



2. If the mark and label are reduced or enlarged, the proportions given in the drawing above shall be respected.

3. Where physically present, the mark and label shall be at least 5 mm high.

ANNEX X: Criteria, documentation and procedure for the authorization of conformity assessment bodies as certification bodies and ITSEF

1. Criteria and documentation for the authorization of certification bodies

1.1. The entity applying to the national cybersecurity certification body in order to obtain authorization as a certification body shall meet the following criteria:

1.1.1. Legal and financial criteria:

a) be registered with the National Business Center as a legal entity with active status;
b) not be under criminal prosecution;
c) not be in legal proceedings related to the exercise of the activity;
ç) not be convicted by judicial bodies;
d) not have unpaid tax liabilities;
dh) not be in bankruptcy or liquidation;
e) be legally, financially and decision-making independent from the organization or the ICT products, ICT services or ICT processes they assess.
ë) not be in the process of compulsory execution for outstanding property obligations at the bailiff's office;

1.1.2 Technical and organizational criteria:

a) be accredited by the authority responsible for accreditation in the Republic of Albania or an accreditation body from a member state of the European Union and which has a mutual recognition agreement with the European Accreditation Organization for this field of accreditation;
b) present the product categories and protection profiles for which authorization is requested;
c) have the structure with the appropriate capacities, qualifications, and competencies according to the requirements set out in the ISO/IEC 19896 standard, to carry out cybersecurity certification activities according to the provisions of the scheme. The structure must have at least 10 (ten) experts with international certifications or 20 (twenty) years of experience in the field of technology or academia, related to the Internet of Things (IoT) and cybersecurity.;
ç) demonstrate the appropriate expertise for the cybersecurity certification of a product ICT or protection profile, collaborating with an ITSEF and an entity interested in participating in a pilot cybersecurity certification process;
d) demonstrate the necessary capacities and capabilities for managing vulnerabilities and undertaking remediation after the certificate has been issued, by presenting data on the issues handled;
dh) demonstrate the assurance continuity;
e) have established a cooperative relationship with an authorized ITSEF, formalized in detailed manner;
ë) demonstrate the appropriate competencies for information protection, through the implementation of technical and organizational measures, conducting risk assessment and threat analysis, as well as maintaining integrity when processing confidential and sensitive data;

f) have a quality management system that guarantees that policies, procedures and measures are implemented and regularly audited and are subject to a cycle of continuous improvement.
g) have the skills for information protection and exchange;

1.2 The documents that shall be submitted by the entity applying to the national cybersecurity certification body for authorization as a certification body in accordance with the criteria of point 1.1 of this Annex are as follows:

1.2.1 Legal and financial documents:
a) extract from the National Business Center, certifying that the company is in active status;
b) attestation issued by the Prosecutor's Office at the Courts of the relevant Jurisdiction that no criminal case has been initiated against the entity related to the activity;
c) attestation issued by the Court of the relevant Jurisdiction that it is not in legal proceedings related to the activity;
ç) attestation of judicial status indicating that the entity has not been convicted;
d) attestation from the tax authorities where the entity is registered, certifying that there are no unpaid tax liabilities;
dh) the statute and the act of establishment of the company;
e) attestation from the bailiff's office that the entity is not in the process of compulsory property execution;
ë) attestation that the entity is not in bankruptcy proceedings;

1.2.2 Technical and organizational documents:
a) accreditation certificate issued by the authority responsible for accreditation in the Republic of Albania or under the mutual recognition agreement with the European Accreditation Organization for this accreditation field;
b) a signed document defining the categories of information technology products and any protection profiles for which authorization is required;
c) the organizational structure, with roles and responsibilities and competencies according to the ISO/IEC 19896 standard, with detailed information for each sector as follows:
    i. description of sector's activities;
    ii. job description for employees;
    iii. skills and professional qualifications of employees;
    iv. appropriate competencies required.
ç) detailed description of the pilot cybersecurity certification process for an ICT product or protection profile, listing the evaluation and certification steps and activities, the certification plan, the certification report including the evaluation plan and the evaluation technical report made available by the authorized ITSEF, as well as a pilot certificate;
d) vulnerability management procedure as well as the register of vulnerabilities successfully addressed for entities that have previously exercised activity within the last 2 (two) years;
dh) the procedure for assurance continuity according to the scheme;
e) cooperation agreement including detailed signed contract with authorized ITSEF;
ë) document with technical and organizational measures according to the ISO/IEC 27001 standard;

f) the most recent internal audit report, along with the list of corrective and preventive actions that evidences periodic evaluations and addressing of findings.
g) procedures for storing and managing information according to ISO/IEC 27001.

2. Criteria and documentation for ITSEF authorization

2.1 The entity applying to the national cybersecurity certification body for the purpose of obtaining authorization as an ITSEF shall meet the following criteria:

2.1.1 Legal and financial criteria:

a) be registered with the National Business Center as a legal entity with active status;
b) not be under criminal prosecution;
c) not be in legal proceedings related to the exercise of the activity;
ç) not be convicted by judicial bodies;
d) not have unpaid tax liabilities;
dh) not be in bankruptcy or liquidation;
e) be legally, financially and decision-making independent from the organization or the ICT products, ICT services or ICT processes they assess.
ë) not be in a compulsory execution process for outstanding property obligations in the bailiff's office;

2.1.2 Technical and organizational criteria:

a) be accredited by the authority responsible for accreditation in the Republic of Albania or an accreditation body from a member state of the European Union and which has a mutual recognition agreement with the European Accreditation Organization for this accreditation field;
b) present the product categories and protection profiles for which authorization is requested;
c) have the structure with the appropriate capacities, qualifications, and competencies according to the requirements set out in the ISO/IEC 19896 standard, for carrying out technical assessment activities including calibration and testing according to the scheme's definitions. The structure must have at least 5 (five) experts with international certifications according to the necessary competencies, as well as more than 5 (five) years of experience in penetration testing, risk assessment, governance and monitoring to international standards, SOC analysis, incident management or forensics analysis.

ç) demonstrate the appropriate expertise for the evaluation of an ICT product or protection profile, by collaborating with a certification body and an interested entity for participating in a pilot cybersecurity evaluation process.

d) have laboratory facilities with sufficient space, technological equipment from the last 5 (five) years, as well as software from well-known national or international companies according to the assessment of NCSA.

dh) prove that it possesses the necessary technical competences and updates them, in the following areas:

i. using threat intelligence and conducting risk assessments;
ii. implementing an assurance level ‘high’ evaluation methodology, with a risk-based approach, to test resilience to sophisticated cyberattacks;

iii. ability to adapt cyberattacks to concrete methodologies, its assessment and improvement;
iv. calculation of the attack scenario according to the ISO/IEC 18045 standard and the state-of-the-art documents as defined in Annex I of this decision;
v. expertise in the use of development, analysis and attack tools as well as IT systems necessary for evaluation activities for the assurance level 'high';
vi. preparing technical descriptions for evaluation activities;
vii. expertise in cryptographic algorithms and protocols and their evaluation;
viii. specific knowledge of the type of product covered by the scope of authorization, including development processes, operational environment and known vulnerabilities;
ix. ability to select and apply source code analysis and penetration testing techniques and tools (Black-box, Grey-box, Crystal Box or White-box);
x. skills in using open source and AI tools for testing, as well as hardware tools for analysis;
xi. performing an advanced reverse-engineering process;
xii. monitoring of evaluation processes for ICT products and protection profiles, and where applicable, for technical domains;
xiii. drafting the evaluation technical report;
xiv. developing procedures for the administration, maintenance and storage of documentation;
xv. technical capabilities to support the certification body in addressing vulnerabilities;
xvi. ability to protect and exchange confidential and sensitive information;

e) demonstrate that it has the appropriate competencies for information protection, through the implementation of technical and organizational measures, conducting risk assessment and threat analysis, as well as maintaining integrity during the processing of confidential data;

ë) have a quality management system that guarantees that policies, procedures and measures are implemented and audited regularly and are subject to a continuous improvement cycle.

2.2 The documents that must be submitted by the entity applying to the national cybersecurity certification body for authorization as an ITSEF in accordance with the criteria are as follows:

2.2.1 Legal and financial documents:

a) extract from the National Business Center, certifying that the company is in active status;

b) attestation issued by the Prosecutor's Office at the Courts of the relevant Jurisdiction that no criminal case has been initiated against the entity related to the activity;

c) attestation issued by the Court of the relevant Jurisdiction that it is not in legal proceedings related to the activity;

ç) attestation of judicial status indicating that the entity has not been convicted;

d) attestation from the tax authorities where the entity is registered, certifying that there are no unpaid tax liabilities;

dh) the statute and act of establishment of the company;

e) attestation from the bailiff's office that the entity is not in the process of compulsory property execution;

ë) attestation that the entity is not in bankruptcy proceedings;

2.2.2 Technical and organizational documents:

a) accreditation certificate issued by the authority responsible for accreditation in the Republic of Albania or under the mutual recognition agreement with the European Accreditation Organization for this accreditation field;
b) a signed document defining the categories of information technology products and any protection profiles for which authorization is required;
c) the organizational structure, with roles and responsibilities and competencies according to the ISO/IEC 19896 standard, with detailed information for each sector as follows:
    i. description of the sector's activities;
    ii. job description for employees;
    iii. the skills and professional qualifications of employees;
    iv. the appropriate competencies required.

ç) detailed description of the pilot evaluation process for an ICT product or profile protection, detailing the pilot evaluation report according to the scheme.

d) plan of the laboratory environment, as well as the list of technological equipment and software with the relevant documentation.

dh) description of the competencies it possesses with the relevant documentation as follows:
i. risk assessment report and evidence that cyber threat intelligence is used;
ii. approved document on the results of an assurance level 'high' evaluation case, with a risk-based approach, for testing resilience to cyberattacks;
iii. adapted evaluation methodology based on cyberattacks;
iv. report of a calculated attack scenario;
v. list of development, analysis and attack tools and IT systems needed for evaluation activities as well as evidence of the qualification of employees to use them;
vi. technical descriptions for evaluation activities;
vii. an evaluation document on the cryptographic algorithms and protocols used;
viii. certifications and training of staff on products included in the scope of authorization, processes and operational environment;
ix. reports on the application of techniques, tools for source code analysis and penetration testing (Black-box, Grey-box, Crystal Box or White-box);
x. list of open source and AI tools for testing, as well as hardware tools for analysis used, as well as evidence of the qualification of employees to use them;
xi. a report on a case where reverse engineering was performed;
xii. monitoring report of the evaluation processes for ICT products and protection profiles, and where applicable, for technical domains;
xiii. evaluation technical report in Albanian;
xiv. approved procedure for the administration, maintenance and storage of documentation;
xv. report on the procedure applied and the measures taken in a specific case to address vulnerabilities in support of the certification body;
xvi. procedures for storing and managing information according to ISO/IEC 27001;

e) technical and organizational measures according to the ISO/IEC 27001 standard;

ë) the most recent internal audit report, together with the list of corrective and preventive actions that evidences periodic evaluation and addressing findings.

3. Procedures and deadlines for reviewing documentation for obtaining authorization from conformity assessment bodies

3.1 Submission of documentation by conformity assessment bodies (CABs) referred to in points 1.1 and 2.1 of this Annex shall be made via official mail or in person to the body responsible for cybersecurity certification.
3.2 The documents referred to in points 1.2 and 2.2 of this Annex shall be originals or certified copies and shall be issued within the validity period.
3.3 The body responsible for cybersecurity certification shall review the documentation submitted by CABs within 30 (thirty) days, where in case of inaccuracies or missing documentation, it shall notify the CAB in writing of the inaccuracies or deficiencies as well as the 15 (fifteen) day deadline for completing the findings in the documentation.
3.4 The body responsible for cybersecurity certification shall, in reasonable cases, extend the deadline for reviewing the documentation submitted by the CABs by 30 (thirty) days.
3.5 In the event that it is confirmed that all the necessary documentation has been submitted, the body responsible for cybersecurity certification shall send the conformity assessment body an authorization plan. The authorization plan shall contain the following elements:

a) Evaluation of the documentation for completeness and content;
b) Structured interviews regarding the cooperation activities between ITSEF and the certification body and the implementation of technical and organizational measures;
c) Where applicable, any other necessary information.

3.6 In cases where additional documentation or clarifications are required for the authorization procedure, the body responsible for cybersecurity certification shall submit the request to the CAB for making it available and shall schedule meetings if necessary.
3.7 The body responsible for cybersecurity certification shall draft the authorization report within a period of 15 (fifteen) days from the completion of the review of the documentation submitted by the CAB.
3.8 The body responsible for cybersecurity certification, when it ascertains that the criteria according to this annex are met, shall issue the authorization for the entity to exercise the activity as a CAB, and shall notify it in writing by making the authorization report available within 7 (seven) days.
3.9 The body responsible for cybersecurity certification, when it ascertains inaccuracies or lack of documentation mentioned in this annex even after the expiration of the deadline for fulfilling the inaccuracies or deficiencies ascertained in the documentation or assessment according to this Annex, shall decide not to grant the authorization to the CAB and shall notify the latter in writing by making the authorization report available.
3.10 The CAB, after receiving the notification of the non-grant of authorization, shall have the right to appeal within 30 (thirty) days from the receipt of the notification to the administrative court.
3.11 The body responsible for cybersecurity certification shall suspend the authorization granted to the CAB, in the following cases:
a) In case of ascertainment of non-fulfillment of the criteria by the CAB on the basis of which the authorization was granted;
b) In case of withdrawal, reduction or suspension by the authority responsible for accreditation of the accreditation scope for the field for which it has received authorization;
c) In case of changes occurring in the conformity assessment body that significantly affect the fulfillment of the requirements for which the CAB is authorized and a re-assessment is required for the renewal of the authorization.