Autoridad Nacional de Certificación de la Ciberseguridad

centro criptológico nacional

ANCC-PO-03

Authorisation of conformity assessment bodies

June 2026
Version 3

MINISTERIO DE DEFENSA

LIMITATION OF LIABILITY

This document is provided in accordance with the terms contained therein, expressly rejecting any type of implied warranty that may be found related. In no event can the National Cryptologic Center be held liable for direct, indirect, incidental or extraordinary damages arising from the use of the information and software indicated even when it is warned of such possibility.

LEGAL NOTICE

It is strictly prohibited, without the written authorization of the National Cryptologic Center, under the sanctions established by law, the partial or total reproduction of this document by any means or procedure, including reprography and computer processing, and the distribution of copies thereof by public rent or loan.

COURTESY TRANSLATION NOTICE

This document is provided solely as a courtesy translation. This translation has been generated using automated tools with minimal human supervision. In the event of any discrepancy, ambiguity, or conflict between this translation and the original Spanish version, the original Spanish version text shall prevail and shall be deemed the only official, authoritative, and legally binding version.

VERSION CONTROL

Version	Comments
1.0	Initial version
2.0	Review of Roles and Responsibilities
3.0	Minor Changes

INDEX

1. INTRODUCTION

1. This document defines the procedure and criteria to be followed by the National Certification Authority **(NCCA)** to authorise conformity assessment bodies **(CABs)** operating at the 'high' assurance level as required by **Regulation (EU) 2019/881 of the European Parliament and of the Council, of 17 April 2019, concerning ENISA (European Union Agency for Cybersecurity) and the certification of cybersecurity of information and communication technologies** (hereinafter referred to as **CSA**). The specific details of the information and evidence required for authorisation are dependent on the specific scheme.

2. CONSIDERATION OF THE AUTHORISATION PROCESS AS A PUBLIC ADMINISTRATIVE PROCEDURE

2. The authorisation of a **CAB** by the **NCCA** is considered a public administrative procedure within the meaning of **Law 39/2015, of 1 October, of the Common Administrative Procedure of Public Administrations [LPAC]**, therefore, all provisions of that law shall apply.

3. This process will be handled as a "simplified" administrative procedure (Article 96 **[LPAC]**), which will include:

   a) Initiation of proceedings at the request of the requesting **CAB** or ex officio.

   b) Possible rectification of the application.

   c) Initial submissions within five working days.

   d) Pre-decision hearing when authorisation is to be refused.

   e) Issuance and notification of the decision.

3. PREPARATORY STEPS

4. The head of the **NCCA** unit **(JAN)** (or delegated staff) shall be responsible for publishing on the official website of that authority **(WNCCA)** the scope options available for authorisation for each **CSA** scheme, indicating the corresponding contact point where this differs between schemes.

5. The **JAN** will also publish in **WNCCA** a general description of the authorisation process and an authorisation application form (e.g. F02 - Application for authorisation from the EUCC Conformity Assessment Body).

6. The application form will require the applicant to provide information on the status of the related accreditation process and will allow for the re-use of the accreditation process as an input for authorisation.

7. The **NCCA** shall make available the complete information required for the authorisation process of each scheme. In the case of **EUCC**, this information is defined in Annex I for **the authorisation of certification bodies and ITSEF for the EUCC scheme [AUTH]**.

4. AUTHORISATION OF CAB. INITIATION OF THE PROCEDURE.

8. The authorisation of a **CAB** shall be made at the application of the **CAB** itself (see Article 54 of the [**LPAC]**).

9. This procedure applies to the **CABs** defined in the **[CSA]**. The schemes may define different types of **CABs**; for example, the **EUCC** considers both **CB** and **ITSEF**. The relationships, dependencies and recommendations on the authorisation calendar are described in the specific state-of-the-art documents of the scheme developed by the European Union Agency for Cybersecurity **(ENISA).**

4.1 APPLICATIONS FOR AUTHORISATION FROM CAB

10. Applications to authorise a **CAB** shall comply with the provisions of Section 3 of the **[LPAC]**, which regulates the minimum content of applications (Article 66) and their time limits.

4.2 RECEIVING APPLICATIONS FOR AUTHORISATION

11. The **JAN** will be the internal focal point for receiving authorisation applications, regardless of the external contact points that can be defined for different schemes.

12. The **JAN** will assign a technical staff from the **NCCA (TA)** to process the authorisation process. The procedure shall respect:

    a) all applicable provisions of the **[LPAC]**; and

    b) the specific state of the art documents of the scheme. In particular, for **EUCC**, shall apply **[AUTH]** by the **NCCA**.

13. The **JAN** will coordinate with the National Accreditation Body **(ENAC)** and the requesting **CAB** the participation of **NCCA** in the associated accreditation process, in accordance with the *ANCC-PO-02, Assistance and Support to the National Accreditation Body*.

4.3 PROCESSING OF APPLICATIONS FOR AUTHORISATION OF IMPLEMENTING REGULATION (EU) 2024/482

4.3.1 VERIFICATION OF THE APPLICATION

14. The **TA** shall verify that the application for authorisation includes all the documentation required, as well as the duly completed form, to authorise a **CAB** under the **EUCC** Scheme, as defined **[AUTH].**

4.3.2 RECTIFICATION OF THE APPLICATION

15. If the request is incorrect or incomplete, the **TA** shall require the **CAB** to remedy it in accordance with Article 68 of the **[LPAC],** as follows**:**

a) Prepare a report detailing incorrect or incomplete information that prevents the commencement of the authorisation process and send it to the **CAB**, opening a period of not less than five days and not more than ten working days for the **CAB** to provide the necessary corrections or submit submissions;

b) If, after the submissions, the application is correct and complete, the process will continue with the processing phase;

c) If, following the submissions, the request cannot be processed, the **JAN** shall notify the **CAB** in writing of the termination of the proceedings, indicating the reasons for the refusal, in accordance with Chapter I of the **[LPAC]**.

16. If the required information is provided within time (or if correction is not necessary), the **JAN** will formally admit the request for processing. From that point on, the procedure shall be governed by the simplified administrative procedure **(Art. 96 of [LPAC]**), with the general objective of resolving within thirty working days of admission. If the complexity of the application so requires, the **JAN** may apply the time limits of the ordinary procedure, guaranteeing in any case a diligent process.

4.3.3 PROCESSING OF THE APPLICATION FOR AUTHORISATION

17. The **TA** will record the updated authorisation application and associated **CAB** information in the National Cybersecurity Certification Authority **(SGA)** information system.

18. In accordance with Article 96(c) of the **[LPAC]**, a short period (five working days) for initial arguments at the start of the proceedings shall be granted once the application has been admitted.

19. The implementation of the authorisation process shall consider the planning, phases and defined guidelines e.g. **[AUTH],** as well as in the guidance published by ENISA**.**

20. Once registered, the **TA** will send the notification of initiation to the Conformity Assessment Body (**CAB**), together with the call for an audit. This audit may be carried out either on-site or remotely, depending on the circumstances. In addition, a verification *checklist* will be sent together with the notification.

21. The assigned **TAs** shall perform the audit based on the established requirements and on the information provided by the **CAB**. This audit shall consider the verification of staff competencies and the assessment of technical and operational measures of the **CAB**.

22. Assessment activities shall be based on evidence from at least one pilot assessment, as set out in state-of-the-art guides or documents e.g. **[AUTH]**. In such assessment, the National Cybersecurity Certification Authority may reuse any relevant evidence from accreditation, prior authorisation or similar activities granted under this regulation, other European cybersecurity certification schemes or applicable national schemes.

23. These activities shall be carried out in compliance with Chapter IV of the **[LPAC]**.

24. The results of the audit shall be reflected in an **'authorisation report'**, drawn up by the **TA** and approved by the **JAN**, which shall meet the content requirements defined in **[AUTH]** and in Chapter IV, Section 3, of the **[LPAC].**

4.3.4 DECISION AUTHORISING THE APPLICATION

25. Based on the results of the audit, the responsible **TA** will draw up a **"Proposal for an Authorisation Decision"**, which will be reviewed by the **JAN**, who will submit it for approval, if appropriate, by the Secretary of State Director of the **CCN** (**SED**).

26. If the results of the evaluation are not sufficient to grant the requested authorisation, the **NCCA** shall open the hearing procedure provided for in Article 82 of the **[LPAC]** ('hearing procedure'), where the interested parties shall have a period of not less than 10 days or more than 15 days to make the submissions they deem appropriate, as well as to provide the documents and justifications they deem relevant in relation to the content. If, before the expiry of the deadline granted, the applicant expressly states his decision not to submit allegations or provide new documentation, the procedure will be understood to have been completed, continuing the processing and producing its effects in the established terms.

27. The formal decision shall be communicated to the applicant Conformity Assessment Body (**CAB)** and shall be signed by the Secretary of State Director of the CCN (**SED**).

28. This decision, if positive, shall be based on the validity of the accreditation issued by **ENAC** and the corresponding authorisation report. The authorisation will be valid for five years from the date of its signature, provided that the **ENAC** accreditation remains in force during that period.

5. RESULTS AND ACTIONS OF THE AUTHORISATION PROCESS

29. Upon successful completion of an application for authorisation, the **JAN** (or delegated staff):

    a) Initiate the notification process under the procedure *'NCCA-PO-09, Notification of Conformity Assessment Bodies',* by which the European Commission (EC) will be notified through **New Approach Notified and Designated Organisations (NANDO),** this being in charge of the final authorisation and its publication after its review.

    b) It shall inform the CAB of the initiation of the notification process and forward the **'authorisation report'** and the **'authorisation decision'.**

    c) It shall update the information published in the **WNCCA** on the authorisation granted once the authorisation has been published by the **EC** in **NANDO**.

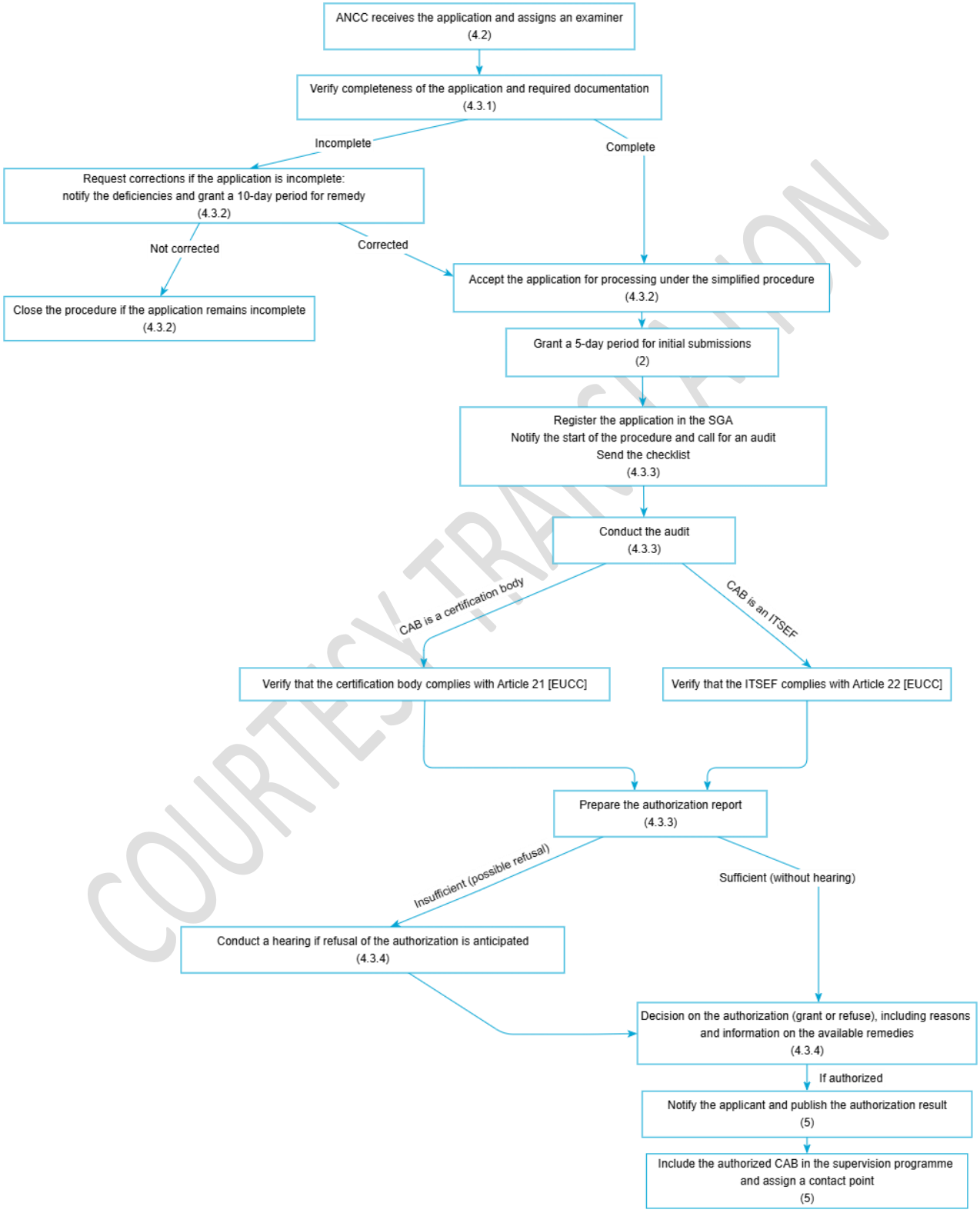
30. After granting the authorisation, the **JAN** (or delegated staff):

    a) It shall include the authorised **CAB** within the scope of the supervision activities of the **NCCA**.

    b) Assign and communicate the contact details of a focal point among the **NCCA** technical staff for the maintenance of the authorisation.

6. PROCESS DIAGRAM

Figure 1— CAB authorisation workflow



7. REFERENCES

ACCCB	Accreditation of certification bodies for EUCC (https://certification.enisa.europa.eu/publications/accreditation-cbs-eucc_en)
ACCITSEF	Accreditation of ITSEF for EUCC (https://certification.enisa.europa.eu/publications/accreditation-itsefs-eucc_en)
AUTH	Authorisation of certification bodies and ITSEF for the EUCC scheme (https://certification.enisa.europa.eu/publications/eucc-guidelines-authorisation-cabs_en)
CSA	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and certification of cybersecurity of information and communication technologies, and repealing Regulation (EU) No 526/2013 (http://data.europa.eu/eli/reg/2019/881/oj)
CSA-E1	Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2019/881 as regards managed security services (http://data.europa.eu/eli/reg/2025/37/oj)
EUCC	Implementing Regulation (EU) 2024/482 of the 31 January 2024 Commission laying down detailed rules for the implementation of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European criteria-based cybersecurity certification scheme common (http://data.europa.eu/eli/reg_impl/2024/482/oj)
LPAC	Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations (https://www.boe.es/eli/es/l/2015/10/01/39/con)
NOTIF	Commission Implementing Regulation (EU) 2024/3143 of 18 December 2024 laying down the circumstances, formats and procedures for notification in accordance with Article 61(5) of Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (European Union Agency for Cybersecurity) and certification of cybersecurity of information and communication technologies (http://data.europa.eu/eli/reg_impl/2024/3143/oj)
VULMD	Guidelines on Vulnerability Management and Disclosure (https://certification.enisa.europa.eu/publications/eucc-guidelines-vulnerability-management-and-disclosure-and-eccg-opinion_en)

8. ACRONYMS

NCCA	National Cybersecurity Certification Authority
CCN	National Cryptologic Center
EC	European Commission
CSIRT	Computer Security Incident Response Teams
ENAC	National Accreditation Body
ENISA	European Union Agency for Cybersecurity
EUCC	European cybersecurity certification scheme based on common criteria
ECCG	European Cybersecurity Certification Group
ITSEF	Information Technology Security Evaluation Facility
JAN	Head of the NCCA unit
CB	Certification Body
CAB	Conformity assessment body
CSA	Cybersecurity Regulations
SED	Secretary of State Director of the CCN
SGA	Information System of the National Cybersecurity Certification Authority
TA	Technical staff attached to the NCCA
ICT	Information and Communication Technologies
EU	European Union
VPA	Voluntary periodic audits
WNCCA	Website of the National Cybersecurity Certification Authority