Autoridad Nacional de Certificación de la Ciberseguridad

centro criptológico nacional

ANCC-PO-09

Notification of conformity assessment bodies

March 2026
Version 2

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

INDEX

1. INTRODUCTION

1. This document defines the procedure to be followed by the National Certification Authority **(NCCA)** in notifying conformity assessment bodies **(CABs)** to the European Commission (**EC)**, as required by **Regulation (EU) 2019/881 of the European Parliament and of the Council, 17 April 2019, on ENISA (European Union Agency for Cybersecurity) and on the certification of cybersecurity of information and communication technologies** (hereinafter **CSA**), and in accordance with **Commission Implementing Regulation (EU) 2024/3143 of the 18 December 2024 [NOTIF]**.

2. CONSIDERATION OF NOTIFICATION AS A PUBLIC ADMINISTRATIVE PROCEDURE

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

3. The process will be handled as a "simplified" administrative procedure (Art. 96 of the **[LPAC]**, including:

   a) initiation of the procedure at the application of the **CAB** or ex officio;

   b) rectification of the application, where applicable;

   c) pre-decision hearing when the application is to be denied;

   d) internal closure of the proceedings.

3. PREPARATORY STEPS

4. The head of the **NCCA** unit **(JAN)** shall identify, obtain and register in the information system of the National Cybersecurity Certification Authority **(SGA)** the access path and requirements of the electronic notification tool developed and managed by the Commission (Decision 768/2008).

5. The **JAN** shall identify and record in the **SGA** the contact points within the **EC** and **ENISA** designated to receive **CAB** notifications.

6. The **JAN** shall publish on the official website of that authority **(WNCCA)** instructions for the **CAB** to communicate their accreditation and authorisation status to the **NCCA**. This channel will also accept accreditation information from **ENAC**.

7. The status of authorisation of a **CAB** will be available internally through the implementation of '*ANCC-PO-03,* Authorisation of Conformity Assessment Bodies'.

8. The outcome of '*ANCC-PO-03,* Authorisation of Conformity Assessment Bodies' shall automatically be considered as input for this notification, without requiring any further action by the **CAB**.

4. NOTIFICATION OF CONFORMITY ASSESSMENT BODIES

9. **CABs** shall be notified upon their own application, when the accreditation of the same has been issued including in the scope the ability to operate in a European cybersecurity certification scheme by a National Accreditation Body or the scope of the **CAB** accreditation has been updated. The **NCCA** shall inform the **CAB** after the notification has been made.

4.1 APPLICATIONS FOR NOTIFICATION

10. Applications to notify the status of accreditation or authorisation of an **CAB** shall comply with the provisions of Section 3 of the **[LPAC]**, which regulates the minimum content of an application (art. 66) and their deadlines.

4.2 RECEIVING INFORMATION ON ACCREDITATION AND AUTHORISATION

11. The **JAN** acts as an internal focal point for receiving notification applications, regardless of the external contact points that may be established for the different schemes.

12. The **JAN** assigns technical staff from the **NCCA (TA)** to process the notification. This procedure is carried out according to the specific state-of-the-art documents for each scheme. For **EUCC**, action is taken in accordance with [**NOTIF**] by **NCCA**.

13. In the case of notifications relating to Implementing Regulation (EU) 2024/482 [**EUCC**], duly completed **F01 – Application for notification from Conformity Assessment Body EUCC** shall be submitted. This form can be found on the official website of the National Cybersecurity Certification Authority (**WNCCA**).

14. The **TA**, previously assigned, shall create a dossier with the associated information of the **CAB** in the **SGA** with a unique tracking number.

4.3 PROCESSING NOTIFICATIONS OF CAB IN IMPLEMENTING REGULATION (EU) 2024/482

4.3.1 VERIFICATION

15. Incoming information on accreditations and authorisations shall be reviewed by the **TA**, which shall:

    a) Identify the corresponding **CAB** and incorporate or update it in the **SGA**.

    b) Collect the following information from the **CAB**:

        1) Name and postal address.

        2) Email address(s).

        3) Telephone number(s).

4) Website.

5) Name and contact details of the **CAB** representative.

6) Type(s) of **CAB** according to scheme (e.g. CB, ITSEF for **EUCC**).

7) Country of registration.

8) **Technical annex for accreditation**.

16. The **TA** shall verify that the **NCCA** has the updated information concerning the Annex as defined in [**NOTIF**].

17. Note that, for the 'High' level, although Protection Profiles are part of the scope of the authorisation, it is not necessary to notify them.

18. This accreditation and authorisation information of the **CAB** may consist of a new accreditation or authorisation, a change in the previously authorised scope of a **CAB**, or the withdrawal of an accreditation or authorisation.

19. If a lack of information is detected or unclear, *Section 4.3.2, "Remediation"* shall apply to allow the applicant to complete or correct the application.

4.3.2 REMEDIATION

20. If the application is incomplete or incorrect, the **TA** shall require the **CAB** to rectify it in accordance with Article 68 of the **[LPAC]**:

a) A report shall be drawn up indicating the incorrect or missing information which prevents the completion of the notification; the report shall be forwarded to the **CAB**, opening a period of ten working days for submissions.

b) After analysing the submissions, a final decision will be issued.

c) If the final decision is to refuse the application, the **JAN** shall notify the **CAB** in writing, including the reasons, in accordance with Chapter I of the **[LPAC]**.

d) If the application is correct and the **CAB** can be notified, the procedure will follow to the next stage.

21. Once the required information has been provided (or if no correction was necessary), the **JAN** will formally admit the application. The procedure will continue under the simplified administrative regime (Art. 96 of the **[LPAC]**), seeking to resolve within a maximum period of thirty working days. If the complexity so requires, the ordinary procedure may be applied without prejudice to the diligence in the decision.

4.3.3 VALIDATION OF THE NOTIFICATION

22. The **TA** shall verify that the scope of accreditation and, where appropriate, authorisation comply with the **EUCC** scheme, in particular:

a) Accreditation of the **ITSEF** for the substantial level of **EUCC**.

b) Accreditation of certification bodies for the **EUCC** substantial level**.**

c) Authorisation of certification bodies and **ITSEF** for the high level of the **EUCC** scheme**.**

d) The scope defined in the **Technical Annex for Accreditation** and in **the audit report provided** by the National Certification Body **(ENAC)**, in accordance with the *ANCC-PO-02, Assistance and Support to the National Accreditation Body*, corresponds to the scope requested.

4.3.4 CLOSURE OF THE PROCEDURE

23. If, as a result of the verification, deficiencies are identified which prevent the continuation of the application, the **NCCA** shall initiate 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 evidence they deem relevant in relation to the content. If, before the expiry of the period granted, the applicant expressly states that they do not intend to submit observations or provide additional documentation, the procedure shall be deemed to be completed, and processing shall continue, with the decision taking effect in accordance with the applicable terms.

24. If the result of the verification is favourable, **JAN** shall be informed of the results of the verification, and shall send the notification, with the information referred to in paragraph 4.3.1, to both the **EC** and **ENISA,** through **New Approach Notified and Designated Organisations (NANDO)**.

25. The **TA** shall record the updated accreditation and authorisation information of the **CAB** in the **SGA**.

26. The **JAN** shall confirm with the **EC** and **ENISA** the receipt of the notification.

27. Once receipt of the notification has been confirmed, both the sending and the confirmation of receipt shall be recorded by the **TA** in the **SGA**, thereby concluding the procedure. The **TA** shall notify the **CAB** of the closure of the proceedings.

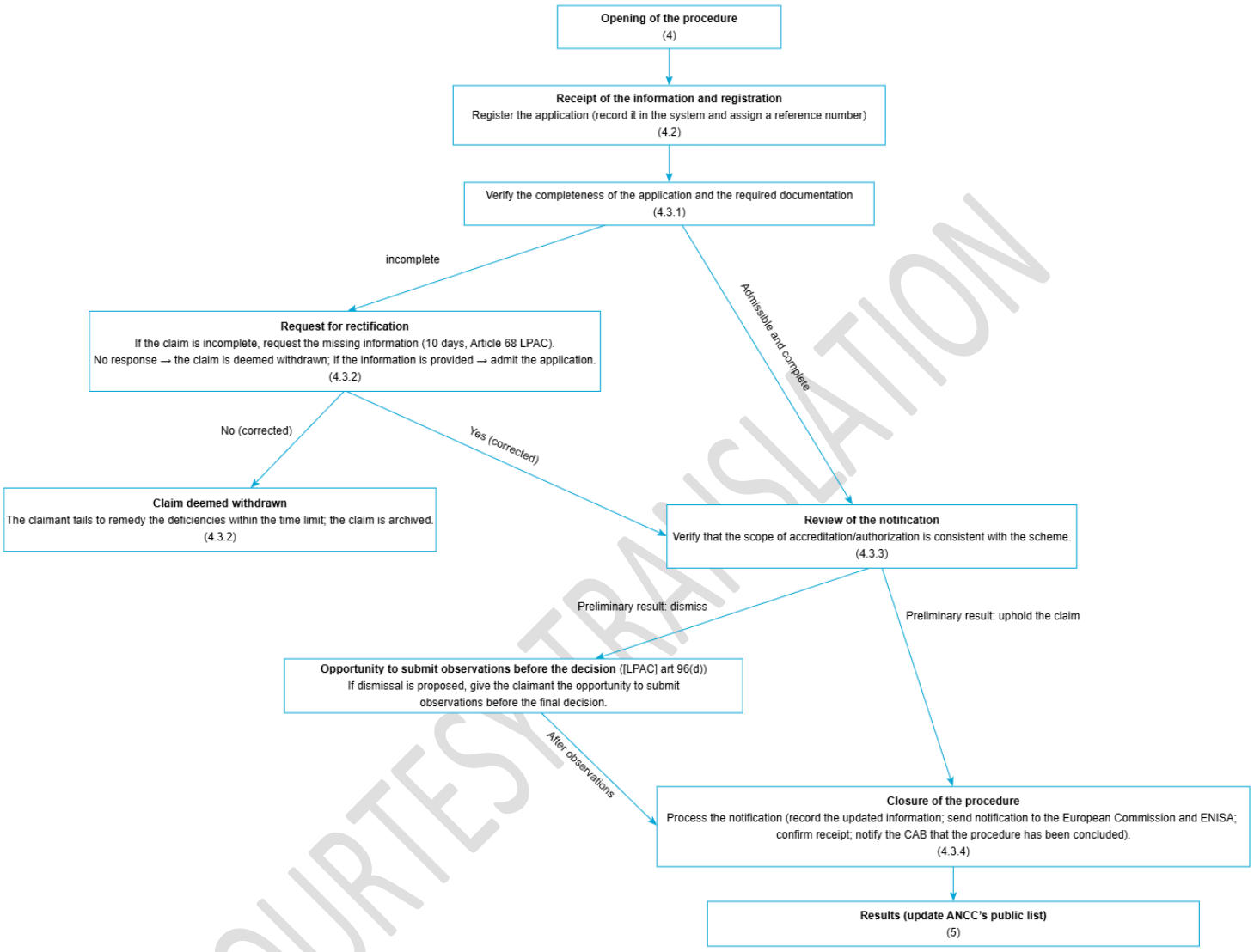
5. RESULTS AND ACTIONS

29. Following successful notification, the **JAN** will ensure that the **CAB** is included in the European lists of notified bodies maintained by the **EC** and that public information from the **NCCA** (e.g. the list of authorised and notified **CABs** on the **WNCCA**) is up to date.

30. If the application is rejected, no notification shall be sent to the **EC** or **ENISA**, and the **CAB** shall remain non-notified under the applicable scheme. The reasons for refusal shall be provided in the decision in accordance with **[LPAC]**.

6. PROCESS DIAGRAM

Figure 1 — CAB notification 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