Autoridad Nacional de Certificación de la Ciberseguridad

centro criptológico nacional

ANCC-PO-02

Assistance and support to the National Accreditation Body

March 2026
Version 1

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

INDEX

1. INTRODUCTION

1. In accordance with **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** (hereinafter: **CSA**) **[CSA]** and also continuing the historical path of collaboration between the National Cryptologic Center (**CCN**) and the National Accreditation Body (**ENAC**) in the area of accreditation of cybersecurity assessment facilities, this document sets out:

   (a) The policy governing collaboration between the National Cybersecurity Certification Authority (**NCCA**) and **ENAC**.
   (b) The resources to be qualified by the **NCCA** to support **ENAC** in its activities related to **CSA** schemes**.**
   (c) The procedure applicable to such cooperation.

2. POLICY GOVERNING THE COLLABORATION BETWEEN NCCA AND ENAC

2. In line with the **CSA**, **NCCA** will actively assist and support **ENAC** in supervision and monitoring the activities of conformity assessment bodies. The **NCCA** will also actively support **ENAC** in the technical assessment activities underpinning the accreditation processes of **CABs**.

3. Close collaboration between the **NCCA** and **ENAC** also helps to optimize the assessment activities needed to support the authorization processes for the 'high' assurance level.

4. The **NCCA** policy governing the collaboration between **NCCA** and **ENAC** is as follows:

   (a) The **NCCA** shall establish continuous and effective communication with **ENAC** on all matters relating to the accreditation status and the results of supervision activities and non-compliance findings.
   (b) The **NCCA** shall qualify the technical staff of the **NCCA (TA**) to be eligible to act as **ENAC** technical experts. Such staff may assist **ENAC** in the accreditation processes of all **CSA** operational schemes and all their assurance levels.
   (c) The **NCCA** may assist **ENAC** in the accreditation processes by carrying out technical evaluation elements of these processes. The participation of **TAs** will be notified to the **CAB** subject to accreditation for acceptance.
   d) Upon request and acceptance by the requesting **CAB**, the results of accreditation processes carried out with **TA** technical support may be considered for the **CAB** authorization process.

3. RESOURCES TO QUALIFY

5. The **NCCA** shall qualify the **TA** as technical experts of **ENAC**. Such staff, as far as possible, will cover all **CSA** certification schemes and all their assurance levels.

6. To ensure the availability of qualified **TA**, the **NCCA** Unit Head **(JAN)** will develop, based on requirements set by **ENAC**, a matrix of skills and knowledge necessary to cover the technical evaluation of **CSA** schemes and their assurance levels.

7. This matrix will be the basis for an annual training and qualification plan. The training and qualification records of the **TA** will be kept updated by the **JAN** with the support of the Information System of the National Cybersecurity Certification Authority **(SGA)**.

8. The **JAN** shall register and maintain a list of qualified **TAs** for the technical assessment of accreditation, as well as the scope of the qualifications granted by **ENAC**.

4. PROCEDURE APPLICABLE TO SUCH COOPERATION

4.1 RECEIVING REQUESTS TO SUPPORT CAB ACCREDITATION PROCESSES

9. Accreditation of a **CAB** is a process managed by **ENAC**. **CAB** must formally apply for such accreditation from **ENAC** and not the **NCCA**. If the **NCCA** receives an application for accreditation, it must indicate to the requesting **CAB** the appropriate procedure, currently documented in https://www.enac.es/quiero-acreditarme.

10. The **JAN** will act as an internal focal point for receiving requests for technical evaluation from **ENAC**. Upon receipt of such requests, **JAN** will identify qualified **TAs** based on the required scope and coordinate with **ENAC** their assignment to the accreditation process.

11. If the accreditation application relates to the "high" assurance level, the **JAN** will request **ENAC** to offer the requesting **CAB** the possibility of reusing the accreditation application as evidence for the corresponding authorization process.

12. If the **CAB** has already applied for authorisation in accordance with *'ANCC-PO-03, authorisation of conformity assessment bodies'*, direct communication between the **NCCA** and the **CAB** may already exist and the **JAN** may make such offer directly.

13. The agreement to reuse the accreditation application as evidence for the authorization process requires that the accreditation process be supported by **TA**. The technical evaluation records and the resulting audit report shall be kept and recorded by **TAs** in the **SGA** with the approval of the requesting **CAB**.

14. A **CAB** may apply for accreditation from **ENAC** without allowing such direct participation. In that case, all authorization activities indicated in the **authorization of certification bodies and ITSEF for the EUCC scheme [AUTH]** shall be carried out «ex novo» by the **NCCA**, without reusing the results of the technical assessment of the accreditation. This lack of coordination does not affect the recognition of the **CAB** accreditation status.

4.2 CONDUCTING TECHNICAL ACCREDITATION ASSESSMENTS

15. The participation and implementation of technical evaluation activities by **TAs** shall be governed by the **ENAC** rules and procedures.

4.3 RESULTS OF THE ACCREDITATION TECHNICAL EVALUATION

16. The result of the accreditation process may be the granting of accreditation by **ENAC** to the requesting **CAB**.

17. If evidence from the accreditation process is reused as evidence for the **CAB** authorization process, **TAs** shall retain the evaluation and audit report records in the **SGA**, with the agreement of the **CAB**.

18. The **NCCA** shall not retain records of accreditation processes other than those successfully concluded for the "high" assurance level where it has been agreed to reuse the accreditation evidence for the **CAB** authorization process.

4.4 COMMUNICATION WITH ENAC

19. The **NCCA** shall maintain close communication with **ENAC** on all matters relating to accreditation status and the results of monitoring, non-compliance activities; **ENAC** will inform the **NCCA** of all accreditation files under the **CSA** that have concluded with the granting of accreditation.

5. 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)

6. 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