Autoridad Nacional de Certificación de la Ciberseguridad

centro criptológico nacional

ANCC-PO-04

Guidelines for cooperation

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. This document defines the following:

   a) The cooperation tasks that the National Certification Authority (**NCCA)** is to carry out, in accordance with **Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019, concerning ENISA (European Union Agency for Cybersecurity) and to the cybersecurity certification of information and communication technologies** (hereinafter referred to as **CSA**)**, and repealing Regulation (EU) and Commission Implementing Regulation (EU) 2024/482/99, of 31 January 2024 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 cybersecurity certification scheme based on the Common Criteria (EUCC).**

   b) For each of these coordination tasks, there should be either a procedure and a guideline to ensure consistent and repeatable implementation, or a link to the relevant **NCCA** general procedure including the relevant coordination task.

2. GENERAL COOPERATION POLICY

2. The National Certification Authority **(NCCA)** shall cooperate with the European Union Agency for Cybersecurity **(ENISA)**, the European Cybersecurity Certification Group **(ECCG)**, other **NCCAs** and relevant national authorities in a timely, structured and secure manner, ensuring confidentiality, the integrity and traceability of all exchanges.

3. The head of the **NCCA** unit **(JAN)** is responsible for cooperation decisions and external commitments, while the technical staff **(TA)** coordinates the day-to-day cooperation activities, acts as a single point of contact, prepare the technical contributions and execute the operational steps required by this procedure.

4. All registrations, notifications, contributions and cooperation decisions shall be recorded in the National Cybersecurity Certification Authority Information System **(SGA)**. Where cooperation relates to other internal procedures, cross-references shall be entered (e.g. '*ANCC-PO-02, assistance and support to the National Accreditation Body*', '*ANCC-PO-03, authorization of conformity assessment bodies*', '*ANCC-PO-09, notification of conformity assessment bodies*', '*ANCC-PO-01, annual report*').

3. PROCEDURES FOR THE IMPLEMENTATION OF THE COOPERATION REQUIREMENTS

3.1 ARTICLE 8(3) OF REGULATION (EU) 2019/881, CONTRIBUTION TO ENISA GUIDELINES AND GOOD PRACTICES

5. **JAN** will compile the annual **TAs** inputs on national certification practices, scheme implementation issues and industry feedback; **JAN** validates the position to be provided to **ENISA** and, where appropriate, to the **ECCG** working structures.

6. Participation in **ENISA** consultations and working groups: **TA** attends sessions, submits written observations and case studies, ensures version control and maintains the registration of submissions in the **SGA**; **JAN** may approve any position or position adopted by the **NCCA**.

7. Integration of results: once **ENISA** publishes guidelines or good practices, **TA** analyzes their applicability, records decisions and follows up on corresponding actions; **JAN** decides on the adoption and necessary updates of internal procedures based on **TAs** proposals.

3.2 ARTICLE 58(H) OF REGULATION (EU) 2019/881, EXCHANGE OF INFORMATION ON POSSIBLE NON-COMPLIANCE

8. Triggering events include market surveillance alerts, complaints, **CB/ITSEF** reports or **NCCA** investigations. **TA** conducts an initial assessment and consolidates evidence; **JAN** determines whether the information warrants cross-border exchange.

9. Without undue delay, **JAN** shares a notice with other **NCCAs (**through the **ECCG** Secure Channel) and with relevant national authorities, including the essential facts, the **ICT** product, service or process affected, the scheme and level of assurance, as well as the suggested actions. Confidential or personal data are minimized and shared only on the basis of the strict need to know them.

10. Link with other procedures: If the case concerns the authorization or supervision of a Conformity Assessment Body (**CAB)**, it shall be coordinated with the *ANCC-PO-03, Authorisation of Conformity Assessment Bodies*; if aspects related to accreditation arise, the National Accreditation Body (**ENAC)** will be informed in accordance with the *ANCC-PO-02, Assistance and Support to the National Accreditation Body*.

3.3 ARTICLE 58(9) OF REGULATION (EU) 2019/881, EXCHANGE OF INFORMATION, EXPERIENCE AND GOOD PRACTICE

11. The head of the unit (**JAN**) or the technical staff (**TA**) designated by the unit participates in the plenary sessions and working groups of the **ECCG**; **TA** prepares summaries (metrics, lessons learned and technical issues), presents national experience, maintains a repository of good practices received and coordinates their adoption at the national level.

12. Requests from the Commission or other **NCCAs** are registered and managed by the **TA**; the **TA** prepare responses for approval by **JAN**, and all exchanges are recorded and kept up to date in the **SGA**.

3.4 ARTICLE 62(2)(G) OF REGULATION (EU) 2019/881, SUPPORT TO THE CCP IN CAPACITY BUILDING AND METHODS OF INFORMATION EXCHANGE

13. Technical staff (**TA**) contribute to the definition and operation of the **ECCG** information exchange tools (secure portals, formats, taxonomies) and participate in capacity-building activities, either as a trainer or as a participant, while the head of the **NCCA** unit (**JAN**) approves the allocation of resources.

14. When the **ECCG** issues cooperation templates, guidelines or reference documents on the state of the art, **TA** ensures its integration into this procedure and related internal workflows; training records are maintained in the **SGA**.

3.5 ARTICLE 7(2) OF IMPLEMENTING REGULATION (EU) 2024/482, DEROGATIONS FROM STATE-OF-THE-ART DOCUMENTS

15. Reception and registration: **NCCA** technical staff (**TA**) records requests for exemptions from the **CAB** with their justification and the proposed alternative methodology, and performs a technical evaluation, optionally consulting external experts subject to confidentiality obligations.

16. Decision and report: The head of the **NCCA** unit (**JAN**) approves or rejects the application; if approved, **TA** notifies the **ECCG** without undue delay of the scope and basis of the decision, records the notification and any opinion of the **ECCG**, and ensures that the associated conditions are applied during supervision of the evaluation.

3.6 ARTICLE 12(3) OF IMPLEMENTING REGULATION (EU) 2024/482, VALIDITY OF THE CERTIFICATE EXCEEDING 5 YEARS

17. Pre-approval procedure: The **CB** presents justification; **TA** assesses life cycle, threat landscape and maintenance measures; **JAN** adopts decision. Upon approval, **TA** notifies the **ECCG** and informs **ENISA** to ensure the accuracy of the repository.

18. Tracking: **TA** plans intermediate checks or status updates for Extended Validity certificates; tracking is recorded in the **SGA**.

3.7 ARTICLE 14(2) OF IMPLEMENTING REGULATION (EU) 2024/482, NOTIFICATIONS OF WITHDRAWAL OF CERTIFICATES

19. After notification of withdrawal by the **CB**, the technical staff of the **NCCA** (**TA**) record the details; verify that **ENISA** has been informed by the **CB**; prepares and sends notifications to national market surveillance authorities and, where appropriate, to sectoral regulators. Optionally, a courtesy notification may be sent to other **NCCA** through the **ECCG** channels.

20. Trend monitoring: **TA** keeps a record of withdrawals to identify possible systemic problems; corrective actions are proposed to the head of the **NCCA** unit (**JAN**). Appropriate interfaces with '*ANCC-PO-09, Notification of Conformity Assessment Bodies*' are established where appropriate.

3.8 ARTICLE 25(9) OF IMPLEMENTING REGULATION (EU) 2024/482, CROSS-BORDER INVESTIGATIONS AND NOTIFICATION TO THE CCP

21. Where investigations involve **ICT** products certified in other Member States, **TA** informs the relevant **NCCAs** to facilitate collaboration and also notifies the **ECCG** of the research and subsequent results. **JAN** coordinates the technical dialog between the authorities and the **CBs** involved.

3.9 ARTICLE 38 OF IMPLEMENTING REGULATION (EU) 2024/482, COOPERATION ON VULNERABILITIES

22. Upon receipt of information on vulnerabilities (in accordance with Article 37 **(EUCC)**), the **JAN** shall be responsible for sharing relevant information with other **NCCAs** and **ENISA** and shall maintain confidentiality until the conditions for publication are met.

23. If requested by another **NCCA**, **TA** facilitates assessments by national **CBs**, ensuring that the certificate holder is informed in advance. In exceptional cases of certifications provided for in Article 38(4), the **JAN** communicates the intention to the **ECCG** and records the opinion delivered.

4. RECORDS, CONFIDENTIALITY AND SECURITY

24. All elements resulting from the cooperation (inputs, notifications, correspondence with the **ECCG** and **ENISA**, opinions, minutes of meetings) shall be stored in the **SGA** with adequate access control and retention periods, in accordance with internal information security policies and scheme requirements.

25. Externally shared documents are subject to version control; sensitive information is marked and managed in accordance with the information protection requirements laid down in Article 43 of **[EUCC]** where applicable.

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
WANCC	Website of the National Cybersecurity Certification Authority