Autoridad Nacional de Certificación de la Ciberseguridad

centro criptológico nacional

ANCC-GU-01

Overview of the National Cybersecurity Certification Authority

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. The Secretary of State Director of the National Intelligence Center, as director of the National Cryptologic Center (**CCN**), has been appointed in Spain as the National Cybersecurity Certification Authority (**NCCA**) for certification schemes developed under **Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and ICT cybersecurity certification** (hereinafter referred to as **CSA**) **[CSA]** and the national implementation of such regulation.

2. According to Article 58 of the **[CSA]**, each Member State is required to designate one or more national cybersecurity certification authorities. The **CCN**, as a support office for the **NCCA**, is responsible for overseeing and managing the implementation of cybersecurity certification schemes in our country.

3. The **CCN** as **NCCA** shall perform the following functions:

   a) Monitor and ensure the application of the standards set out in the European cybersecurity certification schemes, to monitor the conformity of **ICT** products, services and processes with the requirements of the European cybersecurity certificates issued in their respective territories, in cooperation with other relevant market surveillance authorities.

   b) Monitor compliance with the obligations of manufacturers and suppliers of **ICT** products, services or processes established in their respective territories and carrying out conformity self-assessments; in particular, to monitor compliance with and enforcement of the obligations of such manufacturers and suppliers in the relevant European cybersecurity certification scheme.

   c) Actively assist and support national accreditation bodies in monitoring the activities of conformity assessment bodies for the purposes of implementing this regulation.

   d) To monitor and supervise the activities of public bodies referred to in Article 56(5) of the **[CSA]**.

   e) Where appropriate, authorize conformity assessment bodies and restrict, suspend or withdraw authorizations in force in the event of non-compliance by conformity assessment bodies with **CSA** requirements.

   f) To process complaints lodged by natural or legal persons in relation to European cybersecurity certificates issued by national cybersecurity certification authorities or European cybersecurity certificates issued by conformity assessment bodies or, in relation to EU statement of conformity, investigate the subject matter of the complaint to the extent appropriate and inform the complainant of the course and outcome of the investigation within a reasonable time.

   g) To submit to the European Union Agency for Cybersecurity (**ENISA**) and the European Cybersecurity Certification Group **(ECCG)** a summary annual report on the activities carried out under the **CSA**.

h) Cooperate with other national cybersecurity certification authorities or other public authorities, in particular by exchanging information on potential **ICT** products, services and processes that do not comply with the requirements of this Regulation or specific European cybersecurity certification schemes; and

i) follow developments of interest in the field of cybersecurity certification.

4. These responsibilities are essential to ensure a high level of cybersecurity and trust in digital products and services within the European Union.

5. The main roles and positions involved in the performance of the **CCN** as **NCCA** are as follows:

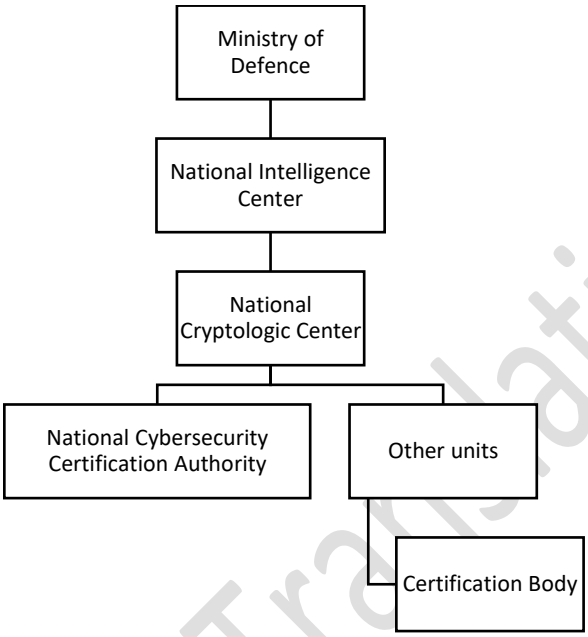
- **SED**: Secretary of State Director of the **CCN**
- **SGCCN**: Deputy Director-General of the **CCN**
- **JAN**: Head of the **NCCA** unit
- **TA**: Technical staff attached to the **NCCA**
- **JOC**: Head of the **CB** unit

6. This document provides a summary of the organization and responsibilities of the **NCCA** under the **CCN**.

2. STRUCTURE

7. The **NCCA** is an administrative unit belonging to the **CCN**, attached to the National Intelligence Centre (**CNI)** according to the following organizational unit diagram:

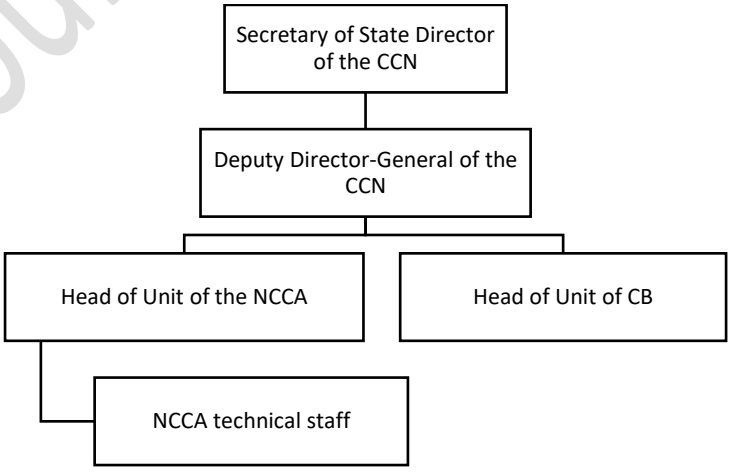
Figure 1 - Structure



8. The following roles are defined by the **CCN** for the implementation of the **NCCA**:

(a) **SED**, the highest-level authority responsible for **NCCA**.
(b) **SGCCN**, the executive authority managing the **NCCA**, is accountable to **SED**.
(c) **JAN**, head of the **NCCA** unit, is accountable to **SGCCN**.
d) **TA**, **NCCA** staff, depends on **JAN**.

Figure 2 - Organizational chart



9. The **CCN** also acts as a Conformity Assessment Body (**CAB)** as a certification body (**CB)** within the meaning of the **CSA**, currently operating within the framework of **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 certification scheme of cybersecurity based on the common criteria [EUCC]** for the "high" assurance level. This **CB** is authorized, supervised and subject to surveillance by the **NCCA**.

10. The impartiality and independence between supervisory and certification activities such as **NCCA** and **CB** respectively is addressed in the document *'CB-001 Risk Analysis and Management of the Impartiality and Independence of the CB/ANCC'* which sets out the requirements applicable to the impartiality and independence of the Certification Body, analyzing the risks to the impartiality and independence required, and establishing the conditions, mechanisms and procedures necessary to mitigate such risks and ensure compliance with those requirements, facilitating the correspondence between the requirements and their compliance mechanism.

11. The following charges are defined by the **CCN** for the implementation of the **CB**:

    (a) **SED**, the highest-level authority responsible for the **CB**.
    (b) **JCCN**, is accountable to **SED**, the executive authority that manages the **CB**.
    (c) **JOC**, head of the **CB** unit, is accountable to **JCCN**.

3. DOCUMENTATION

12. The operating procedures of the **NCCA** are defined in the following documents:

Identifier	Title
ANCC-GU-01	Overview of the National Cybersecurity Certification Authority
ANCC-PO-01	Annual report
ANCC-PO-02	Assistance and support to the National Accreditation Body
ANCC-PO-03	Authorisation of conformity assessment bodies
ANCC-PO-04	Guidelines for cooperation
ANCC-PO-05	Handling of complaints
ANCC-PO-06	Authorisation and supervision procedure for the use of the CCRA mark in the EUCC scheme
ANCC-PO-07	Compliance monitoring
ANCC-PO-08	Monitoring of cybersecurity certification developments
ANCC-PO-09	Notification of conformity assessment bodies
ANCC-PO-10	Peer assessment
ANCC-PO-11	Peer review of the National Cybersecurity Certification Authority
ANCC-PO-12	Receipt of certificates and statements of conformity
ANCC-PO-13	Handling of Vulnerabilities

4. OVERVIEW OF OPERATIONAL ASPECTS

4.1 SERVICES PROCESSED AS PUBLIC ADMINISTRATIVE PROCEDURES

4.1.1 NOTIFICATION OF CAB

13. The **NCCA** is responsible for officially notifying to the European Commission (**EC**) the **CABs** accredited (and, where appropriate, authorized) to issue certificates under each European cybersecurity certification scheme in accordance with **Commission Implementing Regulation (EU) 2024/3143/99, 18 December 2024, laying down the circumstances, formats and procedures for notification pursuant to 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 [NOTIF].** This notification guarantees the recognition of these **CABs** at European level: approximately one year after the entry into force of a scheme, the Commission publishes in the Official Journal of the European Union (**EU**) a list of notified **CABs**, based on information provided by the **NCCA** of each Member State.

14. In addition, the **NCCA** should promptly inform the Commission of any change in the status of **CABs**, such as new authorizations, suspensions or withdrawals, so that the official register of **EU** conformity assessment bodies is kept up to date. Notifications are submitted via an electronic system designated as specified by the **EC**. In Spain, the act of notifying a **CAB** is handled as an administrative procedure, which implies that it follows formal steps. For more details, see the procedure '*ANCC-PO-09, Notification of Conformity Assessment Bodies*'.

4.1.2 AUTHORIZATION OF CAB

15. The **NCCA** is responsible for authorizing **CABs** to operate under the European cybersecurity certification schemes at the corresponding assurance levels (in particular for "high" level schemes such as **EUCC**). Before granting an authorization, the **NCCA** verifies that a candidate **CAB** is duly accredited by the National Accreditation Body (**ENAC**) for the relevant scope and that it meets any additional requirements specific to the scheme defined in the European framework. Once authorized, a **CAB** is formally empowered to issue certificates under the scheme, and the **NCCA** shall notify the **EC** of this status. The **NCCA** also retains the power to restrict, suspend or withdraw an authorization if the **CAB** fails to comply with its obligations or if its competence is in doubt, ensuring that only qualified and compliant bodies can continue to issue certificates. This authorization procedure is described in the procedure '*ANCC-PO-03 authorization of conformity assessment bodies*'.

4.1.3 HANDLING OF COMPLAINTS

16. The **NCCA** maintains a formal procedure for handling complaints from manufacturers, service providers or other stakeholders regarding cybersecurity certifications and **EU**

self-assessments of conformity. Such complaints may concern, for example, a European certificate issued by the **NCCA** or an accredited **CAB**, or issues related to an **EU statement of conformity**. Upon receipt of a complaint, **NCCA** conducts the relevant investigation and keeps the complainant informed of the progress and outcome. This process ensures accountability in the certification system and provides a mechanism to address concerns about certified products or the conduct of **CABs**. It should be noted that the findings arising from complaints may also lead to broader monitoring by the **NCCA** (e.g., substantiated complaints about a **CAB** or certificate may trigger additional scrutiny or remedial action under **NCCA** surveillance procedures). For more details, see the procedure "*ANCC-PO-05, Handling of complaints*".

4.1.4 RECEPTION AND REGISTRATION OF CERTIFICATES

17. The **NCCA** ensures that all cybersecurity certificates issued under European schemes in Spain are duly received by the authority and registered in its national registry. Whenever a notified and/or authorized **CAB** issues a new certificate (e.g. under the **EUCC** scheme), the **NCCA** may require **CAB** to notify or forward the details of the certificate to the **NCCA** Information System. Keeping this register up to date enables the **NCCA** to track certified products and services for supervisory purposes.

18. In addition, as part of the mutual recognition of the European framework, the **NCCA** accepts certificates issued by **CAB** from other Member States as valid at national level without additional certification steps. The **NCCA** registers such incoming certificates and incorporates them into national market surveillance activities (ensuring, for example, that Spanish regulators and users are aware of these certified products). The **NCCA** acts as a national contact point and exchange center for all European cybersecurity certificates in its territory, facilitating their recognition and monitoring. For more details, see the procedure "*ANCC-PO-12, Receipt of certificates and statements of conformity*".

4.1.5 HANDLING OF VULNERABILITIES

19. **NCCA** coordinates a process to manage and disclose vulnerabilities found in products, services, **ICT** processes or managed security services certified under European cybersecurity schemes. If a significant security vulnerability is reported, the **NCCA** works with the issuing **CAB** and relevant **CSIRT** teams to ensure that the product manufacturer is informed and remediation actions are taken in a timely manner.

20. The specific policies of each scheme (e.g. **EUCC** Guidelines) define the role of the **NCCA** in coordinated vulnerability disclosure. The **NCCA** can facilitate communication between security researchers, the affected manufacturer and the **CAB**, monitor the progress of vulnerability mitigation and, if necessary, take measures such as advising on the status or conditions of the certificate until the problem is resolved. By integrating this vulnerability management into the certification lifecycle, **NCCA** helps preserve trust in certified products even in the face of new threats, ensuring that post-certification security incidents are managed responsibly. For more details, see the procedure *ANCC-PO-13, Handling of Vulnerabilities*.

4.1.6 AUTHORISATION AND SUPERVISION FOR THE USE OF THE CCRA MARK IN THE EUCC SCHEME

21. The procedure "*ANCC-PO-06, Authorisation and Supervision Procedure for the Use of the CCRA Mark in the EUCC Scheme*" establishes the framework by which the **NCCA** authorizes and supervises the use of the **CCRA** mark in certificates issued under the **EUCC** Scheme by certification bodies (**CB**) who are not signatories to the international agreement. The process is articulated as a simplified administrative procedure in accordance with Law 39/2015 and includes an initial documentary review, the opening of the file, the exhaustive technical supervision of each certification and, finally, a reasoned resolution that may authorize or deny the use of the mark. Its objective is to ensure that the certificates issued maintain the rigor, traceability and methodological alignment required by the **CCRA**, thus preserving their international recognition and validity.

The procedure also defines the obligations that **CBs** must assume in order to maintain authorization, including participation in the **CCRA** *Voluntary Periodic Assessments* (**VPA**), full delivery of technical documentation, cooperation with **NCCA** and international audit teams, the availability of technical staff and the implementation of corrective actions where appropriate. Failure to comply with these obligations may result in the suspension or withdrawal of the use of the **CCRA** mark. Overall, the procedure ensures that any authorized body operates at a level of requirement equivalent to that of the government schemes that sign the agreement, strengthening the trust and consistency of the European certification ecosystem

4.2 SUPPORT TO THE NATIONAL ACCREDITATION BODY

22. **NCCA** actively supports the National Accreditation Body **(ENAC)** in accrediting cybersecurity conformity assessment bodies. This collaboration includes providing technical knowledge and guidance specific to the scheme during accreditation processes – for example, **NCCA** can assign qualified **TA** to assist **ENAC** in the evaluation of **CABs** candidates for European schemes. **NCCA** also shares information with **ENAC** on the performance and compliance of accredited **CAB** (derived from **NCCA**'s own supervisory activities) to ensure that any issues are recognized and addressed in the context of accreditation. Working closely in line with Article 58(c) of the **[CSA]**, the **NCCA** and the **ENAC** help maintain a high level of competence among accredited **CABs** and speed the path from accreditation to authorization (e.g. the results of technical assessments obtained with the support of the **NCCA** can be used as evidence when these **CABs** apply for authorization from the **NCCA**). For more details, see the procedure *ANCC-PO-02, Assistance and Support to the National Accreditation Body*.

4.3 COOPERATION AND EXCHANGE OF INFORMATION

23. **NCCA** cooperates with other national cybersecurity certification authorities and European institutions to harmonize practices and share critical information. It participates in the European Cybersecurity Certification Group (**ECCG**), where it

interacts with the **EC** and its counterparts in other countries to exchange experiences, discuss cases of non-compliance or emerging risks, and develop coordinated approaches. Through such cooperation (as provided for in Article 58(h) of the **[CSA]**), the **NCCA** contributes to the consistent implementation of certification schemes in all Member States and helps to enable joint responses to cross-border cybersecurity challenges. Information from the **NCCA**'s own activities (e.g. significant monitoring findings or best practices) is shared as appropriate in these forums, encouraging alignment and continuous improvement at European level. For more details, see the procedure "*ANCC-PO-04, Cooperation Guidelines*".

4.4 MONITORING COMPLIANCE AND ENFORCEMENT

24. **NCCA** continuously monitors compliance with issued certificates, certified **ICT** products or services, and activities of notified and authorized **CABs**, to ensure continued adherence to the standards of each cybersecurity certification scheme. It employs mechanisms such as requiring periodic reports from the **CAB**, reviewing samples of certified products or documentation, and conducting its own audits or investigations.

25. If a security breach or deficiency is detected – for example, if a certified product is determined to no longer meet the required security criteria or if a **CAB** is in breach of its obligations – the **NCCA** has the power to take enforcement measures. It may require information or corrective action, coordinate with market surveillance authorities, and in serious cases withdraw or invalidate the certificates concerned and suspend or revoke the authorization of the responsible **CAB**. These powers (granted by the **CSA** and national legislation) enable the **NCCA** to preserve the credibility of the certification framework. By ensuring compliance in this way, the **NCCA** helps maintain confidence in certificates issued under its supervision. For more details, see the procedure *"ANCC-PO-07, Monitoring Compliance"*.

4.5 PEER ASSESSMENT

26. Under certain European schemes – notably the **EUCC** scheme for high-level certifications – authorized certification bodies undergo regular peer assessment conducted by experts from other Member State. The **NCCA** facilitates these peer assessment processes for any high-level **CAB** under its supervision, coordinating with the **ECCG** schedule (which aims to have each relevant **CAB** evaluated at least every five years).

27. During a peer assessment, a team of certification bodies other than the one assessed examines the past procedures, technical competence and certification dossiers of the evaluated certification body (often through documentation review and on-site visits); and then issue a report with findings and recommendations. The **NCCA** ensures that the **CAB** provides full cooperation and that any resulting recommendations or necessary improvements are implemented. These scheme-specific peer assessments complement the **NCCA**'s own oversight and contribute to the consistent quality of certifications across Europe. For more details, see the procedure *'ANCC-PO-10, peer* assessment'.

4.6 PEER REVIEW

28. The **NCCA** itself is subject to periodic peer reviews organized by the **EC** and the **ECCG** to assess its performance as a national certification authority, as set out in **Commission Implementing Regulation (EU) 2025/2540 of 9 December 2025, laying down detailed rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the establishment of a plan for reviews [REV]**. Normally carried out every few years (at least once every five years), these reviews involve a multinational team of experts from other Member States examining how the **NCCA** carries out its functions, such as monitoring **CABs**, enforcing scheme requirements, managing complaints and interacting with other authorities.

29. **NCCA** prepares for each peer review by providing extensive documentation of its procedures and fully cooperating with the review team. Conversely, the **NCCA** also contributes to the system by sending its own experts to peer review the authorities of other countries, thus exchanging best practices. Following a review, the findings and any recommendations for improvement are discussed within the **ECCG**, and are expected to be addressed by the **NCCA**, strengthening its processes as needed. This mutual peer review mechanism helps ensure high and harmonized standards of oversight across all **EU** national cybersecurity certification authorities. For more details, see the procedure *"ANCC-PO-11, peer review of the NCCA"*.

4.7 FOLLOW-UP OF DEVELOPMENTS

30. Each year, **NCCA** produces an annual summary report of its monitoring and certification activities, which is submitted to **ENISA** and the **ECCG** in the first quarter of the following year. This report, required by the **[CSA]**, covers the key areas of the work of the **NCCA** — including the oversight of the **CABs**, the assistance provided to **ENAC**, authorization decisions, and any peer review or evaluation activities that have taken place. It provides both quantitative data (e.g. number of audits, support actions, authorizations) and qualitative analyses (such as observed trends, problems and recommendations for improvement) of the activities of the year. Through this annual report, the **NCCA** contributes to European-level monitoring and the exchange of best practices, as the aggregated national reports help inform discussions and harmonization efforts within the **ECCG.** For more details, see the procedure "*ANCC-PO-01, Annual Report*".

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)
REV	Commission Implementing Regulation (EU) 2025/2540 of 9 December 2025 laying down detailed rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the establishment of a plan for peer reviews (http://data.europa.eu/eli/reg_impl/2025/2540/oj)

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