Autoridad Nacional de Certificación de la Ciberseguridad

centro criptológico nacional

ANCC-PO-06

Authorisation and supervision procedure for the use of the CCRA mark in the EUCC scheme

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 lays down the procedure for Certification Bodies **(CB)** private and public non-signatories to the **CCRA** agreement must continue to obtain authorization for use of the **CCRA** mark on certificates issued under the **EUCC** scheme and under the supervision of the National Cybersecurity Certification Authority **(NCCA**).

2. The objective is to ensure that the certificates issued by these **CBs** maintain a level of technical rigor, reliability, traceability and international recognition equivalent to that of the certificates issued by government agencies that sign the **CCRA** agreement.

3. The procedure includes:

   - The model of supervision prior to the issuance of the certificate required by the document [**CCEU**] for the co-existence of **CCRA** and **EUCC**.
   - Obligations relating to Voluntary Periodic Assessments (**VPA**) as defined in the guide and its technical annex [**VPA**].
   - The adaptation of the procedure to the Spanish legal framework in accordance with Law 39/2015, applying the modality of simplified common administrative procedure.

4. Where a **CB** requests supervision by certificate for the use of the **CCRA** mark, it shall compulsorily sign that it accepts the obligations for its use as set out in the Annex to this document and as defined in paragraph 5.

5. The signing of the application form is an indispensable prerequisite and has the following effects:

   a) Expressly recognizes the authority of the **NCCA** to supervise each **EUCC** certificate that seeks to incorporate the **CCRA** mark.

   b) Commits the **CB** to undergo prior technical reviews, provide complete documentation, attend meetings and apply corrective measures.

   c) Requires the **CB** to undergo audits by international teams of the **CCRA** signatories in the framework of the **VPA,** under the of document [**VPA**].

   d) Enables the **NCCA** to exchange technical information with the Management Committee (hereinafter referred to as **CCMC**) and other members of the **CCRA** when the process so requires.

   e) It establishes the conditions of security, confidentiality and preservation of information in accordance with national requirements (including the framework of Royal Decree 421/2004 that regulates the functions of the **CCN**).

6. Without prior express acceptance of the aforementioned agreement:

   - No administrative file will be opened.

- No request for technical supervision will be accepted.
- Consequently, the use of the **CCRA** mark may not be authorized.

7. This prerequisite ensures that all private and public **CCRA** non-signatories operating under the **EUCC** are subject from the outset to the same level of supervision, control and responsibility as internationally required by the **CCRA**.

2. LEGAL AND RECOGNITION FRAMEWORK

8. This procedure is based on:

- **Law 39/2015, on the Common Administrative Procedure of Public Administrations** (art. 96 – Simplified procedure) [**LPAC**].
- Mutual Recognition Agreement **CCRA** (2014) [**CCRA**].
- Document CCMC011 v1.0 (2025): **CCRA** and **EUCC** Co-Existence [**CCEU**].
- CCES-2005-06-21 v2.7: Conducting VPA [**VPA**].
- ISO/IEC 17065:2012, Basis for **CB** Competence.
- **Regulation (EU) 2019/881** (Cybersecurity Act) and **EUCC** Technical Documentation [**CSA**].

3. CONSIDERATION OF THE AUTHORIZATION PROCESS AS A PUBLIC ADMINISTRATIVE PROCEDURE

9. The authorization of a private and public certification body **(CB)** not signatories to the **CCRA** agreement 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]**, all provisions of this law shall therefore apply.

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

    a) Initiation of the procedure at the request of the **CB**, by submitting the official form (admission decision within a maximum of 15 days).

    b) Possible rectification of the application.

    c) Observations at the start of the proceedings within five working days.

    d) Hearing prior to the decision when authorization is to be refused.

    e) Issuance and notification of the decision.

4. CERTIFICATE SUPERVISION PROCEDURE

11. The supervision procedure prior to issuance of each **CCRA**-marked **EUCC** certificate is the main mechanism by which the **NCCA** ensures that certificates issued by private and public **CBs** non-signatories of **CCRA** meet the requirements of the **CCRA** and maintain a level of technical rigor equivalent to that of the government body that signed the **CCRA** agreement.

12. This procedure includes three main phases:

    a) Application, initial documentary review and admission of the application.

    b) Technical supervision of the file.

    c) Reasoned decision and closure of the file.

13. Each phase is described below.

4.1 INITIATION OF THE PROCEDURE AND RECEIPT OF THE APPLICATION

14. The procedure begins when the **CB** formally submits the application for supervision and use of the **CCRA** mark. The **NCCA** only initiates the processing if the mandatory documentation is presented in a complete and correct manner.

15. The **CB** must submit electronically:

- Official form (Annex I) completed.
- Security Target for the product to be certified
- Designation of the evaluating laboratory responsible for the technical analysis.
- Certification and evaluation plan, including planned activities and level of assurance.

4.2 PROCESSING OF THE APPLICATION

4.2.1 INITIAL DOCUMENTARY REVIEW

16. Upon receipt of the application, a competent technician in the **EUCC** certification scheme (**TA**) shall be appointed who shall conduct a first technical and administrative review with three main objectives:

- Verification of the Security Target
  - Verification of its completeness in accordance with the standard.
  - Clear identification of the TOE and the scope of certification.
  - Confirmation of compliance with applicable protection standards or profiles.
  - Adequacy of the level of assurance requested to the **CB** accreditation.

- Verification of the Evaluation Plan

Assessment of consistency between:
- Planned activities and required level of assurance (EAL/AVA_VAN).
- Test planning and vulnerability analysis activities.
- Consistency of the planned effort with the declared scope.

- Identification of initial risks
  The **NCCA** will identify potential problems that will require attention in subsequent supervision:
  - Ambiguities or inconsistencies in the Security Target.
  - Deficiencies in the preliminary vulnerability analysis.
  - Technical decisions anticipating the need for detailed review.

4.2.2 RECTIFICATION OF THE APPLICATION

17. If the application is incomplete or contains deficiencies, the **TA** shall request the **CB** to rectify it in accordance with Article 68 of the [**LPAC**], as follows:

    a) Prepare a report detailing incorrect or incomplete information that prevents the initiation of the authorization process and send it to the **CB**, opening a period of 10 working days for the **CB** to provide the necessary corrections or submit submissions.

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

    c) If, following the observations, the request remains incapable of being processed, the **JAN** shall notify the **CB** in writing of the termination of the proceedings, indicating the reasons for the refusal, in accordance with Chapter I of the **[LPAC]**.

18. 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.

4.2.3 OPENING OF THE FILE

19. Before admitting the dossier:

    - The **TA** verifies that all mandatory documentation has been provided.
    - If no correction is required, or once completed, the application shall be admitted for processing.

20. Once the application is admitted:

    - The **TA** will open an individual file associated with the requested certificate.

- This dossier shall be recorded in the Administrative System (**SGA**) with a unique tracking number.
- The **CB** shall be formally notified of admission to processing.
- In such notification the **TA** may include initial observations to be considered at the technical supervision stage.

4.2.4 TECHNICAL SUPERVISION OF THE FILE

21. Before authorizing the issuance of an **EUCC** certificate bearing the **CCRA** mark, the **CB** must submit to the **NCCA** all the final technical documentation generated during the assessment. This information serves as a basis for the review of the **NCCA** and for the technical supervisory meeting before authorizing the use of the **CCRA** mark on the issued certificate.

22. In accordance with Article 96(c) of the **[LPAC]**, a short period (five working days) for Initial submissions shall be granted once the application has been accepted.

23. The **CB** should send to the **NCCA**:

a) Complete ETR developed by the laboratory.
b) Complete Security Target.
c) Draft Certification Report.
d) ETR validation reports and justifications for decisions of the certification body.
e) Laboratory observation reports.
f) Records of internal laboratory-**CB** meetings and technical agreements, if any.

4.2.5 DETAILED TECHNICAL REVIEW CARRIED OUT BY NCCA

24. The **TA** designated by **NCCA** will review all the documentation provided before convening the technical meeting. Oversight includes three key areas:

25. The **TA** will review the ETR by verifying at least:

- The scope of the Security Target.
- The adequacy and sufficiency of the tests performed
- The methodological rigor of the AVA analysis (threats, hypothesis, coverage).
- The validity of the technical reasoning of the laboratory and the **CB**.
- The adequacy of the closure of deviations detected during the evaluation.

26. Additionally, the **TA** will specifically analyze critical technical decisions taking into account the points where:

- The laboratory has performed relevant technical interpretations.
- **CC** or **CCRA** interpretations have been applied.
- Alternative or partial evidence has been accepted.

27. As part of the document analysis, the **TA** will review the vulnerability analysis by verifying:

- The completeness of threats and scenarios considered.
- The depth of the vulnerability identification process.
- The correction of the test methods used.
- The soundness of the argument about the absence of exploitable vulnerabilities.

4.2.6 TECHNICAL REVIEW MEETING

28. Once the documentary review of the dossier has been completed, the **TA** designated by **NCCA** will convene a formal technical meeting with the actors involved in the evaluation process. The following shall participate in the meeting:

- The supervisory technical team of **NCCA**, which shall be responsible for verifying the conformity of the process with the requirements of the **CCRA** and **EUCC**.
- The **CB** certification team, which shall be responsible for the decisions taken during certification.
- Optionally, the technical team of the evaluating laboratory, which may present and justify the evaluation activities carried out and the results documented in the ETR.

29. The purpose of the meeting is to carry out a joint, comprehensive and transparent review of the technical file. In general, **NCCA** will look for:

a) Confirm that the evaluation process will have been implemented in accordance with the **Common Criteria** methodology, without unjustified deviations or lack of coverage.
b) Clarify critical technical decisions, especially those in which the laboratory or **CB** has had to interpret requirements, apply complex decisions or resolve situations not foreseen in the schema documentation.
c) To evaluate methodological consistency throughout all phases of the process, verifying the absence of contradictions or inconsistencies between evidence, intermediate conclusions and results.
d) Verify that the dossier will meet the requirements of the **CCRA** necessary to authorize the use of the international mark.
e) Validate that the vulnerability analysis has been sufficient and robust, considering relevant threats, adequate evidence and justifications for the non-existence of exploitable vulnerabilities.
f) Confirm the alignment of the file with the document [**CCEU**], which regulates the coexistence between **EUCC** and **CCRA**.

30. During the meeting, critical elements of the dossier, such as applied interpretations, decisions taken in borderline situations, use of alternative evidence or treatment of relevant findings, will be reviewed with special attention. If inadequacies or aspects

requiring extension or correction are detected during the session, the measures to be adopted and the deadlines in which the **CB** or the laboratory must attend them will be agreed.

4.3 RESOLUTION OF THE PROCEDURE

31. Once the investigation is completed, the **TA** will evaluate the results and decide to propose a decision on the authorization requested from **JAN**.

32. If, after the technical supervisory meeting and after the analysis of all the information provided by the **CB** and, where appropriate, by the evaluating laboratory, the **JAN** issues a favorable administrative decision, this shall terminate the prior supervision procedure for the use of the **CCRA** mark. The decision shall be issued in accordance with the provisions of the simplified administrative procedure.

33. The relevant content derived from technical supervision, including clarifications, commitments and additional requirements, will be directly reflected in the resolution notified to the **CB**, which will serve as a single and binding document for the purposes of the procedure.

34. The resolution to be issued by the **NCCA** may adopt one of the following modalities:

- Authorization for the use of the **CCRA** mark

  It shall be issued when the **NCCA** considers that the dossier, including the evaluation carried out, the decisions taken and the technical clarifications provided, shall fully comply with the requirements established by the **CCRA** and the **EUCC**. The authorization will allow the **CB** to incorporate the **CCRA** mark in the relevant certificate, without additional conditions.

- Reasoned refusal

  If the preliminary finding is dismissive, the applicant shall be given the opportunity to make observations, 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 observations 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 any submissions or provide new documentation, the procedure will be understood to have been completed, continuing the processing and producing the resolution its effects in the established terms.

  Once the submissions have been assessed, if the conclusion is dismissal, the **NCCA** will issue a dismissal decision when it identifies essential breaches, significant methodological discrepancies, insufficient assurance or unresolved risks after the prior hearing that may compromise the confidence of the **CCRA**.

In this case, the decision shall include the corresponding technical reasons and, if appropriate, recommendations for the reopening of the file.

35. The resolution to be notified to the **CB** will reflect in a structured manner:

- Technical considerations arising from the supervision process.
- The conclusions reached by the **NCCA** on the quality and technical adequacy of the dossier with the requirements for the use of the **CCRA** mark.
- Additional requirements, if any.
- The type of resolution adopted and its effects.

36. The resolution:

- The **CB** shall be notified electronically,
- be incorporated into the administrative file,
- And it must be kept by the **CB** during the entire validity of the certificate.

37. With the notification of a favorable resolution, the **NCCA** will register the authorization internally in its system.

38. From this point on, the **CB** shall be entitled to issue the **EUCC** certificate bearing the **CCRA** mark, fully respecting the conditions of use and the requirements established by the **NCCA** and the **CCRA**.

5. OBLIGATIONS OF CERTIFICATION BODIES IN RELATION TO VOLUNTARY PERIODIC AUDITS (VPA) UNDER THE CCRA AGREEMENT.

39. Voluntary Periodic Audits (**VPA**) are international technical assessments conducted periodically under the Common Criteria Recognition Arrangement (**CCRA**), with the aim of verifying that all participants to the agreement —including private and public **CBs** not signatories to the **CCRA** agreement authorized under the **EUCC**— maintain homogeneous levels of competence, methodological rigor, traceability and correctly apply the **Common Criteria** standard.

40. This procedure is regulated by document [**VPA**]. In essence, **VPAs** will seek to ensure that:

- The technical work carried out by **CBs** and laboratories is consistent and aligned with the criteria and practices of the **CCRA**.
- The **Common Criteria** standard is correctly applied in all phases of the evaluation and certification process.
- Technical decisions taken by certifiers are sound, justified and consistent.
- There are no methodological deviations that compromise confidence in the international agreement.
- There is real and complete traceability between evidence, evaluation activities and final conclusions.
- Continuous improvement is promoted, identifying good practices and opportunities for strengthening.

41. In short, **VPA** is not administrative audits, but technical reviews, carried out by teams designated by the **CCRA** countries, aimed at safeguarding the overall quality and credibility of the scheme.

42. The private or public **CB** not signatory to the **CCRA** agreement wishing to use the **CCRA** mark must explicitly and contractually accept that it will be subject to **VPAs**, which shall cooperate fully with the **NCCA**, and that it shall provide all the information requested in accordance with the **CCRA** procedure and the requirements of its Technical Annex.

43. This section details **CBs** obligations in this area.

5.1 CBS OBLIGATIONS FOR THE USE OF THE CCRA MARK

44. To be able to use the **CCRA** mark in certificates issued under the **EUCC** scheme, **CBs** must assume a full and continuous commitment to the supervisory mechanisms established by both the **NCCA** and the **CCRA** itself. This commitment begins with the formal acceptance to participate in the Voluntary Periodic Assessments (**VPA**) in accordance with the procedure defined in [**VPA**], assuming that they may be subject to periodic or extraordinary evaluations carried out by international teams designated by the signatory countries of the agreement.

45. The signing of the Agreement on Supervision and use of the **CCRA** mark constitutes the instrument by which the **CB** explicitly recognizes these obligations and undertakes to comply with them without restriction; its absence makes it impossible, in any case, to authorize the use of the mark.

46. During **VPAs**, **NCCA** will act as a national interlocutor to the **CCMC** and to the international auditing team, which means that the **CB** must provide the **NCCA** with all the necessary support so that the process can be carried out with rigor and transparency.

47. This support shall include access to all documentation generated by the certification body in the evaluation and certification processes of the **EUCC** certification files selected by the auditing team, as well as preliminary and final versions of the ETR, ST and its annexes, review and validation records, vulnerability reports, internal reports and any relevant correspondence with the developer or the evaluating laboratory.

48. Furthermore, the **CB** shall ensure that all such documentation is available and at the level of detail required by the Technical Annex to the **VPA** procedure, including information related to the product life cycle, evidence of evaluation activities, registers of technical decisions and, essentially, the information related to the product life cycle, the evidence of evaluation activities, the technical decision-making and, in particular, the information required by the **CB**. complete traceability between ST, ETR and certificate.

49. The **CB** shall make available to the **NCCA** all documentation related to its quality system, including that linked to its accreditation in accordance with ISO/IEC 17065, provided that such documentation is relevant and likely to be provided in accordance with the technical annex to the **VPA** procedure. This obligation shall include quality manuals, internal procedures, control registers, audit reports, evidence of compliance with accreditation requirements and any other document enabling the **NCCA** or the international team of the **CCRA** to verify the correct application of the **Common Criteria** methodology, the technical competence of the laboratory and the consistency of the evaluation process. The laboratory shall ensure that all this documentation will be accessible, complete and presented in an organized manner, always preserving the established confidentiality requirements.

50. The **CB** shall also ensure the availability of the technical staff involved in the certification body itself. It will be the responsibility of **CBs** to ensure that certifiers will be available to answer technical, methodological or procedural questions during the development of the **VPA**, either in person or through remote sessions. It shall also provide logistical and operational support to **NCCA**, facilitating access to the certification body's facilities, spaces for technical meetings, secure means of communication and appropriate mechanisms for the management of confidential or sensitive documentation.

51. Once a **VPA** has been completed, the **CB** will assume responsibility for analyzing the report issued by the audit team in coordination with the **NCCA** and for drawing up a corrective action plan where necessary. The plan must include clearly defined and

responsible time frames, and the **CB** shall implement the required corrections and periodically notify the **NCCA** of the status of its implementation.

52. Failure to effectively implement corrective actions resulting from a supervisory process or a **VPA** may lead to progressive consequences, ranging from temporary suspension of use of the **CCRA** mark to, in the most serious cases, withdrawal of authorization for its use. Likewise, when the non-compliance is persistent or affects the overall confidence of the scheme, the **NCCA** may request the withdrawal of the **CCRA** mark of all certificates previously issued by the **CB** under that framework, thereby ensuring the integrity of international recognition. This shall be without prejudice to formal communication with the **CCMC**, in accordance with the procedures laid down in the **CCRA**.

53. Finally, the **CB** will have the obligation to maintain complete, up-to-date and accessible records of all evidence, technical decisions, additional documentation and internal procedures applied during the certification processes. These records must be kept for at least five years from the loss of validity of the certification. The results derived from the **VPAs** may impact subsequent supervision procedures, potentially leading to enhanced controls, increased documentary requirements or additional conditions for the authorization of the use of the **CCRA** mark in future certificates.

6. 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)
EUCC-E1	18 December 2024 Commission Implementing Regulation (EU) 2024/3144 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation (http://data.europa.eu/eli/reg_impl/2024/3144/oj)
EUCC-E2	8 December 2025 Commission Implementing Regulation (EU) 2025/2462 amending Implementing Regulation (EU) 2024/482 as regards definitions, certification of ICT product series, continuity of the guarantee and state of the art documents (http://data.europa.eu/eli/reg_impl/2025/2462/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)
CCRA	Common Criteria Certificate Recognition Arrangement. (https://commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf)
VPA	Conducting Voluntary Periodic Assessments of Schemes Participating in the CCRA. (https://commoncriteriaportal.org/files/operatingprocedures/CCES-2005-06-21%20Conducting%20VPAs%20v2.7.pdf)
CCEU	CCRA and EUCC Co-existence. (https://commoncriteriaportal.org/files/supdocs/CCMC-011-v1.0-2025-Mar-19-CCRA%20and%20EUCC%20Co-existence.pdf)

7. 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

8. ANNEX I - APPLICATION FORM FOR AUTHORISATION AND SUPERVISION FOR THE USE OF THE CCRA MARK IN THE EUCC SCHEME

APPLICANT CERTIFICATION BODY	
Business name	
CIF	
Postal address	
ISO/IEC 17065 accreditation number	
Notified Body Number (NANDO)	
Contact person	
Contact email	

REPRESENTATIVE OF THE CERTIFICATION BODY	
First name	
Surnames	
DNI / Passport	
Telephone	
Email	

CONTACT PERSON FOR THE APPLICATION	
First name	
Surnames	
DNI / Passport	
Telephone	
Email	

SUBJECT

Application for authorization and supervision for the use of the CCRA mark in the EUCC scheme.

STATEMENT
The applicant organization submits this application to obtain authorization from the NCCA to use the CCRA mark in the EUCC certificate associated with the certified product. To that end, it declares that it acts in accordance with Regulation (EU) 2019/881 and Implementing Regulation (EU) 2024/482, and that it complies with the requirements applicable to the EUCC evaluation and certification process at the relevant assurance level. By submitting this request, the entity expresses its commitment to the obligations established in the ANCC-PO-06 procedure, including the full provision of the necessary technical documentation, participation in the International Monitoring Mechanisms of the CCRA (VPA) and compliance with the decisions and requirements arising from the process. Accordingly, it formally requests that the NCCA evaluate this application and, where appropriate, authorize the use of the CCRA mark in the certificate to be issued.

REQUEST
The applicant requests that the NCCA evaluate this application and, where appropriate, authorize the use of the CCRA mark in the certificate to be issued.

DATA FROM THE EUCC CERTIFICATION DOSSIER FOR WHICH THE USE OF THE CCRA MARK IS REQUESTED	
Commercial name of the evaluated product (TOE)	
Product version	
Manufacturer / developer	
Assurance Level	
Evaluation Laboratory (ITSEF)	
ISO/IEC 17025 accreditation number	
Notified Body Number (NANDO)	

REFERENCES OF THE DOCUMENTATION PROVIDED	
Security Target (ST)	
Evaluation and certification plan	
Complementary technical evidence	

ACCEPTS THE OBLIGATIONS OF THE CERTIFICATION BODY FOR THE USE OF THE CCRA MARK

The Certification Body (CB) acknowledges and accepts full compliance with the following conditions, which constitute mandatory requirements for prior supervision and authorization of the use of the CCRA mark:

1. Acceptance of supervision and participation in VPAs

The Certification Body (CB) accepts:

- Submit each EUCC certificate to prior technical supervision by NCCA.
- Participate in the Voluntary Periodic Assessments (VPA) under the CCRA framework.
- Be subject to evaluation by international teams designated by the CCRA signatory countries.
- Facilitate interviews, technical meetings and clarifications required by NCCA or VPA teams.

Non-acceptance or non-cooperation will prevent the authorization of the use of the CCRA mark.

2. Provision of complete and accessible documentation

The CB shall provide the NCCA, in a structured and comprehensive digital format:

- Security Target (ST) and annexes, where applicable.
- Evaluation Technical Report (ETR).
- Laboratory evidence, test reports and vulnerability analysis.
- Records of reviews, technical decisions and internal actions.
- Relevant correspondence with developers or laboratories.
- All the information required in the Technical Annex of the VPA procedure.

3. Cooperation with NCCA

The CB

- It will cooperate fully with NCCA and the international VPA teams.
- It will provide all the technical evidence of the evaluation process.
- It shall make available to the NCCA all the documentation associated with the quality system

and its ENAC accreditation, including manuals, procedures, internal audits and records, in accordance with the VPA Technical Annex.
- It will keep such documentation organized, accessible and under strict confidentiality criteria.

4. Staff availability and operational support

The CB agrees to ensure:

- The availability of the certifiers responsible for the file for technical clarifications.
- The presence of technical laboratory personnel when necessary.
- The preparation of facilities, rooms, technical resources and secure channels for the conduct of meetings and reviews.

5. Corrective actions

The CB accepts that:

- It will analyze, in coordination with NCCA, the reports derived from monitoring and VPAs.
- Draw up a corrective action plan where appropriate.
- It will implement all the required measures within the established deadlines.
- It shall periodically inform the NCCA of the degree of implementation.

The CB expressly recognizes that the lack of effective implementation of corrective actions, in addition to formal communication to the CCMC, may result in:

- Temporary suspension of the use of the CCRA mark,
- Withdrawal of authorization for its use, or
- Withdrawal of the CCRA mark from all certificates previously issued under such recognition.

6. Exclusive coordination through the NCCA

The CB accepts that:

- All communication from the international VPA team should preferably be channeled through the NCCA.
- Preferably, it will not respond directly to international auditors without such coordination.
- It shall immediately notify the NCCA of any request received.
- It will maintain the confidentiality of all the information processed.

7. Record keeping

The CB shall retain, for at least five (5) years after the certificate ceases to be valid:

- Complete files.
- Technical evidence and complementary documentation.
- Registers of technical decisions.
- Internal procedures and current templates.

DECLARES

The applicant declares that:

- All the information provided in this form is true to the extent to which it reaches its knowledge

- You have read and understand all the obligations included in this form.
- It accepts in full all derivative obligations.
- It assumes its compliance as an essential requirement for the supervision and authorization of the use of the CCRA mark.

SIGNATURE OF THE REPRESENTATIVE	
Place	
Date	
Signature	
Recipient body	Ministry of Defense – National Intelligence Center National Cryptologic Center