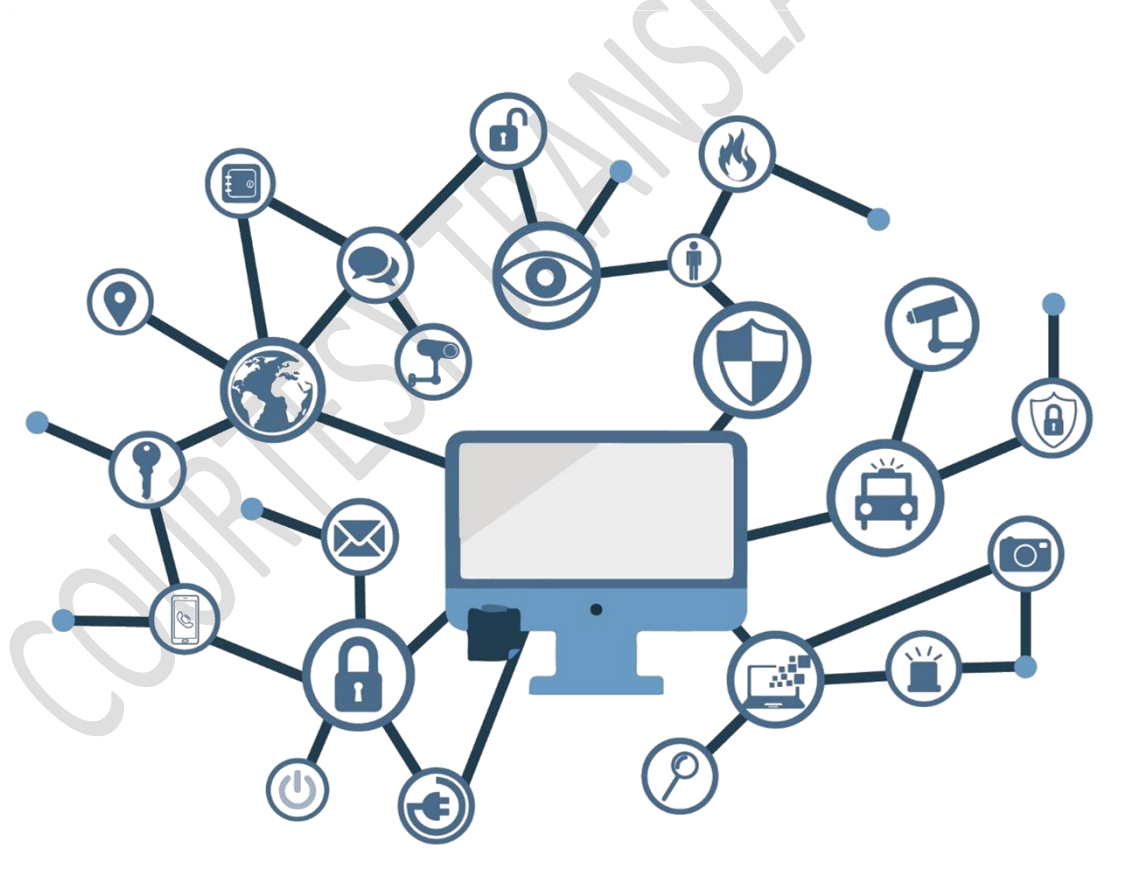


ANCC-PO-12

Receipt of certificates and statements of conformity



March 2026
Version 1

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

COURTESY TRANSLATION

INDEX

1. INTRODUCTION.....	5
2. PREPARATORY STEPS	6
3. START OF THE RECEPTION PROCEDURE	7
3.1 RECEPTION AND REGISTRATION	7
3.2 PROCESSING OF THE SUBMISSION OF THE CERTIFICATE OR STATEMENTS OF CONFORMITY	7
3.2.1 VERIFICATION OF THE APPLICATION.....	7
3.2.2 RECTIFICATION OF THE APPLICATION	8
3.2.3 CLOSING THE APPLICATION.....	8
4. RESULTS AND ACTIONS	9
5. PROCESS DIAGRAM.....	10
6. REFERENCES.....	11
7. ACRONYMS.....	12

1. INTRODUCTION

1. This procedure defines how the National Certification Authority (**NCCA**) receives, examines and registers European cybersecurity certificates, as well as EU statements of conformity issued under **Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification** (hereinafter the **CSA**) [**CSA**], and under European cybersecurity certification schemes. It includes the verification of documentary integrity, the verification of the validity of certificates and statements of conformity, procedures in cases of non-compliance, and registration in the relevant national register.

COURTESY TRANSLATION

2. PREPARATORY STEPS

2. The **NCCA** unit head (**JAN**) shall publish on the website of the National Cybersecurity Certification Authority (**WNCCA**), clear instructions on the submission of EUCC certificates and **EU** conformity self-assessments, including the required forms and information to be submitted by email.
3. A form (or template) shall be made available, including instructions for its completion and specifying the mandatory information to be provided.
4. The **NCCA** shall ensure that its internal systems and resources are prepared to receive and manage these applications efficiently, including their registration and follow-up through the **NCCA** Management System (**SGA**).

3. START OF THE RECEPTION PROCEDURE

5. The receipt of certificates and statements of conformity begins with the submission of the required information by an authorized **CAB** or the responsible manufacturer or supplier. This procedure may also be initiated ex officio by the **NCCA** where it becomes aware of the existence of a relevant certificate or statements of conformity outside a formal application.
6. This procedure applies to the receipt of **EUCC** certificates and statements of conformity issued under the **CSA**. This procedure is limited to these schemes; if a new European cybersecurity certification scheme imposes similar requirements for the submission of certificates to the **NCCA**, this procedure may be revised to incorporate those obligations.

3.1 RECEPTION AND REGISTRATION

7. The required documentation and form must be submitted through the email address provided on the **WNCCA**. The head of the **NCCA** unit (**JAN**) will act as an internal focal point to ensure that all applications received, whatever the channel, are received by the **NCCA**. Once received, each application will be recorded with the **SGA** and assigned an internal reference. The **JAN** (or delegated staff) will acknowledge receipt to the applicant, confirming that the application has been recorded and will be processed. The **JAN** will then assign the file to a technical staff of the **NCCA** (**TA**) for processing.

3.2 PROCESSING OF THE SUBMISSION OF THE CERTIFICATE OR STATEMENTS OF CONFORMITY

3.2.1 VERIFICATION OF THE APPLICATION

8. The designated **TA** shall verify that the submission is complete and admissible for registration, verifying that:
 - a) The form (**F-04**) provided is duly completed, with all the required data.
 - b) All mandatory elements of the presentation are included:
 - a. Certificate.
 - b. Security target.
 - c. Certification report.
9. If mandatory information is missing or the application contains formal deficiencies, the **TA** will require the applicant to correct the deficiencies within the prescribed time. Submissions from non-recognized entities (e.g. an unauthorized body or a third-party manufacturer or supplier) may not be admissible. If the application clearly relates to a matter outside the competence of the **NCCA**, the applicant shall be informed thereof and recorded with the **SGA**.

3.2.2 RECTIFICATION OF THE APPLICATION

10. In the event of an incorrect or incomplete application, the **TA** shall request the applicant to rectify the application in accordance with the following:
 - a) A report detailing the incorrect or missing information that prevents the processing of the application shall be prepared and sent to the applicant, opening a period of ten working days to provide the required corrections or to submit submissions;
 - b) If, after the expiry of that period and the arguments have been assessed, the application is corrected and complete, the procedure will continue as described in the following section;
 - c) if the application remains flawed and cannot be processed after that period, the **JAN** shall notify the applicant in writing of the termination of the procedure and shall be recorded in the **SGA**.
11. If the requested information is provided within the time limit (or no correction is necessary), the **JAN** will formally admit the application for further processing.

3.2.3 CLOSING THE APPLICATION

12. The **TA** shall record all validated information in the **SGA** for follow-up, as the updated maintenance of this register enables the **NCCA** to monitor certified products and services for supervisory purposes as defined in the procedure «ANCC-PO-07, compliance monitoring.»
13. The **TA** shall also be responsible for notifying the applicant of the satisfactory registration of the application.

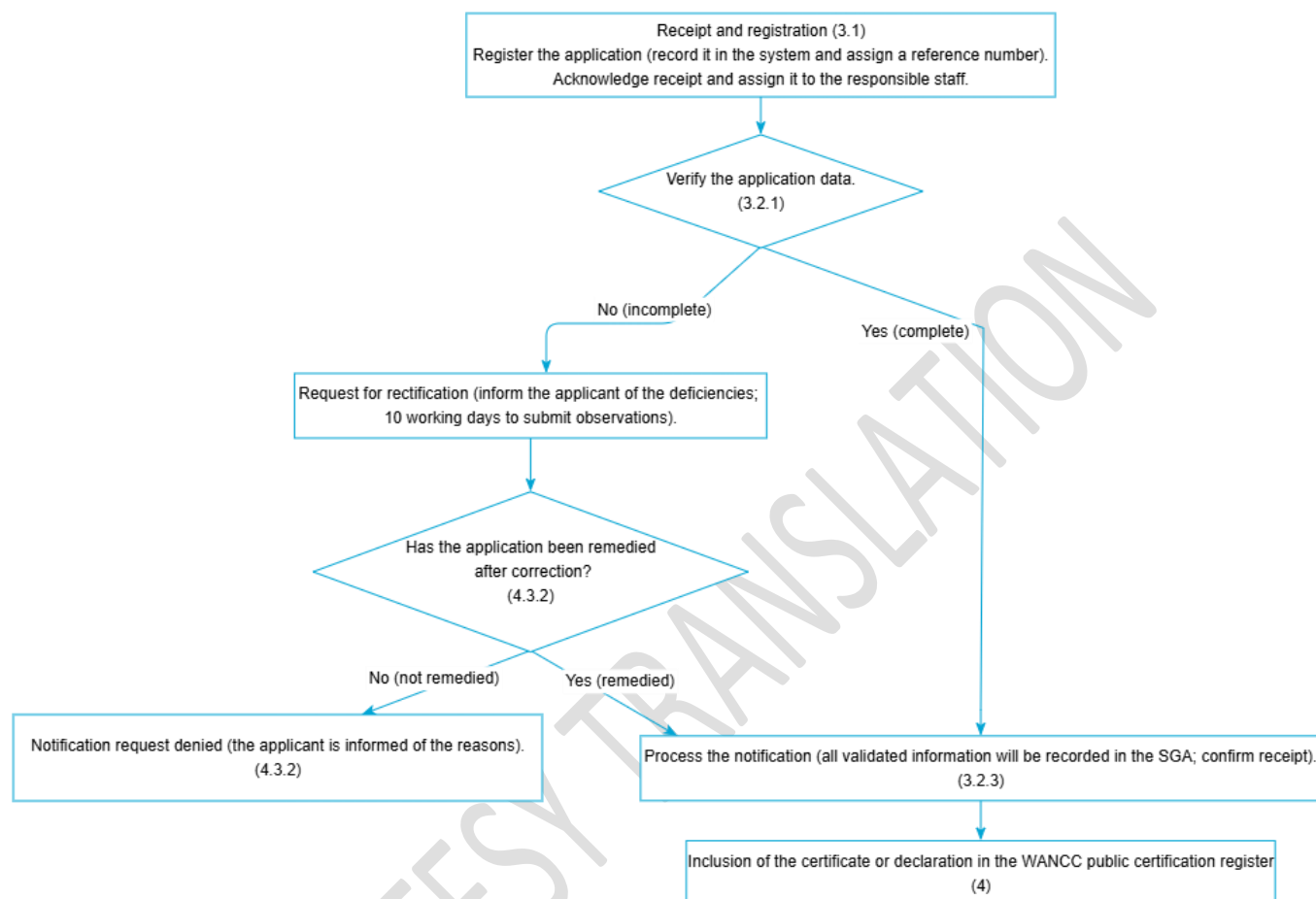
4. RESULTS AND ACTIONS

14. Once the receipt has been successfully completed, the JAN shall, where appropriate, activate:
 - a) The inclusion of the certificate or statement of conformity in the **WNCCA** public certification register, including information such as product or service name, version, assurance level, certification body or issuing supplier, date of issue and references to the certification report or supporting documentation.
15. The **JAN** will monitor the policies for the publication and removal of entries from the register, ensuring that the transparency requirements of the scheme and the **NCCA** are met.

COURTESY TRANSLATION

5. PROCESS DIAGRAM

Figure 1 — Workflow of receipt of 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)
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)

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