



**PREMIER
MINISTRE**

*Liberté
Égalité
Fraternité*

Agence nationale de la sécurité des
systèmes d'information

**Secrétariat général de la défense
et de la sécurité nationale**

Paris, le 24 Février 2026

N° 2419 /ANSSI/SDE/PSS/CCN

Référence : ANSSI-CC-CER-P-01_v5.5

PROCEDURE

CYBERSECURITY CERTIFICATION BASED ON THE COMMON CRITERIA FOR
PRODUCTS AND PROTECTION PROFILES

Application : As soon as published.

Circulation : Public

COURTESY TRANSLATION



REVISION HISTORY

Version	Date	Modifications
1	27/10/2003	Creation
2	08/03/2016	General reorganisation of the document Acknowledgement of standard ISO/IEC 17065
5.1	18/10/2024	EUCC conformity
5.4	27/03/2025	Clarification of the role of the certifier regarding the site visits.
5.5	24/02/2026	Clarifications on the post-certification follow up and link with [VUL-P-01]

In accordance with the April 18th, 2002 decree No. 2002-535 as amended, this this application note has been submitted to the Executive Certification Committee, which gave a favourable opinion.

It is planned that this application note will be submitted to the Executive Certification Committee for comment when major modifications are made.

This application note is available at the ANSSI's institutional website (www.cyber.gouv.fr).

TABLE OF CONTENTS

1. SUBJECT OF THE PROCEDURE	4
2. CONTEXT	4
3. CERTIFICATION REQUEST	4
3.1. The certification request	4
3.2. Processing the request	5
4. SECURITY EVALUATION	6
4.1. Start of the evaluation	6
4.2. Supply delivery	6
4.3. Conduct of the evaluation work	6
4.4. Evaluation report validation	7
4.5. End of the evaluation	7
5. CERTIFICATION ISSUANCE	8
6. VALIDITY PERIOD	8
7. PUBLICATION OF THE CERTIFICATE	8
8. ADVERTISING	9
8.1. Communication rules	9
8.2. Usage rules of marks and logo	9
9. POST-CERTIFICATION FOLLOW UP (MONITORING ACTIVITIES, NON-CONFORMITY, REVIEW, SUSPENSION AND WITHDRAWAL)	9
9.1. Monitoring activities	9
9.2. Management of non-conformity	10
9.3. Review of a certificate	10
9.4. Suspension and withdrawal of a certificate	10
10. COMPLAINTS MANAGEMENT	11
11. APPENDIX	12

1. Subject of the procedure

This document describes the entire Common Criteria (CC) certification process, from the formal request by a sponsor to the award of the certificate for the assessed object. An object refers to a product or a protection profile. The process described in this document applies to both initial certification (a new object) and reassessment (a new version of a previously certified object).

This document describes certification under both the national scheme and the European Common Criteria cybersecurity certification scheme (see [EUCC]).

2. Context

The decree on the evaluation and certification of the security offered by information technology products and systems defines the regulatory framework applicable to this certification process (see [DECREE]), which governs both the national scheme and the national implementation of the European cybersecurity certification scheme based on the Common Criteria (see [EUCC]).

This decree defines the organization required to conduct a third-party evaluation and its monitoring, leading to the issuance of certificates attesting that an object meets the security requirements listed in its security target.

The certification body relies on this same organization to certify the compliance of protection profiles with the requirements of the APE class defined in the Common Criteria [CC]. The corresponding certificates are also issued under Decree 2002-535, as amended.

3. Certification request

3.1. The certification request

The certification sponsor submits an official certification request to ANSSI using form [CER-F-01]. They also submit supporting documents based on the information provided on the form. All of these documents constitute the application form. The version of the form to be used by the applicant shall be the one published on the ANSSI website; otherwise, the application will be systematically rejected.

As indicated in Article 2 of the [DECREE], the file contains, in particular:

- a description of the object to be evaluated, including the security target or, where applicable, the protection profile;
- the selected evaluation criteria;
- the name of the ITSEF selected by the sponsor to conduct the evaluation work and the list of members of the evaluation steering committee;
- the provisional work program for the evaluation.

The application form also includes the general conditions of certification, which the sponsor undertakes to comply with. The application form is signed by the sponsor and the ITSEF in charge of the evaluation.

3.2. Processing the request

When the application form is received (with its documentation) by the certification body, the latter analyzes its contents with a view to officially registering the request.

If, at the time the assessment begins, the certification body considers that the security objectives are not defined in a relevant manner with regard to the applicable standards, technical requirements, or best practice rules, or that the assessment work is not consistent with the objectives, it notifies the sponsor that, given the current status of the file, it cannot proceed with the proposed certification (see Article 2 of the [DECREE]).

If the case is satisfactory, a registration letter is sent electronically or in paper form to the sponsor and the ITSEF. This letter identifies, among other things, the name of the certifier responsible for overseeing the assessment. The certifier is selected based on their recognized expertise in the relevant field, their impartiality, and their workload.

Note: For various reasons (departure, long-term illness, resource management, etc.), the appointed certifier may be replaced by another certifier with the same skills. In this case, the sponsor and the ITSEF will be notified of this change by email.

4. Security evaluation

4.1. Start of the evaluation

Once the request is registered, the project certifier will ask the steering committee identified in the application form if a kick-off meeting is necessary.

If so, the certifier will conduct the meeting according to a pre-established agenda. The meeting will be recorded in minutes prepared by the certifier and sent to the steering committee.

Whether or not a kick-off meeting is held, the certifier shall record the following points:

- any changes to the project since the application was submitted;
- the availability of the ITSEF material and personnel resources.

4.2. Supply delivery

The sponsor is responsible for delivering the supplies required for the evaluation, including the Generic Evaluation Results Reuse Report (see [NOTE-17]) and the "ETR for Composite Evaluation" (see [COMP]). The list of supplies to be delivered is specified in the provisional work program of the evaluation file. The delivery method to the certifier shall comply with the requirements of [SECU-P-01]. All supplies are, by default, sent to the ITSEF and the certifier in charge of the project.

If the sponsor is not the designer of the product or system, the supplies may be delivered directly by its owner (e.g., a developer or subcontractor) to respect the confidentiality of know-how.

The supplies used for the evaluation shall be managed by the ITSEF in accordance with the requirements of standard [17025].

4.3. Conduct of the evaluation work

The ITSEF conducts the assessment work formulated by [CEM], [EUCC] reference documentation, and interpretation notes in accordance with the assessment criteria and assurance level selected in the certification application. This work shall also comply with the provisions of the ITSEF's quality system [17025].

Evidence of completion of the work is recorded:

- in the end-of-task report associated with each assessment task, also known as the Intermedial Technical Report (ITR);
- or directly in the final report, known as the Technical Assessment Report (TAR).

All these reports issued by the ITSEF, whether draft or final, are sent simultaneously to the certifier and the sponsor. The certification body acknowledges receipt and includes them in the project directory. When a report's verdict is "FAIL," the certification body invites the ITSEF to contact the sponsor to correct any remaining issues so that the assessment work can result in a "PASS" verdict. However, the sponsor retains the right to terminate the ongoing assessment at any time. In any case, the certification body shall be kept informed of the progress of the file.

During the assessment, meetings may be initiated by any of the steering committee members.

Work on site:

Certain work shall be performed by the ITSEF at the development, production, or operating site of the product or system under evaluation. This work is identified in [NOTE-02].

Agreements shall be established between the sponsor, the developer, and ITSEF for the performance of this work. This work shall be identified in the evaluation file so that evaluators can access the sites at the appropriate time.

The certifier, if requested, shall also be able to attend this on-site work as an observer in accordance with the requirements of [NOTE-02].

Cryptographic mechanism analysis:

When the security functions of the TOE implement cryptographic mechanisms, the effectiveness of these mechanisms shall be analyzed in accordance with procedure [CRY-P-01]. The results of this analysis are taken into account as part of the vulnerability analysis carried out by the ITSEF.

Reassessments:

For a reassessment, the sponsor shall conduct (or have the product developer conduct) an analysis of the impact of the changes. The conclusions of this analysis shall be presented in a report, known as an "impact analysis report" (IAR), the content of which is indicated in paragraph 5 of the procedure cited in reference [JIL-AC].

There are two types of reassessment:

- a reassessment following a change to the certified elements that cannot be considered minor (see [ANSSI-CC-MAI-P-01]). The assessment is carried out by reusing all the results of the previous assessment that still apply. A new technical assessment report is then issued.
- a reassessment of an unchanged certified product, known as a "reassessment," which assesses the impact of changes in the threat environment. In this case, the reassessment is carried out by the ITSEF that carried out the previous assessment, reusing all the results that still apply. The assessment focuses on assurance activities potentially affected by changes in the threat environment related to the certified product, specifically the affected AVA_VAN family and, in addition, the Assurance Lifecycle (ALC) family. The technical assessment report is then updated.

A renewal request is treated as a "reassessment".

Patches assessment:

Pending the implementation of Annex IV.4 of [EUCC], the patch management is carried out as part of a reassessment as described above.

4.4. Evaluation report validation

In the case of a final evaluation technical report (ETR) with a "PASS" verdict, the certifier analyzes it and ensures that all referenced documents are included. The certifier may request access to any other information from the ITSEF, developer, or sponsor. The certifier may also request technical advice from ANSSI experts; however, the certifier retains the final validation decision.

The conclusions of the evaluation report analysis are recorded in a report review sheet that is sent to the ITSEF. The latter may be required to reissue a new version of the report or carry out additional work, or even repeat certain tasks if anomalies are noted. The additional work requested shall meet the same requirements as those applied during the evaluation.

It is also possible, following a significant number of comments, that the certifier may request a reissue of the report.

4.5. End of the evaluation

When an ETR is received by the certifier, an end-of-assessment meeting may be organized at the request of one of the members of the assessment steering committee.

The meeting's terms and conditions, as well as the agenda, are set by the steering committee.

5. Certification issuance

Once the ETR (PASS verdict only) has been validated by the certifier responsible for monitoring the assessment, the certification issuance procedure begins. The certifier prepares a file that includes:

- the draft certification report;
- the draft certificate.

The draft certification report may be sent to the sponsor so that they can provide comments, which may or may not be incorporated by the certifier.

Following the certification decision based on this draft, this file is forwarded for signature. The Director General of ANSSI then electronically signs the certification report and certificate:

- the signed certificate and certification report are sent to the sponsor(s) mentioned in the application form, along with a customer satisfaction form [QUA-F-03];
- within the framework of [EUCC], the signed certificate and certification report are sent to the control and supervision mission (MCS). MCS sends a copy of the certificate and certification report to ENISA (European Union Agency for Cybersecurity).

The signed certificate and certification report are retained by the certification body.

The issuance of these documents requires the sponsor to comply with certain obligations, including promptly notifying ANSSI (CERT-FR) and the certification body of any discovered vulnerability, along with its associated impact analysis, to enable their investigation.

In the event of a reassessment (non-initial certification), the previous certificate may be archived.

6. Validity period

Product certification is issued for a validity period of five years (see [CER_VALID] for SOG-IS and, with exceptions validated by MCS, for [EUCC]).

For a protection profile, the validity period is twenty years.

At the end of the validity period, the certificate is archived.

If the certificate is not public, its validity can be requested by email from the evaluation sponsor, copying the certification body. The latter can then confirm or deny the response provided.

7. Publication of the certificate

The sponsor may, under certain conditions, request, using form [CER-F-01], that the certificate and certification report remain confidential. By default, the certificate, certification report, and public security target will be published:

- on the ANSSI website: www.cyber.gouv.fr and, where applicable, on the website www.ncca.cyber.gouv.fr and the ENISA website;
- where applicable, on the website of a recognition agreement (for example, the CCRA website) if the requirements of this agreement were met during the evaluation.

The various publication options are listed in note [NOTE-04].

Please note that the initial publication decision, made when the evaluation request was submitted, can be modified upon request by email from the sponsor (certification@ssi.gouv.fr).

After the validity period (see chapter 6), the published documents will then be moved to the list of archived certificates.

8. Advertising

The sponsor may state the certification directly on the product or through documents, brochures or advertising, except for specific provisions specified by ANSSI when registering the evaluation request.

8.1. Communication rules

Sponsors have a duty to inform users of certified products or protection profiles in honest and understandable terms. They shall include:

- the certificate reference;
- the date the product was certified;
- the references and version of the certified product;
- the expiry date, if applicable.

They shall also:

- issue certified copies of the original certification reports and security targets if requested by a client;
- not make misleading statements about the product.

8.2. Usage rules of marks and logo

The "TI SECURITE CERTIFICATION" and "EUCC" trademarks as well as the logos of the CCRA and SOG-IS agreements can be used to assert the obtaining of a certificate, their descriptions and terms of use are described by procedures [MAR-P-01] and [MAR-P-02].

9. Post-certification follow up (monitoring activities, non-conformity, review, suspension and withdrawal)

9.1. Monitoring activities

For [EUCC], the certification body monitors:

- compliance by certificate holders with their obligations under [EUCC] and [CSA] with respect to the EUCC certificate issued by the certification body;
- compliance of the ICT products it has certified with the corresponding security requirements;
- the assurance stated in the certified protection profiles.

The certification body bases its monitoring activities on:

- information provided based on the certification candidate's commitments;
- information from the activities of the competent market surveillance authorities;
- complaints received;
- information relating to vulnerabilities transmitted by CERT-FR that may affect certified products.

Monitoring operations are carried out:

- periodically for the monitoring of marked products and marks in accordance with procedure [MAR-P-03];
- on an ad hoc basis following receipt of specific information or a complaint in accordance with procedure [ANO-P-01]
- or at the request of MCS.

9.2. Management of non-conformity

Following the finding of non-conformity of a product, a protection profile or non-compliance by the holder of a certificate with its obligations, the certification body informs the holder of the EUCC certificate of the non-conformity found and asks him to take corrective measures within thirty calendar days. If the corrective measures are not taken within the given time limit, the corresponding certificate may be suspended or withdrawn.

9.3. Review of a certificate

The ANSSI certification body may decide to review the certification of a product or protection profile:

- at the request of the certificate holder, to ensure continuity of assurance in the following cases:
 - the certificate expires within nine months;
 - a change to the certified product or another factor that could impact the product's security functionality;
 - the certificate holder requires that the vulnerability assessment be performed again to reconfirm the certificate's assurance regarding the product's resistance to current cyberattacks,
- to review the relevance of corrective measures following the discovery of non-compliance;
- following the discovery of a vulnerability in accordance with Chapter VI of [EUCC]. In this case, the procedure [VUL-P-01] is applied ;
- or for other justified reasons discovered, in particular during its monitoring activities, for example: a new fact leads it to suspect that information provided by the sponsor or developer during the assessment was inaccurate and that it may have distorted the assessors' judgment and therefore the final result.

The review may require a reassessment by an ITSEF (see paragraph 4.3). This is particularly the case with regard to continuity of insurance in cases not covered by the maintenance procedure ([MAI-P-01]).

Following this review, the following may be carried out, where appropriate:

- suspension of the certificate according to the procedure [VUL-P-01];
- modification of the certificate, including a scope reduction in accordance with the provisions of [NOTE-25];
- issuance of a maintenance report [MAI-P-01];
- withdrawal of the certificate and, where applicable, issuance of a new certificate.

9.4. Suspension and withdrawal of a certificate

Suspension: Following the finding of non-compliance or the review of a certificate, the certification body may suspend a certificate for a period not exceeding forty-two calendar days except in the case of the implementation of a remediation plan in accordance with [VUL-P-01] or if MCS has authorized an extension of a maximum of 1 year. Consequently, the following publishing websites are updated indicating the state suspended of the certificate:

- the ANSSI website;
- the ENISA website (EUCC case).

Withdrawal: Following the finding of non-compliance, the re-examination of a product, or the outcome of a suspension, the certification body may withdraw a certificate. Consequently, the publishing websites are updated:

- the ANSSI website: the certificate is added to the list of archived products;
- the ENISA website (EUCC case): removal from the list;
- the CCRA (Common Criteria Recognition Arrangement) website, when the certificate is recognized under the international Common Criteria framework: removal from the list.

In cases of suspension or withdrawal, the certification body will notify the sponsors by letter [CER-F-22].

Clients are notified by the sponsor, and MCS is notified by the certification body. ENISA is notified by MCS.

Whatever the reason, the sponsor shall immediately and imperatively cease using all means of communication which refer to the certificate as soon as it is suspended or withdrawn.

10. Complaints management

The sponsor may appeal any decision of the certification body in order to have the decision reconsidered (see [ANO-P-01]).

11. Appendix

Reference	Document
[DECREE]	Decree 2002-535 of the April 18 th , 2002, relating to the evaluation and certification of the security offered by information technology products and systems.
[CC]	<p><i>Common Criteria for Information Technology Security Evaluation:</i></p> <ul style="list-style-type: none"> - <i>Part 1: Introduction and general model</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ; - <i>Part 2 : Security functional components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ; - <i>Part 3 : Security assurance components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003. <p>Ou</p> <ul style="list-style-type: none"> - <i>Part 1: Introduction and general model</i>, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001 ; - <i>Part 2 : Security functional components</i>, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002 ; - <i>Part 3 : Security assurance components</i>, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003. <p>Ou</p> <ul style="list-style-type: none"> - <i>Part 1: Introduction and general model</i>, novembre 2022, version CC :2022, révision 1, référence CCMB-2022-11-001 ; - <i>Part 2 : Security functional components</i>, novembre 2022, version CC :2022, révision 1, référence CCMB-2022-11-002 ; - <i>Part 3 : Security assurance components</i>, novembre 2022, version CC :2022, révision 1, référence CCMB-2022-11-003 ; - <i>Part 4 : Framework for the specification of evaluation methods and activities</i>, novembre 2022, version CC :2022, révision 1, référence CCMB-2022-11-004 ; - <i>Part 5 : Pre-defined packages of security requirements</i>, novembre 2022, version CC :2022, révision 1, reference CCMB-2022-11-005.
[ISO]	<ul style="list-style-type: none"> - <i>Part 1: Introduction and general model</i>, août 2022, référence ISO/IEC 15408-1; - <i>Part 2 : Security functional components</i>, août 2022, référence ISO/IEC 15408-2 ; - <i>Part 3 : Security assurance components</i>, août 2022, référence ISO/IEC 15408-3; - <i>Part 4 : Framework for the specification of evaluation methods and activities</i>, août 2022, référence ISO/IEC 15408-4; - <i>Part 5 : Pre-defined packages of security requirements</i>, août 2022, référence ISO/IEC 15408-5.
[CEM]	<p><i>Common Methodology for Information Technology Security Evaluation, Evaluation Methodology</i>, version 3.1, revision 5 or CC:2022</p> <p>Or</p> <p><i>Information technology — Security techniques — Methodology for IT security</i></p>

	<i>evaluation, ISO/IEC 18045:2008 or ISO/IEC 18045:2022</i>
[EUCC]	European cybersecurity certification scheme based on common criteria (implementing regulation (EU) 2024/482) and its amendments.
[CSA]	European regulation on ENISA (European Union Agency for cybersecurity) and cybersecurity certification of information and communication technologies (implementing regulation (EU) 2019/881), current version
[17025]	NF EN ISO/CEI 17025 standard: General requirements for the competence of testing and calibration laboratories.
[SITE CER]	Site Certification, Supporting Document, référence CCDB-2007-11-001, current version.
[NOTE-02]	Development environment visit, current version.
[NOTE-17]	ALC assurance class re-use, current version.
[COMP]	Joint Interpretation Library - Composite product evaluation for Smart Cards and similar devices, current version.
[CER_VALID]	SOG-IS Recognition Agreement Management Committee - Certificate validity, version 1.0.
[CER-F-01]	Application form for evaluation, current version.
[CER-F-22]	Suspension or withdrawal letter, reference ANSSI-CC-CER-F-22, current version.
[SECU-P-01]	Management of the confidentiality at CB, current version.
[CRY-P-01]	Methods for carrying out cryptographic analyses, current version.
[QUA-F-03]	Formulaire Satisfaction Client, référence ANSSI-CC-QUA-F-03, version en vigueur.
[NOTE-04]	Publication and international recognition of common criteria certificates delivered by ANSSI, current version.
[ANO-P-01]	Anomaly processing, current version.
[MAR-P-01]	Usage of the marks at CCN marks, ANSSI-CC-MAR-P-01, current version.
[MAR-P-02]	Use of CCRA and SOGIS Logos, ANSSI-CC-MAR-P-02, current version.
[MAR-P-03]	Certification mark surveillance, ANSSI-CC-MAR-P-03, version en vigueur.
[NOTE-25]	Scope reduction of a cc certificate, ANSSI-CC-NOTE-25, current version.
[JIL-AC]	Joint Interpretation Library - Assurance Continuity, version en vigueur.
[VUL-P-01]	Vulnerability management procedure for certified products, reference ANSSI-CC-VUL-P-01, current version.

Most of those documents are available on the ANSSI website (www.cyber.gouv.fr).