CERTIFICATION BODY QUALITY MANUAL

Subject:	Certification Body Quality Manual
Application:	As soon as approved
Circulation:	Public

COURTESY TRANSLATION

Version history

Version	Date	Modifications
1.0	01/12/2003	Creation
2.0	08/03/2016	Document reorganisation

Pursuant to amended decree No. 2002-535 of 18th April 2002, this application note has been submitted to the certification management committee, which gave a favourable opinion.

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

TABLE OF CONTENTS

Chapitre 1
The quality manual

1.1. Purpose of the manual

The quality manual presents the methods and procedures used by the national certification body (CCN - Centre de Certification National) to ensure and maintain the quality and continuity of its services to certify the security of IT products and systems.

The quality manual is the reference for:

- any person or entity of the ANSSI exercising a function related to certification activity, in order to define their role and responsibilities;
- any newly hired personnel at the certification body, to inform them of ANSSI policies and to facilitate their integration;
- peer review between ANSSI and other organisations – foreign ones in particular – with a view to mutual recognition.

1.2. Preparation, updating and circulation

The manual is prepared by the quality manager, checked by the head of certification body, validated by the "Security Products and Services" division manager and the "Expertise" sub-director, and then approved by the Directeur Général of the ANSSI. It is subject to review by the certification management committee.

Updates to the quality manual follows the same validation process as the initial version.

The quality manager is responsible for circulating the quality manual, following the same rules as for other documents of the quality system.

All versions are retained by electronic means. However, the French version, on paper, is the reference version.

Chapitre 2
The certification scheme

2.1. Regulatory context

French amended decree 2002-535 of 18 April 2002, relating to the evaluation and certification of the security provided by information technology products and systems, defines the regulatory context and organisation required for an evaluation to be carried out by a third party and for its verification, leading to the issuing of certificates.

These rules are implemented in a third-party certification scheme.

2.2. The certification management committee

Article 15 of amended decree 2002-535 defines the following missions for the IT security certification management committee:

- formulating opinions or proposals on the certification policy, on the rules and standards used for evaluation and certification procedures and on technical guides provided to the public;
- providing an opinion on issuing and revoking approval for evaluation facilities;
- examining, with an objective of conciliation, any dispute, submitted to it by the parties, regarding the evaluation procedures organised by amended decree 2002-535;
- providing an opinion on mutual recognition agreements with foreign organisations.

The management committee meets at least once a year. It is chaired by the Secrétaire général de la défense et de la sécurité nationale or his representative. It reports to the Premier Ministre.

2.3. The user committee

The French certification scheme user committee is composed of a varied range of actors, mainly sponsors and developers of products that are certified, but also contracting parties that rely on certification to specify security requirements for products they use or recommend. The committee is set up, at the initiative of the certification body, to bring together these various actors, thereby creating a forum for exchanging information and consulting with the certification body.

The user committee is designed to allow the ANSSI:

- to communicate changes in rules and standards;
- to identify the needs and expectations of the scheme's users;
- to gather opinions on prospects for change.

The opinions issued by the user committee are advisory.

2.4.The certification body

2.4.1. Status

The ANSSI, created by decree 2009-834 of 7 July 2009, processes the certification (see article 4).

The ANSSI reports to the Secrétaire général de la défense et de la sécurité nationale. The certification body is attached to the Security Products and Services division of the Sub-Directorate for Expertise.

2.4.2. Impartiality

Two key elements contribute to the independence of the certification body:

- its status as a public authority;
- its financial resources, provided by the French State, reinforce this independence. Until further notice, certification is free.

The certification body's activities are carried out in the framework of the French amended decree 2002-535 of 18 April 2002, rather than the framework of contracts, in the commercial sense of the term.

Furthermore, the certification body does not provide advisory or training services intended to help obtain or retain certification.

In addition, it is subject to the European Commission's decision 2000/709/EC of 6 November 2000 relating to national bodies charged with the conformity assessment of secure signature devices.

2.4.3. Organisation

```
┌─────────────────────────────────┐
│  Directeur général de l'Agence  │
│    nationale de la sécurité     │
│   des systèmes d'information    │
└─────────────────────────────────┘
                │
┌─────────────────────────────────┐
│      Sous-directeur Expertise   │
└─────────────────────────────────┘
                │
┌─────────────────────────────────┐
│        Chef de division         │
│   Produits et services de sécurité │
└─────────────────────────────────┘
                │
┌─────────────────────────────────┐
│  Chef du centre de certification │
└─────────────────────────────────┘
```

| Responsables d'agrément des centres d'évaluation | Certificateurs | Assistant CCN | Responsable qualité |
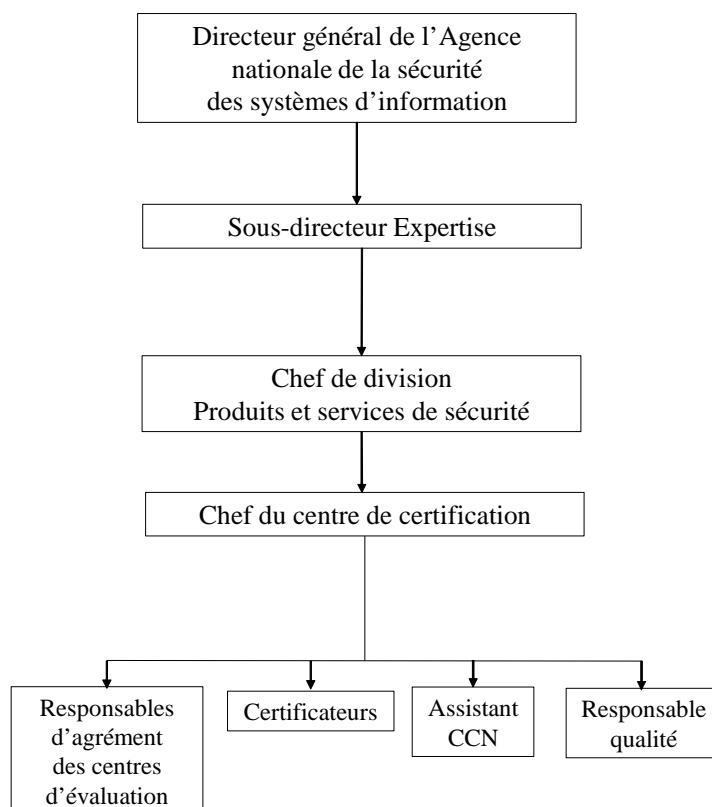
2.4.4. Responsibilities

The responsibilities for certification activities are allocated as follows:

- **The Directeur Général of the ANSSI** is delegated by the Premier Ministre to sign the certificates.
- **The Expertise sub-director** has authority over the certification body.
- **The manager of the Security Products and Services division** has authority over the certification body.
- **The head of certification body** is responsible for the certification body's operational management. He takes part in recruiting his staff, verifying that they are competent to fulfil their duties. He keeps an up-to-date record of staff experience and training. He is responsible for defining the approval process for the evaluation facilities. He is responsible for recognition of foreign certificates and maintains contact with his foreign counterparts. He participates in the management of evaluation and certification criteria. He is responsible for the certifier's proposal (approve or reject), which is presented to management for signature. He is responsible for managing the quality system.
- **Evaluation facility licensing managers** are responsible for monitoring, supervision and continuous training for the evaluation facilities.
- **The quality manager** is responsible for implementing, maintaining and improving the quality system. He is also responsible for the quality training of certification body staff.
- **Certifiers** are responsible for monitoring the evaluations to ensure that the certification rules and procedures are followed. They are not involved in the evaluation work, nor in the final decision on certification.
- **The certifier assistant** is responsible for administrative follow-up on certification body documents and for assisting the head of certification body and certifiers with registration, editing and logistics related to their functions.
- **The Secretariat** is attached to the Sub-Directorate for Expertise. It participates, in particular, in the procedures for sending and receiving correspondence for the certification body.

2.4.5. Certification body staff

The recruitment of staff for the certification body and the monitoring of their qualification are subject to a procedure[1].

Notably, there are two qualification levels for certifiers:

- those with "senior" level, who can carry out certification activities under their own responsibility;
- those with "junior" level, who must carry out these activities under the responsibility of a "senior" certifier.

The certification body does not employ temporary staff for certification activities.

---

[1] Procedure ANSSI-CC-PER-P-01 "Personnel Recruitment And Qualification"

Chapitre 3
Quality system

3.1. Quality policy

3.1.1. Objective

The certification body operates in a field where confidence, rigour and continuity take on their full meaning. Due to the wide geographical and cultural range of its customers, the certification body must, through its quality system, provide the highest levels of confidence in its work, in order to ensure the recognition of its certificates, particularly because of the international framework in which it operates.

Its objectives focus on the recognition of the certificates it issues:

- at national level, to establish confidence in the certification work that it carries out with all concerned parties;
- at international level, to enter in the framework of mutual recognition agreements that it undertakes.

3.1.2. Requirements

To obtain and maintain this recognition, the certification body must prove that it meets the following requirements:

- traceability: all evaluations must be reproducible and all evidence elements related to the issuing of the certificate must be identified and retained;
- continuity: the certification body must be able to carry out its missions irrespective of any internal changes (organisation, staff);
- consistency: all certificates must reflect a comparable level of assurance, regardless of the staff responsible for the monitoring and the evaluation facility that conducted the evaluation;
- confidentiality: the certification body must ensure the confidentiality of sensitive information entrusted to it, or that it develops in the framework of certification.

Complying with the CCRA and SOG-IS agreements, and NF standard EN ISO/IEC 17065, "Requirements for bodies which certify products, processes and services," is a way to ensure that these requirements are respected.

3.2. Quality system

The quality system is designed to meet the requirements of the CCRA and SOG-IS agreements for international recognition of certificates and the NF standard EN ISO/IEC 17065, and complies with regulations that define the missions of the certification body.

The certification body undertakes to:

- publish the rules and requirements for the evaluation and certification scheme, and keep them up to date;
- publish the list of certificates and the list of approved evaluation facilities, and keep them up to date.

The ANSSI undertakes to:

- ensure the competence of the evaluation facilities conducting the evaluation;

- only authorise laboratories accredited according to the ISO/IEC 17025 standard for Common Criteria work in the context of amended decree 2002-535;
- work with competent and qualified staff.

The certification body staff undertakes to respect the confidentiality of sensitive information exchanged in the framework of evaluating and certifying the security provided by IT products and systems.

3.3. Quality planning

3.3.1. Management reviews

The reviews are conducted at an annual meeting organised by the certification body's quality manager[2].
The minutes of the management review are drafted by the quality manager and circulated to those concerned.

3.3.2. Internal audits

Periodic audits of the quality system are organised by the head of certification body and led by qualified auditors who are independent of the functions being audited[3].

The quality manager plans and manages the audits so that every requirement of the NF EN ISO/IEC 17065 standard is audited at least once a year.

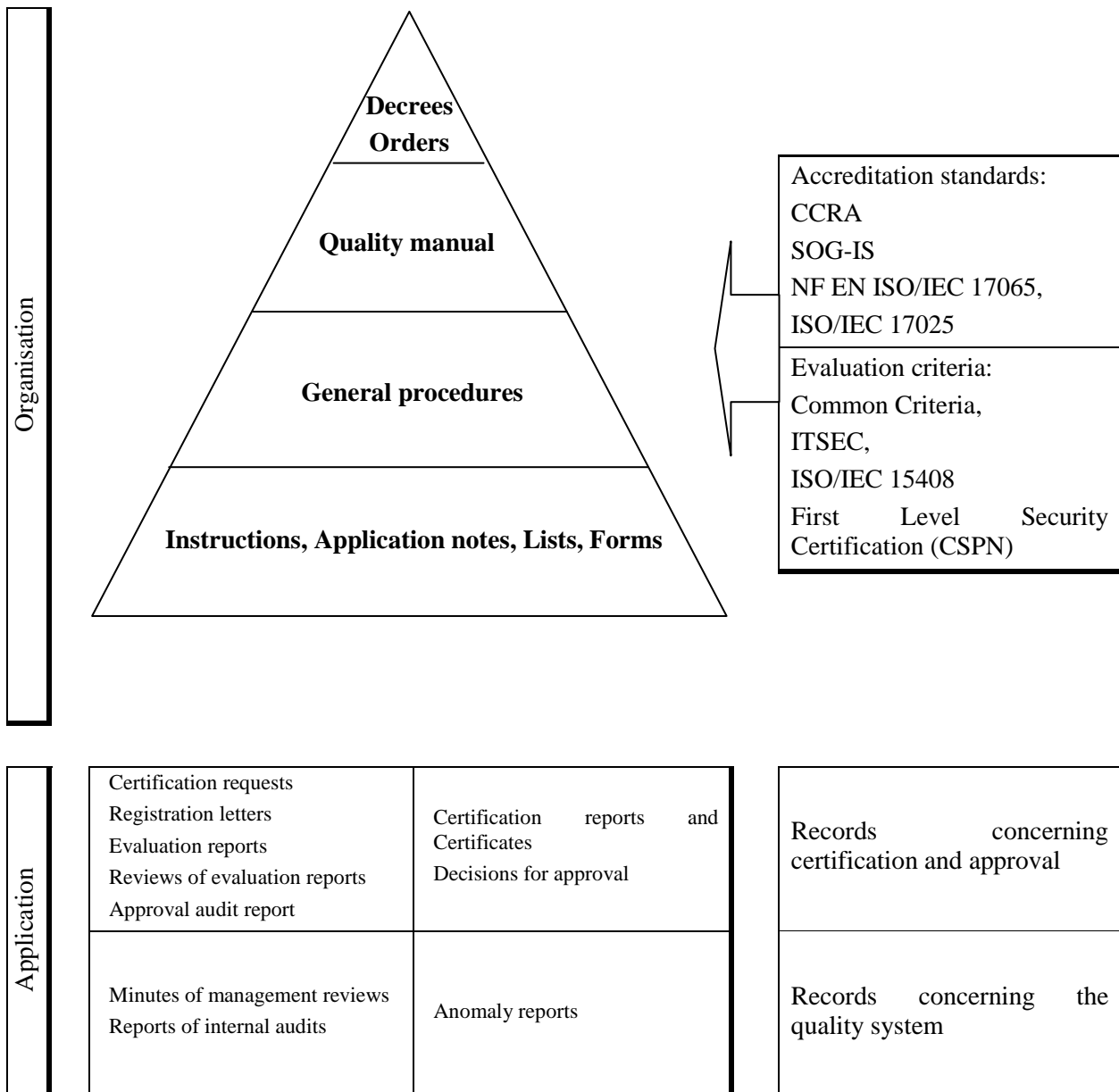## 3.4. Documentation architecture

The certification body has a documentation collection concerning the full range of certification activity.

---

[2] Procedure ANSSI-CC-QUA-P-01 "Management Reviews"

[3] Procedure ANSSI-CC-QUA-P-03 "Internal Audits."

3.4.1. Documentation structure

This documentation collection has the following structure:

```
Organisation

                    Decrees
                    Orders                    ┌─────────────────────────────┐
                                              │ Accreditation standards:    │
                                              │ CCRA                        │
                  Quality manual              │ SOG-IS                      │
                                              │ NF EN ISO/IEC 17065,        │
                                              │ ISO/IEC 17025               │
                                              ├─────────────────────────────┤
                General procedures            │ Evaluation criteria:        │
                                              │ Common Criteria,            │
                                              │ ITSEC,                      │
                                              │ ISO/IEC 15408               │
                                              │ First      Level   Security │
   Instructions, Application notes, Lists, Forms│ Certification (CSPN)      │
                                              └─────────────────────────────┘
```

Application	Certification requests Registration letters Evaluation reports Reviews of evaluation reports Approval audit report	Certification reports and Certificates Decisions for approval	Records concerning certification and approval
	Minutes of management reviews Reports of internal audits	Anomaly reports	Records concerning the quality system

3.4.2. Document control

The certification body has rules for the preparation and control of documentation related to its certification activity[4].

The quality manager maintains a list of all these quality documents prepared by the certification body.

3.4.3. Records concerning certification

Management of records concerning certification depends on their nature and the procedure to which they relate. Consequently, records management is defined in each procedure concerned.

---

[4] Procedure ANSSI-CC-DOC-P-01 "Drafting And Updating Of The Certification Centre's Quality System Documentation"

There are three types of records to show that all procedures and instructions regarding the certification activity have been properly applied:

- records kept on paper, retained at the certification body or in an archive;
- records stored on computer media;
- samples provided by sponsors, retained at the certification body.

Chapitre 4
Methods for certification

4.1. Non-discriminatory access and processing

All developers and suppliers of products and IT systems have access to the ANSSI's certification services.

The ANSSI ensures that all objects submitted for certification receive equal treatment.

Assigning certification is solely contingent on complying with the operating rules of the scheme and satisfying the evaluation criteria.

4.2. Reference documents

All public documents concerning certification are available or referenced on the ANSSI website: www.ssi.gouv.fr.

In particular, these documents include:

- regulations relating to the certification of the security of IT products and systems;
- operating documents (procedures, instructions and application notes) for the certification body;
- evaluation criteria.

4.3. Evaluation criteria

The criteria and evaluation methodologies used are approved by the certification management committee.

These evaluation criteria are subject to change or to be supplemented by technical guides, depending on the technology concerned or specific contexts.

4.4. Changing certification requirements[5]

The requirements for certification may need to change over time.

These changes may be:

- changes to evaluation criteria coming from international or national standards bodies: they are directly available on the websites of those bodies;
- adaptations of the requirements for a particular field: if they are mandatory or dependent on the national scheme, they are announced by way of a scheme application note that specifies the application deadline;
- changes to the certification scheme's practices: major changes require the opinion of the user committee and/or the certification management committee.

---

[5] Procedure MOD/P/01 "Changes To Certification Requirements"

Chapitre 5
Certification request

5.1. Contents of the evaluation file

After selecting an evaluation facility, the sponsor of the evaluation requests the opening of a Common Criteria certification file or CSPN at the certification body via an evaluation file, available on the ANSSI website.

The evaluation file contains:

- the terms and conditions of certification;
- the commitment of the sponsor and the evaluation facility to respect the certification rules;
- a description of the object under evaluation (including its security target);
- the provisional work plan drafted by the evaluation facility during the preparation of the Common Criteria evaluation.

5.2. Registering the request

Upon receipt of the evaluation file, the certification body:

- verifies that the signature on the request engages the company's commitment;
- conducts a thorough document review, particularly regarding the security target and the provisional work plan;
- if it considers that the security objectives are not defined in a relevant manner with regard to standards, technical specifications or best practice rules applicable when the evaluation begins, it notifies the sponsor that, in view of the current state of the file, it cannot proceed with the certification process;
- verify the prospective workload for the evaluation;
- indicate the name of the certifier designated to monitor the evaluation.

By default, the certification body considers the very existence of the evaluation to be confidential. Therefore, the certification body does not make any public disclosure of the evaluation.

Chapitre 6
Evaluation

6.1. The evaluation facilities

6.1.1. Roles and responsibilities

Evaluation facilities carry out the evaluations: they act as third-parties, independent from the product developers and sponsors.

Evaluation facilities are approved by the ANSSI and are therefore obliged to respect all the scheme's rules[6].

Evaluation facilities are made up of teams of experts and managers, often within an organisation with a broader scope. However, the approval criteria require partitioning from the other activities of the organisation to which the evaluation facility is attached.

An evaluation facility must be impartial and independent of any external pressure. It must never be involved in the development (including consulting) and the evaluation of the same product. Nevertheless, it can offer consulting services, which must never affect its impartiality in the evaluations it carries out.

6.1.2. Approval process

The Common Criteria approval criteria include, among others, accreditation of the evaluation facility by the COFRAC (COmité FRançais d'ACcréditation – French accreditation committee) according to ISO/IEC standard 17025 "General requirements for the competence of testing and calibration laboratories." Technical guides for accreditation, developed by the COFRAC, specify the particular field for evaluation of information technology security.

This approval imposes requirements that allow ensuring that the laboratory masters particular techniques and is capable of handling sensitive information.

The approval of an evaluation facility is then accompanied by a monitoring procedure to ensure the sustainability of compliance with approval requirements in the evaluation facility, in particular via a regular audit by the certification body and ANSSI technical experts.

6.1.3. Evaluation work carried out by the evaluation facility

The evaluation facility conducts the evaluation work in accordance with the selected evaluation criteria and the provisional work plan. This work is monitored by the certification body.

The evaluation's sponsor is responsible for providing elements needed for the evaluation. The exact list of elements to be provided to the evaluation facility and to the certification body depends on the evaluation criteria selected. They are listed in the evaluation file.

The evaluation facility analyses the object under evaluation and its documentation to verify that the requirements specified in the evaluation criteria are met. Certain evaluation criteria may require an audit of the development or production site for the object under evaluation.

When an evaluation task is completed, an end of task report is sent to the certifier and the sponsor.

---

[6] Procedures ANSSI-CC-AGR-P-01 "Licensing of Evaluation Facilities" and ANSSI-CSPN-AGR-P-01 "Agrément des centres d'évaluation en vue de la certification de sécurité de premier niveau "

6.1.4. Evaluation Technical Report

When all the evaluation tasks have been completed by the evaluation facility, the evaluation is considered complete.

The evaluation facility then drafts the Evaluation Technical Report (ETR), which it transmits:

- to the certification body and the sponsor, in the framework of CC evaluations;
- exclusively to the certification body, which gives its consent before transmission to the sponsor, in the framework of CSPN evaluations.

This report describes the work carried out during the evaluation and presents the results obtained.

The ETR contains sensitive data covered by industrial and commercial secrecy. Its circulation is controlled: the confidentiality clauses are contractually defined between the evaluation facility and the sponsor during the preparatory phase of the evaluation.

Chapitre 7
Certification

7.1. Preamble

Certification is an overarching process that allows, through a suite of actions, to ensure that the evaluation was conducted with the required levels of competence and impartiality[7].

7.2. Certification report

After validation of the ETR, the certifier drafts a certification report that recommends whether certification should be granted. The certification report, with the security target, is the only document produced as part of the evaluation that a potential purchaser would normally consult.

The certification report accurately describes the object being evaluated and may recommend the implementation of measures necessary for the secure use of the certified object.

The certification report constitutes, together with the security target, the minimum documentation to be provided for international recognition of the certificate.

7.3. Certification decision

The certification body transmits the draft certification report and security target, accompanied by its proposed verdict, to the Directeur Général of ANSSI.

If he decides to grant the certification, the Directeur Général of the ANSSI or the person who has been granted the delegation by the Premier Ministre signs the certificate and certification report.

The certificate bears the date of the certification decision but does not mention any validity period.

7.4. Publication of the certificate

If the sponsor so requests, the certification report and the associated security target are published on the ANSSI website: www.ssi.gouv.fr.

7.5. Revocation of a certificate

The ANSSI may revoke a certificate if, for example, a new fact allows it to demonstrate that information provided by the sponsor or developer during the evaluation was not accurate, and that such information may have distorted the judgment of the evaluators, and thus the final result.

---

[7] Procedures CER-P-01 "Certification Of The Security Provided By It Products And Systems", ANSSI-SITE-P-01 "Site Certification," ANSSI-CC-CPP-01"Certification Of Protection Profiles", ANSSI-CSPN-CER-P-01"Certification de sécurité de premier niveau des produits des technologies de l'information"

Chapitre 8
Use of the certificate

8.1. Communication rules

The sponsor and, where applicable, the developers, have a duty to faithfully and honestly inform users regarding certified products. In particular, the sponsor has the duty:

- to provide the certification report and security target whenever a user so requests;
- not to make misleading statements concerning the product, for example, by announcing or suggesting that the product is certified when it is only under evaluation;
- signal potential users of security issues of which the developer or sponsor is aware;
- immediately inform all registered users of new vulnerabilities.

8.2. Rules for using the mark

The "Certification Sécurité TI" mark reproduced below is the French mark for certification of the security provided by information technology, granted by the Agence Nationale de Sécurité des Systèmes d'Information (ANSSI). This mark is registered at the Institut National de la Propriété Industrielle under number 023 175 658.

It identifies products and systems certified in the framework of amended decree 2002-535.

Its use is defined in a specific procedure[8].

Use of the logos of the CCRA and SOG-IS agreements for the international recognition of certificates is described in a specific procedure[9].

---

[8] Procedure ANSSI-CC-MAR-P-01 "Use Of The "Ti Sécurité Certification" Mark"

[9] Procedure ANSSI-CC-MAR-P-02 "Use Of CCRA And SOG-IS Logos"

Chapitre 9
Surveillance and assurance continuity

The certificate attests, as of its signature date, to the conformity of a product or system with the requirements listed in its security target. To sustain confidence in this conformity and facilitate the further development of a previously certified product, the certification body offers programmes for surveillance and assurance continuity.

9.1. Surveillance[10]

The certification body offers a certificate surveillance programme, under which the product is monitored in order to maintain confidence in the issued certificate.

This monitoring consists of working to update, on a regular basis (the period depends on the technical field concerned), the certified product's vulnerability analysis and carrying out tests, if necessary.

Surveillance is optional and left to the discretion of the sponsor. In certain special cases (e.g. electronic signature creation devices or the qualification process), it may be made mandatory.

9.2. Assurance continuity[11]

A certificate applies solely to the version and configuration of the product evaluated. However, over time, changes are likely in the product, development environment or production environment.

The sponsor may request the evaluation of these new versions of the product.

The certification body offers an assurance continuity procedure for certificates that facilitates certification of these new versions.

9.3. Surveillance or assurance continuity?

Surveillance is specifically designed for sponsors or end customers who want to ensure that a given version of a product or system continues to meet, over time, the security requirements identified when the certificate was issued.

Assurance continuity, on the other hand, is designed for developers who want to reduce the effort required for certification of each new version of their product or system.

---

[10] Procedure ANSSI-CC-SUR-P-01 " Surveillance des produits certifiés"

[11] Procedures ANSSI-CC-MAI-P-01 "Assurance continuity", ANSSI-CSPN-MAI-P-01 "Maintien de la confiance : continuité de l'assurance"

Chapitre 10
Handling confidential information

10.1. Access to premises

The certification body's premises have the same security level that applies to the Secrétariat général de la défense et de la sécurité nationale; it thus benefits from the heightened protection and security measures that apply to the latter.

10.2. Access to information

The information exchanged during the evaluation most often has a sensitive nature. The certification body handles this information using adequate protection rules[12].

In the framework of the approval, the certification body ensures that evaluation facilities apply similar rules for managing sensitive information they handle.

---

[12] Procedure ANSSI-CC-SECU-P-01 "Gestion de la confidentialité au centre de certification"

Chapitre 11
Anomalies, complaints

11.1. *From the certification body*

11.1.1. Recording and processing

The certification body retains a record of certification anomalies in order to take necessary measures and to act on the cause and the precursory or predisposing factors[13].

11.1.2. Disputes

The certification management committee investigates, with the objective of conciliation, any dispute, submitted to it by the parties, regarding the evaluation procedures organised by decree 2002-535.

This mission may be delegated by the committee to one of its members; it must involve the hearing of the parties.

11.2. *From sponsors*

For certified objects, the certification body requires that the sponsor advise it of any complaint brought to its attention regarding the conformity of the object with the requirements listed in its security target.

---

[13] Procedure ANSSI-CC-ANO-P-01 "Anomaly Processing"

Annexe A
Reference documents

Regulations

Certification

Amended decree 2002-535 of 18 April 2002 relating to the evaluation and certification of the security provided by information technology products and systems.
Order of 28 February 2003 nominating the management committee for security certification of information technology.
Order of 1 April 2014 delegating signature (Secrétariat général de la défense et de la sécurité nationale).

SGDSN/ANSSI

Decree No 2009-834 of 7 July 2009 establishing a national service called the "Agence nationale de la sécurité des systèmes d'information."

Electronic signature

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
Law 2000-230 of 13 March 2000 defining the adaptation of the law of proof to information technologies and relating to electronic signatures.
Decree 2001-272 of 30 March 2001, amended, enacted to implement article 1316-4 of the French Civil Code relating to electronic signatures.
Commission Decision (2000/709/EC) of 6 November 2000 on the minimum criteria to be taken into account by Member States when designating bodies in accordance with Article 3, paragraph 4 of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures.

Texts on accreditation

NF EN ISO/IEC 17065:2012	Requirements for bodies that certify products, processes and services.
CPS-Ref-02	Accreditation criteria for certification bodies operating products and services, revision 01, November 2002.
NF EN ISO/IEC 17025	General requirements for the competence of testing and calibration laboratories.

Evaluation criteria

ITSEC	IT system security evaluation criteria (ITSEC), version 1.2, June 1991.
ITSEM	Information technology security evaluation manual, version 1.0 (ITSEM), September 1993.
JIL	ITSEC Joint Interpretation Library (ITSEC JIL), version 2.0, November 1998.
CC	Common Criteria for Information Technology Security Evaluation: • Part 1: Introduction and general model, version 2.3 and 3.1; • Part 2: Security functional requirements, version 2.3 and 3.1; • Part 3: Security assurance requirements, version 2.3 and 3.1.
CEM	Common Methodology for Information Technology Security Evaluation: • Part 1: Introduction and general model, version 0.6, January 1999; • Part 2: Evaluation Methodology, version 2.3 and 3.1.
ISO/IEC 15408	Information technology — Security techniques — Evaluation criteria for IT security 15408:2005: • ISO/IEC 15408-1:2005 (E): Part 1: Introduction and general model; • ISO/IEC 15408-2: 2005 (E): Part 2: Security functional requirements; • ISO/IEC 15408-3: 2005 (E): Part 3: Security assurance requirements.

Annexe B
Definitions and Acronyms

Definitions

Certification body	ANSSI office established by decree 2001-693 and orders 15-02-2002-1 and 15-02-2002-2. Its staff members examine the certification files.
Evaluation facility	Organisation accredited according to the ISO/IEC 17025 reference base and accredited by the certification body to conduct security evaluations for certification under amended decree 2002-535.
Certifier	Staff member of the certification body responsible for examining certification files.
Certificate	It certifies that the example of a product or system complies with the security requirements specified in its security target. It also certifies that the evaluation was carried out according to current rules and standards, with the required levels of competence and impartiality (article 8 of amended decree 2002-535).
Certification	The act of providing assurance of conformity to standards and other normative documents.
Sponsor	Person or organisation requesting an evaluation with the objective of obtaining certification.
Certification management committee	Management committee for security certification of information technology, defined by Chapter III of amended decree 2002-535.
Security target	Set of security requirements constituting the certification standard for ITSEC, Common Criteria and ISO/IEC 15408 evaluations.

Acronyms and Abbreviations

SGDSN	Secrétariat Général de la Défense et de la Sécurité Nationale
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CCRA	Common Criteria Recognition Arrangement
SOG-IS	Senior Officer Group-Information Security
ETR	Evaluation Technical Report
CC	Common Criteria
CSPN	Certification de Sécurité de Premier Niveau (First Level Security Certification).

Annexe C
Correspondence table between the quality manual and the NF EN ISO/IEC 17065:2012 standard

Paragraph of the standard	Chapter of the manual
4 Certification body	
4.1 General provisions	
4.1.1	2.4.2
4.1.2	4.1
4.1.3	4.3
4.1.4	2.1
4.2 Organisation	Chapitre 2
4.3 Operation	Chapitre 4
4.4 Sub-contracting	6.1
4.5 Quality system	
4.5.1	**Erreur ! Source du renvoi introuvable.**
4.5.2	Chapitre 3
4.5.3	Quality manual
4.6 Conditions and procedures for granting, maintaining, extending and revoking certification	
4.6.1	Chapitre 7
4.6.2	Chapitre 7
4.7 Internal audits and management reviews	
4.7.1	3.3.2
4.7.2	3.3.1
4.8 Documentation	
4.8.1	3.4
4.8.2	3.4.2
4.9 Recordkeeping	
4.9.1	3.4.3
4.9.2	3.4.3
4.10 Confidentiality	
4.10.1	Chapitre 10
4.10.2	Chapitre 10
5 Certification body staff	
5.1 Overview	
5.1.1	2.4.5
5.1.2	2.4.4
5.2 Qualification criteria	
5.2.1	2.4.5
5.2.2	2.4.5

5.2.3	2.4.5
6 Modification of requirements for certification	4.4
7 Appeals, complaints and challenges	
7.1	11.1
7.2	11.1
8 Application for certification	
8.1 Information on the procedure	
8.1.1	Chapitre 4
8.1.2	Chapitre 5
8.1.3	Chapitre 5
8.1.4	Chapitre 5
8.2 The application	
8.2.1	5.1
8.2.2	5.1
9 Preparation for the evaluation	
9.1	5.2
9.2	5.2
9.3	5.2
9.4	5.2
10 Evaluation	Chapitre 6
11 Evaluation report	6.1.4
12 Certification decision	
12.1	Chapitre 7
12.2	Chapitre 7
12.3	Chapitre 7
12.4	9.2
13 Surveillance	
13.1	Chapitre 9
13.2	Chapitre 9
13.3	Chapitre 9
13.4	Chapitre 9
14 Use of licenses, certificates and conformity marks	
14.1	Chapitre 8
14.2	Chapitre 8
14.3	Chapitre 8
15 Complaints from the supplier	11.2