Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, April 7th, 2014

No. 1410 /ANSSI/SDE/PSS/CCN

Reference: ANSSI-CSPN-CER-P-01/1.1

PROCEDURE

FIRST LEVEL SECURITY CERTIFICATION FOR INFORMATION TECHNOLOGY PRODUCTS

Application : As soon as approved.

Circulation : Public.

COURTESY TRANSLATION

Version history

Edition	Date	Modifications
Experimental phase	April 25th, 2008	First draft for the experimental phase, circulated under No. 915 SGDN/DCSSI/SDR of April 25th, 2008, and repealed by this procedure.
1.0	May 30th, 2011	End of the experimental phase. Change in constraint load for the basic evaluation (excluding cryptography) from 20 m.d to 25 m.d. Change in name for the certification body (ANSSI) and editorial improvements.
1.1	April 7th, 2014	Addition of the observer status to the evaluation. Addition of the possibility of related methodologies. Addition of the STB and secure execution environment product categories. Addition of products that require specific execution privileges. Limit on the CSPN evaluation process for products with certificates recognised by the ANSSI.

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

This procedure is available online on the ANSSI's institutional website (www.ssi.gouv.fr).

TABLE OF CONTENTS

1 Subject of the procedure

This procedure describes the entire first level security certification (CSPN) process for a product, from the official request by a sponsor to assignment of a certificate for the evaluated product, as well as the role of each actor.

2 Context

Amended decree No. 2002-535 of April 18th, 2002 relating to the evaluation and certification of the security provided by information technology products and systems defines the regulatory framework for the French evaluation and certification scheme.

This scheme defines the organisation for an evaluation to be carried out by a third party and its inspection, leading to the issuance of a certificate stating that a product or system meets the security requirements specified in its security target.

The first level security certification certifies that a product has successfully passed a security evaluation by a certification facility licensed by the ANSSI; the evaluation has the following main characteristics:

- To be carried out in reduced time and with reduced human resources (load);
- To analyse the conformity of the product with its security specifications;
- To measure the effectiveness of the security functions.

3 Reference documents and definitions

3.1 Reference documents

The first level security certification is governed by the following documents, the current versions of which are available on the ANSSI site (www.ssi.gouv.fr).

[LICENSING]: Licensing of evaluation facilities for the first level security certification, procedure ANSSI-CSPN-AGR-P-01.

[CRITERIA] : Criteria for the first level security evaluation of information technologies, instruction ANSSI-CSPN-CER-I-01.

[METHOD] : Evaluation methodology for the CSPN and content expected in the ETR, instruction ANSSI-CSPN-CER-I-02.

[EVAL_FILE] : Evaluation request file for a first level security certification, procedure ANSSI-CSPN-CER-F-01.

[CONTINUITY] : Maintenance of confidence, assurance continuity, procedure ANSSI-CSPN-MAI-P-01.

[SURVEILLANCE]: Surveillance of certified products, procedure ANSSI-CSPN-SUR-P-01.

[RGS] : General security reference base, in particular its appendix B:
[RGS_B1]: Rules and recommendations concerning the choice and dimensioning of cryptographic mechanisms.
[RGS_B2]: Rules and recommendations concerning the management of the keys used in cryptographic mechanisms.
[RGS_B3]: Rules and recommendations concerning authentication mechanisms.

[CRYPTO_SUPPLIES]: Supplies needed to analyse cryptographic mechanisms.

[MAR_P_01] : Procedure ANSSI-CC-MAR-P-01 related to the use of the "IT product certification" mark

3.2 Definitions

Evaluation facility	Organisation licensed by the ANSSI which evaluates the product security for the CSPN.
Evaluation target	Actual product submitted for evaluation.
Security target (ST)	Document that describes the product's security functions which are the subject of evaluation and certification.
Request made by	The sponsor is the party which requests certification from the ANSSI and which finances the evaluation service.
CSPN	First level security certificate (of first level security certification, depending on the context).
Developer	The term developer denotes the organisation which specifies, develops or maintains the product or some of its components.
Observer	The observer is an actor who is concerned by the results of the evaluation. In general, this is a client of a user of the evaluated product.
Certification report	Summary report established by the ANSSI based on the evaluation technical report
Evaluation technical report (ETR)	Report established by the evaluation facility which records the results of its evaluation.

4 The actors

4.1 List of actors

The following actors are involved in the certification process:

- The sponsor;
- The evaluation facility;
- The ANSSI's certification body;
- Possibly, the developer of the product submitted for evaluation;
- Possibly, one of the observers concerned by the results of the evaluation.

4.2 The sponsor

The sponsor provides the product, its security target and its documentation. When essential product security functions are based on cryptographic mechanisms, the sponsor also provides the documentation which describes these mechanisms, as laid down in the document [FOURNITURES_CRYPTO].

They sign a contract with an evaluation facility licensed by the ANSSI to carry out the security evaluation.

They request certification from the ANSSI using an evaluation request file [EVAL_FILE].

They receive the final version of the evaluation technical report (ETR) validated by the ANSSI.

They decide on whether or not to publish the certification report drafted by the ANSSI.

4.3 The evaluation facility

The evaluation facility is licensed for the technical domains in which its skills are estimated to be sufficient by the ANSSI. An evaluation facility may only evaluate products for an CSPN In the technical domains for which it has been licensed. However, several evaluation facilities may combine their skills to cover all the skills needed to evaluate a product.

They sign a contract with the sponsor to evaluate a product in the technical domain for which they are licensed.

They evaluate the product according to the criteria and methodologies drafted by the ANSSI for the CSPN.

They enter the results of their evaluation into an evaluation technical report (ETR) which they send to the ANSSI for validation.

The evaluation facility and its personnel are obliged to maintain professional secrecy for the products they evaluate and the results they obtain during the evaluation.

The list of evaluation facilities licensed for the CSPN is kept up to date on the ANSSI website (www.ssi.gouv.fr).

4.4 The ANSSI's certification body

The ANSSI's certification body drafts the evaluation criteria and generic method for the CSPN, as well as methods specific to certain types of product.

It drafts the procedures, forms, guides and all other documents necessary to implement the CSPN, among which are:

- The evaluation facility licensing procedure;
- The templates for drafting security targets, evaluation technical reports and certification reports;
- The CSPN request form.

It ensures that the evaluation facilities satisfy the criteria listed in the evaluation facilities licensing procedure (see [LICENSING]) and proposes their licensing.

It analyses the certification request files (security target, test duration, etc.) and authorises or prohibits the launch of the evaluation.

It validates the ETR drafted by the evaluation facilities.

It proposes the follow-up for each evaluation (certification or not).

It drafts the certification report and the certificate.

With the sponsors' agreement, it has the security target and the certification report published for the products which obtained a CSPN on the ANSSI website (www.ssi.gouv.fr).

4.5 The developer

The developer is responsible for producing any supplies and for providing technical assistance to the evaluators if necessary (training, testing, provision of an evaluation platform). They are responsible for protecting their know-how and their supplies.

4.6 The observer

The sponsor may propose the presence of an observer who is associated with the evaluation monitoring. The observer is subject to acceptance from the ANSSI.

The observers are actors who have a specific interest in relation to the results or conduct of the evaluation. In general, these are clients who impose the evaluation to authorise the acquisition of products by their organisation or the organisations they represent; they may be risk managers of

these organisations who have a specific interest in the concrete results of the evaluation (for example, knowledge of the residual risks), etc.

The observer is kept informed of the start of the evaluation and the results obtained.

They may ask to receive the evaluation technical report (ETR) or an abbreviated version of this report.

5 Certification request preparation

Before they formulate a CSPN request for a product, the sponsor must ensure that:

- They have a security target for the product, drafted in French, containing at least:
  - The product's commercial name and a reference to identify clearly the product and the version submitted for evaluation;
  - A presentation of the product, describing clearly:
    - The use for which the product has been designed, by whom and in which usage context it is supposed to be used;
    - The technical environment in which the product operates (computer model, operating system, etc.);
    - The sensitive goods that the product must protect;
    - The threats against which the product offers protection;
    - The security functions implemented by the product to counter the threats identified. These are the functions which will be the subject of the evaluation[1];
- They have documentation in French enabling an end user to securely use the product (user documentation, potentially administration and installation documentation);
- If essential product security functions are based on cryptographic mechanisms, that they have the documentation which describes these mechanisms, as well as sets of tests that enable the evaluator to check the conformity of the mechanisms implemented with their description;
- That the product may be associated with one or more of the following technical domains:
  1. Intrusion detection;
  2. Anti-virus, protection against malicious codes;
  3. Firewall;
  4. Data erasure;
  5. Security administration and supervision;
  6. Identification, authentication and access control;
  7. Secure communication;
  8. Secure messaging;
  9. Secure storage;
  10. Secure execution environment;
  11. Set top box (STB);
  12. Hardware and embedded software;

  Note: if the product does not fall under any of the previous conditions or if there is any doubt, the sponsor may contact the certification body to determine whether the product may be evaluated under the CSPN and, if this is the case, the evaluation facilities which may carry out the evaluation;

[1] If the product requires specific privileges to run on the user's station, the evaluation will relate more to the non-alteration of the host system security rather than the functionalities specific to the product.

- If a specific CSPN evaluation methodology exists for this type of product, it is this methodology which is retained and that the produce meets any requirements contained in this methodology;
- The evaluation facility may have access to the product;
- The evaluation facility may have access to test equipment if it is specific or dedicated;
- No Common Criteria certification as part of CCRA or SOGIC mutual recognition agreements is in progress or has been carried out on a similar version of the product[1].

6 Choice of an evaluation facility

The sponsor signs a contract with an licensed evaluation facility (or an association of licenver evaluation facilities) for the technical domains in which the product to be evaluated is classified.

7 Certification request

The sponsor drafts and sends to the certification body:

- The certification request (see [EVAL_FILE]);
- The product's security target;
- Where applicable, the documentation on the cryptographic mechanisms (see [CRYPTO_SUPPLIES]).

8 Analysis of the request

The certification body analyses the request and the product's security target. After these elements are accepted by the certification body, the certification project is registered and the actors (sponsor, evaluation facility) are informed that the project has started by a letter from the ANSSI.

There may be several reasons for an application being refused, in particular:

- Incomplete request;
- Incomplete security target;
- Security target clearly misleading (for example, the product is a firewall and the only security function described as needing to be evaluated is the user authentication to modify the configuration of their product);
- Evaluation facility not licensed for the product's technical domain;
- Product whose complexity is such that an evaluation is not possible in the context of the CSPN;
- Use of cryptographic algorithms that do not conform to a standard;
- Refusal by the sponsor to inform the certification body of the product's potential vulnerabilities;
- Failure to respect the pre-requisites identified in chapter 5.

9 Conduct of the evaluation

9.1 General information about the evaluation procedure

The evaluation is carried out according to a formalised methodological framework (see [CRITERIA] and [METHOD]) to guarantee its objectivity and to encourage the homogeneity of the results between the different evaluation facilities. This methodological framework is also used

[1] The CSPN request may be validated if the product evaluation corresponds to a specific need that the sponsor shall justify in their request; the ANSSI will assess the opportunity and the relevance of this justification.

to facilitate the comparison of the results of evaluations on similar products when they are carried out by different evaluation facilities. There may be a specific methodology for certain types of product[2]. In this case, this methodology must be used by the evaluator.

The ANSSI may request to take part in some or all of the evaluation tasks carried out by the evaluation facility.

If the time scheduled for the evaluation is exceeded, the ANSSI may decide to close the certification project. However, the sponsor is not freed of any contractual obligations they may have in relation to the evaluation facility.

The purpose of the evaluation is to assess the following in terms of time and workload constraints:

- The product's conformity with its security target (§ 9.3);
- The effectiveness of the security functions (§ 9.4);
- The impact of the product on the host system's security (§9.5).

The evaluation process is based on:

- The documentation provided;
- At least the public vulnerability bases for the analysis of the product in relation to the vulnerabilities known for the type of product analysed;
- The product itself, which is installed on a test platform which is as representative as possible of its planned usage environment.

The results are entered into an ETR which is sent to the certification body.

9.2 Constraints imposed

The evaluation is carried out under time and workload constraints to respond to cost and deadline requirements.

Except when another specific workload is recommended in a particular methodology, an evaluation for a CSPN must normally be carried out in 25 man.days and within a calendar period of 8 weeks. The sponsor and the evaluation facility may propose an adaptation to this duration and this workload (for example, this may be the case when the evaluation requires the participation of several evaluation facilities); however, the ANSSI reserves the possibility of refusing an evaluation for which it considered that the failure to respect the nominal constraints highlights the fact that the CSPN is clearly unsuited to the product.

When essential product security functions are based on cryptographic algorithms, the workload is increased by 10 man.days to enable its analysis.

9.3 Conformity analysis

The conformity analysis is carried out on a test platform, which must be described in the ETR.

The objective of this phase is twofold. Which are:

- First of all, to verify that the product conforms to its security specifications: all the non-conformities discovered must be traced and stated in the ETR;
- Secondly, to enable the evaluator to fully understand the product in its entirety to be relevant in the effectiveness analysis.

Where possible and where it has meaning, the conformity analysis may also include:

- An analysis of the product's performances;
- A description of any interoperability of the product with other products.

[2] These methodologies are published on the page of the ANSSI's website dedicated to CSPN evaluation criteria and methodology (www.ssi.gouv.fr).

9.4 Effectiveness analysis

The main objectives of the effectiveness analysis are to:

- Score the theoretical resistance of the security functions and mechanisms and, where applicable, the cryptographic mechanisms;
- Identify the vulnerabilities;
- Provide an opinion on the risks of improper use;
- Provide an expert opinion on the product's effectiveness;
- Potentially, propose a configuration and a usage environment which enables the exploitability of the vulnerabilities to be limited and, in this case, to give a second expert opinion on the product's effectiveness in its new usage environment.

9.5 Analysis of the impact on the host system's security

If the product requires specific privileges on the host system to operate, the evaluation will verify in particular that the product does not degrade the host system's security.

9.6 Evaluation technical report

The ETR contains at least the following information:

- A reminder of the analysis context (usage context, analysis duration and security functions in particular);
- A summary of the documentation providing a description of the security or security-related functions;
- The functional expectations on the product (summary of its security characteristics in particular);
- An inventory of the product vulnerabilities (information from the CERT-FR, public bases or the developer) and the applicable available corrections;
- A list of the main analysis tools used;
- A summary of the results of the tests carried out on the product;
- Scoring for the resistance of the security mechanisms and the cryptographic mechanisms where applicable;
- A report and scoring for any exploitable vulnerabilities identified;
- An opinion on the product's ergonomics and recommendations for use or configuration in the planned usage context.

The ETR's plan is imposed (see [METHOD]).

10 Certification

10.1 Nominal case

When the evaluation is complete, the ETR is sent to the ANSSI's certification body. The nominal certification process is made up of the following steps:

1. Analysis of the ETR. The ANSSI may be required to request further information or even additional work from the evaluation facility if this information or work is considered insufficient.
2. Presentation of the work and the results of the evaluation by the evaluation facility. At this point, the ANSSI may request a demonstration of the product. The evaluation's sponsor may be invited to this presentation.
3. Drafting of the certification report. In particular, this features a scoring for the resistance of the product's security mechanisms and, where applicable, its cryptographic mechanisms to

attacks, as well as any usage recommendations. It indicates all the potential problems raised during the evaluation and which are likely to be of interest to a user. It is written in French.

4. Sending of the draft certification report to the sponsor for validation and, where applicable, for agreement to publication.
5. Presentation of the certification report to the Directeur Général of the ANSSI who, if he decides to announce certification, signs the report, which is published on the ANSSI's website if the sponsor agrees. The " Certification Sécurité TI " mark must be used in accordance with procedure ANSSI-CC-MAR-P-01 [MAR_P_01].

10.2 Specific case

If the ETR shows that the product does not meet or only partially meets its security target and that realistic environmental counter-measures cannot be identified to improve this situation, the certification process is stopped after stage 1 or 2.

The sponsor is informed of this situation. Among the reasons why the ANSSI may estimate that the product does not fully meet its security target are:

- Resistance of the security functions and mechanisms and, where applicable, the cryptographic mechanisms which is too low;
- Malfunction of certain security functions;
- Malfunction of certain product functionalities, preventing normal use;
- Inability to obtain certain information required to understand the product's security functions, preventing the correct estimation of the resistance of the security functions and mechanisms and, where applicable, the cryptographic mechanisms;
- Inability to have sufficiently-detailed elements to conclude the absence of negative impact by the product on the host system.

11 Assurance continuity

A certificate only relates to a precise version of a product. If this product evolves, its new versions are not certified by default. The assurance continuity process (see [CONTINUITY]) is used to determine at low cost whether a new product version may benefit from the certificate of a previously certified version. This process is applicable to the CSPN.

12 Surveillance

As the state of the art in the security sector changes constantly, a certified product may become vulnerable to new attacks. A sponsor may make sure a product is secure by periodically requesting new vulnerability analyses. The procedure [SURVEILLANCE] describes the process proposed by the ANSSI to monitor a product's resistance to new attacks over time. This process is applicable to the CSPN.

13 Advertising

The sponsor may publicise the product's CSPN certification. They must do so in honest terms and understandable by the end user. They must indicate:

- The certificate reference;
- The product's certification date;
- The references and version of the certified product;
- If the product is the subject of a surveillance procedure.

They may also mention the ANSSI's website address where the user may consult the product's security target and the certification report.

The ANSSI reserves the possibility of highlighting any abusive use of the CSPN using any methods it considers necessary.