GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
CENTRO CRIPTOLÓGICO NACIONAL

CCN-LINCE-001

# Definition of the National Essential Security Certification (LINCE)

Version 0.1 June 2018

**COURTESY TRANSLATION**

**VERSION CONTROL**

| Version | Comments | Date |
|---|---|---|
| 0.1 | Version for trial use | June 2018 |
| | | |
| | | |

Published by:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA



This document is a courtesy translation of the official document written in Spanish language. Official document shall be used in LINCE certifications.

This document version is in trial use phase to be used in the National IT Security Evaluation and Certification Scheme ENECSTI. The National Cryptologic Centre (CCN) is currently accepting comments to improve the current version of this document.

Publication date: June 2018

**DISCLAIMER**

The present document is provided in accordance to the terms included in it, categorically refusing any kind of implicit warranty which may be related. In no case CCN will be considered responsible for direct, indirect, fortuitous or extraordinary damage derived from the usage of the information and software which are indicated, even when the possibility of such damage has been warned.

**LEGAL WARNING**

It is strictly forbidden, without a written authorization by CCN, under the penalties established by the law, the partial or total duplication of this document by any mean or procedure, being reprography and computer processing included, and the distribution of any copy through rental or public lease.

# INDEX

# 1. SCOPE OF THIS DOCUMENT

The National Cryptologic Centre (Centro Criptológico Nacional – CCN) develops the LINCE evaluation and certification methodology as a response to the need of certification of products which are to be deployed in environments with a basic or medium threat level. For those cases in which the threat level is higher, it is still recommended to use evaluation methodologies such as Common Criteria [CC], in which the evaluator and certifier have a better knowledge of the correct implementation of the security mechanisms of the product to be certified and a bigger effort is made at the certification process.

This document describes the National Essential Security Certification (LINCE) for an ICT product, including the definition of the roles which are involved in the evaluation process, as well as the different evaluation tasks in the certification process.

The evaluation and certification of an ICT security product is the only unbiased way for assessing and certifying an ICT product's capability for handling information securely. In Spain, such responsibility relies on the Centro Criptológico Nacional (CCN) in accordance to the Royal Decree 421/2004 of March 12th in its articles 1 and 2.1, which establish that the head of the CCN is the authority for certifying the security of information and communication technologies and the authority for cryptologic certification.

In this way, the Centro Criptológico Nacional performs as the Certification Body (OC) for the Esquema Nacional de Evaluación y Certificatión de la Seguridad de las Tecnologías de la Información (National ICT Security Evaluation and Certification Scheme - ENECSTI), which applies to ICT products as indicated in the Presidential Order PRE/2749/2007, September 19th, by which the Rules for Evaluation and Certification of the Security in Information Technologies are sanctioned.

This scheme defines the organization needed for an ICT security evaluation to be carried out by a trusted and technically qualified third party, ending up with the issuance of a certificate which proves that a product or system meets the security requirements specified within its Security Target.

The LINCE certification procedure shall follow in as indicated in the procedure PO-005 (Product Certification) published in the web of the CCN (https://oc.ccn.cni.es).

Throughout this document, the particularities of the LINCE certification will be described, providing information about itself and contextualizing every possible interested party.

An ICT security evaluation (STIC) evaluation is a set of tests which shall be performed by a laboratory to verify and attest that all the Essential Security Requirements (RFS) are met by a product. These tests consist of vulnerability analysis, black box testing and operational environment tests, among others.

For a National Essential Security Certification (LINCE) to be carried out, an evaluation methodology [CCN-LINCE -002] has been defined. This methodology may also be used to perform STIC evaluations as indicated in the CCN ICT security guidance ([CCN-STIC-106]).

The National Essential Security Certification (LINCE) certifies that a product has successfully passed a security evaluation through a certification process authorized by the CCN. The evaluation has the following main characteristics:

a) It must be performed within an enclosed and predefined time length and work load.

b) It must analyze the conformity of the product with its Essential Security Requirements as defined in the CCN ICT security guidance [CCN-STIC-140].

c) It must measure the resistance of the security functions of the product.

d) It must be oriented to vulnerability analysis and penetration testing.

The National Essential Security Certification (LINCE) is composed by a base assurance package and two optional modules which might allow increasing the security assurance of this kind of certification. These optional modules are the following:

a) Cryptographic Evaluation Module (MEC): The objective of this module is to functionally assess the cryptographic mechanisms implemented in a product. The inclusion of this module guarantees that the cryptographic functions used are functionally tested. Throughout this document, the convention (MEC) will be used in order to identify the optional requirements of this module.

b) Source Code Review Module (MCF): The objective of this module is to review some parts of the product's source code related to the declared security mechanisms as part of the evaluation. This allows the product to be evaluated in depth similar to as a "white box" evaluation for those specific security mechanisms. Throughout this document, the convention (MCF) will be used in order to identify the optional requirements for this module.

Thus, the following types of certificates will be available part of the National Essential Security Certification:

a) Essential: LINCE evaluation.

b) Essential + MEC: LINCE evaluation + Cryptographic Evaluation.

c) Essential + MCF: LINCE evaluation + Source Code Review.

d) Essential + MEC + MCF: LINCE evaluation+ Cryptographic Evaluation + Source Code Review.

## 2. DEFINITIONS

**LINCE evaluation laboratory:** Entity authorized by the CCN according to Presidential Order PRE2740/2007 which is in charge of performing the security evaluation of the product following the LINCE methodology.

**Target of Evaluation (TOE):** It may be a complete product or a part of it. Throughout this document, the terms TOE and product will be equally used, being the second one referring to the concept of TOE.

**Security Target (ST):** Document describing the security functions of the product which are to be evaluated.

**LINCE:** National Essential Security Certification.

**Developer:** Entity which specifies, develops, maintains and/or manufactures the product or some of its components.

**Evaluation Technical Report (ETR):** Report, issued by the LINCE evaluating laboratory, which summarizes the results of their evaluation.

**Certification Report:** Report issued by the Certification Body based upon the Evaluation Technical Report and which describes the key elements in performed certification.

**Essential Security Requirements (RFS):** Detailed description of the security characteristics that may mitigate the threats defined in the security problem within the security target. These requirements are to be specified within the CCN ICT security guidance [CCN-STIC-140].

# 3. ROLES AND RESPONSABILITIES IN THE LINCE CERTIFICATION

## 3.1 ROLES LIST

The following roles are involved in the certification process:

a) The sponsor or developer is in charge of requesting the evaluation of the product to the Certification Body, its funding, and designing, developing and/or maintaining the product or its core components.

b) The evaluation laboratory is an entity authorized by the Certification Body to evaluate the product under this scheme.

c) The Certification Body is the one in charge of validating the report coming from the evaluation laboratory and issuing the certificate in case that the evaluation has been successfully completed.

## 3.2 SPONSOR OR DEVELOPER

The developer shall provide the product, its associated security documentation and the security target for the evaluation to take place.

Additionally, the sponsor is in charge of providing the testing environment for the product security evaluation.

The developer is also in charge of the development and the one responsible for providing any sort of information that may be needed as well as providing technical assistance to the evaluators if needed (training, tests, supply of the testing platform).

(MEC) – When the essential security requirements of the product contain cryptographic mechanisms and a cryptographic evaluation module is included as part of the certification process, the developer must also provide the documentation which describes those mechanisms.

(MCF) – When the Source Code Review Module is included within the terms of the evaluation, the developer will provide such code at the beginning of the evaluation.

The developer will have the following additional responsibilities:

a) To sign a contract with a LINCE authorized evaluation laboratory to perform the security evaluation.

b) Apply for a certification process to the CCN by using the certification request form [FOR-001].

c) Support the evaluation laboratory during the evaluation to perform the evaluation tests.

Note: In some cases, the developer and the certification applicant (sponsor) of may be different entities. For simplicity, they have been listed as one single role. In

these cases and in general terms, the sponsor will be the one in charge of funding the evaluation and the developer the one providing the necessary technical support to perform the certification process.

## 3.3 EVALUATION LABORATORY

A LINCE evaluation laboratory is an entity accredited within the ENECSTI in accordance to the definitions of the Presidential Order PRE/2740/2007 of September 19th and according to the Laboratories Accreditation Procedure [PO-006] to perform security evaluations.

Before starting with the evaluation activities, the evaluation laboratory must sign a contract with the developer to evaluate the product. During the negotiation of such contract, the lab will hold responsibility for evaluating the security target provided by the developer to check for the ability of performing the product evaluation given the time and workload restrictions established in the evaluation methodology [CCN-LINCE-002], besides considering its technical qualification. After this, the evaluation laboratory will produce an evaluation plan which will be attached with the evaluation request to the Certification Body. The evaluation laboratory is expected to justify within the evaluation plan the suitability of the security target as well as their technical competence to perform the evaluation.

The evaluation laboratory is in charge of performing the evaluation of the product according to the product certification procedure PO-005 and the methodology defined for LINCE evaluations [CCN-LINCE-002], as well as issuing the Evaluation Technical Report (ETR) (see template in [CCN-LINCE-004]) to the Certification Body for its validation.

The evaluation entities and its personal are bound to maintain confidentiality about the evaluated products and the results obtained during its evaluation.

The updated list of evaluation entities authorized by the CCN can be found in the website of the Certification Body.

## 3.4 CERTIFICATION BODY

The responsibilities of the Certification Body are the following:

- Elaborate the criteria and evaluation methodology for the LINCE certification. The Certification Body may demand the use of specific evaluation methods in accordance to the product's characteristics.
- Specify the procedures, forms, guides and the all the necessary documentation to implement the LINCE certification, among which there are:
    - The certification procedure for products [PO-005].
    - The accreditation procedure for laboratories [PO-006].
    - The LINCE evaluation methodology [CCN-LINCE-002].

  - The LINCE Security Target template [CCN-LINCE-003].
  - The LINCE Evaluation Technical Report template [CCN-LINCE-004].
  - The Product Certification Request form [FOR-001].
  - The Laboratory Accreditation request form [FOR-005].
- Assure and verify that the laboratories satisfy all the criteria listed in the laboratory authorization procedure [PO-006].
- Supervise and review the certification and evaluation requests and authorize or deny the start of an evaluation, taking into account the evaluation plan presented by the laboratory.
- Answer any existing questions (e.g. interpretations of the methodology to be used) during the evaluation process.
- Validate the evaluation tasks documented within the ETR issued by the laboratories.
- Prepare the certification report and issue the corresponding certificate.
- Publish, the LINCE certificate within the CCN certified products list, including the TOE security target and the certification report.

# 4. CERTIFICATION PROCESS STEPS

## 4.1 PREPARATION OF THE CERTIFICATION

Before formulating a LINCE product certification request, the developer must:

a) Prepare the TOE's security target in accordance to the guidelines established in the Template for Security Target [CCN-LINCE-003]. The security target must include at least the Essential Security Requirements which are pertinent to the family of products to which the TOE belongs (see [CCN-STIC-140]).

b) Prepare the necessary documentation to allow the final user to use the product in a secure way (operational and preparative guidance) and prepare the TOE environment to perform the evaluation activities in collaboration with the evaluation laboratory.

c) (MCF) If the Source Code Evaluation Module has been included, the developer must prepare the source code for its delivery.

d) (MEC) If the Cryptographic Evaluation Module has been included, the developer must prepare the documentation which describes such mechanisms and prepare the environment to perform the required cryptologic tests.

**Note**: If the product does not cover any of the previous conditions or if there is any sort of doubt, the developer must contact the Certification Body in order to determine if the product can be evaluated under the LINCE certification process.

## 4.2 SELECTION OF AN EVALUATION LABORATORY

The developer must sign an agreement with a LINCE evaluation laboratory authorized within the ENECSTI before sending a product certification request.

Both the developer and the laboratory must agree on the scope of the evaluation attending to the security target presented by the applicant. The laboratory will be the one in charge of analyzing the security target to verify that its suitability to be evaluated attending to the declared security mechanisms and considering the time and work load restrictions determined in the methodology [CCN-LINCE-002].

## 4.3 CERTIFICATION REQUEST

The developer will prepare and send to the Certification Body the following:

a) The product certification request (see [FOR-001]).

b) The security target of the product (see template [CCN-LINCE-003]).

Note: If necessary, the developer may deliver an annexed document explaining any particularity in relation to the certification process.

## 4.4 EVALUATION REQUEST

The laboratory will produce and send an evaluation request to the Certification Body. This evaluation request will include:

a) A rationale for the suitability of the security target for a CCN-LINCE certification attending to the time and workload restrictions imposed in the [CCN-LINCE-002] evaluation methodology.

b) An evaluation plan where all evaluation activities should be planned and explained.

c) A rationale justifying their technical competence and laboratory and evaluators independence to carry out the evaluation process.

## 4.5 ANALYSIS OF THE REQUESTS

The Certification Body will analyze the certification and evaluation requests and the product security target.

There are different causes to reject a certification request, concretely:

a) Incomplete certification request.

b) Incomplete security target.

c) Misleading security target. The security target does not include the essential security requirements defined for the specific product family it belongs to. For example, a certification request will be rejected if the product is a firewall, and the only security mechanism within the scope of the security target is the user authentication to modify the security configuration of the product.

d) The declared security mechanisms on the scope of the security target are not suitable to perform a LINCE certification according to the time and workload restrictions in this kind of certification.

e) Do not follow the prerequisites identified in section 4.1.

When the certification request is accepted by the Certification Body, a certification dossier is created and registered and applicant and evaluation laboratory are notified about the acceptance of their requests.

If the Certification Body considers it as necessary, it could organize a kick-off meeting with the laboratory in order to check and determine the approximation to be followed by the laboratory during the evaluation.

If the Certification Body considers it is as necessary, additional guidance or supporting documents will be provided to the laboratory to carry out the evaluation activities. The Certification Body may make recommendations, as well as, establish additional supporting evaluation methodologies to be followed by the laboratory.

The assigned date for the evaluation authorization is recognized as evaluation kick-off date to be considered to compute the time restrictions within the evaluation methodology.

## 4.6 EVALUATION PROCESS

### 4.6.1. GENERAL INFORMATION REGARDING THE EVALUATION PROCEDURE

The evaluation must be carried out by an ENECSTI authorized LINCE evaluation laboratory according to the evaluation methodology (see [CCN-LINCE-002]) to guarantee that the LINCE certification meets the final purpose to which it was designed, as well as to assure the homogeneity of the results among different laboratories.

There is a possibility that the Certification Body may define a supplementary and specific associated evaluation guidance for certain products families. In this case, the laboratory will be notified and the proposed guidance shall be used by the evaluation laboratory.

If the time expected for the evaluation is exceeded, the Certification Body may close the certification process, independently of the contractual obligations which may exist between the developer and the laboratory.

The evaluation methodology includes the following activities:

a) Conformity analysis: The evaluator must verify the compliance of the product towards the security target.

b) Vulnerability analysis and penetration testing: The evaluator must perform a vulnerability analysis of the product and run the designed penetration tests, considering the state of the art in regards of publicly available threats and vulnerabilities, to verify the effectiveness of the TOE's security functions.

The evaluation tasks are the following:

a) Security target assessment.

b) Product preparation and configuration.

c) Conformity analysis – documentation analysis.

d) Conformity analysis – functional tests.

e) Vulnerability analysis.

   i. Analysis of the resistance of mechanisms/functions.

   ii. (MCF) Source code revision.

   iii. (MEC) Cryptographic evaluation.

f) TOE penetration testing.

The evaluation results are presented within an ETR [CCN-LINCE004] which is to be sent to the Certification Body for its technical validation.

Given time and effort limitations of the LINCE certification, the evaluator may request to perform work sessions with the developer to gain knowledge on the TOE in the fastest possible way.

Besides, the developer will have to provide an operative and testing environment before the evaluation begins, as well as supporting the evaluator during the preparation of the TOE.

### 4.6.2. EVALUATION TIME AND WORK LOAD RESTRICTIONS

The evaluation must be carried out under strict time and work load restrictions, aiming to limit the effort and duration of the evaluation process.

In general terms, a LINCE evaluation must be performed with an estimated work load of **25 man/days** (25 days by one evaluator) within a maximum period of **8 weeks**.

For time and effort estimation, it has been considered that the evaluators already count with the technical competence and experience needed to perform the evaluation of the product. The time needed to prepare the evaluators (e.g. a new technology) has not been taken into account.

For the optional **modules** (Source Code Review Module and Cryptographic Module), **5 man/day** and **2 weeks** duration are added for each module.

Including both modules, a LINCE evaluation can be carried out with an effort of 35 man/day and with a maximum period of 12 weeks. For more detailed information, see [CCN-LINCE-002].

## 4.7 CERTIFICATION PHASE

Once the evaluation has been completed, the evaluator will send the ETR to the CCN Certification Body. In general terms, the certification process consists in the following steps:

a) Technical analysis and validation of the ETR. The ETR validation phase may be performed by the study and analysis of the ETR. Technical meetings may be convened with the product evaluators in order to have a better knowledge over the performed tasks. Additional information or even additional work may be required from the evaluation laboratory if the information or work is considered insufficient.

b) Produce the certification report, whose content is detailed in section 4.7.1.

c) Carry out the defined tasks for the certificate issuance as specified in PRE/2740/2007 and described in the product certification procedure [PO-005].

### 4.7.1. CERTIFICATION REPORT

The certification report is focused on potential users of the evaluated product (TOE) and its goal is to provide information about the security characteristics that have been the subject of evaluation and the preparation, configuration and secure use conditions established in its guidance. The certification report shall include the following points:

a) An introduction describing the target of the evaluation (TOE).

b) A general view of the TOE, including a general description, including its version and unambiguous TOE identification and a list of the evaluated security functionalities and its associated configuration.

c) The target and limitations of the evaluation.

d) A description of the residual risks of the product when being used according to the evaluated configuration.

e) Guidelines for the secure administration and configuration including the secure delivery, environment preparation and TOE configuration.

f) Guidelines for a secure use of the product.

g) Evaluation and certification results.

## 4.8 CERTIFICATE VALIDITY

A LINCE certificate is issued for the specific version of the product that was evaluated. If this product evolves, its newer version will not be certified by default. The process of “Assurance Continuity” [AC] is used to ease the maintenance of the certificate in newer versions of the product. This process is considered to be also applicable to the LINCE certification.

It is recommended that the certificate validity should be reviewed at most every twenty-four months after being issued, and the applicant may choose to renew the certificate or repeat the certification, in accordance to what is established in the certification procedure PO-005.

## 5. CERTIFICATE ANNOUNCEMENT

The developer may announce or publicly use the certificate condition of LINCE certified product. This must be done in an honest way that can be understood by the final user, according to what is described in PRE/2740/2007. In general terms, they must indicate:

a) Reference of the certificate.

b) Date of the product's certification.

c) References and TOE version of the certified product.

d) References to the security target and certification report of the product.

The Certification Body reserves the possibility of looking after any abusive use of a LINCE certificate in accordance to what is established in the articles 149 and 152 of the PRE/2007/2740.

## 6. REFERENCES


| | |
|---|---|
| [AC] | Assurance Continuity: CCRA Requirements. Version 2.1 |
| [CC] | Common Criteria for Information Technology Security Evaluation. |
| [CCN-LINCE-002] | Evaluation Methodology National Essential Security Certification. |
| [CCN-LINCE-003] | Template for the CBSCCN-LINCE Security Target. |
| [CCN-LINCE-004] | Template for the CBSCCN-LINCE Evaluation Technical Report. |
| [CCN-STIC 106] | Procedure for the inclusion of qualified IT products in the CPSTIC. |
| [CCN-STIC-140] | Reference Taxonomy for the ICT product security. |
| [FOR-001] | Product Certification Request. |
| [FOR-005] | Laboratory Accreditation Request. |
| [PO-005] | Product Certification. |
| [PO-006] | Laboratory Accreditation. |

## 7. ACRONYMS

| | |
|---|---|
| **LINCE** | National Essential Security Certification |
| **CCN** | Centro Criptológico Nacional – National Cryptologic Centre |
| **CNI** | Centro Nacional de Inteligencia – National Intelligence Centre |
| **ENS** | Esquema Nacional de Seguridad – National Security Scheme |
| **ETR** | Evaluation Technical Report |
| **MCF** | Source Code Module |
| **MEC** | Cryptographic Evaluation Module |
| **OC** | Certification Body |
| **RD** | Real Decreto – Royal Decree |
| **ENECSTI** | Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de Información – National ICT Security Evaluation and Certification Scheme |
| **RFS** | Essential Security Requirement |
| **ST** | Security Target |
| **STIC** | Security of Information and Communications Technology |
| **TOE** | Target Of Evaluation |