GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN Centro Criptológico Nacional

CCN-LINCE-002

Evaluation Methodology for 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 will the Centro Criptológico Nacional 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 the Centro Criptológico Nacional, 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

This document establishes the evaluation methodology to be followed during a National Essential Security Certification (LINCE).

2. OBJECTIVE

This methodology has been designed by the National Cryptologic Centre (Centro Criptológico Nacional – CCN) aiming to define the necessary steps to perform an essential security evaluation of ICT products.

The 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 evaluation has a limited scope within an enclosed time and effort, allowing for the costs to be affordable for all kind of manufacturers. It is thus, a methodology created for the evaluation of products with medium or low criticality.

The objective of the evaluation process is to allow for an evaluation laboratory to verify if the product is compliant with its specifications, determining the effectiveness of the implemented security functions and including the results in the Evaluation Technical Report (ETR).

To do so, the evaluation laboratory bases on the Security Target (ST) which defines the scope of the certification, the user and product secure configuration guidance and the product's public information (technical specifications, product files, etc.) as well as the product itself (TOE). All these elements are provided by the developer of the product.

Additionally, in order to perform the evaluation, the laboratory will use all the public information related to the TOE to which they may have access. For example, information published by the manufacturer of this product or similar, public information obtained from third parties in relation to the product or public product vulnerability databases may be used to perform the evaluation activities.

The role performed by the different involved actors during the evaluation process is described in document [CCN-LINCE-001].

3. MINIMUN REQUIRED EVIDENCE

The sponsor or developer shall provide all the evidences included within this section at the beginning of the evaluation process.

All evidences shall be delivered before the beginning of the evaluation process. This measure is necessary to meet the established time and workload limitation in this methodology.

Below, there is a list of mandatory evidence:

a) Security Target (ST).

b) TOE operative and preparative guidance.

c) TOE operational environment.

d) (MCF) Source Code Review Module: The source code of the security mechanisms declared in the scope of the Security Target.

Note: The convention (MCF) will be used throughout this document in order to identify the optional requirements of this module.

e) (MEC) Cryptographic Evaluation Module: The documentation related to the cryptographic mechanisms declared in the scope of the Security Target and the mechanisms that may ease the cryptographic testing.

Note: The convention (MEC) will be used throughout this document in order to identify the optional requirements of this module.

3.1 SECURITY TARGET

The Security Target (ST) is used to describe the security mechanisms of the product to be evaluated (the TOE scope), and to describe the different interaction between the product and the TOE environment where it will be used. The Security Target is an important document for the product developer and for evaluators, but besides, it is of special interest for the TOE consumer. The ST defines the scope of the product's certification and will be published together with the certificate and the certification report.

According to the Security Target Template [CCN-LINCE-003], the ST of an ICT product must include the following information:

a) Unambiguous and clear TOE identification and its preparative and operative guidance.

b) TOE description, including:

   i. A TOE General description including its security functionality and mechanisms.

ii. TOE operational environment (e.g. Operating systems in which the TOE will run, external components needed for the correct TOE operation, etc.)

iii. The sensitive assets that the TOE must protect.

iv. The threats which the TOE must mitigate.

v. Assumptions about the operational environment which must be taken into account while performing the evaluation and that should be observed during the operational use of the TOE.

vi. The implemented security mechanisms and functions in the TOE scope in order to mitigate the identified threats. These functions will be the target of evaluation.

vii. Preparative and operative guidance identification for the evaluated secure use of the product.

Each of these listed elements is described below:

a) Unambiguous and clear TOE identification

It shall be possible to unambiguously identify the TOE that is being evaluated and, particularly its concrete version.

b) Unambiguous and clear operative and preparative guidance

It shall be possible to unambiguously identify operative and preparative guidance within the TOE scope. It expected that at least document version and issuing date should be used to identify these documents.

c) TOE Description

The Security Target shall describe using natural language the TOE scope including its core components, the TOE implemented security functions and mechanisms and its expected use.

d) Operational environment

The Security Target shall specify the TOE operational environment that is required to securely operate of the product. This environment can be generic (for example, a computer with a certain operating system) or a dedicated environment (for example, a computer with a specific configuration).

When the environment is described in general terms, the evaluator is not expected to test the product in all possible platforms. In this case, the specific platform in which the evaluation has been carried out must be determined. These platform specifications shall be clearly identified in the Evaluation Technical Report (ETR) and shall be included within the certification report.

e) Sensitive assets to be protected

The Security Target shall describe the assets that the TOE's security mechanisms are aimed to protect. The asset specification shall include the security dimension or dimensions that are protected for each one of the declared assets (confidentiality, integrity, availability, authenticity). In order to protect the listed assets, the product may use other data which shall be considered as an asset itself. For example, if the confidentiality of a user data is to be protected by an encryption mechanism which uses a certain encryption key, such key is to be considered as a TOE sensitive asset.

f) Threat description

The Security Target shall describe the threats that are mitigated by the security functions and mechanisms. A threat may be characterized by the following elements:

i. An actor (authorized user, administrator, malicious user, external attacker, etc.).

ii. An adverse action which would be executed by the actor (data injection, malicious access, information extraction, etc.).

iii. The asset or assets that would be affected by such action.

For example, the fact that a user may inject information and modify the behavior of a security function may constitute a threat.

f) Security functions and mechanisms specification

The Security Target shall include the specification of the security functions and mechanisms implemented by the TOE. These functions must be specified in natural language. They may be declared explicitly or reference a well-known standard that defines a security functionality.

The security mechanisms specification shall be complete enough as for an evaluator to fully understand how the functionality has been implemented and therefore the TOE is expected to behave.

When a Security Target should reference some standard which may be configured and operated according to different parameters, the concrete parameters in the TOE scope shall be clearly identified in the ST.

If the referenced standard does not provide enough information as to infer the security behavior, additional information must be specified in the Security Target

The security functions shall be present in the TOE operational mode and within the scope of the certification, this is, the security functions that are not to being evaluated will not be described within the Security Target and will thus remain out of the scope of the certification.

The specification of the security functions must prove how each of the functions counters or mitigates the declared threats.

Some developer may not want to include sensitive or proprietary information within the Security Target, given that this document is public. In such cases, it is acceptable to include an annexed confidential document with the Security Target providing the expected level of detail regarding the implementation of the security functions that are sensitive or proprietary and reference this annex along the Security Target.

In either case, a certified product consumer must be able to determine the scope of the product's certification by reading the Security Target, so the laboratory must verify that the information provided within the Security Target is enough to allow consumer to identify the TOE scope and the certified security functionalities.

g) (MEC) The Security Target shall include the list of the cryptographic mechanisms within the scope of the cryptographic evaluation. This list will be detailed in at least in the ST section dealing with the specification of the security functions.

h) (MCF) The Security Target shall include a list of the security mechanisms of the TOE whose source code is to be evaluated. This list will be detailed in at least in the ST section dealing with the specification of the security functions.

3.2 TOE PREPARATIVE AND OPERATIVE GUIDES

The TOE developer shall provide guidance or manuals related to the secure operation and preparation of the product. This guidance will serve as the basis for the evaluation activities.

The TOE developer shall at least describe in the **operational or secure use guidance**:

a) How to securely operate the TOE.

b) The accessible functionality for every user role.

c) The security related configurable parameters to be used while operating the TOE.

The **user guidance** shall describe the security functions which may concern the final user, as well as provide security directives for its secure operation. The reference manuals and user guides must be well-structured, keep internal consistence and must be coherent with other documents provided to the end user.

The **security management and administration guidance** shall describe how the TOE is securely managed, describing those security functions which may concern the administrator users. If and administrator role is defined, this guidance shall describe all the security parameters under their responsibility. This guidance should describe every security event covered within the administration functions, as well as describe the security management procedures at level of detail that should allow its secure use. The security management and administration guidance must provide directives for the coherent and effective use of the security characteristics of the product that are declared in the ST, bearing in mind the way in which these characteristics interact. The security management and administration guidance must be well structured, keep internal consistence and must be coherent with other documents provided to the administration personnel.

The **installation guidance** shall describe the required steps for installing and configuring the product securely. This documentation will include enough information to allow performing a secure installation successfully.

If the TOE supports different configurations, the impact of such configurations on the TOE security shall be described. This implies the need for reviewing the documentation regarding each configuration in the TOE scope.

The procedures to guarantee the secure boot and secure operation shall be described. If a security function can be deactivated or modified during the TOE setup, operation or maintenance, this must be described. If the product contains hardware components providing security functionality in the TOE scope, there must be diagnosis functions implemented which can be executed by the administrator, the final user or in an automatic way in order to verify the correct behavior of the product within its operating environment.

Both operation and preparative guidance shall be used and verified by the evaluation laboratory in order to take the TOE into its secure operating state. Only those TOE configurations detailed in these guides will be evaluated and certified, thus the assurance level provided by the certificate is exclusively linked to the evaluated configuration. The unambiguous references of these guides shall be included in the Security Target. The evaluator shall verify that each TOE configuration described in the Security Target can be applied following the security guidance.

3.3 TEST ENVIRONMENT FOR THE TOE OPERATION

The developer or sponsor shall provide the TOE test environment to the evaluation laboratory. The test environment shall be the one required for testing every security function and mechanism defined in the Security Target within the described TOE operative environment.

The laboratory shall only request the authorization to start the evaluation activities only when the TOE test environment has been deployed within its facilities.

3.4 *(MCF)* SOURCE CODE EVALUATION

The developer shall provide the source code or implementation of the TOE if the Source Code Review Module has been chosen as a part of the evaluation. This module enables the TOE evaluation at a deeper level commensurate to a “white box” evaluation regarding those functionalities whose source code or implementation has been provided.

The manufacturer shall detail within the Security Target the security functions or mechanisms which are to be evaluated applying the Source Code Review Module. These functionalities shall be also detailed within the certification report.

The certificates that use this optional module will be identified as LINCE + MCF, in a way that it is possible to identify which parts of its security mechanisms have been evaluated using the Source Code Review Module.

3.5 *(MEC)* CRYPTOGRAPHIC MECHANISMS EVALUATION

The developer shall provide the information regarding the implementation of the cryptographic mechanisms if the Cryptographic Module has been chosen as a part of the evaluation.

The manufacturer shall describe within the Security Target those algorithms to be evaluated through the Cryptographic Evaluation Module. These algorithms shall be also detailed within the certification report.

The information related to the cryptographic modules shall include:

a) The description of the cryptographic functions provided by the product (encryption, signature, key management, etc.).

b) References of the used algorithms to unambiguous and officially recognized standards. It expected that the technical details are easily accessible and without any restriction, alongside with the parameters and procedures for its implementation.

The information related to the key management shall include:

a) Key size.

b) Key distribution mode.

c) Key generation process.

d) Key deletion process.

e) Key storage mechanisms, formats and location.

f) Key transport mechanisms.

The information related to the data processing shall include the description of how data processing is done before and after the cryptographic operation (compression, format, addition of headers, etc.).

When a random number generator (RNG) is used to implement cryptographic functions, RNG type, method and used architecture shall be described including specific rationale proving that the random number generator is considered effective.

Additionally to the specifics of this document, the evaluation laboratory shall have access to the implemented cryptographic mechanisms in order to test the cryptographic functionality.

To fulfil this last requirement, it may be necessary that the developer provides modified versions of the product that may allow direct access to cryptographic functionality through at least an interface which allows the evaluator to verify if the implementation is correct.

The certificates that use this optional module will be identified as LINCE + MEC, in a way that it is possible to identify which cryptographic algorithms have been evaluated regarding their implementation.

4. EVALUATION PROCEDURE

This chapter establishes the evaluation criteria which are intended to verify the effectiveness and the resistance of the security mechanisms of the product.

The methodology is strongly based in the basic levels of the [CC] and [CEM]. Thus, they may be considered as supporting documents to this evaluation methodology for National Essential Security Certification (LINCE).

The stages of the evaluation procedure will be described in the following sections.

4.1 STAGE 1 – SECURITY TARGET ASSESSMENT

Evaluation activities

1.1. The evaluator shall check that the Security Target includes all the elements described in chapter 3.1 and in [CCN-LINCE-003].

1.2. The evaluator shall check that the description of the TOE is not misleading and that it describes at least the minimum security functionality in the TOE scope.

1.3. The evaluator shall check the existence of a correct delimitation of the parts that comprise the TOE and that those parts belonging to the operational environment, as well as an adequate description of how the operational environment supports the TOE’s operation.

1.4. The evaluator shall check that the security functions and mechanisms mitigate or counter the threats described in the Security Target.

1.5. The evaluator shall check that each one of the security functions or mechanisms are fully traced to threats included in the Security Target.

1.6. The evaluator shall check that the assumptions of the operational environment are relevant in regards to the declared threats and the expected TOE use.

1.7. The evaluator shall check that the security functions and mechanisms are described commensurate to the required detail level so that it enables the evaluator to understand how the security functions are implemented by the TOE and its expected behavior.

1.8. In case of declaring the optional modules (MCF) or (MEC), the evaluator shall check that the functionalities that will be verified as part of the evaluation with these optional modules are detailed.

4.2 STAGE 2 – TOE PREPARATION AND CONFIGURATION

Evaluation activities

2.1. The evaluator shall check that, according to the TOE operative and preparative guidance, it is possible to securely install the product using the configuration or configurations referenced in the Security Target.

- In the case of products that may be installed in different versions operating system, the operating system(s) in the testing configuration and its version must be indicated with the maximum possible precision (patch, service pack, etc.).
- If the product requires installation, it will be installed in its typical configuration. Additionally, the manufacturer shall provide the documentation related to the different configuration modes of the product.

2.2. The evaluator shall check that the manufacturer has provided the testing platforms required to carry out the TOE evaluation activities.

2.3. The evaluator shall register the relevant information to successfully install the TOE.

2.4. The evaluator shall register all system's configuration specific data when appropriate.

2.5. The evaluator shall register every non-conformity in regards to the installation and configuration of the TOE or the test environment.

Note: The manufacturer shall assist the evaluator, if necessary, regarding the TOE installation and configuration of the testing environment. According to the evaluation workload and time constraints, the evaluator shall focus their effort in the analysis and testing of the product, therefore, the manufacturer's support is required for this evaluation activity.

4.3 STAGE 3 – CONFORMITY ASSESSMENT – DOCUMENTATION ANALYSIS

Evaluation activities

3.1. The evaluator shall list the analyzed documents.

3.2. The evaluator shall check that the provided information meets the requirements related to content and presentation (section 3), providing a verdict about its completeness and legibility. If there is a big a volume of information to be reviewed, the evaluator may, after notifying the Certification Body, implement a sampling strategy in accordance to the following priorities

a) The Security Target provided by the manufacturer;

b) TOE preparative and operative guidance;

3.3. The evaluator shall register every non-conformity in regards to any deviation of the evaluated documentation.

4.4 STAGE 4 – CONFORMITY ASSESSMENT – FUNCTIONAL TESTS

Evaluation activities

4.1. The evaluator shall check and test the product's security functions and mechanisms to a level of detail that allows checking that the declared security functionality has been correctly implemented in the product.

If the tests are not complete, the evaluator shall provide a rationale regarding the used sampling strategy. For each test, the evaluator shall provide the following information:

a) The tested functionality.

b) The testing environment,

c) The test procedures.

d) The expected and obtained results.

e) Conclusion and verdict of the test.

See section 7.2 of [CCN-LINCE-004] for further information.

4.2. The evaluator shall register every non-conformity in regards to any test performed.

Note: The evaluator may follow the guides provided in [CEM] in the performance of independent tests.

4.5 STAGE 5 – VULNERABILITY ANALYSIS

The evaluator shall attend to the proposed guidelines in [CEM] to execute the vulnerability analysis, whose purpose is to determine the existence and, if possible, the exploitation of TOE defects and weaknesses within the operational environment.

According to the evaluation workload and time constraints in the evaluation methodology, the evaluator may request work sessions with the developer in order to acquire further knowledge of the TOE in the fastest possible way.

Evaluation activities

5.1. The evaluator shall perform a methodic vulnerability analysis by using any means within their technical competence, using at least the following sources of information:

a) The documentation provided by the manufacturer (e.g. Security Target, user guidance, etc.).

b) Any available information regarding the technologies in the TOE scope.

c) Public vulnerability databases for the TOE type.

d) The TOE itself, which is installed in a representative testing platform regarding the TOE operational environment.

5.2. The evaluator shall document the devised vulnerability analysis methodology.

5.3. The evaluator shall document every identified potential vulnerability applicable to the TOE scope.

4.5.1. SECURITY MECHANISMS/FUNCTIONS RESISTANCE ASSESSMENT

For each of the potential vulnerabilities identified by the evaluator, a study of the TOE's resistance to such vulnerability shall be performed, this means considering the available resources for an attacker to succeed in the vulnerability exploitation.

Below guidance on how to perform this study is provided:

The evaluator may require additional information from the manufacturer in order to devise the calculation of attack potential.

Evaluation activities

5.4. The evaluator shall compute the attack potential for every potential vulnerability in accordance to the following punctuation system:

The following tables show the main data that supports the calculation of attack potential. The evaluator may consult [CEM] and/or the Certification Body for additional guidance to compute the attack potential.

Table 1 – Calculation of attack potential

Factor	Range	Value to identify the vulnerability	Value for exploiting a vulnerability
Elapsed time	< 1 hour	0	0
	< 1 day	2	3
	< 1 month	3	5
	> 1 month	5	8
	Not practical	*	*
Attacker expertise	Layman	0	0
	Proficient	2	2
	Expert	5	4
Knowledge of TOE	None	0	0

	Public information	2	2
	Sensitive information	5	4
Window of opportunity **(TOE access)**	< 0.5 hours or unlimited access	0	0
	< 1 day	2	4
	< 1 month	3	6
	> 1 month	4	9
	Not practical	*	*
Equipment to identify/exploit the vulnerability	None	0	0
	Standard	1	2
	Specialized	3	4
	Bespoke	5	6

Note: * indicates a high level of resistance

Table 2 – TOE attack resitance level

Values	Attack potential required to exploit	TOE resistant to attackers with attack potential
0 to 9	No rating	
10 to 17	Low	Basic
18 to 24	Medium	Moderate
>24	High	High

The resistance level shall be computed keeping in mind the addition of the designated values by the laboratory for the stages of identification and exploitation of Table 1. Those vulnerabilities whose attack potential calculations result in a value higher than 24 points are considered residual for LINCE certifications.

4.5.2. SOURCE CODE REVISION (MCF)

The evaluator shall perform a white box evaluation if the Source Code Review Module is included within the LINCE certification scope for the declared security mechanisms. Therefore, the vulnerability analysis evaluation stage will be supported with this evidence.

Evaluation activities

MCF.1. The evaluator shall clearly state those security functions or mechanisms whose source code has been analyzed according to what is declared in the Security Target.

The evaluator may use a sampling strategy as long as this point has been authorized by the Certification Body and code volume requires so. The sampling strategy will be documented in the Evaluation Technical Report (ETR).

MCF.2. The evaluator shall clearly state the techniques used to carry out the source code review.

MCF.3. The evaluator shall document all non-conformities related to any shortcoming found in the code.

4.5.3. CRYPTOGRAPHIC EVALUATION *(MEC)*

The cryptographic evaluation shall be performed if the certificate applicant has included the Cryptographic Module in their request and the cryptographic mechanisms which are to be evaluated by the Cryptographic Evaluation Module are declared within the Security Target.

The evaluator may need the technical assistance of the developer in order to understand the provided information besides having all the possible information about the cryptographic mechanisms implemented in the product.

Evaluation activities

MEC.1. The evaluator shall carry out a documentary analysis about the compliance of the declared cryptographic mechanisms with the CCN ICT security guidance [CCN-STIC-807].

MEC.2. The evaluator shall verify the implementation of the cryptographic mechanisms in the TOE scope by any of the following means:

- Functional tests: By comparing the results of the cryptographic mechanism carried out by the product in relation to a reference implementation. More information in section 4.5.3.1.

  Note: This means that the evaluator must have a reference implementation authorized by the CCN.

- Source code analysis with possible unitary tests in certain functions, for example, to ascertain that an AES function truly implements an AES function.

MEC.3. The evaluator shall describe the adopted approach to guarantee the conformity of the implementation with the declared specifications.

MEC.4. If there is a random number generator is declared within the TOE scope, the evaluator shall verify that it meets the requirements described in the CCN ICT security guidance [CCN-STIC-807]. The evaluator must document any kind of test performed to verify the randomness nature of the used seed.

MEC.5. The evaluator shall document all non-conformities related to any weakness or vulnerability found.

4.5.3.1. CRYPTOGRAPHIC VERIFICATION USING FUNCTIONAL TESTS

In this section, some guidelines are provided to test the cryptographic functions in a LINCE certification. These tests are based on using test vectors which shall evidence the expected functionalities from particular algorithm. The objective of these tests is testing the security mechanisms of the tested algorithm, just as shown in the following proposed example.

In this example, a product using AES algorithm will be used:

a) *"AES-CBC: There are four possible tests which must be passed in order to verify the correct implementation of the algorithm and its mode of operation. Such tests are described next. It should be considered that, in all these tests, the plain text, the encrypted text and initialization vector values are blocks of 128 bits.*

   i. *Test 0 – In order to test that the functionalities of the encryption and decryption processes are inverse of each other, the evaluator will consider a set of ten plain texts of 128 bits randomly chosen. Five of them will be encrypted using five random 128-bit keys and the other five with other five random 256-bit keys. In every case, the initialization vectors will be random. Next, the obtained texts will be decrypted, each of them with its key and matching vector, verifying that the result of the decryption is the initial plain text.*

   ii. *Test 1 – In order to test the functionalities of the encryption process of AES-CBC, the evaluator must consider a set of ten plain texts, randomly chosen and obtain the corresponding encrypted texts. For every encryption process initialization vectors will be 0 (all IV will be set to zeros).*

   On the one hand, five of the random plain texts will be encrypted with a 128-bit key, all of them equal to 0; the remaining five plain texts will be encrypted with a 256-bit key, at 0 too.

In order to test the functionalities of the decryption process, an analogue test must be carried out using the same initialization vectors and the same keys, using in every case the encrypted texts obtained from the ten encryption processes previously mentioned as input.

iii. *Test 2 – In order to test the functionality of the encryption process, ten plain texts will be encrypted using ten keys, randomly generated, half of which will be of 128 bits and the remaining five of 256 bits.*

   Both the initialization vector and the plain text will exclusively contain zeros.

   To test the functionality of the decryption process, tests similar to the previous will be performed, using for this purpose the corresponding encrypted texts.

iv. *Test 3 – In order to test the functionality of the encryption process of the algorithm, two key sets must be created, one with 128-bit keys and the other with 256-bit keys. The keys will be built in the following way: The i-th key of each group must have the i bits to the left (most significant bits) set to 1 and the remaining N-i bits to the right (least significant bits) set to 0, where i goes through the interval [1, N] being N the number of bits in the key.*

   For each key a plain text containing only zeros will be encrypted by using an initialization vector formed by zeros too.

   To test the functionality of the decryption process of the algorithm, the procedure will be similar, using the same keys, the same initialization vectors and the encrypted texts obtained in the previous encryption process.

v. *Test 4 – In order to test the functionality of the encryption process a set of 128-bit plain text must be created in a way that the i-th text is formed by the i bits to left (more significant bits) are set to 1 and the remaining 128-i bits to the right (least significant) are set to 0, where i goes through the interval [1, 128]. Besides. Two keys are considered, a 128-bit and a 256-bit, both set to 0. The initialization vector will consist of zeroes too. This way, every plain text will result in to encrypted texts, one of the corresponding to each of the two keys.*

   To test the functionality of the decryption process of the algorithm, a similar process as the previous will be carried out, using the same keys, the same initialization vectors and as encrypted texts those obtained in the previous encryption processes.

Test results shall be obtained by the evaluator and in some cases it may be needed some assistance from the TOE developer. The evaluator must compare the TOE obtained results with those obtained from a known implementation.

The Certification Body will provide the corresponding guidelines to test each one of the possible algorithms.

4.6 STAGE 6 – TOE PENETRATION TESTING

The goal of this stage is to verify that the TOE and its security mechanisms are effective enough to counter basic and moderate threats, and therefore it is considered that those attacks performed by individuals or organizations with a high attack potential are out of scope of the LINCE certification process.

The evaluator should optimize their evaluation resources and time to assign to these evaluation activities enough time to test the TOE. Therefore, during the evaluation process TOE penetration tests must be performed to:

- Confirm the exploitability of the potential vulnerabilities identified during the vulnerability analysis.
- Perform new tests aiming to detect new or not known/public vulnerabilities in the product.

The penetration tests are considered to be black-box pentesting (unless the Source Code Review Module is included within the certification scope, in which case the functionalities declared within the scope of Source Code Module will be tested considering the information about their implementation).

Evaluation activities

6.1. The evaluator shall provide a list with all the penetration tests performed on the TOE including, at least, the required steps to reproduce each test, the expected result, the actual result and whether the attack is successful or not.

6.2. The evaluator shall document all non-conformities related to any successful attack.

5. EVALUATION VERDICT

The last stage of the evaluation process is the assignment of a final verdict by the evaluation laboratory. The verdict will be one of the following:

a) PASS: The security functionality of the TOE meets with what is established in the Security Target and the TOE is resistant to an attacker with a low or moderate attack potential according to this methodology. In this case, the evaluator will propose to the Certification Body the positive resolution of the certification dossier.

b) FAIL: The TOE security functionality does not meet with what is established in the Security Target and/or the TOE is not resistant to an attacker with a moderate attack potential (see section 4.5.1). This verdict will be assigned too if the sponsor fails to provide the necessary evidence established in this methodology within the maximum evaluation time. In this case, the evaluator will propose the Certification Body the rejection of the certification dossier.

6. TIME RESTRICTIONS AND EVALUATION EFFORT

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

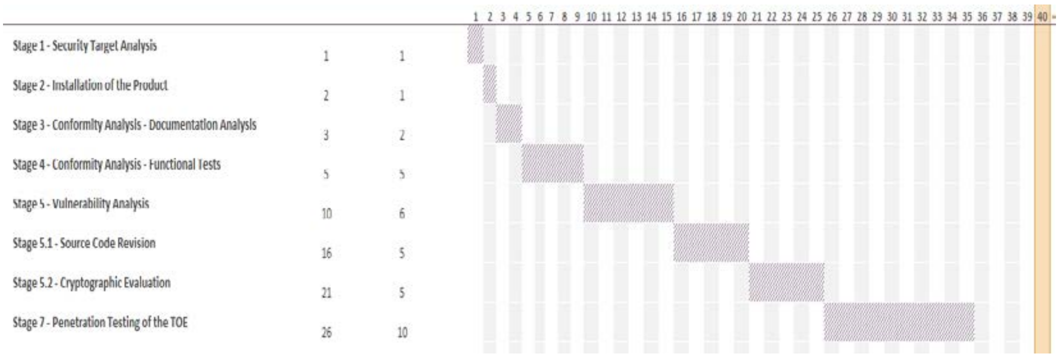
In general terms, a LINCE evaluation must be performed with an estimated work load of **25 man/days** (25 days by one evaluator) within a maximum period of **8 weeks**.

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** 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.

According to this timing, the following image shows an illustrative planning including an estimation of efforts considering each evaluation stage.



Stage 1 - Security Target Analysis	1	1
Stage 2 - Installation of the Product	2	1
Stage 3 - Conformity Analysis - Documentation Analysis	3	2
Stage 4 - Conformity Analysis - Functional Tests	5	5
Stage 5 - Vulnerability Analysis	10	6
Stage 5.1 - Source Code Revision	16	5
Stage 5.2 - Cryptographic Evaluation	21	5
Stage 7 - Penetration Testing of the TOE	26	10

Illustration 1. Example of evaluation planning

7. RESULTS OF THE EVALUATION

The LINCE evaluation of a product in accordance to the criteria highlighted along this methodology must prove that the TOE implements the security mechanisms declared in the Security Target and that the TOE resists attackers with a moderate attack potential considering the evaluation effort in this methodology. This final conclusion should be carefully adopted in the field of IT security, given that it is technically impossible to guarantee that there will be no exploitable vulnerabilities in the TOE.

The result of a LINCE evaluation will be the Evaluation Technical Report (ETR) which shall include at least the following information:

a) A summary of the evaluation activities performed including the evaluation planning and approach, the efforts dedicated to each evaluation activity and the result of the security analysis for each security function declared in the Security Target.

b) A list of the main tools used during the evaluation activities.

c) A list and description of the potential vulnerabilities found during the evaluation process of the product.

d) A list and description of the exploited vulnerabilities in the product.

e) The corrections made to the product in order to mitigate the exploited vulnerabilities, as long as this is possible.

f) TOE test results overview.

g) Verdict and evaluator conclusions.

The issuance of the ETR by evaluation laboratory is mandatory. The Evaluation Technical Report, contains and presents the contents and evaluation results, shall be compliant and include the information required by the template [CCN-LINCE-004]. If the ETR shows that the product does not meet or partially meets its Security Target, it will be considered that the product does not meet its Security Target and thus it will be proposed for a rejection of the certification by the laboratory.

8. GLOSSARY

This section contains the definitions and technical terms used with a specific meaning for this document.

Evaluation activities: Part of the evaluation criteria defined for a stage or a specific evaluation aspect where it is specified what actions shall be executed by the evaluator to verify the information provided by the manufacturer and the complementary tests that shall be carried out during the evaluation.

Administrator: Person in contact with the product and responsible for its maintenance in the operational environment.

Threat: Action or event which may affect the security of the IT product.

Certification: Issuance of a formal declaration in which the results of an evaluation are confirmed and the correct application of the evaluation criteria used.

Confidentiality: Property which guarantees that the information is only accessible to those authorizes to access it.

Configuration: Selection of one of the possible combinations of characteristics/properties of an object to be evaluated.

Security Target: Specification of the security functionality to be evaluated on a specific TOE, the assets it must protect and the security mechanisms implemented by the TOE. Besides, it identifies unambiguously the product to be evaluated and the scope of the evaluation.

Developer: Person or entity who develops, implements or manufactures the object to be evaluated.

Availability: Security characteristic which assures access to resources or information.

Documentation: Written information (or registered somehow) relative to an object of evaluation and required for the evaluation. This information may be contained in an individual document and assigned for that purpose, but it is not mandatory.

Effectiveness: Property of an object which is to be evaluated which represents how it provides security within a real or expected context.

Operational environment: Procedural measures and elements of the environment (e.g. databases, firewalls, etc.) needed for the correct functioning of the TOE.

Evaluation: Valuation of the degree to what a product meets the defined evaluation criteria.

Evaluator: Person or entity which performs the evaluation.

Guarantee: Trust which can be put on the security mechanisms implemented in the product.

Implementation: Stage of the development process in which the specification detailed in a product is transferred to hardware and software. E.g. source code.

Integrity: Property which guarantees that the information is not modified by unauthorized entities.

Security functions or mechanisms: Logic or algorithm which implements, either by hardware or software, a specific security function or which contributes to the security.

Target Of Evaluation (TOE): Product which is subject to a security evaluation.

Operation: Stage of use of a TOE.

Certification Body: National body, independent and impartial which is in charge of the certification process. It is responsible body for the issuance of ICT security certifications. In this case, it refers to the organism created by the RD421/2004 and regulated by PRE/2740/2007.

Sponsor: Person or organism which requests and promotes an evaluation.

IT Product: Software and/or hardware package which implements a given IT functionality.

Requirements of content and presentation: Part of the criteria of the evaluation for a stage or specific aspect of the evaluation which explains what each element of the documentation must contain and how the information it contains must be presented.

Security: Combination of confidentiality, integrity, availability, authentication and non-rejection.

Penetration test: Tests carried out by an evaluator to a TOE in order to confirm whether vulnerabilities are found or not and whether they can be exploited.

Final user: Person or entity which operates the TOE in its operational environment.

Vulnerability: Weakness of any of the security characteristics declared for a TOE in its Security Target (due to, for example, analysis fails, design, manufacturing or operation).

9. REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation. The last approved version must be considered which is published in the website of the Certification Body. (https://oc.ccn.cni.es)

[CCN-LINCE-001] Definition of the CBS – Basic Security Certification

[CCN-LINCE-003] Template for the CBS Declaration of Security.

[CCN-LINCE-004] Template for the CBS Evaluation Technical Report.

[CCN-STIC-807] Use of cryptology within the National Security Scheme (Esquema Nacional de Seguridad).

[CEM] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology.
The last approved version must be considered which is published in the website of the Certification Body. (https://oc.ccn.cni.es)

10. ACRONYMS

AES	Advanced Encryption Standard
LINCE	National Essential Security Certification
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
ENS	Esquema Nacional de Seguridad
ETR	Evaluation Technical Report
ICT	Information and Communication Technology
MCF	Source Code Module
MEC	Cryptographic Evaluation Module
RD	Real Decreto
ST	Security Target
STIC	Information and Communications Technology Security
TIC	Information and Communications Technology
TOE	Target Of Evaluation