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, 5 mai 2015

N° 1818/ANSSI/SDE/PSS/CCN

Référence: ANSSI-CC-CRY-P-01/3.0.EN

PROCEDURE

METHODS FOR CARRYING OUT CRYPTOGRAPHIC ANALYSIS AND RANDOM NUMBER EVALUATIONS

Application : From date of publication.

Circulation : Public.

COURTESY TRANSLATION

SÉCURITÉ CERTIFICATION

Version history

Versions	Dates	Modifications
1.0	15/07/2010	First official edition.
2.0	20/12/2011	Clarification of the work expected to analyse random number generators (chapter 5.2). Integration of instruction CRY/I/01.1 (ref. 423/SGDN/DCSSI/SDR).
3.0	05/05/2015	Clarification of the supplies expected in the evaluation of a product that uses a cryptographic co-processor (appendix A).

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

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

TABLE OF CONTENTS

1. Subject of the procedure

This procedure specifies the methods for carrying out cryptographic analyses in the context of the French evaluation and certification scheme [DECREE].

2. References

[DECREE] Amended decree No. 2002-535 of 18th April 2002 relating to the evaluation and certification of the security provided by information technology products and systems.

[AGR/P/01] Procedure AGR-P-01: Evaluation of ITSEF (www.ssi.gouv.fr).

[SUPPLIES] Supplies needed to analyse cryptographic mechanisms v1.2 available on the ANSSI's institutional website (www.ssi.gouv.fr).

[RGS_B_1] Cryptographic mechanisms: Rules and recommendations concerning the choice and dimensioning of cryptographic mechanisms - Appendix B1 in the general security reference base.

3. Context and definitions

3.1. Justification of the procedure

Cryptographic mechanism resistance evaluation is dealt with specifically in the information technology security evaluations. In the ITSEC criteria, this analysis takes the form of "a declaration of confirmation by the appropriate national body" of the "suitability of the cryptographic mechanisms in terms of the target resistance". The "inherent quality of the cryptographic algorithms" is excluded in the Common Criteria; their processing is left to the discretion of the certification scheme in which the evaluation is carried out. In any case, the cryptographic vulnerability analysis is always required in the context of the evaluations under the French scheme.

In addition, the ANSSI recommends that the cryptographic mechanisms implemented in the evaluated products meet the recommendations in its cryptography reference base (see [RGS_B_1] on www.ssi.gouv.fr). The implementation of these recommendations is compulsory when the products are intended to be "qualified" by the ANSSI. However, a cryptographic mechanism which does not meet these recommendations may still meet the common criteria [CC] recommendations concerning the vulnerability analysis.

Historically, the ANSSI carried out some of the work associated with the cryptographic analysis itself. Given the increase in the number of evaluations processed by the French scheme, the decision was made to entrust this analysis work to the ITSEF. However, in a few specific cases identified in the following paragraph, the ANSSI will also take part in this work.

This note presents the work expected as part of the cryptographic analysis and the random number evaluation, as well as the ITSEF approval process to determine their capacity to carry out this work.

3.2. Content of the cryptographic analysis and the random number analysis

The table below describes the work to be carried out as part of cryptographic analysis and specifies who is in charge of them by default.

Colour code:

🟩 YES by default
🟨 YES subject to exceptions
🟧 NO subject to exceptions
🟥 NO without exception

Type of analysis	ANSSI	ITSEF not approved for cryptography	ITSEF approved for cryptography
A. Theoretical analysis. This analysis is not carried out each time. It is carried out at the request of the person requesting the analysis. It may be imposed by the ANSSI under certain circumstances (products to be used by the government, qualification, etc.). In particular, it is intended to ensure that the cryptographic mechanisms implemented comply with the requirements in the ANSSI reference bases.	🟧 (2)	🟧 (3)	🟩
A1. Cryptographic algorithms and/or procedures and suitability for the objectives sought (confidentiality, integrity, availability, authenticity, performances, etc.)	🟧 (2)	🟧 (3)	🟩
A1bis. Specific case: Intrinsic resistance of the cryptographic algorithms and/or non public procedures used: this case should be rare in the civil field and is not encouraged by the ANSSI. If this case arises, the ANSSI will analyse the proposed mechanism and provide a rating to the ITSEF.	🟩	🟥	🟥
A2. Cryptographic protocols implemented to carry out the target functionality.	🟧 (2)	🟧 (3)	🟩
A3. Random event and key generation characteristics.	🟧 (2)	🟧 (3)	🟩
B. Cryptography implementation conformity analysis (including for the random number generator). The form of this analysis may depend on the evidence elements available.	🟥	🟨 (1)	🟩
C. Cryptography implementation vulnerability analysis (independently of the intrinsic algorithm resistance, does their implementation allow for attacks that may harm the TOE's security objectives?).	🟥	🟨 (1)	🟩

(1) depending on the nature of the evaluation target and/or the evaluation level sought, the ANSSI may impose that these analyses be carried out by an ITSEF approved for cryptography.

(2) depending on the nature of the project, the ANSSI may impose that it carries out these analysis itself. This case is specified at the latest when the certification application file is accepted. The ITSEF decides whether or not to renegotiate their contract with the person requesting the analysis.

On the other hand, the ANSSI continues to be able to carry out these cryptographic analysis in the place of the ITSEF in situations where French ITSEF would be likely to be in competition with foreign ITSEF who do not need to bear the cryptography analysis workload, which is carried out by their national security agency, in order to avoid competition distortion.

(3) The ANSSI may impose that the ITSEF which is not approved for cryptography sub-contracts these tasks to an ITSEF which is approved for cryptography.

4. ITSEF approval in the cryptography field

In accordance with procedure [AGR/P/01], the ITSEF may request an extension of their approval scope to the cryptography field.

4.1. Assessment of ITSEFs competence in the cryptography field

Laboratories' competence to carry out these analyses is assessed by the ANSSI based on:

- Interviews with ITSEF personnel responsible for the cryptographic analysis;
- Examination of any references the ITSEF has in the cryptography field;
- The availability of analysis tools, in particular in the random number generator analysis field;
- Their ability to know and understand the ANSSI's reference bases in this field;
- Other elements that may help the ANSSI to assess the ITSEF competence in this field.

4.2. Provisional approval in the cryptography field

Based on the information collected, the ITSEF may receive a provisional extension to its approval scope, authorising it to propose cryptographic analyses on one or more pilot evaluation projects.

4.3. Approval in the cryptography field

After a first set of results (from one or more evaluations or, where applicable, from expertise work not included in the evaluation) considered significant by the ANSSI is produced, the ITSEF's approval scope is extended to the cryptography field. They are informed by letter or via the approval audit report (see [AGR/P/01]).

4.4. Decision not to grant approval in the cryptography field

If the results of the analysis carried out by the ITSEF are not satisfactory, the ANSSI may announce the withdrawal of the provisional nature of the approval extension. The ITSEF is then obliged to sub-contract any cryptographic analysis it has in progress to another ITSEF which is approved to carry them out.

4.5. Monitoring the approval in the cryptography field

As for its other personnel, the ITSEF must indicate all changes in personnel identified as able to carry out the cryptographic analysis.

4.6. Withdrawal of the approval in the cryptography field

The ANSSI reserves the possibility to announce withdrawal of the extension. In particular, this withdrawal is announced in the following cases:

- Loss of competence in the field;
- Failure to keep up with the state of the art in the field;
- Analysis results considered unsatisfactory.

5. Carrying out the analyses

5.1. Supply delivery

The person who requests the analysis is responsible for providing the ANSSI and the ITSEF with a document relating to the cryptographic aspects of the product being evaluated. This document must describe precisely and fully the algorithms, procedures and cryptographic protocols present in the product being evaluated, as well as the key management architecture used. The [SUPPLIES] document "Supplies needed to analyse cryptographic mechanisms" (available on www.ssi.gouv.fr) specifies the context expected by the ANSSI. To complete their analysis, the ANSSI and the ITSEF may request additional information after the supply is delivered.

5.2. Cryptography analysis

5.2.1. Theoretical cryptography analysis (cryptographic rating)

This analysis is not carried out each time. It is carried out at the request of the person requesting the analysis. It may be imposed by the ANSSI under certain circumstances (products to be used by the government, qualification, etc.).

This analysis relates to the following points:

Cryptographic algorithms and/or procedures and suitability for the objectives sought (confidentiality, integrity, availability, authenticity, performances, etc.)
Cryptographic protocols implemented to carry out the target functionality.

The evaluator's first task is to check that the document which was delivered to carry out the analysis is complete and consistent with the other documents provided to evaluate the product.

The theoretical analysis rests mainly on the document provided. Its objective is to detect any vulnerabilities in the cryptographic mechanisms to achieve the product's security objectives in its operating environment. In the case of cryptographic services, these mechanisms' resistance must be analysed in its usage context. Nevertheless, recommendations may be issued for their use.

An analysis report is produced. It indicates any potential vulnerabilities detected. This report is provided to the certification body for validation and to the owner of the document delivered for the start of the analysis. When the analysis is carried out by the ANSSI, the report is provided to the ITSEF.

5.2.2. Implementation conformity and vulnerability analysis

This analysis relates to the following points:

Cryptography implementation conformity analysis (including for the random number generator). The form of this analysis may depend on the evidence elements available.
Cryptography implementation vulnerability analysis (independently of the intrinsic algorithm resistance, does their implementation allow for attacks that may harm the TOE's security objectives?).

The evaluator takes into account where applicable the results of the previous analysis to verify the conformity of the implementation and to look for any vulnerabilities.

In the normal vulnerability analysis context, the evaluator must determine whether these vulnerabilities can actually be exploited in the product's operating environment.

If recommendations on the use of a cryptographic service were issued during the previous analysis, the evaluator must check that these recommendations are clearly indicated in the product usage and/or administration guides.

All the results of this work are indicated in the usual evaluation reports: vulnerability analysis, usage guidance analysis and evaluation technical report.

5.2.3. Certification

The certification report contains all the useful statements to indicate any analysis limits and any limits on the use of cryptography. It may also mention whether the cryptography is compliant with the ANSSI reference base and the conformity conditions.

5.3. Random number generator evaluation

5.3.1. Random number generation analysis

This analysis is not carried out each time. It is carried out at the request of the person requesting the analysis. It may be imposed by the ANSSI under certain circumstances (products to be used by the government, qualification, etc.).

This analysis relates to the following points:

Random physical source characteristics
Cryptographic reprocessing analysis

The person who requests the analysis must provide a specification of the generator (description of any physical source, reprocessing principle).

The person who requests the analysis must describe the process to be used to evaluate this generator.

The evaluator analyses the specification of generator in order to determine whether it is compliant with the requirements in the reference bases used.

The evaluator carries out the analyses proposed by the reference bases used. The tools to enable the ITSEF to carry out these analysis must be validated by the ANSSI.

The evaluator drafts a report which is sent to the ANSSI and to the owner of the document delivered for the start of the analysis.

5.3.2. Certification

If the analysis is positive, the certification report indicates the results of the random number generator analysis (or indicates that there is no function to generate random numbers used by the product if this is the case). It may also mention whether the random number generator is compliant with the ANSSI reference base and under which conditions.

5.4. Supply of ratings to the ANSSI

The theoretical cryptographic analysis carried out by the ITSEF and the results of the random number generation tests must be provided to the ANSSI early enough before the evaluation is closed and the technical evaluation report is drafted for the ANSSI to have the time to analyse this rating and provide any feedback or recommend additional tests/verifications to the ITSEF.

The ANSSI may decide to take over the rating being evaluated if the ITSEF's work appears to contain any gaps.

APPENDIX A Guide for the use of a cryptographic co-processor

When a product uses, for some or all of the cryptographic processing required to protect a TOE[1] asset or to carry out a TOE security function, a hardware element, if it cannot be included within the evaluation scope or certified at an assurance level enabling a composition, then justification must be provided and the following constraints must be taken into account in addition to the elements present in the body of the document.

A.1 Usage restriction for the use of a cryptographic co-processor which is not controlled in the context of a certification

An uncontrolled cryptographic co-processor must only be used in calculating the primitive symmetrical cryptographic and chopping function and which does not handle any root key or long term operation. This type of co-processor may only be used for non-deterministic calculations such as random generation or IV[2] preparation.

The conformity of the results of co-processor will be checked using a certain number of cryptographic verifications implemented in the product (at least self-test and comparison with a reference software implementation available in the evaluated product). These operations must be carried out on start-up and dynamically (non-inhibiting) every x calls to the co-processor ($1<x<1000$, a random jitter must be introduced).

A.2 Supplies expected

A description of all of the system cryptography on a theoretical level must be provided, along with the source code for the cryptographic functions, including the reference software implementation. A platform to test the co-processor directly on the interfaces must also be provided.

A.3 Specific evaluation tasks

The previous usage restrictions must be checked by the ITSEF. The relevance of the reference software implementation must also be evaluated by the ITSEF.

[1] *Target Of Evaluation*

[2] *Initialization Vector*