

Guía de Seguridad de las TIC CCN-STIC 2100-Anexo C

Random Number Generation Vendor Questionnaire



Noviembre de 2024





Catálogo de Publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2024

Fecha de Edición: noviembre de 2024
NIPO: 083-25-057-3.



CENTRO CRIPTOLOGICO
NACIONAL
cn=CENTRO CRIPTOLOGICO
NACIONAL, 2.5.4.97=VATES-
S2800155J, ou=CENTRO
CRYPTOLOGICO NACIONAL,
o=CENTRO CRIPTOLOGICO
NACIONAL, c=ES
2025.05.27 10:01:24 +02'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

TABLE OF CONTENTS

PRÓLOGO	2
CHANGE CONTROL	¡ERROR! MARCADOR NO DEFINIDO.
1 INTRODUCTION	5
1.1 OBJECTIVE	5
1.2 STRUCTURE OF THE DOCUMENT	5
1.3 VENDOR INSTRUCTIONS	6
2 TRUE RANDOM NUMBER GENERATORS (TRNG)	7
2.1 PTG.2 DESIGN	7
2.1.1 INTRODUCTION	7
2.1.2 NOISE SOURCE, DIGITALIZATION AND STOCHASTIC MODEL	9
2.1.3 POST-PROCESSING MECHANISMS.....	12
2.1.4 ONLINE TEST, TOTAL FAILURE TEST AND START-UP TEST.....	13
2.1.5 AIS-31 REQUIREMENTS	14
2.2 PTG.3 DESIGN	16
2.2.1 INTRODUCTION	16
2.2.2 NOISE SOURCE, DIGITALIZATION AND STOCHASTIC MODEL.....	18
2.2.3 POST-PROCESSING MECHANISMS.....	21
2.2.4 ONLINE TEST, TOTAL FAILURE TEST AND START-UP TEST.....	21
2.2.5 AIS-31 REQUIREMENTS	23
2.3 NTG.1 DESIGN	25
2.3.1 INTRODUCTION	25
2.3.2 NOISE SOURCES AND ENTROPY POOL	27
2.3.3 AIS-31 REQUIREMENTS	29
3 DETERMINISTIC RANDOM NUMBER GENERATORS (DRNG)	30
3.1 DRG.3 DESIGN	30
3.2 DRG.4 DESIGN	32
4 REFERENCES	34
5 ACRONYMS	35

Note:

This document is an official reference document as part of the [CCN-MEMeC] methodology, so the **vendor shall** complete the vendor-specific version of this document.

1 INTRODUCTION

1.1 OBJECTIVE

1. This document is a vendor questionnaire that aims to list and gather the required information related to the RNG design employed by the TOE in the context of the CCN Cryptographic Mechanisms Evaluation Methodology [CCN-MEMeC].
2. As described in the methodology, an approved RNG (Random Number Generator) design entails an agreed TRNG (True Random Number Generator) belonging to an AIS-31 functionality class, seeding an agreed DRNG (Deterministic Random Number Generator) belonging to an AIS-20 functionality class considered as agreed by the [CCN-MEMeC] methodology.
3. This document serves a dual purpose: firstly, it aids vendors in presenting details about the design of the Random Number Generator (RNG) implemented by the Target of Evaluation (TOE), as well as its adherence to AIS-20/31 functionality classes. Secondly, it assists testers by consolidating the necessary information to assess the RNG against the specified requirements of these functionality classes as per “A Proposal for Functionality Classes for Random Number Generators” [FCRNG].
4. Given the inherent challenges associated with evaluating Random Number Generators (RNGs), the **tester may** request additional evidence specific to the RNG's design. In such cases, the **vendor shall** supply these supplementary materials to facilitate a thorough assessment of the design.

1.2 STRUCTURE OF THE DOCUMENT

5. This document contains different sections detailing the required pieces of evidence for the different agreed functionality classes. The first part of the document treats true random number generators (TRNGs), while the second part deals with the requirements of deterministic random number generators (DRNGs).
6. For each functionality class, evidence requirements are organized in different sections.
7. The specific structure is as detailed below:
 - Some evidence requirements are listed in tables. Each table contains one or several questions related to vendor requirements and evaluation tests that will be identified with the same number as the question number indicated under the column name **Q-ID**.
 - On the other hand, most evidence requirements are articulated through paragraphs that either start with or include the directive “**the vendor shall**”.
8. The format of the tables is as detailed below:

Q-ID	Table Name
1	Description of Question 1
	Row for vendor Answer 1
2	Description of Question 2
	Row for vendor Answer 2
...	...
	...
N	Description of Question N
	Row for vendor Answer N

1.3 VENDOR INSTRUCTIONS

9. This section details general instructions that shall be followed by the vendor in order to produce the derivable described in this document.
10. For each TRNG implemented or used by the TOE, the **vendor shall** provide all the evidence required in the appropriate section of this document (e.g., if the TOE implements a PTG.2 TRNG, the vendor shall take into account the PTG.2 section).
11. Likewise, for each DRNG implemented by the TOE, the **vendor shall** provide all the evidence required in the correct section of this document (e.g., if the TOE implements a DRG.3 DRNG, the vendor shall take into account the DRG.3 section).
12. The **vendor shall** omit from their document any sections on functionality classes that are not applicable to their RNG design.
13. The **vendor shall** provide the required evidence within the space (indicated by *[Please, provide the evidence here]*) provided in the document, if feasible. If this is not possible, the **vendor shall** provide references to the specific parts of other documents where the evidence can be found and include those documents as annexes to this document.

For instance, evidence requirements in functionality classes PTG.2 and PTG.3 often reference a stochastic model, the **vendor shall** include it as an annex. For each evidence requirement related to the stochastic model, the **vendor shall** provide a reference to the specific part of the stochastic model where the requirement is met.

2 TRUE RANDOM NUMBER GENERATORS (TRNG)

2.1 PTG.2 DESIGN

2.1.1 INTRODUCTION

14. This section contains an introduction to the TRNG. The **vendor shall** provide, at least, the evidence detailed in the table below.

Q-ID	TRNG Description
1	TRNG Name and Intended Usage The vendor shall provide the name/model of the TRNG under evaluation and its intended usage.
2	TRNG Versioning Information The vendor shall provide the version of the TRNG under evaluation. Note: Indicate (N/A) if hardware, firmware, or software versions do not apply.
	TRNG Version
	Hardware Version
	Firmware Version
	Software Version
3	AIS-31 Functionality Class The vendor shall indicate the claimed functionality class.
	PTG.2
4	Lower Entropy Bound The vendor shall indicate the claimed lower entropy bound per internal random bit. This claim shall be made in terms of Shannon entropy, min-entropy, or both.
5	Internal Random Numbers The vendor shall indicate if the internal random numbers are bits or m-bit vectors.
	Physical Noise Source

Q-ID	TRNG Description
6	The vendor shall describe the physical phenomena exploited for the generation of physical noise in the noise source.

15. The **vendor shall** provide a figure and component description of the TRNG, showing its boundary and its contents (noise source/s, post-processing, and the output interface) as well as the points where the online tests are applied. The description shall also make the distinction between raw and internal random numbers if a post-processing mechanism is employed.

[Please, provide the evidence here]

16. The **vendor shall** provide a table enumerating all the relevant environmental conditions under which the TRNG properly operates, determining min and max ranges.

[Please, provide the evidence here]

17. The **vendor shall** provide the evidence detailed in the table below.

Q-ID	Operational Modes and Interfaces
1	Operational Modes The vendor shall provide a description of all the operational modes.
2	Power Interface The vendor shall provide a description of the power interface.
3	Output Interface The vendor shall provide a description of the output interface.
4	Other Interfaces The vendor shall provide a description of other possible interfaces.

Q-ID	Operational Modes and Interfaces

2.1.2 NOISE SOURCE, DIGITALIZATION AND STOCHASTIC MODEL

18. If the TRNG makes use of more than one noise source, the **vendor shall** provide evidence to assess their independence by means of theoretical arguments based on mathematical considerations and statistical tests.

[Please, provide the evidence here]

19. The **vendor shall** provide a stochastic model for the noise source that begins its description in the physical randomness and that is supported by technical and mathematical arguments based on the design of the physical noise source and findings in the literature. The physical phenomena responsible for the unpredictable nature of the TRNG shall be clearly identified.

[Please, provide the evidence here]

20. The **vendor shall** provide mathematical evidence, within the stochastic model, that the (PTG.2.1) requisite is fulfilled.

[Please, provide the evidence here]

21. The **vendor shall** provide evidence, within the stochastic model, describing how the raw random numbers depend on the environmental conditions and to what extent.

[Please, provide the evidence here]

22. The **vendor shall** provide, within the stochastic model, a mathematical description of the digitalization mechanism.

[Please, provide the evidence here]

23. The **vendor shall** provide evidence for the quantification of the claimed lower entropy bound for the raw random numbers as part of the stochastic model mathematical considerations.

[Please, provide the evidence here]

24. The **vendor shall** provide a report that contains the justification for the fitting of the stochastic model to the noise source. This report shall, at least, include:

- Theoretical considerations from the scientific literature.
- Empirical data gained from the physical entropy source that takes into account measurement errors for the relevant environmental conditions. If the physical noise source is not accessible, empirical data may be substituted by data gathered from a simulation method that shall be described and theoretically justified.
- A description of the measurement techniques employed for data collection: devices, sensibility, number of measurements for each magnitude, and justification for that number, etc.
- Goodness of fit metrics and justification based on them to support the fitness of the stochastic model to the empirical data.

[Please, provide the evidence here]

25. If the raw random numbers are claimed to be *iid* (independent and identically distributed), the **vendor shall** provide evidence comprising:

- A theoretical demonstration for the claim derived from the stochastic model.

[Please, provide the evidence here]

- Statistical testing evidence, following that the raw random numbers pass:
 - The SP800-90B IID test suite described in section 5 of the [SP800-90B] document, or
 - A custom statistical testing suite for which the vendor shall justify theoretically that the selection of tests, parameters, assumptions, and error types are relevant and sufficient to sustain the *iid* claim.

Note: the statistical testing evidence entails a table with the numerical results and a pass or fail claim for each test, a file containing the original dataset of at least 1 000

000 sample values to which the tests have been applied, a description of how the tests have been applied, the software testing environment employed to perform the tests and evidence that the dataset has been drawn from the correct output of the TRNG.

[Please, provide the evidence here]

26. To support the claimed lower entropy bound for raw random numbers, the **vendor shall** provide statistical testing evidence, under all relevant environmental conditions, for the raw random numbers, using, at least, one of the following testing suites:

- If the raw random numbers are successfully proven to be *iid*:
 - The Coron's entropy test (Test T5) as described in section 4.6.1 of the [FCRNG] document, or
 - The min-entropy "*most common value*" estimator as described in section 6.1 of the [SP800-90B] document.
- In any other case (*non-iid*):
 - All the min-entropy estimators described in section 6.2 of the [SP800-90B] document.

Note: the statistical testing evidence entails a table with the numerical results for each test or estimator, a file containing the original dataset of at least 1 000 000 sample values to which the tests have been applied, a description of how the tests have been applied, the software testing environment employed to perform the tests and evidence that the dataset has been drawn from the correct output of the TRNG.

[Please, provide the evidence here]

27. The **vendor shall** provide statistical testing evidence that the raw random numbers pass, at least, the following testing suite under all relevant environmental conditions:

- The raw random numbers testing suite, T_{rrn} , described in section 4.6.2 of the [FCRNG] document.

Note: the statistical testing evidence entails a table with the numerical results for each test or estimator, a file containing the original dataset of at least 1 000 000 sample values to which the tests have been applied, a description of how the tests have been applied, the software testing environment employed to perform the tests and evidence that the dataset has been drawn from the correct output of the TRNG.

[Please, provide the evidence here]

2.1.3 POST-PROCESSING MECHANISMS

28. If the TRNG applies post-processing mechanisms, the **vendor shall** provide its algorithmic description and specify:

- The compression rate, c_{rate} , tailored to a mathematical and theoretical-based description.
- The claimed entropy bound for the internal random numbers. If the post-processing doesn't decrease the entropy claim, it may suffice to provide technical proof.

[Please, provide the evidence here]

29. If the TRNG doesn't apply post-processing mechanisms, the **vendor shall** provide such evidence.

[Please, provide the evidence here]

30. To support the claimed lower entropy bound for internal random numbers, the **vendor shall** provide statistical testing evidence, under all relevant environmental conditions, for the internal random numbers, using one of the following testing suites:

- If the raw random numbers are successfully proven to be *iid*:
 - The Coron's entropy test (Test T5) as described in section 4.6.1 of the [FCRNG] document, or
 - The min-entropy "*most common value*" estimator as described in section 6.1 of the [SP800-90B] document.
- In any other case (*non-iid*):
 - All the min-entropy estimators described in section 6.2 of the [SP800-90B] document.

Note: the statistical testing evidence entail a table with the numerical results for each test or estimator, a file containing the original dataset of at least 1 000 000 sample values to which the tests have been applied, a description of how the tests have been applied, the software testing environment employed to perform the tests and evidence that the dataset has been drawn from the correct output of the TRNG.

[Please, provide the evidence here]

31. The **vendor shall** provide testing evidence that the internal random numbers pass, at least, the following testing suite under all relevant environmental conditions:

- The raw random numbers testing suite, T_{irn} , described in section 4.6.2 of the [FCRNG] document.

Note: the statistical testing evidence entails a table with the numerical results for each test or estimator, a file containing the original dataset of at least 1 000 000 sample values to which the tests have been applied, a description of how the tests have been applied, the software testing environment employed to perform the tests and evidence that the dataset has been drawn from the correct output of the TRNG.

[Please, provide the evidence here]

2.1.4 ONLINE TEST, TOTAL FAILURE TEST AND START-UP TEST

32. The **vendor shall** provide as evidence a description of the online test and justification that it is tailored to the stochastic model. As part of this evidence, the **vendor shall** provide with:

- A full algorithmic description of the online test.
- The source code of the online test.
- The calling scheme of the online test (where it is applied; to all raw/internal random numbers, to the raw/internal random numbers that are used to generate the output data of the current request, to the raw/internal random numbers that precede those raw/internal random numbers that are used to generate the current request...) and a justification for its appropriate selection.
- A theoretical demonstration for the tailoring of the online test to the stochastic model, based on the description of the parameter sets A_{good} and A_{bad} .

[Please, provide the evidence here]

33. The **vendor shall** provide a description of the noise alarm, demonstrating that it is properly triggered when the online test fails.

[Please, provide the evidence here]

34. The **vendor shall** provide a description of the consequences of noise alarms and a justification of the suitability of the specified consequences.

[Please, provide the evidence here]

35. The **vendor shall** provide a description of the total failure test and provide evidence that it is appropriate. As part of this evidence, the **vendor shall** provide:
- A full algorithmic description of the total failure test.
 - The source code of the total failure test.
 - If it is sensor-based or based on statistical tests.
 - The effectiveness of the total failure test in terms of time of detection.
 - A thorough failure analysis of the physical noise source, that shall clarify all the technically plausible failures and their impact on raw random numbers.

[Please, provide the evidence here]

36. The **vendor shall** provide a description of the consequences of a total failure and a justification of the suitability of the specified consequences.

[Please, provide the evidence here]

37. The **vendor shall** provide a description of the start-up test and provide evidence that it is appropriate and tailored to the stochastic model.

[Please, provide the evidence here]

2.1.5 AIS-31 REQUIREMENTS

38. The **vendor shall** provide evidence that the requisite (PTG.2.2) is fulfilled.

[Please, provide the evidence here]

39. The **vendor shall** provide evidence that the requisite (PTG.2.3) is fulfilled.

[Please, provide the evidence here]

40. The **vendor shall** provide evidence that the requisite (PTG.2.4) is fulfilled.

[Please, provide the evidence here]

41. The **vendor shall** provide evidence that the requisite (PTG.2.5) is fulfilled.

[Please, provide the evidence here]

42. The **vendor shall** provide evidence that the requisite (PTG.2.6) is fulfilled.

[Please, provide the evidence here]

2.2 PTG.3 DESIGN

2.2.1 INTRODUCTION

43. This section contains an introduction to the TRNG. The **vendor shall** provide, at least, the evidence detailed in the table below.

Q-ID	TRNG Description	
1	TRNG Name and Intended Usage The vendor shall provide the name/model of the TRNG under evaluation and its intended usage.	
2	TRNG Versioning Information The vendor shall provide the version of the TRNG under evaluation. Note: Indicate (N/A) if hardware, firmware, or software versions do not apply.	
	TRNG Version	
	Hardware Version	
	Firmware Version	
	Software Version	
3	AIS-31 Functionality Class The vendor shall indicate the claimed functionality class.	
	PTG.3	
4	Lower Entropy Bound The vendor shall indicate the claimed lower entropy bound per internal random bit. This claim shall be made in terms of Shannon entropy, min-entropy or both.	
5	Internal Random Numbers The vendor shall indicate if the internal random numbers are bits or m-bit vectors.	
6	Physical Noise Source The vendor shall describe the physical phenomena exploited for the generation of physical noise in the noise source.	

Q-ID	TRNG Description

44. The **vendor shall** provide a figure and component description of the TRNG, showing its boundary and its contents (noise source/s, post-processing, and the output interface) as well as the points where the online tests are applied. The description shall also make the distinction between raw and internal random numbers if a post-processing mechanism is employed.

[Please, provide the evidence here]

45. The **vendor shall** provide a table enumerating all the relevant environmental conditions under which the TRNG properly operates, determining min and max ranges.

[Please, provide the evidence here]

46. The **vendor shall** provide the evidence detailed in the table below.

Q-ID	Operational Modes and Interfaces
1	Operational Modes The vendor shall provide a description of all the operational modes.
2	Power Interface The vendor shall provide a description of the power interface.
3	Output Interface The vendor shall provide a description of the output interface.
4	Other Interfaces The vendor shall provide a description of other possible interfaces.

2.2.2 NOISE SOURCE, DIGITALIZATION AND STOCHASTIC MODEL

47. If the TRNG makes use of more than one noise source, the **vendor shall** provide evidence to assess their independence by means of theoretical arguments based on mathematical considerations and statistical tests.

[Please, provide the evidence here]

48. The **vendor shall** provide a stochastic model for the noise source that begins its description in the physical randomness and that is supported by technical and mathematical arguments based on the design of the physical noise source and findings in the literature. The physical phenomena responsible for the unpredictable nature of the TRNG shall be clearly identified.

[Please, provide the evidence here]

49. The **vendor shall** provide mathematical evidence, within the stochastic model, that the (PTG.3.1) requisite is fulfilled.

[Please, provide the evidence here]

50. The **vendor shall** provide evidence, within the stochastic model, describing how the raw random numbers depend on the environmental conditions and to what extent.

[Please, provide the evidence here]

51. The **vendor shall** provide, within the stochastic model, a mathematical description of the digitalization mechanism.

[Please, provide the evidence here]

52. The **vendor shall** provide evidence for the quantification of the claimed lower entropy bound for the raw random numbers as part of the stochastic model mathematical considerations.

[Please, provide the evidence here]

53. The **vendor shall** provide a report that contains the justification for the fitting of the stochastic model to the noise source. This report shall, at least, include:

- Theoretical considerations from the scientific literature.
- Empirical data gained from the physical entropy source that takes into account measurement errors for the relevant environmental conditions. If the physical noise source is not accessible, empirical data may be substituted by data gathered from a simulation method that shall be described and theoretically justified.
- A description of the measurement techniques employed for data collection: devices, sensibility, number of measurements for each magnitude, and justification for that number, etc.
- Goodness of fit metrics and justification based on them to support the fitness of the stochastic model to the empirical data.

[Please, provide the evidence here]

54. If the raw random numbers are claimed to be *iid* (independent and identically distributed), the **vendor shall** provide evidence comprising:

- A theoretical demonstration for the claim derived from the stochastic model.

[Please, provide the evidence here]

- Statistical testing evidence, following that the raw random numbers pass:
 - The SP800-90B IID test suite described in section 5 of the [SP800-90B] document, or
 - A custom statistical testing suite for which the vendor shall justify theoretically that the selection of tests, parameters, assumptions, and error types are relevant and sufficient to sustain the *iid* claim.

Note: the statistical testing evidence entail a table with the numerical results and a pass or fail claim for each test, a file containing the original dataset of at least 1 000 000 sample values to which the tests have been applied, a description of how the tests have been applied, the software testing environment employed to perform the tests and evidence that the dataset has been drawn from the correct output of the TRNG.

[Please, provide the evidence here]

55. To support the claimed lower entropy bound for raw random numbers, the **vendor shall** provide statistical testing evidence for the raw random numbers, using, at least, one of the following testing suites:

- If the raw random numbers are successfully proven to be *iid*:
 - The Coron's entropy test (Test T5) as described in section 4.6.1 of the [FCRNG] document, or
 - The min-entropy "*most common value*" estimator as described in section 6.1 of the [SP800-90B] document.
- In any other case (*non-iid*):
 - All the min-entropy estimators described in section 6.2 of the [SP800-90B] document.

Note: the statistical testing evidence entail a table with the numerical results for each test or estimator, a file containing the original dataset of at least 1 000 000 sample values to which the tests have been applied, a description of how the tests have been applied, the software testing environment employed to perform the tests and evidence that the dataset has been drawn from the correct output of the TRNG.

[Please, provide the evidence here]

56. The **vendor shall** provide statistical testing evidence that the raw random numbers pass, at least, the following testing suite under all relevant environmental conditions:

- The raw random numbers testing suite, T_{rm} , described in section 4.6.2 of the [FCRNG] document.

Note: the statistical testing evidence entail a table with the numerical results for each test or estimator, a file containing the original dataset of at least 1 000 000 sample values to which the tests have been applied, a description of how the tests have been applied, the software testing environment employed to perform the tests and evidence that the dataset has been drawn from the correct output of the TRNG.

[Please, provide the evidence here]

2.2.3 POST-PROCESSING MECHANISMS

57. For the post-processing mechanisms, the **vendor shall** provide its algorithmic description and specify:

- The compression rate, c_{rate} , tailored to a mathematical and theoretical-based description.
- The claimed entropy bound for the internal random numbers. If the post-processing doesn't decrease the entropy claim, it may suffice to provide technical proof.

[Please, provide the evidence here]

58. To support the claimed lower entropy bound for internal random numbers, the **vendor shall** provide statistical testing evidence, under all relevant environmental conditions, for the internal random numbers, using, at least, one of the following testing suites:

- If the raw random numbers are successfully proven to be *iid*:
 - The Coron's entropy test (Test T5) as described in section 4.6.1 of the [FCRNG] document, or
 - The min-entropy "*most common value*" estimator as described in section 6.1 of the [SP800-90B] document.
- In any other case:
 - All the min-entropy "*most common value*" estimators described in section 6.1 of the [SP800-90B] document.

Note: the statistical testing evidence entail a table with the numerical results for each test or estimator, a file containing the original dataset of at least 1 000 000 sample values to which the tests have been applied, a description of how the tests have been applied, the software testing environment employed to perform the tests and evidence that the dataset has been drawn from the correct output of the TRNG.

[Please, provide the evidence here]

2.2.4 ONLINE TEST, TOTAL FAILURE TEST AND START-UP TEST

59. The **vendor shall** provide as evidence a description of the online test and justification that it is tailored to the stochastic model. As part of this evidence, the **vendor shall** provide with:

- A full algorithmic description of the online test.

- The source code of the online test.
- The calling scheme of the online test (where it is applied; to all raw/internal random numbers, to the raw/internal random numbers that are used to generate the output data of the current request, to the raw/internal random numbers that precede those raw/internal random numbers that are used to generate the current request...) and a justification for its appropriate selection.
- A theoretical demonstration for the tailoring of the online test to the stochastic model, based on the description of the parameter sets A_{good} and A_{bad} .

[Please, provide the evidence here]

60. The **vendor shall** provide a description of the noise alarm, demonstrating that it is properly triggered when the online test fails.

[Please, provide the evidence here]

61. If the TRNG doesn't apply post-processing mechanisms, the **vendor shall** provide such evidence.

[Please, provide the evidence here]

62. The **vendor shall** provide a description of the consequences of noise alarms and a justification of the suitability of the specified consequences.

[Please, provide the evidence here]

63. The **vendor shall** provide a description of the total failure test and provide evidence that it is appropriate. As part of this evidence, the **vendor shall** provide:

- A full algorithmic description of the total failure test.
- The source code of the total failure test.
- If it is sensor-based or based on statistical tests.
- The effectiveness of the total failure test in terms of time of detection.

- A thorough failure analysis of the physical noise source, that shall clarify all the technically plausible failures and their impact on raw random numbers.

[Please, provide the evidence here]

64. The **vendor shall** provide a description of the consequences of a total failure and a justification of the suitability of the specified consequences.

[Please, provide the evidence here]

65. The **vendor shall** provide a description of the start-up test and provide evidence that it is appropriate and tailored to the stochastic model.

[Please, provide the evidence here]

2.2.5 AIS-31 REQUIREMENTS

66. The **vendor shall** provide evidence that the requisite (PTG.3.2) is fulfilled.

[Please, provide the evidence here]

67. The **vendor shall** provide evidence that the requisite (PTG.3.3) is fulfilled.

[Please, provide the evidence here]

68. The **vendor shall** provide evidence that the requisite (PTG.3.4) is fulfilled.

[Please, provide the evidence here]

69. The **vendor shall** provide evidence that the requisite (PTG.3.5) is fulfilled.

[Please, provide the evidence here]

70. The **vendor shall** provide evidence that the requisite (PTG.3.6) is fulfilled.

[Please, provide the evidence here]

71. The **vendor shall** provide evidence that the requisite (PTG.3.7) is fulfilled.

[Please, provide the evidence here]

72. The **vendor shall** provide evidence that the requisite (PTG.3.8) is fulfilled.

[Please, provide the evidence here]

73. The **vendor shall** provide evidence that the requisite (PTG.3.9) is fulfilled.

[Please, provide the evidence here]

2.3 NTG.1 DESIGN

2.3.1 INTRODUCTION

74. This section contains an introduction to the TRNG. The **vendor shall** provide, at least, the evidence detailed in the table below.

Q-ID	TRNG Description	
1	TRNG Name and Intended Usage The vendor shall provide the name/model of the TRNG under evaluation and its intended usage.	
2	TRNG Versioning Information The vendor shall provide the version of the TRNG under evaluation. Note: Indicate (N/A) if hardware, firmware, or software versions do not apply.	
	TRNG Version	
	Hardware Version	
	Firmware Version	
	Software Version	
3	AIS-31 Functionality Class The vendor shall indicate the claimed functionality class.	
	NTG.1	
4	Lower Entropy Bound The vendor shall indicate the claimed lower entropy bound per internal random bit. This claim shall be made in terms of min-entropy.	
5	Internal Random Numbers The vendor shall indicate if the internal random numbers are bits or m-bit vectors.	
6	Source Code The vendor shall provide the source code of the NPTRNG Note: Provide a pointer to the source code of the NPTRNG under evaluation.	

Q-ID	TRNG Description

75. The **vendor shall** provide a figure and component description of the TRNG, showing its boundary and its contents (noise source/s, entropy pool, post-processing, and the output interface) as well as the points where the online tests are applied. The description shall also make the distinction between raw and internal random numbers if a post-processing mechanism is employed.

[Please, provide the evidence here]

76. The **vendor shall** provide a table describing the operational conditions of the NPTRNG, detailing the system on which it runs and for which the evaluation is going to be performed. For each system, all the detailed evidence in this document has to be provided by the vendor.

[Please, provide the evidence here]

77. The **vendor shall** provide the evidence detailed in the table below.

Q-ID	Operational Modes and Interfaces
1	Operational Modes The vendor shall provide a description of all the operational modes.
2	Power Interface The vendor shall provide a description of the power interface.
3	Output Interface The vendor shall provide a description of the output interface.
4	Other Interfaces The vendor shall provide a description of other possible interfaces.

2.3.2 NOISE SOURCES AND ENTROPY POOL

78. If the TRNG makes use of more than one noise source, the **vendor shall** provide evidence to assess their independence by means of theoretical arguments based on mathematical considerations and statistical tests.

[Please, provide the evidence here]

79. The **vendor shall** provide a heuristic/mathematical description of the noise sources. The phenomena responsible for the unpredictable nature of the TRNG shall be clearly identified. The description shall specify the necessary operational requirements for the noise source to function and deliver a conservative lower bound for the expected amount of entropy (e.g., the type of CPU, whether virtualization is allowed, or assumptions regarding the security features that protect against an adversary).

The description shall survey conceivable attack vectors on the noise source (and assess (under realistic assumptions) the ability of an adversary to influence or observe the data and the impact on its entropy).

[Please, provide the evidence here]

80. The **vendor shall** provide evidence that justifies the fitting of the heuristic/mathematical description to the noise sources.

[Please, provide the evidence here]

81. The **vendor shall** provide a description of the entropy pool, the seeding procedure from the noise sources, and a full explanation of its operation.

[Please, provide the evidence here]

82. The **vendor shall** provide a description of the entropy estimator used by the NPTRNG during the operation.

[Please, provide the evidence here]

83. The **vendor shall** specify all possible failure modes for the noise sources and entropy pool. The explanation shall comprise the heuristic analysis of the noise sources and the operational analysis of the entropy pool as a justification for the entropy estimator during operation.

[Please, provide the evidence here]

84. If the raw random numbers are claimed to be *iid* (independent and identically distributed), the **vendor shall** provide evidence comprising:

- A theoretical demonstration for the claim derived from the heuristic/mathematical arguments.

[Please, provide the evidence here]

- Statistical testing evidence, following that the raw random numbers pass:
 - The SP800-90B IID test suite described in section 5 of the [SP800-90B] document, or
 - A custom statistical testing suite for which the vendor shall justify theoretically that the selection of tests, parameters, assumptions, and error types are relevant and sufficient to sustain the *iid* claim.

Note: the statistical testing evidence entail a table with the numerical results and a pass or fail claim for each test, a file containing the original dataset of at least 1 000 000 sample values to which the tests have been applied, a description of how the tests have been applied, the software testing environment employed to perform the tests and evidence that the dataset has been drawn from the correct output of the TRNG.

[Please, provide the evidence here]

85. To support the claimed lower entropy bound for internal random numbers, the **vendor shall** provide statistical testing evidence for the raw random numbers, using, at least, one of the following testing suites:

- If the raw random numbers are successfully proven to be *iid*:
 - The min-entropy “*most common value*” estimator as described in section 6.1 of the [SP800-90B] document.
- In any other case (*non-iid*):

- All the min-entropy estimators described in section 6.2 of the [SP800-90B] document.

Note: the statistical testing evidence entail a table with the numerical results for each estimator, a file containing the original dataset of at least 1 000 000 sample values to which the tests have been applied, a description of how the tests have been applied, the software testing environment employed to perform the tests and evidence that the dataset has been drawn from the correct output of the TRNG.

[Please, provide the evidence here]

2.3.3 AIS-31 REQUIREMENTS

86. The **vendor shall** provide evidence that the requisite (NTG.1.1) is fulfilled.

[Please, provide the evidence here]

87. The **vendor shall** provide evidence that the requisite (NTG.1.2) is fulfilled.

[Please, provide the evidence here]

88. The **vendor shall** provide evidence that the requisite (NTG.1.3) is fulfilled.

[Please, provide the evidence here]

89. The **vendor shall** provide evidence that the requisite (NTG.1.4) is fulfilled.

[Please, provide the evidence here]

90. The **vendor shall** provide evidence that the requisite (NTG.1.5) is fulfilled.

[Please, provide the evidence here]

3 DETERMINISTIC RANDOM NUMBER GENERATORS (DRNG)

3.1 DRG.3 DESIGN

91. The **vendor shall** provide evidence that the requisite (DRG.3.1) is fulfilled.

[Please, provide the evidence here]

92. The **vendor shall** provide evidence that the requisite (DRG.3.2) is fulfilled.

[Please, provide the evidence here]

93. The **vendor shall** provide evidence that the requisite (DRG.3.3) is fulfilled.

[Please, provide the evidence here]

94. The **vendor shall** provide evidence that the requisite (DRG.3.4) is fulfilled.

[Please, provide the evidence here]

95. The **vendor shall** provide evidence that the requisite (DRG.3.5) is fulfilled.

[Please, provide the evidence here]

96. The **vendor shall** provide evidence that the requisite (DRG.3.6) is fulfilled.

[Please, provide the evidence here]

97. The **vendor shall** provide evidence that the requisite (DRG.3.7) is fulfilled.

[Please, provide the evidence here]

98. The **vendor shall** provide evidence that the requisite (DRG.3.8) is fulfilled.

[Please, provide the evidence here]

99. The **vendor shall** provide evidence that the requisite (DRG.3.9) is fulfilled.

[Please, provide the evidence here]

100. The **vendor shall** provide evidence that the requisite (DRG.3.10) is fulfilled.

[Please, provide the evidence here]

3.2 DRG.4 DESIGN

101. The **vendor shall** provide evidence that the requisite (DRG.4.1) is fulfilled.

[Please, provide the evidence here]

102. The **vendor shall** provide evidence that the requisite (DRG.4.2) is fulfilled.

[Please, provide the evidence here]

103. The **vendor shall** provide evidence that the requisite (DRG.4.3) is fulfilled.

[Please, provide the evidence here]

104. The **vendor shall** provide evidence that the requisite (DRG.4.4) is fulfilled.

[Please, provide the evidence here]

105. The **vendor shall** provide evidence that the requisite (DRG.4.5) is fulfilled.

[Please, provide the evidence here]

106. The **vendor shall** provide evidence that the requisite (DRG.4.6) is fulfilled.

[Please, provide the evidence here]

107. The **vendor shall** provide evidence that the requisite (DRG.4.7) is fulfilled.

[Please, provide the evidence here]

108. The **vendor shall** provide evidence that the requisite (DRG.4.8) is fulfilled.

[Please, provide the evidence here]

109. The **vendor shall** provide evidence that the requisite (DRG.4.9) is fulfilled.

[Please, provide the evidence here]

110. The **vendor shall** provide evidence that the requisite (DRG.4.10) is fulfilled.

[Please, provide the evidence here]

111. The **vendor shall** provide evidence that the requisite (DRG.4.11) is fulfilled.

[Please, provide the evidence here]

4 REFERENCES

- | | |
|--------------------|---|
| [CCN-MEMeC] | CCN Cryptographic Mechanisms Evaluation Methodology v1.3.3. November 2024 |
| [FCRNG] | BSI: A Proposal for Functionality Classes for Random Number Generators, 2023 version (v2.36-DRAFT) |
| [SP800-90B] | NIST. Recommendation for the Entropy Sources Used for Random Bit Generation. National Institute of Standard and Technology, Special Publication, SP800-90B, 2018. |

5 ACRONYMS

DRNG	Deterministic Random Number Generator
IID	Independent and Identically Distributed
RNG	Random Number Generator
TOE	Target Of Evaluation
TRNG	True Random Number Generator

