

Guía de Seguridad de las TIC CCN-STIC 2110-Anexo 1

CCN-MEGA Evidence Matrix Document



Noviembre 2025





Catálogo de Publicaciones de la Administración General del Estado
cpage.mpr.gob.es

cpage.mpr.gob.es

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2025
NIPO pendiente de asignación.



CENTRO CRIPTOLOGICO
NACIONAL
cn=CENTRO CRIPTOLOGICO
NACIONAL, 2.5.4.97=VATES-
S2800155J, ou=CENTRO
CRIPTOLOGICO NACIONAL,
o=CENTRO CRIPTOLOGICO
NACIONAL, c=ES
2025.11.21 13:25:23 +01'00'

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

1 INTRODUCTION.....	4
1.1 OBJECTIVE	4
1.2 STRUCTURE OF THE DOCUMENT	4
1.3 VENDOR INSTRUCTIONS	5
2 TOE DEFINITION	7
3 CCN-PTRNG.....	9
3.1 GENERAL DESCRIPTION	9
3.2 PTRNG DESIGN	10
3.3 STOCHASTIC MODEL ANALYSIS	11
3.4 STOCHASTIC MODEL VALIDATION	12
3.5 POST-PROCESSING EVALUATION	13
3.6 HEALTH TESTING REVIEW	14
3.7 BLACK-BOX STATISTICAL TESTING.....	15
4 CCN-HPTRNG	16
4.1 GENERAL DESCRIPTION	16
4.2 HPTRNG DESIGN	17
4.3 ENTROPY SOURCE EVALUATION	17
4.4 POST-PROCESSING EVALUATION	17
5 CCN-NPTRNG	19
5.1 GENERAL DESCRIPTION	19
5.2 DESIGN REVIEW.....	20
5.3 ENTROPY ESTIMATION	20
5.4 HEALTH TESTING REVIEW	21
5.5 BLACK-BOX STATISTICAL TESTING.....	22
6 CCN-DRNG	23
6.1 GENERAL DESCRIPTION	23
6.2 DRNG IMPLEMENTATION.....	24
6.3 ENTROPY ACQUISITION EVALUATION.....	24
6.4 ALGORITHMIC SECURITY PROPERTIES	25
6.4.1 GENERIC DRNGS	25
6.4.2 NIST-APPROVED HASH-BASED DRBGS	28
7 CCN-EDRNG	29
7.1 GENERAL DESCRIPTION	29
7.2 EDRNG IMPLEMENTATION.....	30
7.3 ENTROPY ACQUISITION EVALUATION.....	30
7.4 ALGORITHMIC SECURITY PROPERTIES	31
7.4.1 GENERIC DRNGS	31
7.4.2 NIST-APPROVED HASH-BASED DRBGS	33
8 REFERENCES.....	34
9 ACRONYMS.....	35

1 INTRODUCTION

1.1 OBJECTIVE

1. This document is an evidence traceability matrix that aims to map the requirements defined in the CCN Random Generators Evaluation Methodology [CCN-MEGA] to the corresponding vendor-provided evidence related to the TOE. As described in the methodology, an agreed RNG belongs to a CCN-RNG functionality class considered as agreed by the [CCN-MEGA] methodology.
2. This traceability document serves a dual purpose: firstly, it helps vendors understand the evidentiary expectations associated with each evaluation requirement; secondly, it enables evaluators to efficiently verify coverage, completeness, and consistency of the evidence with respect to the methodology.
3. Each functionality class defined in the [CCN-MEGA] methodology has its own set of required inputs, which are described in the corresponding sections of the methodology. The purpose of this document is to further specify the expected evidence to be provided under each input and to allow the vendor to explicitly indicate where each piece of evidence can be found. This facilitates a structured and traceable evaluation process, ensuring that all methodological requirements are adequately addressed.

1.2 STRUCTURE OF THE DOCUMENT

4. This evidence traceability document is organized into several sections. Section 2 contains general questions related to the TOE definition, while Sections 3 to 7 correspond to the five CCN-RNG functionality classes. The **vendor shall** complete the sections corresponding to the claimed CCN-RNG functionality classes
5. Section 2 “TOE Definition” and subsections labeled “General Description” contain general and specific questions related to the TOE, presented in tables. For each table, these questions are identified by the number indicated under the column name **Q-ID**. 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

6. On the other hand, Sections 3 to 7 follow the structure of the evaluation tests defined in [CCN-MEGA] for each functionality class. For each evaluation test from [CCN-MEGA], there is a corresponding subsection including an evidence traceability table. These traceability tables link each requirement and its corresponding specific notes to the required evidence. The format of the tables is as detailed below:

Note: In [CCN-MEGA], the requirements are denoted as [XRNG.YY], where “XRNG” corresponds to the declared functionality class, and “YY” is a numerical tag.

Requirement	Evidence
[XRNG.YY]	<i>[Please, provide a pointer of the evidence supporting this requirement]</i>
	Note 1[Name of the Note 1]
	<i>[Please, provide a pointer of the evidence supporting this note]</i>
	Note 2 [Name of the Note 2]
	<i>[Please, provide a pointer of the evidence supporting this note]</i>

1.3 VENDOR INSTRUCTIONS

- This section details general instructions that shall be followed by the vendor in order to produce the derivable described in this document.
- The **vendor shall** provide all the required evidence and omit from their document any sections related to functionality classes that are not applicable to their RNG design.

9. In Section 2 “TOE Definition” and subsections labeled “General Description”, the **vendor shall** complete the documentation tables with the required information.
10. In Sections 3 to 7, the **vendor shall** complete the traceability tables by providing a pointer in the corresponding input from the [CCN-MEGA] to the required evidence in the designated space (indicated by '*Please, provide a pointer for the location in **[input]** of the evidence supporting this requirement*'). The pointer shall clearly indicate the location of the evidence that supports the specific requirement within the vendor’s [CCN-MEGA] submitted inputs.

2 TOE DEFINITION

11. This section contains the general information related to the Target of Evaluation (TOE). The **vendor shall** provide the evidence detailed in the table below.

Q-ID	TOE Definition
1	TOE Name The vendor shall provide the name/model of the TOE.
2	Intended Usage The vendor shall provide the TOE intended usage.
3	TOE Versioning Information The vendor shall provide the version of the TOE. Note: Indicate (N/A) if hardware, firmware, or software versions do not apply.
	TOE Version
	Hardware Version
	Firmware Version
	Software Version
4	CCN-RNG Functionality Class The vendor shall indicate the claimed CCN-RNG functionality class of the TOE. Note: the selected RNG functionality classes determine the sections of the present document that the vendor shall complete.
	☐ CCN-PTRNG ☐ CCN-HPTRNG ☐ CCN-NPTRNG ☐ CCN-DRNG ☐ CCN-EDRNG
5	TOE Description The vendor shall provide a general description specifying the RNG capabilities of the TOE. This general description shall include at least the following information:

Q-ID	TOE Definition
	- Description of the TOE, indicating its main components and functionalities. - Descriptive figure of the TOE, indicating the boundary that will be subject to evaluation.
	<i>[TOE Description]</i> <i>[TOE Figure]</i>

3 CCN-PTRNG

12. This section provides the traceability mapping of all evidence required for the evaluation of a Physical True Random Number Generator (PTRNG), in compliance with the CCN-PTRNG functionality class as specified in [CCN-MEGA].
13. The **vendor shall** complete this section if the TOE is claimed to belong to the CCN-PTRNG or the CCN-HPTRNG functionality class.

3.1 GENERAL DESCRIPTION

14. This section contains general properties of the PTRNG required to perform the TOE evaluation. The **vendor shall** provide the evidence detailed in the table below.

Q-ID	PTRNG Description	
1	PTRNG Name The vendor shall provide the name/model of the PTRNG.	
2	PTRNG Versioning Information The vendor shall provide the version of the PTRNG. Note: Indicate (N/A) if hardware, firmware, or software versions do not apply.	
	PTRNG Version	
	Hardware Version	
	Firmware Version	
	Software Version	
3	Operational Environment The vendor shall specify the operational environment in which the PTRNG operates.	
4	Environmental Conditions The vendor shall provide tables specifying the entire admissible range of environmental conditions under which the PTRNG operates as intended and provides the claimed entropy.	
	Post-Processing Component	

Q-ID	PTRNG Description
5	Note: Please, indicate the type of post-processing component employed by the PTRNG.
	☐ Identity mapping (no post-processing component) ☐ Algorithmic post-processing ☐ Cryptographic post-processing
6	MEMeC Evaluation If the PTRNG implements a cryptographic post-processing component, the vendor shall provide evidence that it has been successfully validated in accordance with the [CCN-MEMeC] methodology at levels CL2 or CL3 .
7	Lower Entropy Bound The vendor shall indicate the claimed min-entropy lower bound per internal random bit.

3.2 PTRNG DESIGN

Requirement	Evidence
[PTRNG.01]	<i>[Please, provide a pointer for the location in I_TDS of the evidence supporting this requirement]</i>
	Note 1 [Functional Design Description]
	<i>[Please, provide a pointer for the location in I_TDS of the evidence supporting this requirement]</i>
	Note 2 [Analog Noise Source]
	<i>[Please, provide a pointer for the location in I_TDS of the evidence supporting this requirement]</i>
	Note 3 [Digitizer]
	<i>[Please, provide a pointer for the location in I_TDS of the evidence supporting this requirement]</i>
	Note 4 [Post-Processing Block]
	<i>[Please, provide a pointer for the location in I_TDS of the evidence supporting this requirement]</i>
	Note 5 [Health Tests Block]
	<i>[Please, provide a pointer for the location in I_TDS of the evidence supporting this requirement]</i>
	Note 6 [Interfaces Identification]

Requirement	Evidence
	<i>[Please, provide a pointer for the location in I_TDS of the evidence supporting this requirement]</i>
[PTRNG.02]	<i>[Please, provide a pointer for the location in I_TDS and I_IMP of the evidence supporting this requirement]</i>

3.3 STOCHASTIC MODEL ANALYSIS

Requirement	Evidence
[PTRNG.03]	<i>[Please, provide a pointer for the location in I_SM of the evidence supporting this requirement]</i>
	Note 7 [Physical Phenomenon]
	<i>[Please, provide a pointer for the location in I_SM of the evidence supporting this requirement]</i>
	Note 8 [Deterministic Noise]
	<i>[Please, provide a pointer for the location in I_SM of the evidence supporting this requirement]</i>
	Note 9 [Analog Stochastic Model Definition]
	<i>[Please, provide a pointer for the location in I_SM of the evidence supporting this requirement]</i>
	Note 10 [Assumptions]
[PTRNG.04]	<i>[Please, provide a pointer for the location in I_SM of the evidence supporting this requirement]</i>
	Note 11 [Digitalization Function]
	<i>[Please, provide a pointer for the location in I_SM of the evidence supporting this requirement]</i>
	Note 12 [Digital Stochastic Model Definition] ¡Error! No se encuentra el origen de la referencia.
	<i>[Please, provide a pointer for the location in I_SM of the evidence supporting this requirement]</i>
	Note 13 [Auxiliary Processes]
	<i>[Please, provide a pointer for the location in I_SM of the evidence supporting this requirement]</i>
	Note 14 [Avoiding Post-Processing]
	<i>[Please, provide a pointer for the location in I_SM of the evidence supporting this requirement]</i>
	Note 15 [PTG.2.1]

Requirement	Evidence
	<i>[Please, provide a pointer for the location in I_SM of the evidence supporting this requirement]</i>
[PTRNG.05]	<i>[Please, provide a pointer for the location in I_SM of the evidence supporting this requirement]</i>
	Note 16 [Entropy Bound Formulation]
	<i>[Please, provide a pointer for the location in I_SM of the evidence supporting this requirement]</i>
	Note 17 [Entropy Bound Computation]
	<i>[Please, provide a pointer for the location in I_SM of the evidence supporting this requirement]</i>
[PTRNG.06]	<i>[Please, provide a pointer for the location in I_SM of the evidence supporting this requirement]</i>
	Note 18 [Good Parameters]
	<i>[Please, provide a pointer for the location in I_SM of the evidence supporting this requirement]</i>

3.4 STOCHASTIC MODEL VALIDATION

Requirement	Evidence
[PTRNG.07]	<i>[Please, provide a pointer for the location in I_VAL of the evidence supporting this requirement]</i>
	Note 19 [Validation Conditions]
	<i>[Please, provide a pointer for the location in I_VAL of the evidence supporting this requirement]</i>
	Note 20 [Pre-silicon Design Validation]
	<i>[Please, provide a pointer for the location in I_VAL of the evidence supporting this requirement]</i>
	Note 21 [Analog Model Assumptions]
	<i>[Please, provide a pointer for the location in I_VAL of the evidence supporting this requirement]</i>
	Note 22 [PTG.2.1 Validation]
[PTRNG.08]	<i>[Please, provide a pointer for the location in I_VAL of the evidence supporting this requirement]</i>
	Note 19 [Validation Conditions]
	N/A
	Note 23 [Noise Component Separation]

Requirement	Evidence
	<i>[Please, provide a pointer for the location in I_VAL of the evidence supporting this requirement]</i>
	Note 24 [Estimation Methods]
	<i>[Please, provide a pointer for the location in I_VAL of the evidence supporting this requirement]</i>
	Note 25 [Real Parameters]
[PTRNG.09]	<i>[Please, provide a pointer for the location in I_VAL of the evidence supporting this requirement]</i>
	Note 19 [Validation Conditions]
	N/A
	Note 26 [Prediction Estimate]
	<i>[Please, provide a pointer for the location in I_VAL of the evidence supporting this requirement]</i>

3.5 POST-PROCESSING EVALUATION

Requirement	Evidence
[PTRNG.10]	<i>[Please, provide a pointer for the location in I_IRN of the evidence supporting this requirement]</i>
	Note 27 [PTG.2.2]
	<i>[Please, provide a pointer for the location in I_IRN of the evidence supporting this requirement]</i>
	Note 28 [Post-Processing Types]
	<i>[Please, provide a pointer for the location in I_IRN of the evidence supporting this requirement]</i>
	Note 29 [Algorithmic Post-Processing]
	<i>[Please, provide a pointer for the location in I_IRN of the evidence supporting this requirement]</i>
	Note 30 [Cryptographic Post-Processing]
[PTRNG.11]	<i>[Please, provide a pointer for the location in I_IRN of the evidence supporting this requirement]</i>

3.6 HEALTH TESTING REVIEW

Requirement	Evidence
[PTRNG.12]	<i>[Please, provide a pointer for the location in I_HEALTH of the evidence supporting this requirement]</i>
	Note 31 [Tailored to the Stochastic Model]
	<i>[Please, provide a pointer for the location in I_HEALTH of the evidence supporting this requirement]</i>
	Note 32 [Performance Justification]
	<i>[Please, provide a pointer for the location in I_HEALTH of the evidence supporting this requirement]</i>
	Note 33 [Testing Real Parameters]
	<i>[Please, provide a pointer for the location in I_HEALTH of the evidence supporting this requirement]</i>
	Note 34 [Sufficiently Soon]
[PTRNG.13]	<i>[Please, provide a pointer for the location in I_HEALTH of the evidence supporting this requirement]</i>
	Note 35 [Immediate Detection]
	<i>[Please, provide a pointer for the location in I_HEALTH of the evidence supporting this requirement]</i>
	Note 36 [Failure Modes]
	<i>[Please, provide a pointer for the location in I_HEALTH of the evidence supporting this requirement]</i>
	Note 37 [Implementation]
	<i>[Please, provide a pointer for the location in I_HEALTH of the evidence supporting this requirement]</i>
[PTRNG.14]	<i>[Please, provide a pointer for the location in I_HEALTH of the evidence supporting this requirement]</i>
	Note 38 [Warm-Up]
	<i>[Please, provide a pointer for the location in I_HEALTH of the evidence supporting this requirement]</i>
	Note 39 [Detection Objective]
	<i>[Please, provide a pointer for the location in I_HEALTH of the evidence supporting this requirement]</i>
	Note 40 [Known Answer Test]
	<i>[Please, provide a pointer for the location in I_HEALTH of the evidence supporting this requirement]</i>

Requirement	Evidence
[PTRNG.15]	<i>[Please, provide a pointer for the location in I_HEALTH of the evidence supporting this requirement]</i>
	Note 41 [Health Testing Alarms]
	<i>[Please, provide a pointer for the location in I_HEALTH of the evidence supporting this requirement]</i>

3.7 BLACK-BOX STATISTICAL TESTING

Requirement	Evidence
[PTRNG.16]	<i>[Please, provide a pointer for the location in I_TEST of the evidence supporting this requirement]</i>
	Note 42 [Validation Conditions]
	<i>[Please, provide a pointer for the location in I_TEST of the evidence supporting this requirement]</i>
	Note 43 [AIS-31 Test Suite]
	<i>[Please, provide a pointer for the location in I_TEST of the evidence supporting this requirement]</i>
	Note 44 [Evaluation Rules]
[PTRNG.17]	<i>[Please, provide a pointer for the location in I_TEST of the evidence supporting this requirement]</i>
	Note 42 [Validation Conditions]
	N/A
	Note 45 [Block Assessment]
	<i>[Please, provide a pointer for the location in I_TEST of the evidence supporting this requirement]</i>
	Note 46 [Restart Assessment]
	<i>[Please, provide a pointer for the location in I_TEST of the evidence supporting this requirement]</i>

4 CCN-HPTRNG

15. This section provides the traceability mapping of all evidence required for the evaluation of a Hybrid Physical True Random Number Generator (HPTRNG), in compliance with the CCN-HPTRNG functionality class as specified in [CCN-MEGA].
16. The **vendor shall** complete this section if the TOE is claimed to belong to the CCN-HPTRNG functionality class.

4.1 GENERAL DESCRIPTION

17. This section contains general properties of the HPTRNG required to perform the TOE evaluation. The **vendor shall** provide the evidence detailed in the table below.

Q-ID	HPTRNG Description	
1	HPTRNG Name The vendor shall provide the name/model of the TOE.	
2	HPTRNG Versioning Information The vendor shall provide the version of the HPTRNG. Note: Indicate (N/A) if hardware, firmware, or software versions do not apply.	
	HPTRNG Version	
	Hardware Version	
	Firmware Version	
	Software Version	
3	Operational Environment The vendor shall specify the operational environment in which the HPTRNG operates.	
4	Inner PTRNG The vendor shall indicate the implemented inner PTRNG, which shall be evaluated as CCN-PTRNG-compliant. Note: If the inner PTRNG has previously been successfully evaluated under the [CCN-MEGA] requirements for functionality class CCN-PTRNG, the vendor shall provide the evidence of this successful evaluation.	

Q-ID	HPTRNG Description
5	DRNG Component The vendor shall indicate the implemented DRNG component, which shall be evaluated as CCN-DRNG-compliant.

4.2 HPTRNG DESIGN

Requirement	Evidence
[HPTRNG.01]	<i>[Please, provide a pointer for the location in I_HPTRNG of the evidence supporting this requirement]</i>
	Note 47 [Integration Evidence]
	<i>[Please, provide a pointer for the location in I_HPTRNG to this evidence]</i>

4.3 ENTROPY SOURCE EVALUATION

Requirement	Evidence
[HPTRNG.02]	This requirement implies the use of a CCN-PTRNG compliant inner PTRNG. Thus, the vendor shall provide all the evidence listed in Section 3 “CCN-PTRNG”
	Note 48 [Inner PTRNG Health]
	<i>[Please, provide a pointer for the location in I_HEALTH of the evidence supporting this requirement]</i>

4.4 POST-PROCESSING EVALUATION

Requirement	Evidence
[HPTRNG.03]	This requirement implies the use of a CCN-DRNG compliant DRNG component. Thus, the vendor shall provide all the evidence listed in Section 6 “CCN-DRNG”.
[HPTRNG.04]	This requirement implies the use of a CCN-DRNG compliant DRNG component. Thus, the vendor shall provide all the evidence listed in Section 6 “CCN-DRNG”.
	Note 49 [Compression Rate]
	This requirement implies the use of a CCN-DRNG compliant DRNG component. Thus, the vendor shall provide all the evidence listed in Section 6 “CCN-DRNG”.
	Note 50 [Reseeding Option]

Requirement	Evidence
	This requirement implies the use of a CCN-DRNG compliant DRNG component. Thus, the vendor shall provide all the evidence listed in Section 6 “CCN-DRNG”.
	Note 51 [Entropy Injection Justification]
	N/A

5 CCN-NPTRNG

18. This section provides the traceability mapping of all evidence required for the evaluation of a Non-Physical True Random Number Generator (NPTRNG), in compliance with the CCN-PTRNG functionality class as specified in [CCN-MEGA].
19. The **vendor shall** complete this section if the TOE is claimed to belong to the CCN-NPTRNG functionality class.

5.1 GENERAL DESCRIPTION

20. This section contains some general properties of the NPTRNG required to perform the TOE evaluation. The **vendor shall** provide the evidence detailed in the table below.

Q-ID	NPTRNG Description	
1	NPTRNG Name The vendor shall provide the name/model of the NPTRNG.	
2	NPTRNG Versioning Information The vendor shall provide the version of the NPTRNG. Note: Indicate (N/A) if hardware, firmware, or software versions do not apply.	
	TOE Version	
	Hardware Version	
	Firmware Version	
	Software Version	
3	Operational Environment The vendor shall specify the operational environment on which the NPTRNG operates.	
	<i>[Please, provide the evidence here]</i>	
4	Lower Entropy Bound The vendor shall indicate the claimed min-entropy lower bound per internal random bit.	

5.2 DESIGN REVIEW

Requirement	Evidence
[NPTRNG.01]	<i>[Please, provide pointers for the location in I_TDS_NP and in I_IMP_NP of the evidence supporting this requirement]</i>
	Note 52 [Noise Source Conditions]
	<i>[Please, provide pointers for the location in I_TDS_NP and in I_IMP_NP of the evidence supporting this requirement]</i>
[NPTRNG.02]	<i>[Please, provide pointers for the location in I_TDS_NP and in I_IMP_NP of the evidence supporting this requirement]</i>
	Note 53 [Entropy Counter]
	<i>[Please, provide pointers for the location in I_TDS_NP and in I_IMP_NP of the evidence supporting this requirement]</i>
	Note 54 [Mixing Entropy]
	<i>[Please, provide pointers for the location in I_TDS_NP and in I_IMP_NP of the evidence supporting this requirement]</i>
	Note 55 [NTG.1.4]
[NPTRNG.03]	<i>[Please, provide pointers for the location in I_TDS_NP and in I_IMP_NP of the evidence supporting this requirement]</i>
	This requirement implies the use of a CCN-DRNG compliant DRNG component. Thus, the vendor shall provide all the evidence listed in Section 6 “CCN-DRNG”.
	Note 56 [Fresh Entropy]
	This requirement implies the use of a CCN-DRNG compliant DRNG component. Thus, the vendor shall provide all the evidence listed in Section 6 “CCN-DRNG”.

5.3 ENTROPY ESTIMATION

Requirement	Evidence
[NPTRNG.04]	<i>[Please, provide a pointer for the location in I_ENT of the evidence supporting this requirement]</i>
	Note 57 [Unpredictability Justification]
	<i>[Please, provide a pointer for the location in I_ENT of the evidence supporting this requirement]</i>
	Note 58 [Heuristic Estimate] ¡Error! No se encuentra el origen de la referencia.
	<i>[Please, provide a pointer for the location in I_ENT of the evidence supporting this requirement]</i>
	Note 59 [Rigor Requirement]

Requirement	Evidence
	<i>[Please, provide a pointer for the location in I_ENT of the evidence supporting this requirement]</i>
	<i>[Please, provide a pointer for the location in I_ENT of the evidence supporting this requirement]</i>
[NPTRNG.05]	Note 60 [Entropy Counter]
	<i>[Please, provide a pointer for the location in I_ENT of the evidence supporting this requirement]</i>

5.4 HEALTH TESTING REVIEW

Requirement	Evidence
[NPTRNG.06]	<i>[Please, provide a pointer for the location in I_HEALTH_NP of the evidence supporting this requirement]</i>
	Note 61 [Continuous Tests Specifications]
	<i>[Please, provide a pointer for the location in I_HEALTH_NP of the evidence supporting this requirement]</i>
	Note 62 [Failure Modes]
	<i>[Please, provide a pointer for the location in I_HEALTH_NP of the evidence supporting this requirement]</i>
	Note 63 [Performance Justification – NP]
[NPTRNG.07]	<i>[Please, provide a pointer for the location in I_HEALTH_NP of the evidence supporting this requirement]</i>
	Note 61 [Continuous Tests Specifications]
	<i>[Please, provide a pointer for the location in I_HEALTH_NP of the evidence supporting this requirement]</i>
	Note 62 [Failure Modes]
	<i>[Please, provide a pointer for the location in I_HEALTH_NP of the evidence supporting this requirement]</i>
	Note 63 [Performance Justification – NP]
	<i>[Please, provide a pointer for the location in I_HEALTH_NP of the evidence supporting this requirement]</i>
	Note 64 [Detection Objective]
	<i>[Please, provide a pointer for the location in I_HEALTH_NP of the evidence supporting this requirement]</i>
	Note 65 [Start-Up Specifications]
	<i>[Please, provide a pointer for the location in I_HEALTH_NP of the evidence supporting this requirement]</i>

Requirement	Evidence
[NPTRNG.08]	Note 66 [Known Answer Test]
	<i>[Please, provide a pointer for the location in I_HEALTH_NP of the evidence supporting this requirement]</i>
	<i>[Please, provide a pointer for the location in I_HEALTH_NP of the evidence supporting this requirement]</i>
	Note 67 [Health Testing Alarms]
	<i>[Please, provide a pointer for the location in I_HEALTH_NP of the evidence supporting this requirement]</i>

5.5 BLACK-BOX STATISTICAL TESTING

Requirement	Evidence
[NPTRNG.09]	<i>[Please, provide a pointer for the location in I_TEST_NP of the evidence supporting this requirement]</i>
	Note 68 [Block Assessment]
	<i>[Please, provide a pointer for the location in I_TEST_NP of the evidence supporting this requirement]</i>
	Note 69 [Restart Assessment]
	<i>[Please, provide a pointer for the location in I_TEST_NP of the evidence supporting this requirement]</i>

6 CCN-DRNG

21. This section provides the traceability mapping of all evidence required for the evaluation of a Deterministic Random Number Generator (DRNG), in compliance with the CCN-DRNG functionality class as specified in [CCN-MEGA].
22. The **vendor shall** complete this section if the TOE is claimed to belong to the CCN-DRNG, CCN-HPTRNG or CCN-NPTRNG functionality classes.
23. Many of the evidence required for the evaluation of a DRNG belonging to the CCN-DRNG functionality class do not require the vendor to provide an explicit pointer in the tables of this section, since the inputs **I_VQ_DRNG** and **I_90A** follow a Vendor Questionnaire format that explicitly requests the necessary evidence from the vendor. Nevertheless, this section preserves the same format as in the other classes to facilitate the traceability between evidence and requirements for both the vendor and the tester. For those requirements where no pointer is needed, the format '*The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG (or I_90A)*' has been indicated.

6.1 GENERAL DESCRIPTION

24. This section contains some general properties of the DRNG required to perform the TOE evaluation. The **vendor shall** provide the evidence detailed in the table below.

Q-ID	DRNG Description	
1	DRNG Implementation	
	The vendor shall provide the implementation name of the DRNG.	
2	TOE Versioning Information	
	The vendor shall provide the version of the DRNG.	
	Note: Indicate (N/A) if hardware, firmware, or software versions do not apply.	
	TOE Version	
	Hardware Version	
	Firmware Version	
	Software Version	
3	Cryptographic DRNG Scheme	
	The vendor shall indicate the employed DRNG scheme and its underlying cryptographic mechanisms	

Q-ID	DRNG Description	
	☐ Hash-DRBG	[Cryptographic mechanism(s)]
	☐ HMAC-DRBG	[Cryptographic mechanism(s)]
	☐ CTR-DRBG	[Cryptographic mechanism(s)]
	☐ Other - Please indicate which one and its underlying cryptographic mechanisms.	
4	Cryptographic Evaluation of the DRNG The vendor shall provide evidence that the DRNG implementation has been validated in accordance with the Cryptographic Mechanisms Evaluation Methodology ([CCN-MEMeC]) at evaluation level CL2 or CL3 .	
5	Security Strength The vendor shall indicate the claimed security strength of the DRNG.	

6.2 DRNG IMPLEMENTATION

Requirement	Evidence
[DRNG.01]	The vendor shall provide this evidence that the TOE has been successfully evaluated against the [CCN-MEMeC] methodology in I_VQ (or I_90A).
	Note 70 [Self-Tests]
	The vendor shall provide this evidence that the TOE has been successfully evaluated against the [CCN-MEMeC] methodology in I_VQ (or I_90A).

6.3 ENTROPY ACQUISITION EVALUATION

Requirement	Evidence
[DRNG.02]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG (or I_90A).
[DRNG.03]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG (or I_90A).
	Note 71 [DRG.3.4]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG (or I_90A).
	Note 72 [Seeding Evidence]

Requirement	Evidence
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG (or I_90A).
[DRNG.04]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG (or I_90A).
	Note 71 [DRG.3.4]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG (or I_90A).
	Note 73 [Reseeding Evidence] Error! No se encuentra el origen de la referencia.
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG (or I_90A).

6.4 ALGORITHMIC SECURITY PROPERTIES

25. This section is divided into two subsections.

- Subsection 6.4.1 addresses the traceability mapping between requirements and evidence for “generic” DRNG schemes (those not based on the NIST-approved Hash-based DRBGs).
- Subsection 6.4.2 addresses the traceability mapping between requirements and evidence for DRNGs that follow a NIST-approved Hash-based DRBG scheme (either Hash_DRBG or HMAC_DRBG).

26. The **vendor shall** only consider the appropriate subsection according to the declared scheme in Section 6.1.

6.4.1 GENERIC DRNGS

Requirement	Evidence
[DRNG.06]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 74 [Algorithmic Structure Formal Model]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 75 [Seeding and Reseeding Formal Model]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 76 [Parameters]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 77 [Link to Implementation]

Requirement	Evidence
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
[DRNG.07]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 78 [Request Counter]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 79 [Zeroize Non-Output Bits]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
[DRNG.08]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 80 [Attacker Assumption.1]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
[DRNG.09]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 81 [Algorithmic Properties.1]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 82 [Attacker Assumption.2]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 83 [Security Strength]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
[DRNG.10]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 81 [Algorithmic Properties.1]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 82 [Attacker Assumption.2]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 83 [Security Strength]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
[DRNG.11]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.

Requirement	Evidence
	Note 81 [Algorithmic Properties.1]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG .
	Note 83 [Security Strength]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG .
	Note 84 [Algorithmic Properties.2]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG .
	Note 85 [Attacker Assumption.3]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG .
	Note 86 [One-Way Function]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG .
[DRNG.12]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG and I_IMP_DRNG .
	<i>[Please, provide a pointer for the location in I_IMP_DRNG of the evidence supporting this requirement]</i>
	Note 81 [Algorithmic Properties.1]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG and I_IMP_DRNG .
[DRNG.13]	<i>[Please, provide a pointer for the location in I_IMP_DRNG of the evidence supporting this requirement]</i>
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG and I_IMP_DRNG .
[DRNG.14]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG .
	Note 87 [Justification]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG .
[DRNG.15]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG .

6.4.2 NIST-APPROVED HASH-BASED DRBGs

Requirement	Evidence
[DRNG.05]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
[DRNG.15]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.

7 CCN-EDRNG

27. This section provides the traceability mapping of all evidence required for the evaluation of a Deterministic Random Number Generator (DRNG), in compliance with the CCN-EDRNG functionality class as specified in [CCN-MEGA].
28. The **vendor shall** complete this section if the TOE is claimed to belong to the CCN-EDRNG functionality class.
29. Many of the evidence required for the evaluation of a DRNG belonging to the CCN-EDRNG functionality class do not require the vendor to provide an explicit pointer in the tables of this section, since the inputs **I_VQ_DRNG** and **I_90A** follow a Vendor Questionnaire format that explicitly requests the necessary evidence from the vendor. Nevertheless, this section preserves the same format as in the other classes to facilitate the traceability between evidence and requirements for both the vendor and the tester. For those requirements where no pointer is needed, the format *'The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG (or I_90A)'* has been indicated.

7.1 GENERAL DESCRIPTION

30. This section contains some general properties of the DRNG required to perform the TOE evaluation. The **vendor shall** provide the evidence detailed in the table below.

Q-ID	EDRNG Description	
1	EDRNG Implementation	
	The vendor shall provide the implementation name of the DRNG.	
2	TOE Versioning Information	
	The vendor shall provide the version of the DRNG.	
	Note: Indicate (N/A) if hardware, firmware, or software versions do not apply.	
	TOE Version	
	Hardware Version	
	Firmware Version	
	Software Version	
3	Cryptographic DRNG Scheme	
	The vendor shall indicate the employed DRNG scheme and its underlying cryptographic mechanisms	

Q-ID	EDRNG Description	
	☐ Hash-DRBG	<i>[Cryptographic mechanism(s)]</i>
	☐ HMAC-DRBG	<i>[Cryptographic mechanism(s)]</i>
	☐ CTR-DRBG	<i>[Cryptographic mechanism(s)]</i>
	☐ Other - Please indicate which one and its underlying cryptographic mechanisms.	
4	Cryptographic Evaluation of the DRNG The vendor shall provide evidence that the DRNG implementation has been validated in accordance with the Cryptographic Mechanisms Evaluation Methodology ([CCN-MEMeC]) at evaluation level CL2 or CL3 .	
5	Security Strength The vendor shall indicate the claimed security strength of the DRNG.	

7.2 EDRNG IMPLEMENTATION

Requirement	Evidence
[EDRNG.01]	The vendor shall provide this evidence that the TOE has been successfully evaluated against the [CCN-MEMeC] methodology in I_VQ (or I_90A).
	Note 70 [Self-Tests]
	The vendor shall provide this evidence that the TOE has been successfully evaluated against the [CCN-MEMeC] methodology in I_VQ (or I_90A).

7.3 ENTROPY ACQUISITION EVALUATION

Requirement	Evidence
[EDRNG.02]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG (or I_90A).
[EDRNG.03]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG (or I_90A).
	Note 72 [Seeding Evidence]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG (or I_90A).
[EDRNG.04]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG (or I_90A).

Requirement	Evidence
	Note 73 [Reseeding Evidence]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG (or I_90A).

7.4 ALGORITHMIC SECURITY PROPERTIES

32. This section is divided into two subsections.
- Subsection 6.4.1 addresses the traceability mapping between requirements and evidence for “*generic*” DRNG schemes (those not based on the NIST-approved Hash-based DRBGs).
 - Subsection 6.4.2 addresses the traceability mapping between requirements and evidence for DRNGs that follow a NIST-approved Hash-based DRBG scheme (either Hash_DRBG or HMAC_DRBG).
33. The **vendor shall** only consider the appropriate subsection according to the declared scheme in Section 6.1.

7.4.1 GENERIC DRNGS

Requirement	Evidence
[EDRNG.06]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 74 [Algorithmic Structure Formal Model]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 75 [Seeding and Reseeding Formal Model]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 76 [Parameters]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 77 [Link to Implementation]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
[EDRNG.07]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 78 [Request Counter]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 79 [Zeroize Non-Output Bits]

Requirement	Evidence
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
[EDRNG.08]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 80 [Attacker Assumption.1]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
[EDRNG.09]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 81 [Algorithmic Properties.1]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 82 [Attacker Assumption.2]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 83 [Security Strength]
[EDRNG.10]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 81 [Algorithmic Properties.1]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 82 [Attacker Assumption.2]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 83 [Security Strength]
[EDRNG.11]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 81 [Algorithmic Properties.1]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 83 [Security Strength]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG.
	Note 84 [Algorithmic Properties.2]

Requirement	Evidence
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG .
	Note 85 [Attacker Assumption.3]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG .
	Note 86 [One-Way Function]
[EDRNG.12]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG and I_IMP_DRNG .
	<i>[Please, provide a pointer for the location in I_IMP_DRNG of the evidence supporting this requirement]</i>
	Note 81 [Algorithmic Properties.1]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG and I_IMP_DRNG .
	<i>[Please, provide a pointer for the location in I_IMP_DRNG of the evidence supporting this requirement]</i>
[EDRNG.13]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG and I_IMP_DRNG .
	<i>[Please, provide a pointer for the location in I_IMP_DRNG of the evidence supporting this requirement]</i>
[EDRNG.14]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG .
	Note 87 [Justification]
	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG .
[EDRNG.15]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG .

7.4.2 NIST-APPROVED HASH-BASED DRBGs

Requirement	Evidence
[EDRNG.05]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG .
[EDRNG.15]	The vendor shall provide the evidence supporting this requirement within I_VQ_DRNG .

8 REFERENCES

- | | |
|---------------------|--|
| [CCN-MEGA] | CCN Metodología de Evaluación de Generadores Aleatorios
TBD |
| [CCN-MEMeC] | CCN Cryptographic Mechanisms Evaluation Methodology
v1.3.3. November 2024 |
| [SP 800-90A] | NIST. Recommendation for Random Number Generation
Using Deterministic Random Bit Generators. National
Institute of Standard and Technology, Special Publication,
SP800-90A, 2015. |

9 ACRONYMS

DRBG	Deterministic Random Bit Generator
DRNG	Deterministic Random Number Generator
RNG	Random Number Generator
TOE	Target Of Evaluation

