

MEGA

SP 800-90A Vendor Questionnaire



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
CRYPTOLOGICO NACIONAL,
o=CENTRO CRIPTOLOGICO
NACIONAL, c=ES
2025.11.21 13:31:59 +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 DETERMINISTIC RANDOM NUMBER GENERATORS	6
2.1 DRNG CHARACTERIZATION	6
2.2 ENTROPY ACQUISITION EVALUATION.....	7
2.2.1 ENTROPY SOURCE VERIFICATION.....	7
2.2.2 SEEDING PROCEDURE.....	7
2.2.3 RESEEDING PROCEDURE	8
2.3 NIST-SPECIFIC REQUIREMENTS	9
2.3.1 INSTANTIATION	9
2.3.2 SEEDLIFE	10
2.3.3 INPUT CHECKS	10
2.3.4 ERROR HANDLING	13
3 ENHANCED DETERMINISTIC RANDOM NUMBER GENERATOR	14
3.1 SEEDING AND RESEEDING PROCEDURES	14
3.2 ALGORITHMIC PROPERTIES.....	14
4 REFERENCES.....	15
5 ACRONYMS.....	16

1 INTRODUCTION

1.1 OBJECTIVE

1. This document is a vendor questionnaire that aims to list and gather the required evidence related to the TOE in the context of CCN-DRNG and CCN-EDRNG evaluations according to the CCN Cryptographic Mechanisms Evaluation Methodology [CCN-MEMeC].

1.2 STRUCTURE OF THE DOCUMENT

2. This document contains different sections detailing the required pieces of evidence for the different CCN deterministic random number generators functionality classes; CCN-DRNGs (Section 2) and CCN-EDRNG (Section 3).
3. For each DRNG, evidence requirements are organized in different subsections, following the [CCN-MEGA] structure.
4. The specific structure of this document 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**”.
5. 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

6. This section details general instructions that shall be followed by the vendor in order to produce the derivable described in this document.
7. For the claimed functionality class of the TOE, the **vendor shall** provide all the evidence required in the correct section of this document.
 - In the case of a CCN-DRNG evaluation, the **vendor shall** provide all the evidence required in Section 2.
 - In the case of a CCN-EDRNG evaluation, the **vendor shall** provide all the evidence required in Section 2 and Section 3.
8. 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.
9. In this document, requirements from [SP 800-90A] are referenced using the format [L₁L₂L₃...SX], denotes the top-level section of the document (level 1), and L₂, L₃, etc., represent successive subsection levels. SX refers to the Xth requirement within the deepest section level indicated in the reference.

2 DETERMINISTIC RANDOM NUMBER GENERATORS

10. The **vendor shall** provide the evidence detailed in this section if the TOE is claimed to be compliant with CCN-DRNG functionality class.

2.1 DRNG CHARACTERIZATION

11. 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	
	☐ Hash-DRBG	[Cryptographic mechanism(s)]
	☐ HMAC-DRBG	[Cryptographic mechanism(s)]
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.	

Q-ID	DRNG Description

2.2 ENTROPY ACQUISITION EVALUATION

2.2.1 ENTROPY SOURCE VERIFICATION

12. The **vendor shall** provide evidence that the TOE obtains seed material (for the seeding and the reseeding procedures) from an entropy source belonging to classes CCN-PTRNG, CCN-NPTRNG, CCN-HPTRNG or CCN-EDRNG (evidence that the requirement [DRNG.02] is fulfilled).

[Please, provide the evidence here]

2.2.2 SEEDING PROCEDURE

13. The **vendor shall** provide evidence that the TOE performs its seeding procedure employing seed material generated by a RNG which complies to [DRNG.02] and the resulting effective internal state contains at least 240 bits of min-entropy after seeding (evidence that the requirement [DRNG.03] is fulfilled).

Note: The evidence shall at least contain (Note 72):

- The algorithmic description of the procedure,
- The interfaces (logical or physical) used to receive and inject the seed material into the TOE,
- The operational conditions under which the procedure is triggered (e.g., at startup, on demand), and
- The implemented protections or error-handling mechanisms for invalid or insufficient seed material.
- The impact of the seeding procedure on the entropy of the effective internal state.

[Please, provide the evidence here]

14. If the seed material is generated by a CCN-EDRNG compliant DRNG, the **vendor shall** provide evidence that (evidence that Note 71 is fulfilled):

- The DRNG shall have been provided with enhanced forward secrecy prior to generating the seed material.

[Please, provide the evidence here]

- The seed material shall comprise at least 256 bits.

[Please, provide the evidence here]

- It shall be justified that if the seed material contains at least 250 bits of min-entropy, then the effective internal state resulting from the seeding procedure contains at least 240 bits of min-entropy.

[Please, provide the evidence here]

2.2.3 RESEEDING PROCEDURE

15. The **vendor shall** provide evidence that the TOE performs its reseeding procedure employing seed material generated by a RNG which complies to [DRNG.02] and the resulting effective internal state contains at least 240 bits of min-entropy after reseeding (evidence that the requirement [DRNG.04] is fulfilled).

Note: The evidence shall at least contain (Note 73):

- The algorithmic description of the procedure.
- The interfaces (logical or physical) used to receive and inject the seed material into the TOE.
- The reseeding policy, including the conditions or thresholds that trigger the procedure, and the maximum seedlife permitted.
- The implemented protections or error-handling mechanisms for invalid or insufficient seed material.
- The impact of the reseeding procedure on the entropy of the effective internal state.

[Please, provide the evidence here]

16. If the seed material is generated by a CCN-EDRNG compliant DRNG, the **vendor shall** provide evidence that (evidence that Note 71 is fulfilled, for the reseeding procedure):

- The DRNG shall have been provided with enhanced forward secrecy prior to generating the seed material.

[Please, provide the evidence here]

- The seed material shall comprise at least 256 bits.

[Please, provide the evidence here]

- It shall be justified that if the seed material contains at least 250 bits of min-entropy, then the effective internal state resulting from the seeding procedure contains at least 240 bits of min-entropy.

[Please, provide the evidence here]

2.3 NIST-SPECIFIC REQUIREMENTS

2.3.1 INSTANTIATION

17. The **vendor shall** provide evidence that the seed used to initialize one instantiation of a DRBG is not intentionally used to reseed the same instantiation or used as the seed for another DRBG instantiation [869S1].

[Please, provide the evidence here]

18. The **vendor shall** provide evidence that a DRBG instantiation does not reseed itself [869S2].

[Please, provide the evidence here]

19. The **vendor shall** provide evidence that each DRBG instantiation has its own internal state [83S3] and it is not used as the internal state for a different instantiation [83S4].

[Please, provide the evidence here]

2.3.2 SEEDLIFE

20. The **vendor shall** provide evidence that, when the DRBG's maximum seedlife is reached, the DRBG does not generate outputs until it has been reseeded [868S2].

[Please, provide the evidence here]

21. The **vendor shall** provide evidence that implementations enforce the limits on seedlife specified for the DRBG mechanism used or more stringent limits selected by the implementer [868S1].

[Please, provide the evidence here]

2.3.3 INPUT CHECKS

22. The **vendor shall** provide evidence that the values in Table 2 of [SP800-90A] for each hash function are used for the function envelopes and DRBG algorithm [101S1].

[Please, provide the evidence here]

23. The **vendor shall** provide evidence that the security strength of the hash function to be used meets or exceeds the desired security strength required by the consuming application for DRBG output [1011S2].

[Please, provide the evidence here]

2.3.3.1 ENTROPY INPUT

24. The **vendor shall** provide evidence that the randomness source provides input that supports the security strength requested by the DRBG mechanism [71S2].

[Please, provide the evidence here]

25. The **vendor shall** provide evidence that the entropy input has entropy that is equal or greater than the security strength of the instantiation [863S1].

[Please, provide the evidence here]

26. The **vendor shall** provide evidence that the maximum length for the *entropy_input* is less than or equal to the maximum value specified for the given DRBG mechanism [92S5].

[Please, provide the evidence here]

27. The **vendor shall** provide evidence that, during instantiation, the *entropy_input* is not provided by the consuming application as an input parameter during instantiate request [91S4].

[Please, provide the evidence here]

28. The **vendor shall** provide evidence that, during reseeding, the *entropy_input* is not provided by the consuming application as an input parameter during the reseed request [92S3].

[Please, provide the evidence here]

2.3.3.2 NONCE

29. When required, the **vendor shall** provide evidence that the nonce is either [867S1]:

- A value with at least $(security_strength/2)$ bits of entropy, or
- A value that is expected to repeat no more often than a $(security_strength/2)$ -bit random string would be expected to repeat.

[Please, provide the evidence here]

30. When required, the **vendor shall** provide evidence that each nonce is unique to the cryptographic module in which instantiation is performed [867S2].

[Please, provide the evidence here]

31. The **vendor shall** provide evidence that, during instantiation, the *nonce* is not provided by the consuming application as an input parameter during instantiate request [91S4].

[Please, provide the evidence here]

2.3.3.3 OTHER INPUTS

32. The **vendor shall** provide evidence that the *max_number_of_bits_per_request* is less than or equal to the value provided for the given DRBG mechanism [931S2].

[Please, provide the evidence here]

33. The **vendor shall** provide evidence that, during reseeding, the internal state values are not provided by the consuming application as an input parameter during the reseed request [92S3].

[Please, provide the evidence here]

34. When the DRBG mechanism accepts personalization input, the **vendor shall** provide evidence that the maximum length of the *personalization_string* is less than or equal to the maximum length specified for the given DRBG mechanism [91S3].

[Please, provide the evidence here]

35. When the DRBG mechanism accepts additional input, the **vendor shall** provide evidence that the maximum length for the *additional_input* is less than or equal to the maximum value specified for the given DRBG mechanism [92S2].

[Please, provide the evidence here]

2.3.4 ERROR HANDLING

36. The status is an output to a consuming application after instantiation. The **vendor shall** provide evidence that, if any status other than SUCCESS is returned, either no *state_handle* or an invalid *state_handle* is returned to the consuming application [91S6].

[Please, provide the evidence here]

37. The status is an output to a consuming application after generation. The **vendor shall** provide evidence that, if any status other than SUCCESS is returned, a null string is returned as the output string and must not be used as the pseudorandom output of the DRBG [931S4].

[Please, provide the evidence here]

3 ENHANCED DETERMINISTIC RANDOM NUMBER GENERATOR

38. The **vendor shall** provide the evidence detailed in this section, and in section 2, if the TOE is claimed to be compliant with CCN-EDRNG functionality class.

3.1 SEEDING AND RESEEDING PROCEDURES

39. The **vendor shall** provide evidence that the TOE performs its seeding procedure employing seed material generated by a RNG which complies with [EDRNG.02] and ensures that the resulting effective internal state contains at least 240 bits of min-entropy after seeding.

[Please, provide the evidence here]

40. If the TOE implements a reseeding procedure, the **vendor shall** provide evidence that the TOE performs its seeding procedure employing seed material generated by a RNG which complies with [EDRNG.02] and ensures that the resulting effective internal state contains at least 240 bits of min-entropy after seeding.

[Please, provide the evidence here]

3.2 ALGORITHMIC PROPERTIES

41. The **vendor shall** provide evidence that the TOE provides enhanced forward secrecy.

Note: Enhanced forward secrecy shall be achieved by the reseeding procedure or by high-entropy additional input such as that the effective internal state has a min-entropy of, at least, 240 bits.

[Please, provide the evidence here]

4 REFERENCES

[CCN-MEGA]	CCN Metodología de Evaluación de Generadores Aleatorios v1.0
[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.

5 ACRONYMS

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

