

Guía de Seguridad de las TIC CCN-STIC 2110 - Anexo 2

Deterministic Random Number Generators 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 13:19:36 +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 ALGORITHMIC SECURITY PROPERTIES	9
2.3.1 DRNG FORMAL MODEL	9
2.3.2 REQUEST LENGTH.....	10
2.3.3 EFFECTIVE INTERNAL STATE	10
2.3.4 FORWARD SECRECY.....	11
2.3.5 BACKWARD SECRECY.....	11
2.3.6 ENHANCED BACKWARD SECRECY	12
2.3.7 ADDITIONAL INPUT	12
2.3.8 DRNG FUNCTIONS	12
2.3.9 STATISTICAL INCONSPICUOUSNESS	13
2.3.10 SECURITY STRENGTH	13
3 ENHANCED DETERMINISTIC RANDOM NUMBER GENERATORS	14
3.1 EDRNG CHARACTERIZATION	14
3.2 ENTROPY ACQUISITION EVALUATION.....	15
3.2.1 ENTROPY SOURCE VERIFICATION.....	15
3.2.2 SEEDING PROCEDURE.....	15
3.2.3 RESEEDING PROCEDURE	15
3.3 ALGORITHMIC SECURITY PROPERTIES	16
3.3.1 DRNG FORMAL MODEL	16
3.3.2 REQUEST LENGTH.....	17
3.3.3 EFFECTIVE INTERNAL STATE	17
3.3.4 FORWARD SECRECY.....	18
3.3.5 BACKWARD SECRECY.....	18
3.3.6 ENHANCED BACKWARD SECRECY	19
3.3.7 ADDITIONAL INPUT	19
3.3.8 DRNG FUNCTIONS	19
3.3.9 STATISTICAL INCONSPICUOUSNESS	20
3.3.10 SECURITY STRENGTH	20
4 REFERENCES.....	21
5 ACRONYMS.....	22

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 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.

2 DETERMINISTIC RANDOM NUMBER GENERATORS

9. 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

10. 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
	☐ CTR-DRBG
	☐ 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.

Q-ID	DRNG Description

2.2 ENTROPY ACQUISITION EVALUATION

2.2.1 ENTROPY SOURCE VERIFICATION

11. 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

12. 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 on the effective internal state.

[Please, provide the evidence here]

13. 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

14. 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 on the effective internal state.

[Please, provide the evidence here]

15. 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 ALGORITHMIC SECURITY PROPERTIES

2.3.1 DRNG FORMAL MODEL

16. The **vendor shall** provide a formal model for the DRNG algorithmic structure (evidence that the requirement Note 74 is fulfilled).

[Please, provide the evidence here]

17. The **vendor shall** provide a formal model for the seeding procedure, and (if applicable) a formal model for the reseeding procedure, (evidence that Note 75 is fulfilled).

[Please, provide the evidence here]

18. The **vendor shall** provide evidence that, if public parameters and/or secret parameters affect any of the mappings ϕ, ϕ_{req}, ϕ_0 , then these data items are part of S (evidence that Note 76 is fulfilled).

[Please, provide the evidence here]

19. The **vendor shall** provide evidence that the formal model of the DRNG is aligned with its concrete implementation. A mapping shall be provided between the elements of the different tuples in the model and the corresponding functions, algorithms, processes and variables in the actual implementation (evidence that Note 77 is fulfilled).

[Please, provide the evidence here]

2.3.2 REQUEST LENGTH

20. The **vendor shall** provide evidence that the TOE accepts requests that comprise a maximum length of 2^{19} bits (evidence that the requirement [DRNG.07] is fulfilled).

[Please, provide the evidence here]

21. The **vendor shall** provide evidence that the TOE implements a counter for the number of internal random numbers necessary per request (evidence that Note 78 is fulfilled).

[Please, provide the evidence here]

22. The **vendor shall** provide evidence that the TOE securely destroys and does not store any internal random number not included in the responses to the requests (evidence that Note 79 is fulfilled).

[Please, provide the evidence here]

2.3.3 EFFECTIVE INTERNAL STATE

23. The **vendor shall** provide evidence, derived from the DRNG formal models, that the TOE has an effective internal state that comprises at least 246 bits (evidence that the requirement [DRNG.08] is fulfilled).

Note: The effective internal state and its size shall be determined under the assumption that the attacker knows a large number of internal random numbers. For the reseeding procedure, the least favorable scenario shall be assumed where an attacker knows the previous internal state (see Note 80).

[Please, provide the evidence here]

2.3.4 FORWARD SECURITY

24. The **vendor shall** provide evidence, derived from the DRNG formal models, that the TOE provides forward secrecy on the granularity level of internal random numbers (evidence that the requirement [DRNG.09] is fulfilled).

Note₁: This requirement shall be guaranteed by the algorithmic properties of the DRNG, i.e., by the interaction of the state transition function and the output function (see Note 81).

Note₂: When providing the forward secrecy property, it shall be assumed that an attacker knows a sequence of internal random numbers generated within one or several requests. The sequence needs not start nor terminate a request (see Note 82).

Note₃: For k-bit output strings the security strength (of cryptographic mechanisms) shall not be significantly lower than 240 bits. (see Note 83).

[Please, provide the evidence here]

2.3.5 BACKWARD SECURITY

25. The **vendor shall** provide evidence, derived from the DRNG formal models, that the TOE provides backward secrecy on the granularity level of internal random numbers (evidence that the requirement [DRNG.10] is fulfilled).

Note₁: This requirement shall be guaranteed by the algorithmic properties of the DRNG, i.e., by the interaction of the state transition function and the output function (see Note 81).

Note₂: When providing the backward secrecy property, it shall be assumed that an attacker knows a sequence of internal random numbers generated within one or several requests. The sequence needs not start nor terminate a request (see Note 82).

Note₃: For k-bit output strings the security strength (of cryptographic mechanisms) shall not be significantly lower than 240 bits. (see Note 83).

[Please, provide the evidence here]

2.3.6 ENHANCED BACKWARD SECRECY

26. The **vendor shall** provide evidence, derived from the DRNG formal models, that the TOE provides enhanced backward secrecy on the granularity level of internal random numbers (evidence that the requirement [DRNG.11] is fulfilled).

Note₁: For k-bit output strings the security strength (of cryptographic mechanisms) shall not be significantly lower than 240 bits. (see Note 83).

Note₂: Enhanced backward secrecy is an algorithmic property. This requirement shall be guaranteed by the algorithmic properties of the DRNG. It shall not be compensated for or supported by technical security measures that (are claimed to) prevent the internal state from being compromised or modified (Note 84).

Note₃: To provide this evidence, the vendor must assume that the attacker knows the current internal state of the DRNG (after the request is performed) and (if relevant) the last additional input (Note 85).

Note₄: A one-way state transition function is required (see Note 86).

[Please, provide the evidence here]

2.3.7 ADDITIONAL INPUT

27. If additional input is permitted, the **vendor shall** provide evidence that the TOE accepts additional input that does not weaken the strength of the DRNG even if an attacker is able to control the additional input (evidence that the requirement [DRNG.12] is fulfilled).

Note: This requirement shall be guaranteed by the algorithmic properties of the DRNG, i.e., by the interaction of the state transition function and the output function (see Note 81).

[Please, provide the evidence here]

2.3.8 DRNG FUNCTIONS

28. The **vendor shall** provide evidence, derived from the DRNG formal models, that the TOE is defined by a cryptographic and one-way transition function, ϕ , and a cryptographic output function, ψ (evidence that the requirement [DRNG.13] is fulfilled).

[Please, provide the evidence here]

2.3.9 STATISTICAL INCONSPICUOUSNESS

29. The **vendor shall** provide evidence that the TOE outputs internal random numbers that have statistical inconspicuousness (evidence that the requirement [DRNG.14] is fulfilled).

Note: This justification shall be based on theoretical considerations supported by statistical tests, with justification of the choice.

[Please, provide the evidence here]

2.3.10 SECURITY STRENGTH

30. The **vendor shall** provide evidence that the TOE achieves the declared security strength, supported by justification based on its algorithmic security properties (evidence that the requirement [DRNG.15] is fulfilled).

[Please, provide the evidence here]

3 ENHANCED DETERMINISTIC RANDOM NUMBER GENERATORS

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

3.1 EDRNG CHARACTERIZATION

32. 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 EDRNG. 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
	☐ CTR-DRBG
	☐ Other - Please indicate which one and its underlying cryptographic mechanisms.
4	Cryptographic Evaluation of the EDRNG 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 EDRNG.

Q-ID	EDRNG Description

3.2 ENTROPY ACQUISITION EVALUATION

3.2.1 ENTROPY SOURCE VERIFICATION

33. 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 or CCN-HPTRNG (evidence that the requirement [EDRNG.02] is fulfilled).

[Please, provide the evidence here]

3.2.2 SEEDING PROCEDURE

34. 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 [EDRNG.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]

3.2.3 RESEEDING PROCEDURE

35. The **vendor shall** provide evidence that the TOE performs its reseeding procedure employing seed material generated by a RNG which complies to [EDRNG.02] and the resulting effective internal state contains at least 240 bits of

min-entropy after reseeding (evidence that the requirement [EDRNG.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]

3.3 ALGORITHMIC SECURITY PROPERTIES

3.3.1 DRNG FORMAL MODEL

36. The **vendor shall** provide a formal model for the DRNG algorithmic structure (evidence that the requirement Note 74 is fulfilled).

[Please, provide the evidence here]

37. The **vendor shall** provide a formal model for the seeding procedure, and (if applicable) a formal model for the reseeding procedure, (evidence that Note 75 is fulfilled).

[Please, provide the evidence here]

38. The **vendor shall** provide evidence that, if public parameters and/or secret parameters affect any of the mappings ϕ, ϕ_{req}, ϕ_0 , then these data items are part of S (evidence that Note 76 is fulfilled).

[Please, provide the evidence here]

39. The **vendor shall** provide evidence that the formal model of the DRNG is aligned with its concrete implementation. A mapping shall be provided between the elements of the different tuples in the model and the corresponding functions, algorithms, processes and variables in the actual implementation (evidence that Note 77 is fulfilled).

[Please, provide the evidence here]

3.3.2 REQUEST LENGTH

40. The **vendor shall** provide evidence that the TOE accepts requests that comprise a maximum length of 2^{19} bits (evidence that the requirement [EDRNG.07] is fulfilled).

[Please, provide the evidence here]

41. The **vendor shall** provide evidence that the TOE implements a counter for the number of internal random numbers necessary per request (evidence that Note 78 is fulfilled).

[Please, provide the evidence here]

42. The **vendor shall** provide evidence that the TOE securely destroys and does not store any internal random number not included in the responses to the requests (evidence that Note 79 is fulfilled).

[Please, provide the evidence here]

3.3.3 EFFECTIVE INTERNAL STATE

43. The **vendor shall** provide evidence, derived from the DRNG formal models, that the TOE has an effective internal state that comprises at least 246 bits (evidence that the requirement [EDRNG.08] is fulfilled).

Note: The effective internal state and its size shall be determined under the assumption that the attacker knows a large number of internal random numbers. For the reseeding procedure, the least favorable scenario shall be assumed where an attacker knows the previous internal state (see Note 80).

[Please, provide the evidence here]

3.3.4 FORWARD SECURITY

44. The **vendor shall** provide evidence, derived from the DRNG formal models, that the TOE provides forward secrecy on the granularity level of internal random numbers (evidence that the requirement [EDRNG.09] is fulfilled).

Note₁: This requirement shall be guaranteed by the algorithmic properties of the DRNG, i.e., by the interaction of the state transition function and the output function (see Note 81).

Note₂: When providing the forward secrecy property, it shall be assumed that an attacker knows a sequence of internal random numbers generated within one or several requests. The sequence needs not start nor terminate a request (see Note 82).

Note₃: For k-bit output strings the security strength (of cryptographic mechanisms) shall not be significantly lower than 240 bits. (see Note 83).

[Please, provide the evidence here]

3.3.5 BACKWARD SECURITY

45. The **vendor shall** provide evidence, derived from the DRNG formal models, that the TOE provides backward secrecy on the granularity level of internal random numbers (evidence that the requirement [EDRNG.10] is fulfilled).

Note₁: This requirement shall be guaranteed by the algorithmic properties of the DRNG, i.e., by the interaction of the state transition function and the output function (see Note 81).

Note₂: When providing the backward secrecy property, it shall be assumed that an attacker knows a sequence of internal random numbers generated within one or several requests. The sequence needs not start nor terminate a request (see Note 82).

Note₃: For k-bit output strings the security strength (of cryptographic mechanisms) shall not be significantly lower than 240 bits. (see Note 83).

[Please, provide the evidence here]

3.3.6 ENHANCED BACKWARD SECRECY

46. The **vendor shall** provide evidence, derived from the DRNG formal models, that the TOE provides enhanced backward secrecy on the granularity level of internal random numbers (evidence that the requirement [EDRNG.11] is fulfilled).

Note₁: For k-bit output strings the security strength (of cryptographic mechanisms) shall not be significantly lower than 240 bits. (see Note 83).

Note₂: Enhanced backward secrecy is an algorithmic property. This requirement shall be guaranteed by the algorithmic properties of the DRNG. It shall not be compensated for or supported by technical security measures that (are claimed to) prevent the internal state from being compromised or modified (Note 84).

Note₃: To provide this evidence, the vendor must assume that the attacker knows the current internal state of the DRNG (after the request is performed) and (if relevant) the last additional input (Note 85).

Note₄: A one-way state transition function is required (see Note 86).

[Please, provide the evidence here]

3.3.7 ADDITIONAL INPUT

47. If additional input is permitted, the **vendor shall** provide evidence that the TOE accepts additional input that does not weaken the strength of the DRNG even if an attacker is able to control the additional input (evidence that the requirement [DRNG.12] is fulfilled).

Note: This requirement shall be guaranteed by the algorithmic properties of the DRNG, i.e., by the interaction of the state transition function and the output function (see Note 81).

[Please, provide the evidence here]

3.3.8 DRNG FUNCTIONS

48. The **vendor shall** provide evidence, derived from the DRNG formal models, that the TOE is defined by a cryptographic and one-way transition function, ϕ , and a cryptographic output function, ψ (evidence that the requirement [DRNG.13] is fulfilled).

[Please, provide the evidence here]

3.3.9 STATISTICAL INCONSPICUOUSNESS

49. The **vendor shall** provide evidence that the TOE outputs internal random numbers that have statistical inconspicuousness (evidence that the requirement [DRNG.14] is fulfilled).

Note: This justification shall be based on theoretical considerations supported by statistical tests, with justification of the choice.

[Please, provide the evidence here]

3.3.10 SECURITY STRENGTH

50. The **vendor shall** provide evidence that the TOE achieves the declared security strength, supported by justification based on its algorithmic security properties (evidence that the requirement [DRNG.15] is fulfilled).

[Please, provide the evidence here]

4 REFERENCES

[CCN-MEGA]	CCN Metodología de Evaluación de Generadores Aleatorios TBD
[CCN-MEMeC]	CCN Cryptographic Mechanisms Evaluation Methodology v1.3.3. November 2024

5 ACRONYMS

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

