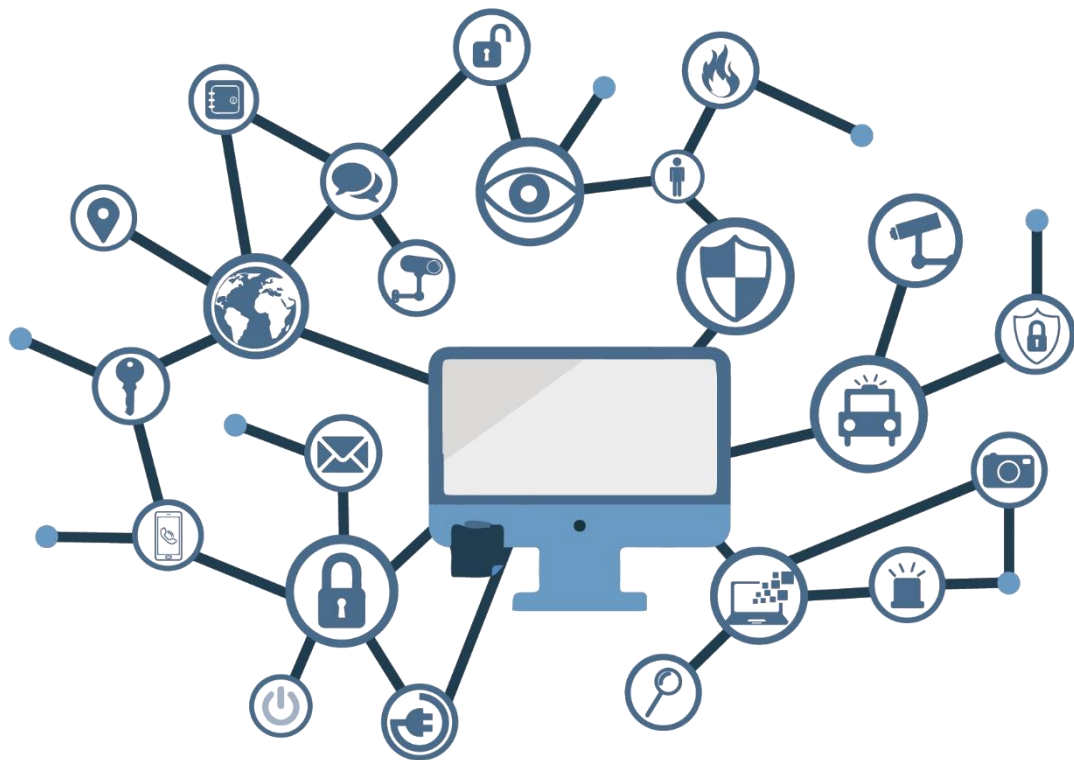


Differential Analysis Report (IAD) Template



October 2026

Published by:



Centro Criptológico Nacional, 2026



CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-
S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.10.08 13:02:22
+02'00'

Publication date: October 2026

LIMITATION OF LIABILITY

This document is provided in accordance with the terms set out herein, expressly disclaiming any implied warranty that may be related to it. Under no circumstances may the Centro Criptológico Nacional be held liable for any direct, indirect, incidental or extraordinary damage arising from the use of the information and software referred to herein, even when advised of such a possibility.

LEGAL NOTICE

Without the written authorisation of the Centro Criptológico Nacional, and subject to the penalties established by law, the partial or total reproduction of this document by any means or process, including reprography and computer processing, and the distribution of copies thereof by means of public rental or lending, are strictly prohibited.

VERSION CONTROL

Version	Comment	Date
1.0	Initial version	10/2026

CONTENTS

1 INTRODUCTION.....	6
1.1 PURPOSE OF THE DOCUMENT	6
1.2 TYPE OF EXTENSION	6
1.3 SCOPE OF THE ANALYSIS	7
1.4 TERMS USED.....	7
1.5 APPLICANT AND PRODUCT INFORMATION	7
2 CHARACTERISATION OF THE ORIGINAL CERTIFICATION.....	9
2.1 REQUESTED SCOPE VERSUS ORIGINAL SCOPE.....	9
2.2 RELEVANT ASSIGNMENTS AND SELECTIONS	9
2.3 PREVIOUS EXTENSIONS.....	10
3 ANALYSIS CRITERIA	11
4 IDENTIFICATION OF DIFFERENCES.....	12
4.1 FEATURE MATRIX	12
4.2 HOMOGENEOUS TECHNOLOGY GROUPINGS	13
4.3 LIST OF CHANGES BETWEEN VERSIONS.....	14
4.4 SUMMARY OF DIFFERENCES	14
5 AFFECTED REQUIREMENTS AND SCOPE PENDING VERIFICATION	16
5.1 LIST OF AFFECTED REQUIREMENTS	16
5.2 EXAMPLES	16
5.3 SCOPE MATRIX	18
6 CRYPTOGRAPHIC CONFORMITY.....	19
7 INSTALLATION AND OPERATION GUIDES.....	20
7.1 MANUFACTURER'S GUIDES.....	20
7.2 CCN-STIC GUIDE IN THE 1000 SERIES.....	20
8 CONCLUSIONS.....	21
8.1 CONCLUSION OF THE ANALYSIS.....	21
8.2 DELIVERABLES	21
9 APPLICANT'S OBSERVATIONS	22
10 RESPONSIBLE STATEMENT.....	23
10.1 DOCUMENTATION PROVIDED AS EVIDENCE	23
11 REFERENCES.....	25

INSTRUCTIONS FOR COMPLETION AND SUBMISSION

This template constitutes Annex B of CCN-STIC-106. The document resulting from its completion is the product's Differential Analysis Report (IAD) and, once electronically signed by the applicant's technical manager, it is regarded as a responsible statement.

The IAD is submitted together with the application for inclusion or extension (FOR-CPSTIC-02), accompanied by the evidence listed in the responsible statement.

Content instructions

Text in grey italics consists of completion instructions and must be deleted from the final document. Text in black forms part of the report and of the responsible statement signed by the applicant.

All sections are mandatory. Where a section is not applicable, the heading shall be retained and its non-applicability shall be expressly stated.

Any statement regarding the absence of impact must be technically justified and referenced to the evidence supporting it.

Evidence shall be provided together with the responsible statement or, where it is public, shall be identified by indicating the address at which it can be accessed.

No credentials, keys, customer data or commercial content shall be included.

Checks before submission

- a) *All text in grey italics, including the examples, has been deleted.*
- b) *Sections that are not applicable have been retained with their justification.*
- c) *All evidence cited is listed in the responsible statement, indicating how it is provided.*
- d) *The document has been electronically signed by the applicant's technical manager.*

1 INTRODUCTION

1.1 PURPOSE OF THE DOCUMENT

[This document is a reference template for drafting the Differential Analysis Report (IAD) provided for in guide CCN-STIC-106 [REF1].]

The IAD is a statement by the applicant, signed by its technical manager, analysing the extent to which the Fundamental Security Requirements (RFS) of the corresponding family of the CCN-STIC-140 taxonomy [REF2] are affected by the differences between the scope requested and the subject of the certification provided, and which part of them, if any, constitutes scope pending verification. Its submission neither replaces nor conditions the CCN's decision, which may depart from the analysis it contains, giving reasons.

The IAD identifies the Fundamental Security Requirements that must be verified again by means of a Complementary STIC Evaluation, which may be none if the differences do not impact them. Where the result of that evaluation is favourable, the file continues with the preparation of the Inclusion Technical Report (ITI) and the notification of the Result of the Inclusion Technical Report (RITI).

1.2 TYPE OF EXTENSION

[The IAD is provided when the scope to be qualified does not coincide with that of the basis of the analysis, either because it incorporates models not included in it or a later version. Extension of scope is only applicable to on-premise ICT security products.]

This document, in its entirety, is regarded as a responsible statement by the applicant and is provided in all cases, whether or not the changes impact the RFS; its content must therefore be complete and truthful. Where the analysis concludes that the changes introduced do not impact the RFS, this statement constitutes the evidence on which the qualification of the requested scope is based, without the need for a Complementary STIC Evaluation. For this reason, the document must be completed exhaustively.

[Indicate the type of extension to which the analysis refers.]

Type of extension	Applicable (Yes / No)	Scope
Hardware extension — models		[List of additional models]
Software extension — version		[Candidate version and original version]

1.3 SCOPE OF THE ANALYSIS

The analysis contained in this document refers exclusively to the RFS of the family and ENS category for which inclusion in the CPSTIC is requested. Any other security functionality of the product falls outside its scope.

The analysis of the coverage of the RFS by the security target also falls outside the scope of this template; it is carried out using the Requirements Justification (JR) template in Annex A of CCN-STIC-106 [REF3] where that guide so requires.

1.4 TERMS USED

For the purposes of this document, the following terms are used:

- a) Original scope: the set of product models and versions covered by the original certification or by the latest IAD accepted by the CCN, which constitutes the reference for the analysis.
- b) Requested scope: the set of product models and versions for which qualification is requested.
- c) Homogeneous technology grouping: a set of models sharing the platform, firmware and security-relevant components, which are treated as a single unit in the analysis.
- d) DIF-HW-XX and DIF-SW-XX: codes uniquely identifying platform differences and changes between versions, respectively.
- e) Scope pending verification: the part of the requested scope which, because it is affected by the differences identified, must be verified before the qualification is extended.
- f) Complementary STIC Evaluation: an evaluation, carried out by a laboratory accredited under the ENECSTI, which verifies the affected requirements where the differences impact them.
- g) Fundamental Security Requirements (RFS): requirements applicable to the requested family and ENS category, defined in the CCN-STIC-140 taxonomy [REF2].

1.5 APPLICANT AND PRODUCT INFORMATION

Applicant name	
Manufacturer or developer	

Technical manager (name, position and contact details)	
Commercial name of the product	
Taxonomy family (CCN-STIC-140)	
ENS category requested	
CPSTIC file number	
Current status in the CPSTIC (not included / included / provisional inclusion)	
Document date	

2 CHARACTERISATION OF THE ORIGINAL CERTIFICATION

This section sets out what has actually been evaluated and what the basis of this analysis is: the original certification or, where the product has been the subject of previous extensions, the latest IAD accepted by the CCN. The scope covered by that basis is referred to as the original scope and constitutes the reference against which the analysis in the following sections is carried out.

Certification scheme (Common Criteria / LINCE)	
Certificate reference and date	
Certification body and laboratory	
Security target reference, version and date	
Original models and versions	
Basis of this analysis	[Original certification or previous IAD, indicating its reference and date]

2.1 REQUESTED SCOPE VERSUS ORIGINAL SCOPE

[Identifies the dimensions in which the requested scope differs from the original scope.]

Dimension	Original scope	Requested scope
Models		
Firmware or software version		
Configuration		

2.2 RELEVANT ASSIGNMENTS AND SELECTIONS

[List the assignments and selections in the security target that determine the coverage of the RFS, in particular those relating to cryptographic mechanisms, protocols, authentication methods and update mechanisms.]

SFR	Declared assignment or selection	Taxonomy affected	RFS

2.3 PREVIOUS EXTENSIONS

Where the product has been the subject of previous extensions, the IADs previously submitted shall be listed, and section 2 shall indicate which of them, or the certification, constitutes the basis of this analysis.

Previous (reference date)	IAD and	Scope incorporated (models or version)	CCN file or decision

3 ANALYSIS CRITERIA

The analysis starts from the differences identified in section 4 and determines, for each of them, the RFS whose implementation is affected. The affected requirements constitute the scope pending verification; the remaining RFS of the family do not require additional verification.

The statements of absence of impact contained in this document are technically justified. In particular, mere identity of firmware is not considered sufficient where the differences affect components involved in the implementation of cryptographic mechanisms, key or credential storage, entropy sources, secure boot or integrity verification.

Requirements associated with security functionality introduced by the candidate version are always considered affected, the justification stating that their origin is the extension itself and not a shortcoming of the original certification.

It follows from the above that additional models for which the absence of impact is declared and justified do not generate scope pending verification and do not require individual testing.

4 IDENTIFICATION OF DIFFERENCES

This section sets out the exhaustive identification of the differences with respect to the original scope, which constitute the input to the analysis in section 5. Each difference is uniquely identified by the code DIF-HW-XX, for the platform differences set out in section 4.1, and DIF-SW-XX, for the changes between versions set out in section 4.3.

4.1 FEATURE MATRIX

[Complete one column for each additional model or homogeneous technology grouping. Add as many rows as necessary. The rows listed are indicative: only those applicable to the product's characteristics shall be retained, and any specific to the product shall be added. The "Difference" column shall indicate whether there is a divergence from the certified TOE and, if so, the DIF-HW-XX identifier.]

Feature	Original scope	Model or grouping 1	Model or grouping n	Difference
Commercial reference				
Chassis and form factor				
Processor (CPU / SoC): manufacturer, family and model				
Memory and non-volatile storage				
Cryptographic module or accelerator				
Entropy source or random number generator				
Secure key storage (TPM, HSM, secure element)				

Feature	Original scope	Model or grouping 1	Model or grouping n	Difference
Secure boot and integrity verification				
Network interfaces				
Management interfaces				
Other security-relevant components				
Firmware or software: name and version				
Firmware or software image: identifier and hash				
Cryptographic libraries and third-party components				
Supported security functionalities				
Capacity and performance				

4.2 HOMOGENEOUS TECHNOLOGY GROUPINGS

Models sharing the platform, firmware and security-relevant components are grouped for the purposes of the analysis, justifying the homogeneity of the group. The groupings so defined are used as the reference unit in the scope matrix in section 5.

Grouping	Models included	Justification of homogeneity
AGR-01		

Grouping	Models included	Justification of homogeneity
AGR-n		

4.3 LIST OF CHANGES BETWEEN VERSIONS

Where the extension refers to a later version, all changes between the original version and the candidate version, including intermediate versions, are listed.

[The product's changelog or change detail document is provided as mandatory evidence, with sufficient granularity to identify the components affected by each change. This document is listed in section 11.]

Id.	Version	Type of change	Description	Affected component
DIF-SW-01		[Bug fix / Functional improvement / New security functionality / Third-party component update / Vulnerability fix]		
DIF-SW-n				

4.4 SUMMARY OF DIFFERENCES

Id.	Brief description	Affected models, groupings or versions	Potentially affected RFS
DIF-HW-01			
DIF-SW-n			

[Where no difference has been identified in any of the above categories, this is expressly stated.]

5 AFFECTED REQUIREMENTS AND SCOPE PENDING VERIFICATION

The RFS of the *[indicate family]* family applicable to the *[indicate ENS category]* category, in accordance with the nomenclature of the corresponding annex of CCN-STIC-140 [REF2], whose implementation is affected by the differences identified in section 4, are listed below. RFS not listed are not affected by those differences and do not generate scope pending verification.

5.1 LIST OF AFFECTED REQUIREMENTS

[Include one row for each affected RFS. The statement of pending scope must be self-contained and verifiable, so that it can be transferred directly to the evaluation plan.]

RFS	Associated differences	Justification of impact	Affected models, groupings or versions	Scope pending verification
[ID]	[DIF-HW-XX / DIF-SW-XX]	[Technical justification]	[Models, groupings or versions]	[Statement of what is pending verification]

5.2 EXAMPLES

[The following examples are included for illustrative purposes and must be deleted from the final document.]

RFS	Associated differences	Justification of impact	Affected models, groupings or versions	Scope pending verification

RFS	Associated differences	Justification of impact	Affected models, groupings or versions	Scope pending verification
CIF.1A	DIF-HW-04	Grouping AGR-02 incorporates a cryptographic accelerator from a different manufacturer . Although the cryptographic library and the algorithm configuration remain unchanged, the encryption primitives are delegated to a hardware component different from the one evaluated.	AGR-02	Verify that the encryption mechanisms and key lengths used by grouping AGR-02 match those declared and are among those authorised by the CCN for the requested ENS category.

RFS	Associated differences	Justification of impact	Affected models, groupings or versions	Scope pending verification
AUT.3	DIF-SW-07	The candidate version replaces the library that implements the verification of administrator credentials, a functionality directly associated with the requirement.	Candidate version	Verify the administration or authentication mechanism in the candidate version, including failed attempt control and account lockout.

5.3 SCOPE MATRIX

[Complete where there are requirements whose pending scope does not cover the entire requested scope. The relevant models, technology groupings or versions may be used as columns.]

Requirement	Original scope	AGR-01 / Model 1	AGR-n / Model n	Candidate version
[ID]				

6 CRYPTOGRAPHIC CONFORMITY

The conformity of the cryptographic mechanisms with guide CCN-STIC-807 [REF7] is analysed transversally in this section, since a single mechanism may affect several requirements and its assessment depends on the specific assignments and selections declared, and not on the mere presence of the corresponding SFR.

The cryptographic mechanisms used by the product that are affected by the differences identified in section 4 are listed, indicating their classification according to [REF7] for the requested ENS category.

Mechanism, length and mode	Use in the product	Classification according to [REF7]	Affected RFS	Compliance (Yes / No)
	[Data encryption / Key establishment / Signature / Hash / Message authentication / Key derivation]	[Recommended / Legacy / Not included]		

[Where a mechanism is not classified as recommended, or where the security target does not make it possible to determine which mechanism is actually used, this is stated and reflected in the corresponding requirement in section 5, as well as in the scope pending verification].

[Particular attention must be paid to pseudorandom functions, Diffie-Hellman groups and key establishment schemes, as there are frequent cases in which the security target does not specify them or includes non-recommended options.]

7 INSTALLATION AND OPERATION GUIDES

This section analyses whether the installation and operation documentation remains valid for the requested scope, since the secure configuration of the product forms part of the conditions of its qualification.

7.1 MANUFACTURER'S GUIDES

Guide (name, version and date)	Included in the original scope (Yes / No)	Does it cover the requested scope?	Planned action
			[None / Update of the guide]

7.2 CCN-STIC GUIDE IN THE 1000 SERIES

[State expressly whether or not the inclusion of the requested scope requires the modification of the CCN-STIC guide in the 1000 series published for the product, identifying it by its specific name.]

CCN-STIC guide in the 1000 series published for the product: *[Indicate the specific name and version, or state that no guide has been published]*

Is modification required?: *[Yes / No]*

Justification: *[Give reasons for the answer. Where the extension affects only the names of the models or the versions referred to in the guide, this shall also be stated]*

[Where modification of the guide is required, it shall be made on a provisional basis at the time of inclusion and shall become final upon publication of the corresponding Secure Use Procedure (PES). It is not necessary to provide the modified text of the guide with this document.]

8 CONCLUSIONS

The conclusion is drawn on the impact of the differences analysed in section 4.

The course of the file depends on the conclusion: if the differences do not impact the RFS, the extension is resolved with this responsible statement; if they do, the requirements listed in section 5 must be verified by means of a Complementary STIC Evaluation before the qualification is extended.

8.1 CONCLUSION OF THE ANALYSIS

Include the appropriate conclusion:

- a) *The differences identified in section 4 do not impact the Fundamental Security Requirements of the family; therefore, a Complementary STIC Evaluation arising from the differences analysed is not considered necessary.*
- b) *The differences identified in section 4 impact the Fundamental Security Requirements listed in section 5, for the models, groupings or versions indicated therein.*

This conclusion refers exclusively to the differences analysed in section 4 and is without prejudice to the coverage of the RFS by the security target, which is analysed, where appropriate, in the JR.

8.2 DELIVERABLES

[Complete where the analysis results in affected requirements.]

The applicant shall make the following items available to the laboratory:

- a) The product in the configuration corresponding to the requested scope.
- b) The models, groupings or versions on which the pending scope must be verified.
- c) The operating environment required to carry out the tests.
- d) The applicable installation and operation documentation.

9 APPLICANT'S OBSERVATIONS

[This section sets out any additional information that the applicant considers relevant to the assessment of the analysis and which does not fit into the previous sections.]

[Complete where appropriate; otherwise, state that there are no observations.]

10 RESPONSIBLE STATEMENT

Mr/Ms [full name], holder of DNI/NIE [document number], in the capacity of [position] of [organisation], in the name and on behalf of the applicant, declares under their own responsibility that the content of this document is true and complete and that, in particular:

- a) It sets out all the hardware, firmware and software differences between the original scope and the requested scope.
- b) The statements of absence of impact on the Fundamental Security Requirements are technically justified and supported by the product documentation provided.
- c) The evidence referenced in section 11 corresponds to the versions of the product and the certification identified in section 2.
- d) The Fundamental Security Requirements not listed in section 5 are not affected by the differences identified.
- e) The documentation listed in the following section is provided together with this responsible statement or, where it is public, is identified by indicating the address at which it can be accessed.

10.1 DOCUMENTATION PROVIDED AS EVIDENCE

The documentation provided as evidence of the analysis is listed below, indicating in each case whether it accompanies this responsible statement or whether it is public and where it can be accessed.

[Include one row for each document. The reference must match the one used in the references section.]

Reference	Document (title, version and date)	Method of provision
[REFn]	[Title, version and date]	[Provided together with this statement / Public, accessible at (address)]

Full name	
Position	
Organisation	
Place and date	
Signature	<i>[Space reserved for the electronic signature of the applicant's technical manager. Scanned handwritten signatures are not accepted.]</i>

11 REFERENCES

The guides and documents used in preparing the analysis are listed below. The method of providing the evidence is indicated in the responsible statement section.

Reference	Document
REF1	CCN-STIC-106 — Procedure guide for inclusion in the CPSTIC.
REF2	CCN-STIC-140 — Reference Taxonomy for ICT Security Products, Annex [indicate annex and family].
REF3	CCN-STIC-106, Annex A — Requirements Justification (JR) Template.
REF4	Product security target [indicate reference, version and date].
REF5	Certificate of the original evaluation [indicate reference and date].
REF6	Evaluation technical report or certification report [indicate reference].
REF7	CCN-STIC-807 — Cryptology for Use in the National Security Framework.
REF8	Product changelog or change detail document [indicate reference, version and date].
REF9	Installation and operation guides [indicate reference, version and date].
REF10	[Other evidence provided].

