

Requirements Justification (JR) 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 13:01:24 +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.....	4
1.1 APPLICANT, TOE AND EVALUATION INFORMATION.....	4
1.2 APPLICABILITY OF THE REQUIREMENTS.....	5
2 JUSTIFICATION OF THE REQUIREMENTS.....	6
2.1 FS. NAME OF THE SECURITY FUNCTION	6
3 REFERENCES.....	8

1 INTRODUCTION

This document is a reference template for drafting the Requirements Justification (JR), in which the applicant analyses the applicability of each of the Fundamental Security Requirements (RFS) of the CCN-STIC-140 taxonomy family [1] to which the product belongs and their correspondence with the Security Target (DS).

In accordance with section 4.5.1.1 of CCN-STIC-106 [2], the JR shall be provided together with the application for inclusion in the following cases: a) on-premise ICT security products with a valid certification, where there are differences between the RFS of the requested family and those declared in the DS; b) on-premise ICT security products without a valid certification; and c) cloud-deployed security products.

The CCN will analyse the JR together with the DS: in the review phase of the proposed security target (section 4.5.3 of CCN-STIC-106 [2]), whose result is communicated by means of the Result of the Review of the Proposed Security Target (RRPDS), or, for products with a valid certification, in the certification review phase (section 4.5.4).

Text in grey italics consists of instructions for completing the template and must be deleted in the final version of the document. Text in square brackets and italics must be replaced with the corresponding information.

1.1 APPLICANT, TOE AND EVALUATION INFORMATION

Applicant name	
TOE name	
TOE version	
Type of evaluation	<i>[Common Criteria / LINCE / Complementary STIC Evaluation / CICLON]</i>
Original certification or evaluation	<i>[Identifier of the certificate or evaluation; "Not applicable" if none]</i>
DS reference and version	<i>[DS identifier, version and date]</i>
ENS category requested	<i>[HIGH / MEDIUM]</i>
Taxonomy family (CCN-STIC-140)	<i>[Taxonomy family or families]</i>

1.2 APPLICABILITY OF THE REQUIREMENTS

For each RFS, its applicability must be analysed and one of the following results indicated:

- **DIRECT CHECK (CD):** for requirements that are applicable and can be evaluated by the laboratory. They are included in the Security Target (DS).
- **INDIRECT CHECK (CI):** for requirements that the laboratory cannot test and for which the applicant must provide adequate evidence covering them. They are included in the DS if the methodology provides for this, as is the case with CICLON; in LINCE they remain outside the DS and the evidence is provided by means of a Complementary STIC Evaluation.
- **NOT APPLICABLE (NA):** for requirements that are not applicable (for example, specific hardware requirements when the TOE is a software solution). They are not included in the DS and a justification of their non-applicability is provided.
- **INTEGRATION (INT):** for requirements covered by an integration component defined in the environment and configured by the developer or manufacturer itself. They are included in the DS, adapting their wording where necessary.
- **COVERED (CU):** for requirements covered by an integration component defined in the execution environment and configured by the end user, or covered by a component defined in the execution environment. The DS shall include the wording of the requirement that makes the call to the component covering it.

2 JUSTIFICATION OF THE REQUIREMENTS

The applicability of the RFS of the *[indicate family]* family for the product *[indicate TOE name]* is analysed below.

If one part of a requirement can be checked directly and another part is covered by indirect check, integration or a previous evaluation or certification, the requirement shall be split into two using the following format: REQ.XA (part of the requirement checked by CD) and REQ.XB (part of the requirement covered by CI, INT or CU). If part B is CU, the DS shall include the wording of the requirement that makes the call to the component covering it.

Each security requirement must be analysed from the point of view of each of the actors in order to determine its applicability. Where a requirement falls on more than one actor, it shall be split into as many requirements as actors identified, using the format "REQ.X_actor" (for example, REQ.1_USER and REQ.1_VENDOR). The following actors are defined for this purpose:

- a) End user (USER).
- b) Product manufacturer (VENDOR).

The applicability of each requirement must be indicated in the table in the section for each security function, using the format shown below.

2.1 FS. NAME OF THE SECURITY FUNCTION

The title of this section shall indicate the name of the corresponding security function. There must be as many sections as there are security functions. The "Justification" column shall explain the result assigned and, for CI requirements, the evidence provided; it is mandatory for NA, CI, INT and CU requirements. The "RFS in DS" column shall contain the final wording of the requirement as it will be included in the proposed DS; "Not applicable" shall be indicated for NA requirements and for CI requirements which, according to the methodology, remain outside the DS. The example rows must be deleted.

RFS	Description	Actor	Applicability	Justification	RFS in DS
REQ.1	<i>[Example] The TOE authenticates administrators before allowing any management action.</i>	<i>VENDOR</i>	<i>CD</i>	<i>Functionality implemented in the TOE and verifiable by the laboratory through functional testing.</i>	<i>[Final wording of the requirement in the DS]</i>
REQ.2	<i>[Example] Recording and safekeeping of the audit events</i>	<i>USER</i>	<i>CU</i>	<i>The TOE exports the events to the logging component of the</i>	<i>The TOE shall export the audit events to the</i>

	<i>generated by the TOE.</i>			<i>execution environment, which is configured by the end user; the component and its configuration are described.</i>	<i>logging component defined in the execution environment.</i>

3 REFERENCES

This section shall reference all the documents that have been used to analyse the justification of the various requirements.

Reference	Title, version and date
[1]	CCN-STIC-140 Reference Taxonomy for ICT Security Products.
[2]	Guide CCN-STIC-106 and its annexes.
[3]	<i>[Product Security Target: identifier, version and date]</i>

