

ICT Security Guide Annex C CCN-STIC-106

Secure Use Procedure Template (PES)



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 13:03:12 +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.

CONTENTS

1 INTRODUCTION	7
1.1 PRODUCT DESCRIPTION	7
1.2 PURPOSE AND SCOPE	7
1.3 ORGANISATION OF THE DOCUMENT	7
2 PRE-INSTALLATION PHASE	8
2.1 SECURE DELIVERY OF THE PRODUCT	8
2.2 SECURE INSTALLATION ENVIRONMENT	8
2.3 REGISTRATION AND LICENCES	8
2.4 PRELIMINARY CONSIDERATIONS	8
2.5 OPERATING ENVIRONMENT COMPONENTS	8
3 INSTALLATION PHASE	8
4 CONFIGURATION PHASE	9
4.1 SECURE MODE OF OPERATION	9
4.2 IDENTITY AND ACCESS	9
4.2.1 AUTHENTICATION	9
4.2.2 LOCAL AND REMOTE ADMINISTRATION	9
4.2.3 ADMINISTRATOR CONFIGURATION	10
4.2.4 AUTHENTICATION SERVERS	11
4.3 COMMUNICATIONS AND CRYPTOGRAPHY	11
4.3.1 CONFIGURATION OF INTERFACES, PORTS AND SERVICES	11
4.3.2 CERTIFICATE MANAGEMENT	11
4.3.3 SYNCHRONISATION	11
4.4 LOGGING AND AUDITING	11
4.4.1 EVENT LOGGING	11
4.4.2 LOCAL STORAGE	12
4.4.3 REMOTE STORAGE	12
4.5 AVAILABILITY AND BACKUP	12
4.5.1 HIGH AVAILABILITY	12
4.5.2 BACKUPS	12
4.6 UPDATES AND SELF-TESTS	12
4.6.1 UPDATES	12
4.6.2 SELF-TESTS	12
4.7 SUMMARY OF THE SECURE CONFIGURATION	13
5 OPERATION AND MAINTENANCE PHASE	14
5.1 SECURITY SUPPORT	14
5.2 VULNERABILITY NOTIFICATION	14
5.3 APPLICATION OF SECURITY UPDATES	14
5.4 PRODUCT END OF LIFE	14
6 SPECIFIC PROVISIONS FOR APPROVED PRODUCTS	14
6.1 REGISTRATION AND LICENCES	14
6.2 EXCLUSIVELY ON-PREMISE DEPLOYMENT	15
6.3 OFFLINE UPDATES	15
6.4 NO SENDING OF LOGS TO THE CLOUD	15
6.5 SELF-TESTS	15
7 REFERENCES	15
8 ABBREVIATIONS	16

LIST OF TABLES

TABLE 1: EXAMPLE TABLES

LIST OF FIGURES

FIGURE 1: EXAMPLE FIGURES

INSTRUCTIONS FOR COMPLETION, SUBMISSION AND PUBLICATION

This template constitutes Annex C of CCN-STIC-106. The document resulting from its completion will be the product's secure use procedure (PES), and the CCN will publish it as a guide in the CCN-STIC-1000 series, assigning it the guide number and completing the cover, headers and credits page.

Annex C of CCN-STIC-106 is published in PDF format. The editable version of the template, in Word format, may be requested from the mailbox soporte.cpstic@ccn.cni.es.

The texts in this template are completion instructions and must be deleted from the final document, as must the table, figure and note included as examples. Sections that are not applicable shall be retained, expressly stating their non-applicability.

The applicant shall send the proposed PES, in editable format, to soporte.cpstic@ccn.cni.es, stating the product name and the CPSTIC file code in the subject line.

The PES shall be sent in Word format, respecting the structure, styles and sections of this template, so that the CCN can review it and publish it as a CCN-STIC guide in the 1000 series.

The delivery deadline is six (6) months from the notification of the favourable RITI, in accordance with section 4.5.5 of CCN-STIC-106. Failure to deliver within the deadline will result in the exclusion of the product from the catalogue.

The CCN will review the proposal and may return it with comments. The applicant shall send the corrected versions through the same channel until the CCN's approval is obtained.

Once approval has been obtained, the CCN will publish the guide, at which point the inclusion of the product becomes final in accordance with section 4.5.6 of CCN-STIC-106.

Any extension of scope or new qualified version affecting the content of the PES will require an updated version to be sent through the same channel, which will give rise to a new edition of the guide.

Content instructions

Everything the administrator has to carry out in order to leave the product in its secure configuration must be described in full in this document: the steps, the parameters and the specific values.

Anything that does not determine the secure configuration may be referenced to the manufacturer's documentation, provided that the referenced document is public and accessible, is identified by title, version and date, is listed in the references section and is cited in the text as [REFn].

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

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

If the document covers several models or platforms and the configuration differs between them, it shall be expressly indicated to which models each step applies.

Formatting instructions

The template styles shall be used: Heading 1 to 3 for headings, Paragraph for body text, Code for commands and Caption for table and figure captions.

Tables and figures shall be numbered with their corresponding caption and cited in the text. Text boxes and images of text shall not be used, and screenshots must be legible.

The cover, headers and footers shall not be modified: the CCN replaces them when publishing the guide, together with the credits page and the CCN-STIC-1000 series number.

Tables, figures, captions and code fragments shall be inserted using the format shown below.

Text written by the manufacturer shall use the Paragraph style, in black and without italics, as in the following example:

This is an example of paragraph text. Content written by the manufacturer must be in this format, so that it can be distinguished from the template instructions, which appear in grey italics and must be deleted from the final document.

HEADINGS	HEADINGS
SUBHEADINGS	SUBHEADINGS

Table : Example table

```
This is code text
```



Figure : Example figure

NOTE: Example note, valid for the whole document

Checks before submission

- *All grey italic text in the template has been deleted, including the table, figure, note and code examples.*
- *The table of contents, list of tables and list of figures have been updated.*
- *Sections that are not applicable have been retained with their justification.*
- *All references cited in the text appear in the references section, with title, version and date.*
- *Screenshots are legible and contain no sensitive information.*
- *The document is sent in editable format to soporte.cpstic@ccn.cni.es.*

1 INTRODUCTION

1.1 PRODUCT DESCRIPTION

General description of the product.

1.2 PURPOSE AND SCOPE

Indicate the product – version – hardware models – hardware platforms – etc. for which this guide has been developed.

The product PRODUCT NAME has been included in the CPSTIC catalogue; to find out the list, category or level and family, consult the CPSTIC website [REF1].

1.3 ORGANISATION OF THE DOCUMENT

- a) Section 2. This section sets out aspects and recommendations to be considered before proceeding with the installation of the product.*
- b) Section 3. This section sets out recommendations to be taken into account during the installation phase of the product.*
- c) Section 4. This section sets out the recommendations to be taken into account during the configuration phase of the product, in order to achieve a secure configuration.*
- d) Section 5. This section sets out the aspects relating to the secure maintenance of the product throughout its useful life.*
- e) Section 6. This section sets out the specific provisions applicable when the product, in addition to being qualified, is to be approved for handling national classified information.*
- f) Cloud-deployed products. In these cases, sections 2 and 3 shall be completed with the specific features of the service: registration and secure access to it, configuration of the tenant or subscription and the division of responsibilities between the service provider and the user.*

2 PRE-INSTALLATION PHASE

2.1 SECURE DELIVERY OF THE PRODUCT

Describe the procedure for the secure receipt of the product.

- *If it is a hardware device (appliance), describe **step by step in this document** how to check the outer and inner packaging, tamper-evident seals, etc.*
- *If it is a software product, describe **step by step in this document** how to verify the integrity of the download. For example, if it is received by email it may carry an electronic signature; if it is downloaded via a URL, a hash file could be downloaded, etc.*

*If hash values are used to verify files, **SHA-256 functions** or higher must be used.*

For cloud-deployed products, describe the service registration process and the secure delivery of the initial access credentials, as well as how to verify the authenticity of the service access point (domain and certificate).

2.2 SECURE INSTALLATION ENVIRONMENT

Indicate whether any of the product components must be installed in a Data Processing Centre (CPD), access to which shall be restricted to a group of people with express authorisation.

2.3 REGISTRATION AND LICENCES

*Reference the **public documentation** describing the process for registering the hardware, software and/or licences. Where the product is to be approved in addition to being qualified, the provisions of section 6 shall be taken into account.*

2.4 PRELIMINARY CONSIDERATIONS

*If any additional **security-related** configuration is required **before starting the installation and configuration** of the product, the aspects to be taken into account must be indicated **step by step in this document**, since they will influence how to configure it securely.*

For example: preparation of other necessary components (entropy token, cryptographic key store, hardware platforms, etc.), decisions on aspects of the physical architecture (for example, high availability) or the logical architecture (for example, authentication methods).

2.5 OPERATING ENVIRONMENT COMPONENTS

Indicate which components must be present in the product's operating environment: external authentication server, external syslog server, management workstation, etc.

3 INSTALLATION PHASE

This section shall refer to the public documentation describing how to install each component of the product:

- *Appliance: how the corresponding firmware must be installed.*
- *Software: how the software component must be installed, indicating the platform on which it will run (server, workstation, etc.), including the operating system and any necessary base software.*

*This document shall include an indication and description of the **relevant parameters and necessary aspects** for a secure installation.*

*If the product requires the installation of other additional components, this document shall indicate **what they are and what they are configured for**, referring to their installation process in the corresponding public documentation.*

For cloud-deployed products, this section shall set out the provisioning process and the initial configuration of the tenant or subscription, indicating which elements are the responsibility of the service provider and which are the responsibility of the user.

4 CONFIGURATION PHASE

4.1 SECURE MODE OF OPERATION

*This document must **describe step by step** how to activate the product-specific configuration so that the product operates in secure mode.*

4.2 IDENTITY AND ACCESS

4.2.1 AUTHENTICATION

Describe in the document the authentication mechanisms used by the product for:

- *User authentication (local credentials, external authentication server, certificate, etc.).*
- *Authentication between product components and with external servers or devices (certificate, pre-shared keys, etc.).*
- *Session authentication (e.g. SSH with public key, etc.).*

The use of pre-shared keys must not be recommended if the product supports another method (for example, certificates).

4.2.2 LOCAL AND REMOTE ADMINISTRATION

Indicate which mechanisms will be used to administer the product: both local (console) and remote (GUI and/or CLI).

*Insecure **protocols** must NOT be allowed for administration, such as:*

- *Telnet (SSH must be used)*
- *TLS version lower than 1.2 (TLSv1.2 or higher must be used)*
- *IKEv1 (IKEv2 must be used)*
- *SSHv1 (SSHv2 must be used)*
- *FTP (SFTP or SCP must be used)*
- *HTTP (HTTPS must be used)*

This document must describe step by step how to disable insecure protocols, where possible. Where this is not possible, it must be stated that their use is not recommended.

Include a reference to the public documentation describing how to configure the secure administration protocols (for example, HTTPS/TLS, SSH).

Describe step by step in this document how to configure the product's cryptographic algorithms and functions, which must comply with the specifications of guide CCN-STIC-807. This means that the configuration of these protocols must be specified so as to use only the following algorithms and functions:

- DSA or RSA with keys of at least 3072 bits in length.
- ECDSA with P-256 curves or higher.
- SHA-256 hash functions or higher.
- AES-128 encryption or higher.
- Diffie-Hellman groups 15, 16, 19, 20, 21, 28, 29 or 30.
- Elliptic Curve Diffie-Hellman P-256 or higher.

As a general criterion, whenever an encryption algorithm, hash or cryptographic function is mentioned in the secure use procedure, the parameters used must be indicated. If the administrator user must carry out any configuration for these to be secure, a reference to the public documentation describing how to configure them must be included (for example: how to use the algorithms and functions indicated above, how to configure passwords protected by a hash value or encrypted backup storage).

4.2.3 ADMINISTRATOR CONFIGURATION

Include a reference to the manufacturer's documentation describing the administration user roles supported by the product and how to configure them.

Take the following aspects into account:

- **Configuration of the secure password policy.** It must meet the following minimum requirements:
 - Minimum password length: twelve (12) characters.
 - Password composition: upper-case letters, lower-case letters, numbers and special symbols. Recommend the use of all four (4) groups if the product allows it, and at least a minimum of three (3) groups.
 - Number of previous passwords that may not be reused: at least five (5).
 - Password validity period in days, after which passwords expire: approximately two months (60 days).
 - Number of days that must elapse after a password change before it can be changed again: ten (10) days.
- **Configuration of session parameters.** It must meet the following minimum requirements:
 - Session inactivity timeout: five (5) minutes.
 - Number of failed login attempts: three (3) attempts.
 - Lockout time after failed attempts: five (5) minutes.
- Configuration of the warning and consent message at login (**login banner**).

4.2.4 AUTHENTICATION SERVERS

*If the product uses external authentication servers (RADIUS, LDAP, SAML, Kerberos, etc.), refer to the **documentation** describing how to configure them and indicate the relevant parameters for a secure configuration (for example, use of RADSEC, LDAPv3 or TLSv1.2).*

4.3 COMMUNICATIONS AND CRYPTOGRAPHY

4.3.1 CONFIGURATION OF INTERFACES, PORTS AND SERVICES

*Where appropriate, **describe step by step in this document** the recommendations for the necessary secure configuration of interfaces, ports and services.*

For example: disabling unused services on the device, entering a label identifying the intended use of each interface, associating each interface with the IP and MAC address of the connected machine, etc.

4.3.2 CERTIFICATE MANAGEMENT

*The product's cryptographic algorithms and functions that comply with the specifications of guide CCN-STIC-807 must **be indicated**, and **reference must be made to the public documentation** describing how to configure them. These parameters are:*

- *RSA with keys of at least 3072 bits in length.*
- *ECDSA with P-256 curves or higher.*
- *DSA with keys of at least 3072 bits in length.*
- *SHA-256 hash functions or higher.*

***Reference must be made to the documentation** describing how to make the certificate signing request (CSR), import the server certificate, import CA certificates and other necessary parameters.*

4.3.3 SYNCHRONISATION

***Include a reference to the public documentation** describing how secure synchronisation of the product and its components must be configured. **Integration with an NTP service** must be recommended where possible, together with how to enable authentication where possible.*

4.4 LOGGING AND AUDITING

4.4.1 EVENT LOGGING

***Refer to the public documentation** indicating which events are logged and how logging is carried out. For example: configuration log file, system log file, etc.*

Indicate the format of the log records, including an example.

4.4.2 LOCAL STORAGE

*Refer to the **public documentation** describing how local storage of audit records works in the product.*

If any configuration is required for the secure storage of records, describe it in this document.

4.4.3 REMOTE STORAGE

*Refer to the **public documentation** indicating how to configure the sending of records to a remote syslog server and how to configure that server. A secure protocol must always be used for sending records (for example, TLSv1.2 or IPsec).*

4.5 AVAILABILITY AND BACKUP

4.5.1 HIGH AVAILABILITY

*Refer to the **public documentation** describing the product's high availability configuration. Indicate in this document the configuration parameters required for a secure configuration.*

4.5.2 BACKUPS

The components, data and configurations to be backed up must be indicated.

*Refer to the **public documentation** describing the process for configuring and performing backups securely.*

Periodic backups must be recommended.

4.6 UPDATES AND SELF-TESTS

4.6.1 UPDATES

*Refer to the **documentation** describing the process to be followed to update firmware, software, services, etc. securely.*

*Where necessary, **this document must indicate the use of secure protocols** such as SCP or SFTP and refer to the documentation describing how to configure them where necessary. The security update policy is described in section 5.3. Where the product is to be approved in addition to being qualified, the provisions of section 6 shall be taken into account.*

4.6.2 SELF-TESTS

Describe the self-tests of software integrity and of the operation of the cryptographic algorithms and functions, indicate when they are performed (at start-up or on demand by the administrator) and what happens in the event of failure. Where the product is to be approved in addition to being qualified, the provisions of section 6 shall be taken into account.

4.7 SUMMARY OF THE SECURE CONFIGURATION

Include a summary table of the security parameters configured and the value set for each, indicating the section of this document in which its configuration is described.

Parameter	Configured value	Section
<i>[Security parameter]</i>	<i>[Value set]</i>	<i>[4.x]</i>

5 OPERATION AND MAINTENANCE PHASE

This section sets out the aspects relating to the secure maintenance of the product throughout its useful life.

5.1 SECURITY SUPPORT

Indicate the security support period for the qualified version and the planned end-of-support date. The manufacturer is obliged to notify the CPSTIC of the end of security support, in accordance with CCN-STIC-106.

5.2 VULNERABILITY NOTIFICATION

Indicate the manufacturer's vulnerability notification channel, the committed response times and the means by which security advisories are communicated to the product's users.

5.3 APPLICATION OF SECURITY UPDATES

Describe the security update policy: frequency, verification of the authenticity and integrity of the packages before installation, and the effect of the update on the secure configuration described in this document. The configuration of the update mechanism is described in section 4.6.1.

5.4 PRODUCT END OF LIFE

Describe the procedure for the secure erasure of the information, credentials and cryptographic material stored in the product before its withdrawal, return or reassignment.

6 SPECIFIC PROVISIONS FOR APPROVED PRODUCTS

Where, in addition to its inclusion in the CPSTIC as a qualified product or in the Compliance and Governance list, the product is to be approved for handling national classified information in accordance with CCN-STIC-102 [REF4], the secure use procedure must also cover the use case described in this section, characterised by the absence of an Internet connection.

The manufacturer may state that the configuration described in the previous sections is equally valid for this use case, or provide an annex to the PES setting out the necessary modifications. In the latter case, the annex shall be sent through the same channel indicated at the beginning of this document.

6.1 REGISTRATION AND LICENCES

Describe the process for registering the hardware, software and licences, taking into account that the product cannot connect to the Internet.

6.2 EXCLUSIVELY ON-PREMISE DEPLOYMENT

It must be possible to deploy the product entirely locally, including the server implementing the product logic. Describe the local deployment architecture and its components.

6.3 OFFLINE UPDATES

It must be possible to update the product locally, without the need for an external Internet connection. Describe step by step in this document how the administrator obtains the corresponding update package and deploys it locally.

These updates include both those for the product software and those relating to its logic; for example, antivirus signature updates.

6.4 NO SENDING OF LOGS TO THE CLOUD

The product shall not send any type of log to the cloud or outside the customer's environment or, at the very least, must be configurable to that effect. Describe step by step in this document how to disable any such sending.

6.5 SELF-TESTS

State expressly that the product will not send diagnostic information under any circumstances.

7 REFERENCES

List the documentation referenced throughout the guide.

REF1	CPSTIC https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic
REF2	CCN-STIC-807 Cryptology for Use in the National Security Framework.
REF3	Guide CCN-STIC-106 and its annexes.
REF4	CCN-STIC-102 Procedure for the Approval of ICT Security Products for Handling National Classified Information.

8 ABBREVIATIONS

ENS	National Security Framework (Esquema Nacional de Seguridad).
CPSTIC	Catalogue of Information and Communications Technology Security Products and Services (Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación).
CA	Certification Authority.
CLI	Command Line Interface.
CPD	Data Processing Centre (Centro de Proceso de Datos).
CSR	Certificate Signing Request.
GUI	Graphical User Interface.
LDAP	Lightweight Directory Access Protocol.
NTP	Network Time Protocol.
PES	Secure Use Procedure (Procedimiento de Empleo Seguro).
RADIUS	Remote Authentication Dial-In User Service.
SAML	Security Assertion Markup Language.
SSH	Secure Shell.
TLS	Transport Layer Security.

