centro criptológico nacional

ICT Security Guide
Annex B CCN-STIC 2010

Template for the Service Architecture Document of Cloud Products Evaluation

March 2026

Edited by:

Edition date: march 2026

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.06.12 12:18:47 +02'00'

LIMITATION OF LIABILITY

The present document is provided in accordance with the terms set forth herein, expressly rejecting any type of implied warranty related thereto. Under no circumstances shall the National Cryptologic Center be liable for any direct, indirect, incidental, or extraordinary damages arising from the use of the information and software provided herein, even if advised of such possibility.

LEGAL NOTICE

Version Control

Version	Comment	Date
1.0	Initial Version	March 2026

INDEX

1 APPLICANT, TOE AND EVALUATION INFORMATION

APPLICANT DATA	
Trade Name	
Postal Adress	
Corporate Identity	
Company Number	
LEGAL REPRESENTATIVE OF THE APPLICANT	
Name	
National ID or Passport Number	
TOE AND EVALUATION INFORMATION	
TOE name	
Evaluation type	CICLON version 1.0

2 MANUFACTURER'S STATEMENT OF CONFORMITY

By signing this document, the legal representative of **[Applicant name]** assures the reliability and accuracy of all the information provided herein.

The information declared in this document is aligned with that provided in the Security Target and states the following:

a) The structure of the TOE and its operational environment: in terms of subsystems and interfaces.
b) Description of information flows: declared between the service components.
c) Data jurisdiction of the cloud-deployed product.
d) Compliance with the established transparency requirements.
e) Authorization for direct access to the cloud-deployed product without WAF.
f) Certification of conformity with ENS or EUCS.
g) Cryptographic requirements.
h) Encryption services.

2.1 SERVICE ARCHITECTURE DIAGRAM (DIAS)

A diagram shall be included, detailing the cloud-deployed product and its integration with the components, whether proprietary or third party, of operational environment required for the normal operation of the service. Any component considered part of the TOE shall be clearly identified.

The purpose of the diagram is to clearly detail the integrations of the operational environment with the cloud platform where the TOE is deployed.

Each component shown in the diagram shall be identified according to the following table:

Component / service	Owner	Included in CPSTIC	Component Usage	Interfaces and Protocols	Interactions
		Indicate YES / NO		List the external and internal interfaces provided by each component and specify the protocols used	Describe interactions with other components or services (if any)

2.2 DATA JURISDICTION

It is assured that **the cloud-deployed product** complies with the geographical data restrictions in accordance with:

a) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

b) Organic Law 3/2018 of 5 December on the Protection of Personal Data and assurance of digital rights.

c) Royal Decree-Law 14/2019 of 31 October, adopting urgent measures for reasons of public security in the field of digital administration, public sector procurement and telecommunications.

2.3 TRANSPARENCY

It is assured that the manufacturer of **the cloud-deployed product** is able to provide the customer, if required, with:

1) The list of available security tools, including those intended for monitoring, analysis, recovery and notification of security incidents.

2) The description or specification of the virtualization technology used and the level and mechanisms of segregation of hosted data or cloud applications.

3) The list and specification of secure data deletion mechanisms and procedures of the provider stored information to be used upon termination of the contractual relationship.

4) The geographical location of the data (including backups and log storage), before and during service provision.

5) Access to and analysis of logs, access records and any other information required to ensure compliance with legal obligations. In case of a security incident, all required information (configuration, logs, etc.) from physical equipment, network devices, shared services and security devices shall be provided to the customer.

2.4 AUTHORIZATION FOR DIRECT ACCESS WITHOUT WAF

This section records whether the entity authorizes direct access to the cloud-deployed service without WAF protection.

Its purpose is to determine whether such access may be enabled to perform the necessary tests during the evaluation phase within the context of the submitted request.

For these controlled accesses, whitelisting may be used, consisting of authorizing only specific IP addresses or specific ranges to access the service without passing through the WAF, reducing the exposure surface.

Alternatively, mechanisms such as secure tunnels, corporate VPNs or temporary access with hourly restrictions may be enabled, always aimed at minimizing risks while allowing the required operation.

☐ **YES**, I authorize direct access without WAF.

☐ **NO**, I do not authorize direct access without WAF.

2.5 CERTIFICATION OF CONFORMITY WITH ENS OR EUCS

The system providing the cloud-deployed product holds a valid certification of conformity with the National Security Scheme (ENS) or EUCS, as defined in the Resolution of 13 October 2016 of the *Secretaría de Estado de Administraciones Públicas* (State Secretariat for Public Administrations) approving the Technical Security Instruction for conformity with the National Security Scheme (ENS).

Platform Provider	ENS Level	Validity Date	Geographical Location of the Data

2.6 CRYPTOGRAPHIC REQUIREMENTS

The cloud-based product includes encryption mechanisms that ensure assets designated as Critical Security Parameters (CSPs) or Sensitive Security Parameters (SSPs) within the TOE are protected, both in transit and at rest, so that they cannot be read or modified in the event of unauthorized access, as follows:

Component / service	Protected Assets	Protection in Transit	Protection at Rest
Component	Asset 1	Indicate YES or NO and, if YES, specify protocol and ciphersuites	Indicate YES or NO and the protection method (e.g. AES-256)
	Asset 2		

2.7 ENCRYPTION SERVICE

The cloud-deployed product:

☐ **YES,** it is an encryption service**.**

☐ **NO,** it is not an encryption service.

If the cloud-deployed product is an encryption service, the following shall be described:

a) The functioning of the encryption mechanisms without keys being stored in the cloud, and indicate the architecture of the system used, including details of the brand, model and version of the HSM (Hardware Security Module) used.

b) The process ensuring that the customer can manage and store the encryption mechanisms.

For the record, I hereby sign this document.