Reference: 2024-51-INF-4692- v1
Target: Limitada al expediente
Date: 04.02.2026

Created by: I008
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2024-51**
TOE	**Cryptographic Security Platform (CSP) | PKI Hub, Version 1.2**
Applicant	**B81188047 - Entrust EU, S.L.**

References

[EXT-9350] Solicitud de certificación

[EXT-9924] Informe técnico de evaluación

Certification report of the product Cryptographic Security Platform (CSP) | PKI Hub, Version 1.2, as requested in [EXT-9350] dated 18/11/2024, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-9924] received on 28/11/2025.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Cryptographic Security Platform (CSP) | PKI Hub, Version 1.2.

The TOE is a software component that reliably and efficiently verifies the status of digital certificates from one or multiple CAs and provides services for the generation of time-stamps.

Developer/manufacturer: Entrust EU, S.L.

Sponsor: Entrust EU, S.L..

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: DEKRA Testing and Certification S.A.U

Evaluation Level: Common Criteria version 2022 release 1. EAL 4 + ALC_FLR.2

Evaluation end date: 27/11/2025

Expiration Date[1]: 24/01/2031

All the assurance components required by the evaluation level EAL4 (augmented with ALC_FLR.2) have been assigned a "PASS" verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4, as defined by the CC2022 r1 and the CEM2022.

Considering the obtained evidences during the instruction of the certification request of the product Cryptographic Security Platform (CSP) | PKI Hub, Version 1.2, a positive resolution is proposed.

TOE SUMMARY

The TOE is a software component that reliably and efficiently verifies the status of digital certificates from one or multiple CAs and provides services for the generation of time-stamps.

The main functions of the TOE are to:

- Receive and process OCSP requests on the status of the digital certificates from external users or applications (requesters), protecting the integrity of the requests and responses when managed by the TOE.

- Generate OCSP responses including the date and status of the certificates.

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

- Guarantee the non-repudiation, integrity and authentication of the responses, by means of the digital signature of these responses.

- Generate the OCSP´s key pairs in an HSM and manage the certificates issued by the OCSP Certification Authority (CA).

- Store information on the status of the certificates generated by one or more Certification Authorities. The status of a digital certificate is updated by downloading the revocation lists or the information provided by Certification Authorities (CA).

- Generate event logs so operators can monitor the system status, its security and to what extent the corporate specifications are being met.

- It is able to receive via the Internet and process time-stamping requests from external users or applications (requesters) to add timestamps, protecting the integrity of the requests when managed by the TOE.

- Generate timestamp responses that include the time of the request and the information that securely binds the stamp to the data.

- The integrity of the time-stamps produced by the TOE is protected when created and managed by the TOE and during transfer from the TOE to an external entity.

- Generate the time-stamping units' key pairs in an HSM and managing the certificates issued by the timestamp Certification Authority (CA).

- Connect with external trusted time sources to detect time drifts or jumps out of synchronization with UTC.

- Any external entity can verify the authentication of the time-stamps produced by the TOE.

- The TOE services (user identity and role management, TSU initialization, start of TSU operation, stop of TSU operation, finalization of TSU operation, generation of key pair, public key export for certificate request, certificate import, timestamp token generation and internal audit) are only used in an authorized way.

- Send the auditing logs generated to a SIEM.

SECURITY ASSURANCE REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v2022 r1.

Requirement Class	Requirement Component
Security Target (ASE)	ST Introduction (ASE_INT.1)
	Conformance Claims (ASE_CCL.1)
	Security Objectives (ASE_OBJ.2)

	Extended Components Definition (ASE_ECD.1)
	Derived Security Requirements (ASE_REQ.2)
	Security Problem Definition (ASE_SPD.1)
	TOE Summary Specification (ASE_TSS.1)
Development (ADV)	Security Architecture Description (ADV_ARC.1)
	Complete functional specification (ADV_FSP.4)
	Implementation representation of the TSF (ADV_IMP.1)
	Basic modular design (ADV_TDS.3)
Guidance Documents (AGD)	Operational User Guidance (AGD_OPE.1)
	Preparative Procedures (AGD_PRE.1)
Lifecycle support (ALC)	Production support, acceptance procedures and automation (ALC_CMC.4)
	Problem tracking CM coverage (ALC_CMS.4)
	Delivery procedures (ALC_DEL.1)
	Identification of security measures (ALC_DVS.1)
	Developer defined life-cycle model (ALC_LCD.1)
	Well-defined development tools (ALC_TAT.1)
	Flaw Reporting Procedures (ALC_FLR.2)
Tests (ATE)	Independent Testing – sample (ATE_IND.2)
	Functional testing (ATE_FUN.1)
	Analysis of coverage (ATE_COV.2)
	Testing: basic design (ATE_DPT.1)
Vulnerability evaluation (AVA)	AVA_VAN.3 Focused vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v2022 r1.

Security requirement	FDP_ACC.1/Context_Management_Policy
	FDP_ACF.1/Context_Management_Policy
	FMT_MSA.3/Context_Management_Policy
	FMT_MSA.1/Context_Management_Policy
	FMT_MSA.1/Multiple_Policies

	FMT_SMF.1/Context_Management_Policy
	FDP_ITC.1/Context_Management_Policy
	FDP_ITC.2/Context_Management_Policy
	FDP_ETC.1/Non_Operational_Context_Public_Key
	FDP_ITC.2/ OCSP_And_Timestamp_unit_Certificate
	FPT_TDC.1/OCSP_Unit_Certificate
	FPT_TDC.1/Timestamping_Unit_Certificate
	FTP_TRP.1/ OCSP_And_Timestamping_Unit_Certificate
	FDP_IFC.1/Key_Management_Policy
	FDP_IFF.1/Key_Management_Policy
	FCS_CKM.1
	FCS_CKM.6
	FCS_CKM.3
	FCS_RNG.1
	FMT_MSA.3/Date_and_Time
	FMT_MSA.1/Date_and_Time
	FMT_SMF.1/Date_and_Time
	FMT_MTD.1/Date_and_Time
	FDP_ITC.1/Date_and_Time
	FMT_SMF.1/Temporary_Interruption
	FDP_ACC.1/OCSP_Response_Generation_Policy
	FDP_ACF.1/OCSP_Response_Generation_Policy
	FDP_OCSP_EXT.1.1
	FDP_ACC.1/Timestamp_Token_Generation_Policy
	FDP_ACF.1/Timestamp_Token_Generation_Policy
	FDP_TST_EXT.1.1
	FCS_COP.1
	FMT_SMR.1
	FIA_UID.2
	FIA_UAU.2
	FAU_GEN.1
	FAU_SAR.1
	FAU_SAR.3
	FPT_STM.1
	FAU_STG.4
	FAU_STG.2
	FCS_TLSC_EXT.1/TLS communications with the Database
	FCS_TLSC_EXT.1/TLS communications with the CA Gateway

	FCS_TLSC_EXT.1/TLS communications with the External Audit Server
	FCS_TLSS_EXT.1/TLS communications with the Auditor
	FTP_ITC.1/Trusted channel with the HSM
	FTP_ITC.1/Trusted channel with the Database
	FTP_ITC.1/Trusted channel with the CA Gateway
	FTP_ITC.1/Trusted channel with the External Audit Server

IDENTIFICATION

Product: Cryptographic Security Platform (CSP) | PKI Hub, Version 1.2

Security Target: Security Target – Cryptographic Security Platform (CSP), version 1.8

Evaluation Level: Common Criteria version 2022 release 1. EAL 4 + ALC_FLR.2

SECURITY POLICIES

The use of the product Cryptographic Security Platform (CSP) | PKI Hub, Version 1.2 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target, section 3.3 ("Organizational Security Policies").

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The detail of these assumptions is documented in the Security Target, section 3.4 ("Assumptions").

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Cryptographic Security Platform (CSP) | PKI Hub, Version 1.2, although the agents implementing attacks have the attack potential according to the ENHANCED BASIC of EAL4 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are those defined in the Security Target, section 3.2 (“Threats”).

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 4.2 (“Security Objectives for the operational Environment”).

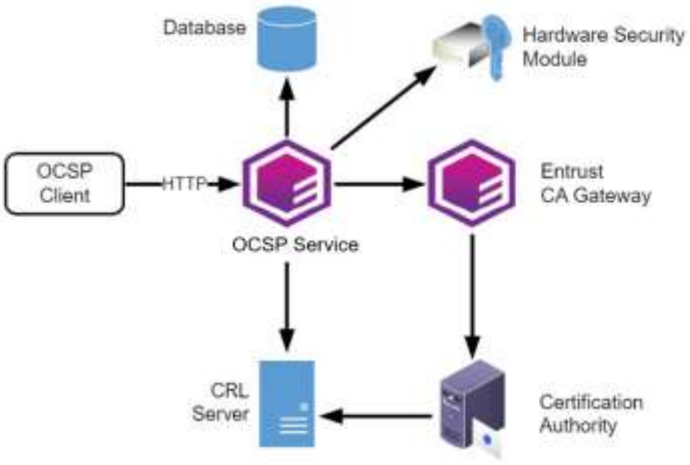
ARCHITECTURE

LOGICAL SCOPE

The TOE Entrust Cryptographic Security Platform (CSP) | PKI Hub (hereafter, PKI Hub) is a software component running on an operating system that provides OCSP and time-stamps generation services to its requesters. Hardware and other software components that might be needed by the TOE to provide its services are considered part of the TOE operational environment. The TOE shall use a Hardware Secure Module (HSM) for the implementation of the cryptographic operations.

PHYSICAL SCOPE

The below figure illustrates the general architecture of the OCSP service and how it interrelates with the network components (under the IETF RFC 6960 OCSP protocol). Entrust PKI Hub operates with external HSMs and requires connecting with one or more external NTP (Network Time Protocol) servers. External Certification Authorities provide OCSP certificates operated by Entrust PKI Hub.



To respond to OCSP requests, Entrust PKI Hub connects with different components. In this architecture:

- Multiple clients (users/applications) send requests to the validation service of Entrust PKI Hub.
- An OCSP request manager that handles the exchanges with the requesters, handling OCSP requests and providing corresponding OCSP responses.
- A Hardware Security Module (HSM) manages the OCSP signing key.
- A Database Management System (DBMS) hosts the certification information.
- An external Certification Authority (CA) issues a PKI certification from a Certificate Signing Request (CSR) of the OCSP service of the Entrust PKI Hub unit.
- An internal CertStatus feeder service API that offers an HTTP API to store information in the DBMS about the certificate issued and revoked by external CAs.
- When the TOE uses CRLs to get certification information, the CRL Server (HTTP/LDAP) provides certificate status information.
- A CRL Shim TOE; It's a background task in charge of periodically polling the CRL Server (HTTP/LDAP) to retrieve an updated CRL (and optionally a Serial Number list) and convert them into calls to the Cert Status Feeder.
- When the TOE uses CAs to get certification information, the Entrust CA Gateway provides certificate status information.
- A CA Gateway Shim. It's a background task in charge of periodically polling an Entrust CA Gateway to ask for certificate events (cert issuance and cert status changes) and convert them into calls to the Cert Status Feeder.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- [ST18] Security Target – Cryptographic Security Platform (CSP), version 1.8. October 2025

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

The independent testing approach has been testing all the SFRs declared in the Security Target, all the TSFIs declared in the Functional Specification and all the subsystems declared in the TOE Design. On the other hand, the vulnerability analysis approach has been based in:

- Search of public vulnerabilities for the TOE components and the third-party libraries used by the TOE.
- Exploitation of potential vector path found by the evaluator

Based on the vulnerabilities found, the evaluator calculated the attack potential and designed a test for each vulnerability with ENHANCED-BASIC attack potential.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product Cryptographic Security Platform (CSP) | PKI Hub, Version 1.2, the evaluated configuration is shown in Figure 1 - Evaluated Configuration and consists of the TOE, the microprocessor and the Host hardware.

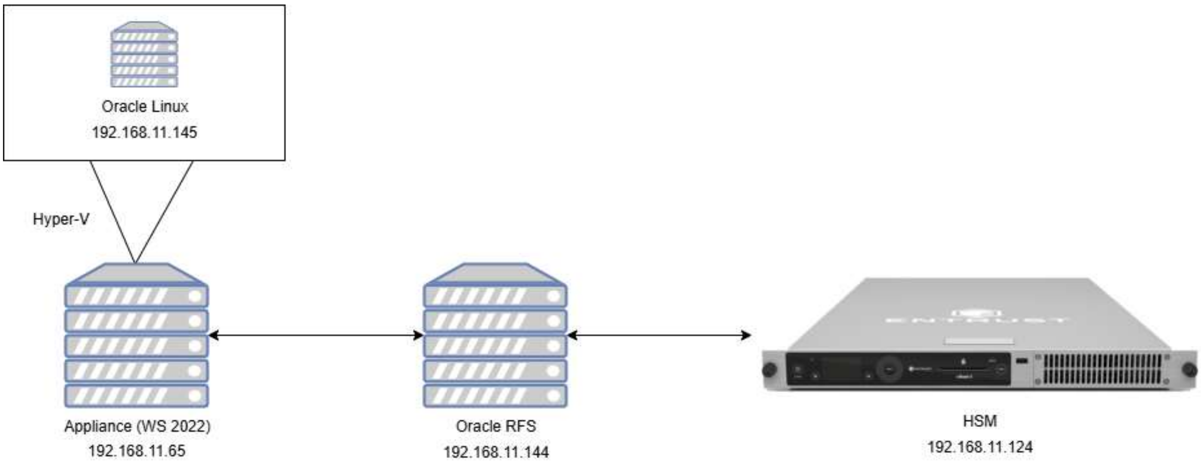


Figure 1. Evaluated Configuration

Based on the previous diagram, the components of the testing environment are the following:

- **Appliance:** A machine with Windows Server 2022 which using Hyper-V virtualized an Oracle Linux where is installed the TOE.
- **HSM (nCipher nShield 5s)** the TOE relies on the cryptographic module for cryptographic functionality and random number generation
- **Oracle RFS:** A machine with Oracle Linux Server release 9.4 which permit the communication between the TOE and the HSM.

All tests are performed in the Oracle Linux virtualized. No extra tools are needed to perform the tests cases.

EVALUATION RESULTS

The product Cryptographic Security Platform (CSP) | PKI Hub (hereafter, PKI Hub) version 1.2 has been evaluated against the Security Target - Cryptographic Security Platform (CSP), version 1.8. October 7, 2025.

All the assurance components defined in the Security Target and in Common Criteria version 2022 revision 1, and have been assigned a “PASS” verdict. Consequently, the laboratory DEKRA Testing and Certification, S.A.U. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the assurances packages defined, according to the Common Criteria v2022, revision 1.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

The TOE user must read and understand the user guides in order to operate the TOE properly in accordance with the Security Target.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Cryptographic Security Platform (CSP) | PKI Hub, Version 1.2, a positive resolution is proposed.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target of Evaluation
ST	Security Target
OE	Operational Environment

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC2022p1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model Revision 1, November 2022.

[CC2022p2] Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components Revision 1, November 2022.

[CC2022p3] Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components Revision 1, November 2022.

[CC2022p4] Common Criteria for Information Technology Security Evaluation. Part 4: Framework for the specification of evaluation methods and activities Revision 1, November 2022.

[CC2022p5] Common Criteria for Information Technology Security Evaluation. Part 5: Pre-defined packages of security requirements Revision 1, November 2022.

[CEM2022] Common Criteria for Information Technology Security Evaluation. Evaluation Methodology Version 2022 Revision 1, November 2022.

[CCAdd] CC and CEM addenda. Exact Conformance, Selection-Based SFRs, Optional SFRs, version 0.5, May 2017.

[ST18] Security Target - Cryptographic Security Platform (CSP), version 1.8. October 7, 2025.

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for assurance components up to EAL4.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.