Reference: 2020-3-INF-3845- v1
Target: Pública
Date: 14.07.2022

Created by: CERT10
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2020-3**
TOE	**Entrust SAM, version 1.0.3**
Applicant	**B81188047 - Entrust EU, S.L.**
References	

[EXT-5758] Certification request

[EXT-7702] Evaluation technical report

Certification report of the product Entrust SAM, version 1.0.3, as requested in [EXT-5758] dated 20/01/2020, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-7702] received on 20/04/2022.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Entrust SAM, version 1.0.3.

Entrust Signature Activation Module (SAM) is part of the architecture of a Trustworthy System Supporting Server Signing (TW4S). It integrates with a Server Signing Application (SSA) product to provide remote signing/sealing functionality to client applications via APIs or services operated by a TSP (Trust Service Provider).

Entrust Signature Activation Module is a software component that interacts with the Cryptographic Module (CM) in order to implement a Signature Activation Module (SAM) according to the European Standard [CEN EN 419 241-2].

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.

Protection Profile: Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing Protection Profile, version 0.16, May 11, 2018, European Committee for Standardization (CEN) TC 224.

Evaluation Level: Common Criteria version 3.1 release 5 - EAL4+ (ALC_FLR.2, AVA_VAN.5).

Evaluation end date: 01/06/2022

Expiration Date[1]: 12/07/2027

All the assurance components required by the evaluation level EAL4 (augmented with ALC_FLR.2 and AVA_VAN.5) 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 Common Criteria version 3.1 release 5 and the Common Criteria Evaluation Methodology version 3.1 release 5.

Considering the obtained evidences during the instruction of the certification request of the product Entrust SAM, version 1.0.3, a positive resolution is proposed.

[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.

TOE SUMMARY

Entrust Signature Activation Module is a software component that interacts with the Cryptographic Module (CM) in order to implement a Signature Activation Module (SAM) according to the European Standard [CEN EN 419 241-2]. The main objective of the Entrust Signature Activation Module component is to ensure the signer the sole control of their signing keys, which is carried out authorizing the signature operation. The SAM activates the signing key within a CM, handling a Signature Activation Protocol (SAP) which requires that Signature Activation Data (SAD) be provided at the local environment. The SAD binds together the signer authentication with the signing key and the data to be signed. The SAM component uses the SAD in order to guarantee with a high level of confidence -SCAL 2- that the signing keys are used under sole control of the signer.

SCAL 2 also requires the signing keys and the software of the SAM are protected by a tamper-protected environment. Entrust Signature Activation Module component uses a dedicated tamper protected environment according to the requirements of [CEN EN 419 241-2] standard.

Entrust Signature Activation Module has been designed and conforms to the European Standard [CEN EN 419 241-2] which is aimed to meet (together with the CM) the requirements of a QSCD as specified in Regulation (EU) No 910/2014 [eIDAS].

The major security features of the TOE are the following:

- Identification and authentication of TOE users.
- Secure creation of TOE users.
- Signer Key Pair generation and deletion.
- Supply DTBS/R.
- Signing/Sealing.
- Secure Audit.
- Secure communication between the TOE and the SSA.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4 and the evidences required by the additional components ALC_FLR.2 and AVA_VAN.5, according to Common Criteria version 3.1 release 5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2

	ASE_SPD.1
	ASE.TSS.1
ADV	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1
	ADV_TDS.3
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.1
	ALC_LCD.1
	ALC_TAT.1
	ALC_FLR.2
ATE	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.5

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria version 3.1 release 5:

SECURITY FUNCTIONAL REQUIREMENT
FAU_GEN.1
FAU_GEN.2
FCS_CKM.1/RSA
FCS_CKM.1/EC based DSA
FCS_CKM.1/AES
FCS_CKM.4
FCS_COP.1/Digital signature generation and verification
FCS_COP.1/Encryption and decryption
FCS_COP.1/Message digest
FCS_COP.1/Message authentication
FCS_RNG.1
FDP_ACC.1/Privileged User Creation
FDP_ACF.1/Privileged User Creation
FDP_ACC.1/Signer Creation
FDP_ACF.1/Signer Creation
FDP_ACC.1/Signer Maintenance

FDP_ACF.1/Signer Maintenance
FDP_ACC.1/Signer Key Pair Generation
FDP_ACF.1/Signer Key Pair Generation
FDP_ACC.1/Signer Key Pair Deletion
FDP_ACF.1/Signer Key Pair Deletion
FDP_ACC.1/Supply DTBS/R
FDP_ACF.1/Supply DTBS/R
FDP_ACC.1/Signing
FDP_ACF.1/Signing
FDP_ACC.1/TOE Maintenance
FDP_ACF.1/TOE Maintenance
FDP_ETC.2/Signer
FDP_IFC.1/Signer
FDP_IFF.1/Signer
FDP_ETC.2/ Privileged User
FDP_IFC.1/Privileged User
FDP_IFF.1/Privileged User
FDP_ITC.2/Signer
FDP_ITC.2/Privileged User
FDP_UCT.1
FDP_UIT.1
FIA_ATD.1
FIA_UAU.1
FIA_UAU.5/Signer
FIA_UAU.5/Privileged User
FIA_UID.2
FIA_USB.1
FMT_MSA.1/Signer
FMT_MSA.1/Privileged User
FMT_MSA.2
FMT_MSA.3/Signer
FMT_MSA.3/Privileged User
FMT_MTD.1
FMT_SMF.1
FMT_SMR.2
FPT_PHP.1
FPT_PHP.3
FPT_RPL.1
FPT_STM.1
FPT_TDC.1
FTP_TRP.1/SSA
FTP_TRP.1/SIC
FTP_ITC.1/CM

IDENTIFICATION

Product: Entrust SAM, version 1.0.3

Security Target: Security Target – Entrust Signature Activation Module version 2.1.

Protection Profile: Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing Protection Profile, version 0.16, May 11, 2018, European Committee for Standardization (CEN) TC 224.

Evaluation Level: Common Criteria version 3.1 release 5 – EAL4+ (ALC_FLR.2, AVA_VAN.5).

SECURITY POLICIES

The use of the product Entrust SAM, version 1.0.3 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 3.5 ("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 3.3 ("Secure Usage Assumptions").

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Entrust SAM, version 1.0.3, although the agents implementing attacks have the attack potential according to the high attack potential of EAL4+ (ALC_FLR.2, AVA_VAN.5) 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 3.4 ("Threats").

OPERATIONAL ENVIRONMENT FUNCTIONALITY

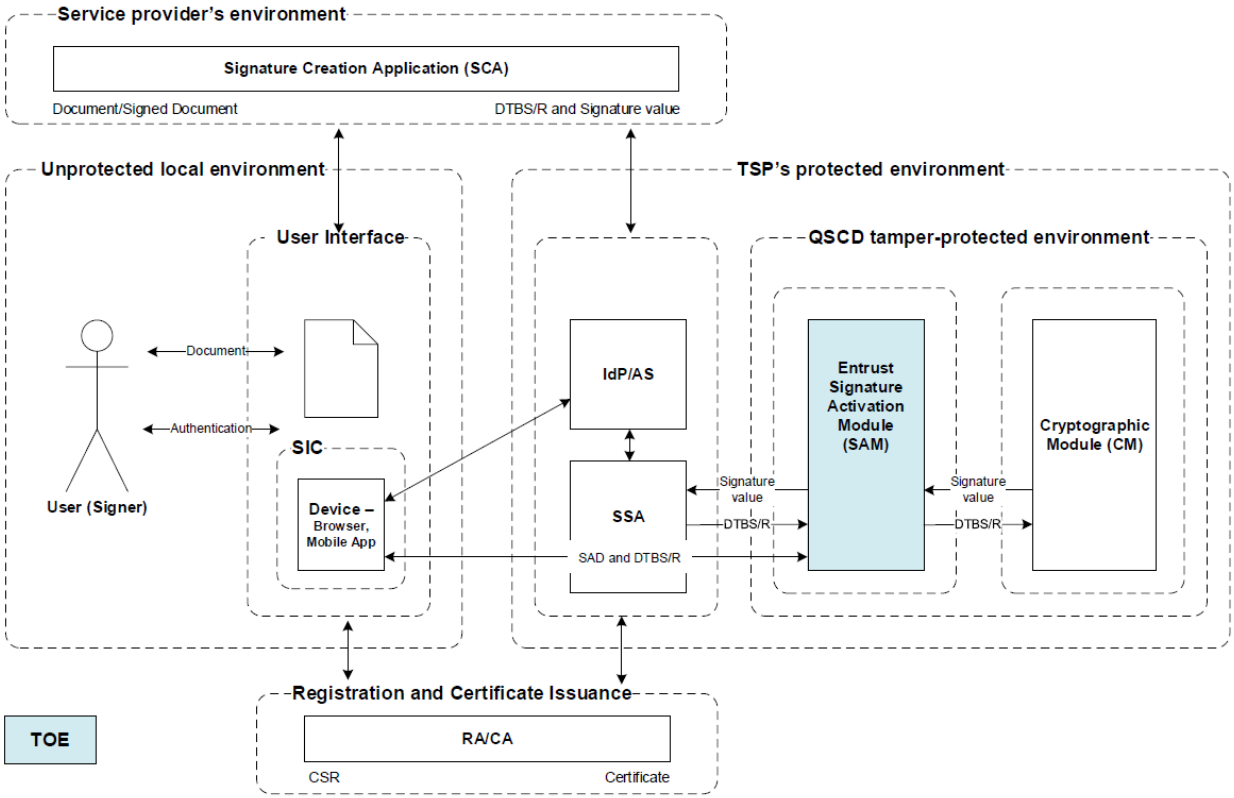
The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

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 ARCHITECTURE

The Entrust Signature Activation Module (SAM) software component is the TOE, which implements the Signature Activation Protocol (SAP) to obtain user Signature Activation Data (SAD). The TOE uses the SAD from the signer to activate the corresponding signing key for use in a Cryptographic Module (CM). The TOE uses a Cryptographic Module certified according the Protection Profile [CEN EN 419 221-5], as mandates the standard [CEN EN 419 241-2]. The TOE and the Cryptographic Module are a QSCD as specified in [eIDAS] Regulation.



PHYSICAL ARCHITECTURE

The TOE is a software composed of several components that is supplied in the file Entrust SAM 1.0.3.zip.

File	SHA-256
Entrust SAM 1.0.3.zip	4BE3403826BEB1A31154CD7E77424205C9497B32183DF0159FC941AD92DDCD54

This file has the following resources necessary to provide the functionality indicated in the Logical scope of the TOE section:

- Folder “bin”. Binary files in format ELF 64-bit LSB executable, x86-64 GNU/Linux, with the software component Entrust Signature Activation Module, the server component which provides the API (sam file) and the tool which provides the administration procedures (admin file).
- Folder “doc”. Documentation files in which the installation, configuration and operation of the software component are described. The TOE documentation is distributed in two languages: Spanish (folder “es”) and English (folder “en”). Inside these folders is folder “ENTRUST_SAM”, where there are several HTML resources corresponding to documentation referenced as ENTRUST_SAM and version 1.0.3.

DOCUMENTS

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

All the documents and guides are distributed in the Entrust SAM 1.0.3.zip:

- Folder “doc”. Documentation files in which the installation, configuration and operation of the software component are described. The TOE documentation is distributed in two languages: Spanish (folder “es”) and English (folder “en”). Inside these folders is folder “ENTRUST_SAM”, where there are several HTML resources corresponding to documentation referenced as ENTRUST_SAM and version 1.0.3.

PRODUCT TESTING

The main objective of the tests performed by the evaluator is to check that the security functional requirements stated in the Security Target [ST] are implemented as expected, that the subsystems defined behave as expected and the only accessible TSFI is consistent with the TOE.

The evaluator has designed an independent testing plan that is focused on the tests performance about the security functional requirements stated in the Security Target [ST].

The main objective of the tests performed by the evaluator is to check that the security functional requirements defined in the security target are implemented as expected.

The evaluator has designed a set of tests following a suitable strategy for the TOE type taking into account:

1. All SFRs have been tested whether through TSFI excitation or subsystem checking.
2. The testing criteria of the only accessible TSFI is based on:
    - Developer tests rigor.
    - Developer test results including the Web interface and subsystems which tests results are not reliable.
    - Importance of the accessible TSFIs and subsystems.
    - Types of subsystems.
    - Number of subsystems.

In order to create adequate tests, the evaluator has chosen the following criteria: search for critical SFRs and parameters in the TSFI and subsystems, requirements implemented by the only accessible TSFI, exhaustive tests over it and subsystems, incorrect behaviour suspicion with specific input values and the performance of testing every subsystem.

Moreover, the evaluator has carried out tests with the instructions provided for the only accessible TSFI and all subsystems that could have special importance in the maintenance of the TOE security. The evaluator has designed the independent test cases including all the security requirements defined in the Security Target [ST].

The evaluator testing plan is SFR oriented, and the functionality of each SFR included at the Security Target [ST] has been considered.

All the test cases have been performed using the connection between the local client machine and the REST and the Administration interfaces. This allow testing appropriately both the SFRs defined in the Security Target [ST] and the subsystems.

PENETRATION TESTING

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals. The TOE does NOT present exploitable vulnerabilities under the environment defined in the Security Target [ST]. All identified vulnerabilities can be considered closed if the TOE is installed and operated according to the Security Target [ST] and related documentation. The overall test result is that no deviations were found between the expected and the actual test results taking into account that environment. No attack scenario with the attack potential “High” has been successful in the TOE’s operational environment as defined in the Security Target [ST] when all measures required by the developer are applied.

EVALUATED CONFIGURATION

The TOE configuration used to execute the independent testing plan is consistent with the evaluated configuration according to Security Target [ST] and the installation and operation manual provided in the "doc" folder in Entrust SAM 1.0.3.zip.

EVALUATION RESULTS

The product Entrust SAM, version 1.0.3 has been evaluated against the Security Target: Security Target – Entrust Signature Activation Module version 2.1.

All the assurance components required by the evaluation level EAL4+ 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 evaluation level EAL4+ (ALC_FLR.2, AVA_VAN.5), as defined by the Common Criteria version 3.1 release 5 and the Common Criteria Evaluation Methodology version 3.1 release 5.

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.

- It is mandatory to strictly follow the steps indicated in the installation documentation in order to download and install the correct version of the TOE in a proper manner.
- The user guidance must be read and understood in order to operate the TOE in an adequate manner according to the security target.

COMMENTS & RECOMMENDATIONS FROM THE CERTIFIER

Considering the obtained evidences during the instruction of the certification request of the product Entrust SAM, version 1.0.3, a positive resolution is proposed.

- The user must follow the "Operational Environment Security Measures", provided in the guidance "ENTRUST_SAM version 1.0.3", to meet the security objectives of the operating environment described in [ST].

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

BIBLIOGRAPHY

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

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[CEN EN 419 241-2] CEN EN 419 241-2 Trustworthy Systems Supporting Server Signing; Part 2: Protection Profile for QSCD for Server Signing.

[CEN EN 419 221-5] CEN EN 419 221-5 Protection Profiles for TSP Cryptographic Modules; Part 5 - Cryptographic Module for Trust Services.

[eIDAS] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[ST] Security Target – Entrust Signature Activation Module version 2.1

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- Security Target – Entrust Signature Activation Module version 2.1.

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 all assurance components selected.

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.