Reference: 2024-19-INF-4579- v1
Target: Limitada al expediente
Date: 29.07.2025

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

CERTIFICATION REPORT

Dossier #	**2024-19**
TOE	**SENTRY Secured RX and Secured TX Devices 1.0**
Applicant	**401 321 856 00031 - SENTRY**
References	
	[EXT-9085] 2024-06-06_2024_19_solicitud_certificacion
	[EXT-9583] 2025-05-16_2024-19_ETR_v1.1

Certification report of the product SENTRY Secured RX and Secured TX Devices 1.0, as requested in [EXT-9085] dated 23/04/2024, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-9583] received on 12/05/2025.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product SENTRY Secured RX and Secured TX Devices 1.0.

The TOE is a hardware TOE comprised of two devices, the SENTRY Secured RX and Secured TX v1.0, that act as a data diode for audio/video signals between a source device and output device. The TOE is a subset of the SENTRY Secure Video Wall solution, which provides the capability to remove data channels from the video signal, enforcing a one-way video and audio channel to the Video Wall.

Developer/manufacturer: SENTRY

Sponsor: SENTRY.

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

ITSEF: DEKRA Testing and Certification S.A.U..

Protection Profile: N/A.

Evaluation Level: Common Criteria for Information Technology Security Evaluation, CC:2022, Revision 1, November 2022, EAL2.

Evaluation end date: 25/06/2025

Expiration Date[1]: 22/07/2030

All the assurance components required by the evaluation level EAL2 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 EAL2, as defined by the CC:2022 r1 and the CEM:2022.

Considering the obtained evidences during the instruction of the certification request of the product SENTRY Secured RX and Secured TX Devices 1.0, 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

The TOE is comprised of two hardware devices: The Sentry Secured TX (STX) - a video/audio encoder device, and the Sentry Secured RX (SRX) – a video/audio decoder device. The STX and SRX are configured in sequence between the source device and a secure display output.

The SENTRY SRX & STX is a display adapter with an HDMI-in port, HDMI-out loopout port, one-way optical fiber port, and a 12V power connector. The STX device is the main device transforming HDMI digital signals into optical signals transferred via optical fiber. It includes an HDMI loopout port (to provide a local copy of the video source displayed), an EDID emulator that forces signal resolution to avoid communication errors with the final display, and a HDMI to Optical Fiber transceiver.

The SENTRY SRX is a display adapter with an optical fiber-in port, an HDMI-out port, and a 12v power connector. The SRX transforms optical signal back into HDMI digital signals.

The TOE major security feature is protection of data through enforcement of a one-way data stream at the hardware level, by physically removing all unessential data streams, and emulating a clean signal in order to ensure compatibility.

The TOE enforces a one-way video and audio data stream from the source device to a secure output display device, ensuring that only the video and audio channels are passed through, and no data can be passed back to the source device through the TOE, therefore protecting all other connected devices from unwanted communications.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2, according to Common Criteria 2022 R1.

ASSURANCE CLASS	ASSURANCE COMPONENT
ADV	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1

	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
ATE	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria 2022 R1:

Requirement Class	Requirement Component
User Data Protection (FDP)	IFC.2 Complete information Flow control
	IFF.1 Simple security attributes

IDENTIFICATION

Product: SENTRY Secured RX and Secured TX Devices 1.0

Security Target: SENTRY Secured RX and Secured TX v1.0 Security Target, version 0.5, 27/02/25.

Evaluation Level: Common Criteria 2022 R1 EAL2.

SECURITY POLICIES

The use of the product SENTRY Secured RX and Secured TX Devices 1.0 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 **3.2 "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 "Assumptions"**.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product SENTRY Secured RX and Secured TX Devices 1.0, although the agents implementing attacks have the attack potential according to the Basic of EAL2 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 **3.1 "Threats to Security"**.

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

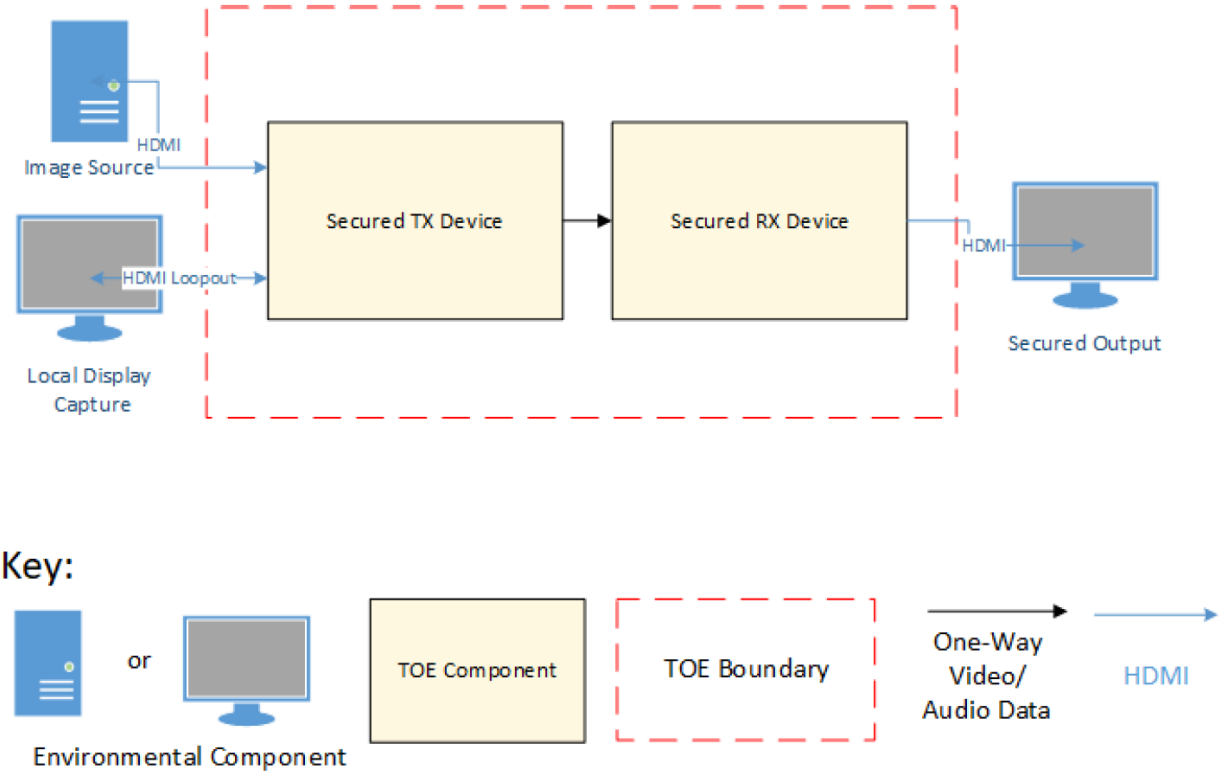
LOGICAL ARCHITECTURE

The fundamental security features of the TOE are summarized in:

- **User data protection:** The TOE enforces a one-way video and audio data stream from the source device to a secure output display device, ensuring that only the video and audio channels are passed through, and no data can be passed back to the source device through the TOE, therefore protecting all other connected devices from unwanted communications.

PHYSICAL SCOPE

The TOE is a hardware platform. The TOE is installed as depicted in the next figure.



The TOE is a hardware-only TOE and is comprised of the SRX & STX v1.0

Customers can verify that the TOE hardware they receive is from SENTRY rather than an imposter by confirming that the package is being delivered either through MOD (Ministry of Defense) agreed transport companies or in-person by SENTRY employees. SENTRY employees are identified by their company-issued badges.

With either delivery method, the TOE hardware is provided with tamper-evident labels. In the event the label appears to have been tampered with, SENTRY will declare the device unusable.

The following PDF-formatted guide, which is available for SENTRY customers with an active account to download through the SENTRY website, are required reading and part of the TOE:

The essential physical components for the proper operation of the TOE in the evaluated configuration are:

- SENTRY Secured RX and Secured TX Devices Guidance Supplement v0.5

DOCUMENTS

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

- SENTRY Secured RX and Secured TX Devices Guidance Supplement v0.5

PRODUCT TESTING

The developer has executed tests for all the TSFIs. 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 has been identified and 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.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests in the developer premises in the testing platform implemented in the evaluation facility.

In addition, the lab has devised a test for each of the TSFi of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The essential physical components for the proper operation of the TOE in the evaluated configuration are:

- Video/audio source device
- HDMI display (for local display loopout)
- HDMI display (for secure output)
- 3x HDMI cables
- 1x LC Optical Fiber cable

EVALUATION RESULTS

The product SENTRY Secured RX and Secured TX Devices 1.0 has been evaluated against the Security Target SENTRY Secured RX and Secured TX v1.0 Security Target, version 0.5, 27/02/25.

All the assurance components required by the evaluation level EAL2 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 EAL2, as defined by the CC:2022 r1 and the CEM:2022.

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 user guidance must be read and understood in order to operate the TOE in an adequate manner according to the security target.
- The fulfilment of the assumptions indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product SENTRY Secured RX and Secured TX Devices 1.0, a positive resolution is proposed.

GLOSSARY

Acronym	Definition
HDMI	High-Definition Multimedia Interface
TOE	Target of Evaluation

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. Version 2022, Revision 1

[CC2022p2]	Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components Version 2022, Revision 1
[CC2022p3]	Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components Version 2022, Revision 1
[CC2022p4]	Common Criteria for Information Technology Security Evaluation. Part 4: Framework for the specification of evaluation methods and activities Version 2022, Revision 1
[CC2022p5]	Common Criteria for Information Technology Security Evaluation. Pre-defined packages of security requirements Version 2022, Revision 1
[CEM2022]	Common Criteria for Information Technology Security Evaluation. Evaluation Methodology Version 2022 Revision 1
[CCAdd]	CC and CEM addenda. Exact Conformance, Selection-Based SFRs, Optional SFRs, version 0.5, May 2017.

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 selected.