Reference: 2021-46-INF-3919- v1
Target: Pública
Date: 01.03.2023

Created by: CERT9
Revised by: CALIDAD
Approved by: TECNICO

# CERTIFICATION REPORT

| | |
|---|---|
| Dossier # | **2021-46** |
| TOE | **NetMaster R21B00 - Build 1028** |
| Applicant | **512352444 - Ceragon Networks Ltd.** |
| References | |

[EXT-7969] ETR v2.0 NetMaster

Certification report of the product NetMaster R21B00 - Build 1028, as requested in [EXT-7175] dated 08/09/2021, and evaluated by jtsec Beyond IT Security, S.L., as detailed in the Evaluation Technical Report [EXT-7969] received on 14/09/2022.

**CONTENTS**

EXECUTIVE SUMMARY ..... 3
TOE SUMMARY ..... 4
SECURITY ASSURANCE REQUIREMENTS ..... 4
SECURITY FUNCTIONAL REQUIREMENTS ..... 5
IDENTIFICATION ..... 6
SECURITY POLICIES ..... 6
ASSUMPTIONS AND OPERATIONAL ENVIRONMENT ..... 6
CLARIFICATIONS ON NON-COVERED THREATS ..... 6
OPERATIONAL ENVIRONMENT FUNCTIONALITY ..... 7
ARCHITECTURE ..... 7
LOGICAL ARCHITECTURE ..... 7
PHYSICAL ARCHITECTURE ..... 8
DOCUMENTS ..... 8
PRODUCT TESTING ..... 9
EVALUATED CONFIGURATION ..... 9
EVALUATION RESULTS ..... 9
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM ..... 9
CERTIFIER RECOMMENDATIONS ..... 10
GLOSSARY ..... 10
BIBLIOGRAPHY ..... 10
SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE) ..... 10
RECOGNITION AGREEMENTS ..... 11
European Recognition of ITSEC/CC – Certificates (SOGIS-MRA) ..... 11
International Recognition of CC – Certificates (CCRA) ..... 11

# EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product NetMaster R21B00 - Build 1028.

The Target Of Evaluation (TOE) is a Network Management System developed by Ceragon Networks Ltd, and will hereafter be referred to as the TOE throughout this document. The TOE is a Network Management System offering centralized operation and maintenance capability for a range of network elements.

The TOE provides the following functionality:

- Security Audits.
- User Data Protection.
- Identification and Authentication.
- Security Management.
- TOE Access.
- Trusted path/channels.

**Developer/manufacturer**: Ceragon Networks Ltd.

**Sponsor**: Ceragon Networks Ltd..

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

**ITSEF**: jtsec Beyond IT Security, S.L.

**Evaluation Level**: EAL2

**Evaluation end date**: 15/09/2022.

**Expiration Date**[1]: 28/10/2027.

All the assurance components required by the evaluation level EAL2 have been assigned a “PASS” verdict. Consequently, the laboratory jtsec Beyond IT Security, S.L. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2, as defined by the “Common Criteria for Information Technology Security Evaluation” and the “Common Criteria for Information Technology Security Evaluation. Evaluation methodology, Version 3.1 Revision 5, April 2017”.

[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.

Considering the obtained evidences during the instruction of the certification request of the product NetMaster R21B00 - Build 1028, a positive resolution is proposed.

## *TOE SUMMARY*

The Target Of Evaluation (TOE) is a Network Management System developed by Ceragon Networks Ltd, and will hereafter be referred to as the TOE throughout this document. The TOE is a Network Management System offering centralized operation and maintenance capability for a range of network elements.

NetMaster offers complete range monitoring of all Ceragon and third-party network elements. NetMaster is designed for managing large-scale wireless backhaul networks.

The TOE provides the following functionality:

- Security Audits.
- User Data Protection.
- Identification and Authentication.
- Security Management.
- TOE Access.
- Trusted path/channels.

## *SECURITY ASSURANCE REQUIREMENTS*

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2, according to Common Criteria v3.1 R5.

| Assurance class | Assurance components |
|---|---|
| ASE | ASE_CCL.1<br>ASE_ECD.1<br>ASE_INT.1<br>ASE_TSS.1<br>ASE_OBJ.2<br>ASE_REQ.2<br>ASE_SPD.1 |
| ADV | ADV_TDS.1 |

| | |
|---|---|
| | ADV_ARC.1<br>ADV_FSP.2 |
| AGD | AGD_OPE.1<br>AGD_PRE.1 |
| ALC | ALC_CMC.2<br>ALC_CMS.2<br>ALC_DEL.1 |
| ATE | ATE_FUN.1<br>ATE_COV.1<br>ATE_IND.2 |
| AVA | AVA_VAN.2 |

## *SECURITY FUNCTIONAL REQUIREMENTS*

The product security functionality satisfies the following functional requirements, according to the [CC_P1], [CC_P2], [CC_P3] y [CEM].

| **SECURITY FUNCTIONAL REQUIREMENTS** |
|---|
| FAU_GEN.1 |
| FAU_GEN.2 |
| FAU_STG.1 |
| FIA_AFL.1 |
| FMT_SMF.1 |
| FMT_SMR.1 |
| FTA_SSL.3 |
| FTA_SSL.4 |
| FTP_ITC.1/HTTPS |
| FTP_ITC.1/SNMP |
| FDP_ACC.1 |

| |
|---|
| FDP_ACF.1 |
| FMT_MSA.1 |
| FMT_MSA.3 |
| FIA_UAU.2 |
| FIA_UID.2 |
| FAU_SAR.1 |

## IDENTIFICATION

**Product**: NetMaster R21B00 - Build 1028

**Security Target:** Ceragon NetMaster Security Target version 1.4

**Evaluation Level**: EAL2.

## SECURITY POLICIES

The use of the product NetMaster R21B00 - Build 1028 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 3.4 (“Organisational 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 3.5 (“Assumptions”).

### *CLARIFICATIONS ON NON-COVERED THREATS*

The following threats do not suppose a risk for the product NetMaster version R21B00 - Build 1028, although the agents implementing attacks have the attack potential according to the 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 3.2 (“Threats Agents”).

### *OPERATIONAL ENVIRONMENT FUNCTIONALITY*

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

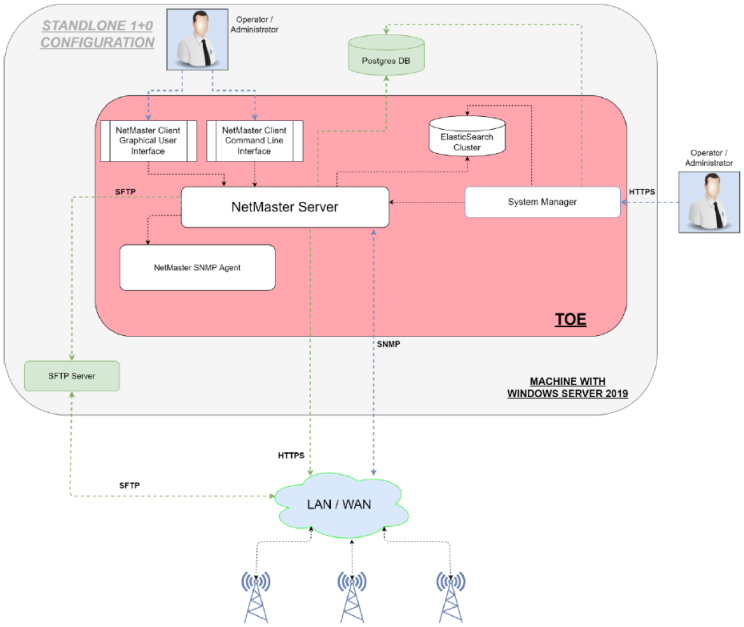
The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 4.2 (“Security objectives for the operational environment”).

## ARCHITECTURE

### *LOGICAL ARCHITECTURE*

The TOE is a Network Management System.

The [ST] in the logical scope section defines the scenario where the TOE is deployed. All within the red figure is considered to be part of the TOE and is installed on the same machine according to the standalone 1+0 configuration. Likewise, the database and the SFTP server are installed on the same device, even though there are part of the operational environment (not TOE).




### *PHYSICAL ARCHITECTURE*

The physical scope of the TOE is as described below:

- **NetMaster:** Depicted inside the red rectangle from the logical architecture diagram. Component is provided through an executable file (NetMaster_R21B00_1028_windows.exe) that installs the TOE.

## DOCUMENTS

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

- [AGD_PRE] Ceragon NetMaster Preparative Procedures version 0.6
- [AGD_OPE] Ceragon NetMaster Operational User Guidance version 0.5
- [ST] Ceragon NetMaster Security Target version 1.4
- NetMaster Installation Guide version R21B00 Rev A
- NetMaster Technical Description version R21B00 Rev A
- NetMaster User Guide version R21B00 Rev A


https://oc.ccn.cni.es
organismo.certificacion@cni.es

## PRODUCT TESTING

The tests performed by both the evaluator and the developer are based on the TSFIs description included in the functional specification and the SFRs description included in the Security Target [ST].

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 configuration used to execute the independent tests is consistent with the evaluated configuration according to the Security Target [ST].

The evaluator has repeated all the cases specified by the developer in the test documentation and has compared the obtained results with those obtained by the developer and documented in each associated report. The test repetition performed by the evaluator has demonstrated that the test plan and report provided by the vendor contains information enough to make a reader able to repeat all tests included. Additionally, after the repetition, the evaluator has obtained the same results as the expected ones. The independent testing has covered 100% of SFRs of the [ST] and TSFIs defined in the functional specification for the TOE, sampling has not been performed. The test cases have taken into account critical parameters values, searching that the TOE behaves in a nonexpected manner. There has not been any deviation from the expected results under the environment defined in the Security Target [ST].

## EVALUATED CONFIGURATION

The acceptance and installation procedures are given in section 2 (TOE Secure Acceptance) of the preparative user guidance [AGD_PRE] Ceragon NetMaster Preparative Procedures version 0.6.

## EVALUATION RESULTS

The product NetMaster version R21B00 - Build 1028 has been evaluated against the Security Target “Ceragon NetMaster Security Target version 1.4”.

All the assurance components required by the evaluation level EAL2 have been assigned a “PASS” verdict. Consequently, the laboratory jtsec Beyond IT Security, S.L. 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_P1], [CC_P2], [CC_P3] y [CEM].

## 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 use of the TOE is recommended as it has no exploitable vulnerabilities in its operational environment.

## CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product NetMaster R21B00 - Build 1028, 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 |

## 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.

## 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:

- Ceragon NetMaster Security Target version 1.4.

# 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.