Federal Office
for Information Security

# Certification Report

## BSI-DSZ-CC-1207-2025

for

## Check Point R82 for Gateway and Maestro Configurations, Version R82

from

## Check Point Software Technologies Ltd

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

# Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

**BSI-DSZ-CC-1207-2025** (*)

Firewall

**Check Point R82 for Gateway and Maestro Configurations**
Version R82

| | |
|---|---|
| from | Check Point Software Technologies Ltd |
| PP Conformance: | none |
| Functionality: | Product specific Security Target<br>Common Criteria Part 2 extended |
| Assurance: | Common Criteria Part 3 conformant<br>EAL 4 augmented by ALC_FLR.1 and AVA_VAN.4 |
| valid until: | 09. April 2030 |

SOGIS
Recognition Agreement
for components up to
EAL 4

Common Criteria

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 10 April 2025

For the Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Sandro Amendola L.S.
Director-General

**Bundesamt für Sicherheit in der Informationstechnik**
Godesberger Allee 87 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

# Contents

# A. Certification

## 1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

## 2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs [3]
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

2 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

3 BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

# 3. 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.

## 3.1. European Recognition of 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. 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 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 related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of SOGIS-MRA, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the component AVA_VAN.4 which is not mutually recognised in accordance with the provisions of the SOGIS MRA. For mutual recognition the EAL 4 component of this assurance family is relevant.

## 3.2. 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 current list of signatory nations and approved certification schemes can be seen on the website: https://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 related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

[4] Proclamation of the Bundesministerium des Innern und für Heimat of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2 and ALC_FLR components.

# 4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Check Point R82 for Gateway and Maestro Configurations, Version R82 has undergone the certification procedure at BSI.

The evaluation of the product Check Point R82 for Gateway and Maestro Configurations, Version R82 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 9 April 2025. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Check Point Software Technologies Ltd.

The product was developed by: Check Point Software Technologies Ltd.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

# 5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 10 April 2025 is valid until 9 April 2030. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

# 6. Publication

The product Check Point R82 for Gateway and Maestro Configurations, Version R82 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Check Point Software Technologies Ltd
Shlomo Kaplan St 5, 6789159
Tel Aviv-Yafo
Israel

# B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

# 1. Executive Summary

The Target of Evaluation (TOE) is a combination of the firmware for Security Gateway Module(s), a Security Management Server and (when deployed in Scalable Platform configuration) the firmware for the Maestro Orchestrator appliance(s):

- The Security Gateway Module (SGM) is a managed packet filtering firewall application, with IPS pattern matching (software) blade. The TOE provides controlled connectivity between two or more network environments. It mediates information flows between clients and servers located on internal and external networks governed by the firewalls. The SGM can either be deployed using instances of a single Security Gateway appliance, which incorporates the SGM or a combination of Security Gateway Modules (SGM) operating in a cluster as part of a Scalable Platform (SP).
- The Security Management Server is used to manage and deploy the security policies and rules to SGM.
- When operating as part of a Scalable Platform (SP), the Orchestrator appliance provides load balancing services for the SGMs.

The Security Management Server is located on a logically protected LAN behind the firewall in single deployment mode, and behind the load-balancing Orchestrator in Scalable deployment mode. All management traffic is communicated between TOE components over secured channels provided by the TOE.

The purpose of the firewall blade is to protect the assets operating on a customer's network from malicious attempts to control or gain access to those assets. The IPS pattern matching blade provides protection against signatures defining malicious and unwanted network traffic, focusing on application and server vulnerabilities, as well as in-the-wild attacks by exploit kits and malicious attackers. The firewall filtering rules, and IPS rules are defined, managed and deployed by the Security Management Server. When in Scalable Deployment, the Orchestrator appliance(s) provide load-balancing across the gateway resources.

Security Gateway Modules or one or more Security Gateway appliances are managed by a Security Management server installation (includes GAiA operating system and Security Management application). The Security Management server maintains security policy information for the gateways, and collects audit records from the gateways for review by Security Management Server administrator. The audit records may also be sent to an external log server (which in the evaluated configuration must be hosted on the logically protected dedicated management LAN hosted behind the firewall).

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.1 and AVA_VAN.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

| TOE Security Functionality | Addressed issue |
|---|---|
| Security audit | The SGM and Management Server generate audit logs of security events. GaiA generates OS-related security events on both the SGM and the Management Server. The SGM kernel is responsible for generating the traffic logs and a Security Management process is responsible for generating security management audit logs. |
| Packet filtering and stateful traffic filtering firewall | If the TOE is configured as a Scalable Platform the Orchestrator appliance(s) will distribute the traffic to the appropriate SGM according to the distribution algorithm on the Orchestrator appliance. This all happens within the TOE environment, before the traffic is forwarded to the TOE. No traffic inspection is performed by the Orchestrator appliance. Every IPv4 packet received by the Check Point Security SGM is intercepted by the firewall kernel. Fragmented packets are first reassembled. IPv4 packets with unauthorized IP options (e.g. source route option) are dropped. |
| Intrusion Prevention Systems | Network traffic that passes through the firewall and IPS security policies is compared with signatures encoded as regular expressions, keywords, and INSPECT language code. The signatures database can be manually updated by the Security Management Server administrator. |
| Identification and authentication | The TOE provides a password mechanism for authenticating users to the Management Server. Users are associated with a username, password, and one or more roles. Users may authenticate to the Management Server locally or via the web interface. |
| Security management | User accounts on the Management Server are associated with the profile “read write all”. User accounts associated with this profile are called Security Management Server administrators. |
| TOE access | The TOE provides an inactivity timeout for Check Point REST API sessions to the Management Server and (when in SP deployment) to Orchestrator. |
| Protection of the TSF | Each TOE component (SGM, Security Management Server and – when in SP deployment – Orchestrator) provides a system clock. During installation the TOE is configured to synchronize its clock with a time server. |

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions and Threats. This is outlined in the Security Target [6], chapters 3.2 and 3.4, respectively.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

# 2. Identification of the TOE

The Target of Evaluation (TOE) is called:

**Check Point R82 for Gateway and Maestro Configurations,** Version R82

The following table outlines the TOE deliverables:

| No | Type | Identifier | Release | Form of Delivery |
|---|---|---|---|---|
| 1 | SW | Security Gateway or Management Server | R82 | Download |
| 2 | SW | Scalable Platform (Maestro) Gateway and Maestro Hyperscale Orchestrator | R82 | Download |
| 3 | SW | QLS Security Gateway | R82 | Download |
| 4 | SW | MLS Security Gateway | R82 | Download |
| 5 | DOC | R82 CC Firmware for Gateway and Maestro Configurations, Installation and Configuration, BSI Administration Guide | Rev 008, 2025-03-03 | Download |

Table 2: Deliverables of the TOE

The TOE is delivered to customers from the Check Point User Center (https://usercenter.checkpoint.com) by user download. The TOE guidance is provided via a SecureKnowlege SK entry – SK181211. A User Center account is required in order to download the TOE. If a user does not possess a User Center account, then one can be created.

The hash values are provided on the download page. Once the TOE files have been downloaded, they can be verified by the user with the aid of standard hash utilities.

Items 1 to 4 in table 2 are part of one ISO image with the following SHA-256 Hash:
71d71b33f1f5b64e4ee9c93bb00d4d0d5c512c577ff8181d5e836c314dfabd65

Item 5 is a PDF file with SHA-256 Hash:
3518b7fc4273a16d60cdb4dedb95e07d41d20386ab40f18956f8811c92bc9ce9

# 3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Security Audit,
- Packet Filtering and Stateful Traffic Filtering Firewall,
- Intrusion Prevention Systems,
- Identification and Authentication,
- Security Management,
- Protection of the TSF,
- TOE Access.

Specific details concerning the above mentioned security policies can be found in the Security Target [6], Chapters 6 and 7.

# 4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- OE.Physical: Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment to TOE components.
- OE.NO_GENERAL_PURPOSE: There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the hardware components on which the TOE executes, other than those services necessary for the operation, administration, and support of the TOE.
- OE.TRUSTED_ADMIN: TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
- OE.CONNECTIONS: TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic of monitored networks.
- OE.LOCAL_NETWORK: Log servers (and also NTP and syslog log servers in the case of single gateway deployment) are connected to the same dedicated management LAN as the Management Server appliance.

Details can be found in the Security Target [6], chapter 4.2.

# 5. Architectural Information

The TOE consists of the following subsystems:

- The Management Server handles policy, log, alert and system status data flows. In handling the policy data flow, it receives policy data entered via the Check Point Management API by the TOE administrator, and processes (compiles), stores and distributes it to the Security Gateway.
- The Gateway, either as a single Gateway or – when in Scalable Platform deployment – as multiple Security Gateway Modules (SGMs), is the policy enforcement point for traffic flowing through the TOE. Traffic filtering is performed by kernel-level code to ensure maximum performance. User-level components perform write-to-file duties, log handling, inter-host communication and management.
- When in Scalable Platform deployment, Maestro Hyperscale Orchestrator (MHO) is used to administer the Security Groups and automatically distributes user network traffic between the Security Appliances (Maestro SGMs) assigned to Security Groups for inspection. The Orchestrator appliance acts as a load-balancing device for the distribution of user network traffic to an appropriate SGM, which will scan the traffic according to the configured traffic filtering policies (the same traffic filtering policies are deployed to, and applied by, all SGMs).

# 6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

# 7. IT Product Testing

The TOE was tested in multiple set-ups, as a single gateway appliance and as part of a Scalable Platform deployment. The tests of the TOE as outlined in table 2 and in the Security Target [6] in Chapter 1.4 were run on several hardware platforms, by the developer and the evaluators, as described in the following sections.

## 7.1. Developer Testing

The developer used automatic and manual testing, as well as positive and negative testing. For manual tests the Check Point Management API Interface commands are initiated. The developer used a framework where the tests are executed in scenarios, with or without dependencies between tests, according to requirements. Each scenario execution generated a detailed report, where each test and its steps are detailed in the execution report with a clear Pass / Fail status. The developer provided his test concept for testing also to the ITSEF. He also provided the required hardware and software to enable the evaluation facility to repeat at least a subset of his testing.

The tested scenarios include the following appliances:

- Security Gateway environment consisting of:
  - Management Server 600-S
  - Security Gateway 19200
  - SMB 3600
  - Security Gateway 19100
  - Security Gateway 9300
- Scalable Platform environment consisting of:
  - Management Server 600-S
  - Security Gateway 19200
  - Maestro Hyperscale Orchestrator 175
  - Maestro Hyperscale Gateway 9400 (2 times)

## 7.2. Independent Testing

The Evaluator devised several additional tests. Those tests were run under full control and at the premises of the ITSEFs. The following hardware is used in the independent testing scenario:

- Maestro Hyperscaler Gateway 9700
- Security Gateway 19200

- Smart-1 Security Management Server 600-S
- Maestro Hyperscaler Orchestrator 175

During the evaluator's testing the TOE operated as specified. Furthermore, the evaluator verified the developer's test results by executing a subset of the developer's tests.

### 7.3. Penetration Testing

The penetration testing was performed using the developer's testing environment, partially using the test environment of the ITSEF. All configurations of the TOE being intended to be covered by the current evaluation were tested.

The penetration tests were devised to consider the following attack scenarios: Bypassing connection, fragmentation handling, cloning cleanup rule, malformed firewall policy, changed policies, ARP spoofing, bypass the rule base or anti spoofing controls, misuse of security zones, SQL injection, undefined protocols or types.

The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential Moderate was actually successful.

## 8. Evaluated Configuration

This certification covers the TOE components as specified in table 2 in the tested configuration as outlined in Chapter 7 IT Product Testing. The R82 CC Firmware for Gateway and Maestro Configurations, Installation and Configuration, BSI Administration Guide [9] as specified in table 2 must be followed.

## 9. Results of the Evaluation

### 9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.1 and AVA_VAN.4 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: none
- for the Functionality: Product specific Security Target<br>Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant<br>EAL 4 augmented by ALC_FLR.1 and AVA_VAN.4

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

## 9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 120 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 120 Bits*' of the following table with '*no*' achieves a security level of lower than 120 Bits (in general context) only. Note that the column “Security Level” given in table 7 refers to the pure cryptographic (mathematical) strength only, and does not take into account whatever exploitable weaknesses induced by side-channel leakage, physical attacks, or implementation flaws of any kind.

| No. | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Security Level above 120 Bits |
|---|---|---|---|---|---|
| 1 | Authenti-cation | RSA key pair Signature generation (2048-bit/3072-bit with SHA-256, SHA-384 or SHA-512)<br>Signature verification (with SHA-256, SHA-384 or SHA-512) | FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3 and Section 5.5, using PKCS#1 v2.1 Signature Schemes RSASSA-PSS<br>RFC 8446, RSA key pair used for TLS v1.3 authentication | Generation 2048 or 3072 bits<br>Verification 2048 bits | No |
| 2 | | SHA-256 hashing (validation of administrator credentials)<br>public key credentials are stored in the Security Management Server database as PKCS#12 formatted files (private keys in PKCS#1 format) | FIPS 180-4 (SHA)<br>PKCS#12 (RFC7292)<br>PKCS#1 v2.1 | N/A | - |
| 3 | Confiden-tiality and Integrity | AES in GCM mode | FIPS 197 (AES), ISO 19772/ NIST SP800-38D (GCM) | 128 and 256 bits | Yes |
| 4 | | CHACHA20<br>encryption/ | RFC 7905 | 256 bits | Not Rated[7] |

[7] No rating of the security level has been performed, as the 'Technische Richtlinie BSI TR-02102' does not recommend Chacha20-Poly1305.

| No. | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Security Level above 120 Bits |
|---|---|---|---|---|---|
| | | decryption and<br>POLY1305 authenticator | | | |
| 5 | Key distribution | RSAES-PKCS1-v1_5 | RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1”<br>RFC 8446, TLS v1.3 | 2048 or 4096 bits | No |
| 6 | Crypto Primitives | Random number generator: CTR DRBG based on AES 256 | NIST SP800-90A | N/A | Yes |
| 7 | | Hashing: SHA-256, SHA-384 or SHA-512 | FIPS 180-4 | N/A | Yes |
| 8 | | Message Authentication Code: HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 | FIPS 198-1 | N/A | Yes |

Table 3: TOE cryptographic functionality

The strength of the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

# 10. Obligations and Notes for the Usage of the TOE

The document as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

# 11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

# 12. Regulation specific aspects (eIDAS, QES)

None

# 13. Definitions

## 13.1. Acronyms

| | |
|---|---|
| **AIS** | Application Notes and Interpretations of the Scheme |
| **API** | Application Programming Interface |
| **ARP** | Address Resolution Protocol |
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany |
| **BSIG** | BSI-Gesetz / Act on the Federal Office for Information Security |
| **CCRA** | Common Criteria Recognition Arrangement |
| **CC** | Common Criteria for IT Security Evaluation |
| **CEM** | Common Methodology for Information Technology Security Evaluation |
| **cPP** | Collaborative Protection Profile |
| **EAL** | Evaluation Assurance Level |
| **ETR** | Evaluation Technical Report |
| **IPS** | Intrusion Prevention System |
| **IPv4** | Internet Protocol version 4 |
| **ISO** | International Organization for Standardization;<br>here: abbrevation for the IS0 9660 file system |
| **IT** | Information Technology |
| **ITSEF** | Information Technology Security Evaluation Facility |
| **LAN** | Local Area Network |
| **NTP** | Network Time Protocol |
| **OS** | Operating System |
| **PDF** | Portable Document Format |
| **PP** | Protection Profile |
| **REST** | Representational State Transfer |
| **SAR** | Security Assurance Requirement |
| **SFP** | Security Function Policy |
| **SFR** | Security Functional Requirement |

| | |
|---|---|
| **SGM** | Security Gateway Module |
| **SP** | Scalable Platform |
| **SQL** | Structured Query Language |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TSF** | TOE Security Functionality |

### 13.2. Glossary

**Augmentation** - The addition of one or more requirement(s) to a package.

**Collaborative Protection Profile -** A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

**Extension** - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

**Formal** - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

**GaiA** - An Operating System by Check Point.

**Informal** - Expressed in natural language.

**Object** - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

**Package** - named set of either security functional or security assurance requirements

**Protection Profile** - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

**Security Target** - An implementation-dependent statement of security needs for a specific identified TOE.

**Semiformal** - Expressed in a restricted syntax language with defined semantics.

**Subject** - An active entity in the TOE that performs operations on objects.

**Target of Evaluation** - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

**TOE Security Functionality** - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

## 14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017,
https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-1207-2025, Version 015, 2025-04-04, Check Point R82 for Gateway and Maestro Configurations, Check Point Software Technologies Ltd.

[7] Evaluation Technical Report BSI-DSZ-CC-1207, Version 7, 2025-04-09, TÜV Informationstechnik GmbH (confidential document)

[8] Configuration list for the TOE, 2024-11-23, R82_EAL4_files_list, Check Point Software Technologies Ltd. (confidential document)

[9] Guidance documentation for the TOE, Version 008, 2025-03-03, R82 CC Firmware for Gateway and Maestro Configurations, Installation and Configuration, BSI Administration Guide, Check Point Software Technologies Ltd.

[8] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

# C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

# D. Annexes

## List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report