



Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0931-2015

for

**MaxPatrol Vulnerability and Compliance
Management System, V8.25.1.20707**

from

Positive Technologies

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-0931-2015(*)

MaxPatrol Vulnerability and Compliance Management System
V8.25.1.20707

from Positive Technologies
Functionality: Product specific Security Target
Common Criteria Part 2 extended
Assurance: Common Criteria Part 3 conformant
EAL 2



SOGIS
Recognition Agreement

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 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.

(*) 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 4..

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, 29 April 2015

For the Federal Office for Information Security

Thomas Gast
Head of Division

L.S.



Common Criteria
Recognition Arrangement



Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189 - 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.

Preliminary Remarks

Under the BSI¹ 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.

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

Contents

- A. Certification..... 7
 - 1. Specifications of the Certification Procedure..... 7
 - 2. Recognition Agreements..... 7
 - 3. Performance of Evaluation and Certification..... 8
 - 4. Validity of the Certification Result..... 9
 - 5. Publication..... 10
- B. Certification Results..... 11
 - 1. Executive Summary..... 12
 - 2. Identification of the TOE..... 13
 - 3. Security Policy..... 14
 - 4. Assumptions and Clarification of Scope..... 14
 - 5. Architectural Information..... 14
 - 6. Documentation..... 15
 - 7. IT Product Testing..... 15
 - 8. Evaluated Configuration..... 17
 - 9. Results of the Evaluation..... 17
 - 10. Obligations and Notes for the Usage of the TOE..... 18
 - 11. Security Target..... 18
 - 12. Definitions..... 18
 - 13. Bibliography..... 20
- C. Excerpts from the Criteria..... 23
 - CC Part 1:..... 23
 - CC Part 3:..... 24
- D. Annexes..... 31

A. Certification

1. 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 Security²
- BSI Certification and Approval Ordinance³
- BSI Schedule of Costs⁴
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Technical information on the IT security certification, Procedural Description (BSI 7138) [3]
- BSI certification: Requirements regarding the Evaluation Facility (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1⁵ [1] also published as ISO/IEC 15408.
- 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]

2. 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.

2.1. 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.

² Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

³ 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

⁴ Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

⁵ Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

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. This Domain is linked to a conformance claim to one of the related SOGIS Recommended Protection Profiles. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

As of September 2011 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. Details on recognition and the history of the agreement can be found at <https://www.bsi.bund.de/zertifizierung>.

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

This certificate is recognized under SOGIS-MRA for all assurance components selected.

2.2. 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), certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and 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 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.

As the product certified has been accepted into the certification process before 08 September 2014, this certificate is recognized according to the rules of CCRA-2000, i.e. for all assurance components selected.

3. 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 MaxPatrol Vulnerability and Compliance Management System, V8.25.1.20707 has undergone the certification procedure at BSI.

The evaluation of the product MaxPatrol Vulnerability and Compliance Management System, V8.25.1.20707 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 31 March 2015. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)⁶ recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Positive Technologies.

The product was developed by: Positive Technologies.

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

4. Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only 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 levels please refer to the excerpts from the criteria at the end of the Certification 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-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 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 29 April 2015 is valid until 28 April 2020. The validity date can be extended by re-assessment or re-certification.

The owner of the certificate is obliged

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 and the Security Target and user guidance documentation mentioned herein to any applicant 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,

⁶ Information Technology Security Evaluation Facility

3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the product's evaluated life cycle, e.g. related to development and production sites or processes, occur or the confidentiality of documentation and information related to the product or resulting from the evaluation and certification procedure is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the product or resulting from the evaluation and certification procedure that do not belong to the product deliverables according to the Certification Report part B chapter 2 to third parties, permission of the Certification Body at BSI has to be obtained.
4. to provide latest at of half of the certificate's validity period unsolicitedly and at his own expense current qualified evidence to the Certification Body at BSI that demonstrates that the requirements as outlined in the Security Target are up-to-date and remain valid in view of the respective status of technology. In general, this evidence is provided in the form of a re-assessment report according to the rules of the BSI Certification Scheme.

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.

5. Publication

The product MaxPatrol Vulnerability and Compliance Management System, V8.25.1.20707 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 developer⁷ of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

⁷ Positive Technologies
Schelkovskoe shosse 23A
107241 Moscow
Russian Federation

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 the 'Max Patrol Compliance and Vulnerability Management System (CC) and its related guidance documentation V8.25.1.20707' is part of a Vulnerability and Compliance Management System that is used to detect potential vulnerabilities within the scanned system or networks. Especially the TOE consists of parts of the MaxPatrol Server and the MaxPatrol Console.

The MaxPatrol Server is the primary part of the Compliance and Vulnerability Management System.

Figure 1.1 of the ST [6] illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the operational environment of the TOE. The TOE is a software only product and the TOE components are specified in Table 1.3 of the ST [6].

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 2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. 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
SF1	Security Audit
SF2	Access Control
SF3	Security Management
SF4	Scanning and Reporting
SF5	Identification and Authentication

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, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

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:

MaxPatrol Vulnerability and Compliance Management System, V8.25.1.20707

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW/D OC	TOE distribution kit (installer) including the Administrator guide [11], Quick Start Guide [12] and the MaxPatrol Help File (MaxPatrol_en) [10]	File MP-25.1.20707.100229.exe Hash (SHA-512): a5bf71d247d7943cbd6050de6d0c cf4602952706f7e025716cb69eae 7ad72f7ffed90e558ff74626866aa 5ab0bc0232b7b2ac7163c3cb705 18fd2b169e089505 Helpfile Maxpatrol_en.chm, Hash (SHA-512): ee739d9debb30b4bdddff2dd5b3 62b6047f9dbe587824660e6d7c5c ecbfc7fa691dd35b86f3154e32cd7 44a0fcdc3ff9be5daf155b8a3da42 d466b567273ad9 MaxPatrol Compliance and Vulnerability Management System Administrator Guide, Hash (SHA-512): cdd266ece7485edbb7b5040fac5f 0388c97241d714ceb3cb3c1e9ee da128bf44c0935d6f4c804617950 66cc26a8ec2814deae2233384a8 6843c5fe610e060be3 MaxPatrol Compliance and Vulnerability Management System Quick Start Guide, Hash (SHA-512): 595e7a71edfe94c156bef18dd9e3 39705fa4742896705880154963cf 7ddefca36c7b3c184055779e0a96 55baf5d1984739e39616feb75c47 f030ab2234240914	Download from secure website as a downloadable archive, via mail or on a DVD.
2	DOC	MaxPatrol compliance and vulnerability management system Installation guide [8]	File InstallationGuide(en).pdf Hash (SHA-512): c53dfa3ad49501f23c6beb78da06 5ce67e7cfbd807f29aedfb49143f0 6f4ae49a91f7b47ebbe34a27a39d 785be00bcf7885faa8a01905f904 d9c0fb213f589fa	Download from secure website as a downloadable archive, via mail or on a DVD.

No	Type	Identifier	Release	Form of Delivery
3	DOC	MaxPatrol compliance and vulnerability management system. Guidance Addendum [9]	File PT_AGD_1.0.pdf. Hash (SHA-512): 14aedda107065f2ff291ca27c360e515328bdf7508b543300dfe31c27884d9b30cfef4bd0405700146fcf883ba81ae4076bf025bbd182eae08f8325a3d5e06a	Download from secure website as a downloadable archive, via mail or on a DVD.

Table 2: Deliverables of the TOE

The TOE accompanied by its guidance documentation and an individual license file is provided to customers as a downloadable archive or via mail on a DVD. Further, a notification letter that contains SHA-512 checksums for every file of the downloadable archive or the DVD is sent to the respective customer separately via e-mail, fax or express delivery.

The customer can use any SHA-512 calculation tool to verify that the archive is the correct one that contains the evaluated version of the TOE.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. They cover security audit, identification and authentication, security management, security access, and scanning and reporting. Some more details can be found in chapter 1.3.3 of the ST [6].

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 list of objectives which have to be met by the the environment can be found in the Security Target [6] , chapter 4.2.

5. Architectural Information

The following components comprise the TOE:

- Scanning core (This component implements the scanning process for network checks and brute force attacks in PenTest mode, system checks in Audit mode, and compliance control in Compliance mode), as part of the MaxPatrol Server,
- Report service (This component generates reports based on the scanning results. The content and structure of the reports depends on templates configured by authorized TOE users), as part of the MaxPatrol Server,
- Control system (This component communicates with the MP Console and manages the processes within the TOE), as part of the MaxPatrol Server, and
- MaxPatrol Console (This component is a graphical user interface. Its services are employed by TOE users to communicate with the TOE and to configure the MP Server).

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

As the TOE is a software product it requires at least the following environment for its operation:

- CPU: Intel Pentium 4 processor 2,2 GHz
- RAM: 4 GB
- HDD: 50 GB
- OS: Microsoft Windows 2008 R2 Enterprise (x64) (including the .NET framework 4.0)
- DB: Microsoft SQL Server 2008 R2
- Other Software: MP Server V8.25.1.20707

The TOE under evaluation has been tested in its scheduled configuration. According to the operational environment of the TOE as specified in the ST the developer's and evaluator's tests have been performed in the test configuration specified as follows:

Hardware:

- Intel Core 2 Quad CPU Q8200 2.33 GHz
- 4 GB RAM
- 200 GB HD

Software

- Microsoft Windows 2008 R2 Enterprise (x64)
- .Net Framework 4.0
- Microsoft SQL Server 2008 R2
- MaxPatrol Server Version 8.25.1.20707

7.1. Developer Testing

TOE Test configuration

The following configuration was in place:

- A computer complying with the TOE minimum requirements listed in the ST [6], Table 1.4,
- A group of target computers containing installed software from the list of products that are supported by the TOE. Software that can be analysed by the TOE is given in the ST [6], chapter 1.3.1.

All of these computers have been included into a TCP/IP network. The computer with the TOE installed had network access to the target computer group to perform the different kind of scans. Additionally the computer with the TOE installed had Internet access to activate its license.

Testing approach

The developer decided to test every Security Function and every security function requirement to have complete test coverage. For each test he described the test case purpose, the tested SFRs, the used environment and prerequisites as well as each single test step in a detailed way. Additionally the developer described for each single step the expected and the actual result.

Because of the nature of the TOE (software product with a GUI), all tests have been performed manually by the developer. Therefore among the TOE itself and the testing environment including external clients no other tools or materials have been used by the developer.

The TOE was systematically tested at the level of the TSFI and SFRs given in the functional specification and the ST [6].

Conclusion

The developer's test effort has been proven sufficient to demonstrate that the TOE security functions perform as specified. Overall the TSF have been tested systematically, the test results demonstrate that no discrepancy between the TOE behavior and the TOE specification has been found

7.2. Evaluator Independent Testing

TOE Test configuration

The final TOE (version 8.25.1.20707) was tested in the abovementioned configuration.

Additionally, for testing the scanning functionality of the TOE Windows XP SP3 clients have been used as targets.

Test subset size and selection criteria

The tests performed and provided by the developer had a complete coverage of all security functions. The evaluator decided to repeat a subset developer tests in order to verify the adequateness of the tests. Furthermore, the evaluator developed additional manual test cases for functional testing. Thereby the evaluator chose the approach to cover all TSF from all the functional areas of the TOE.

Conclusion

The overall judgment on the results of independent testing consisting of

- Developer test repetition (sampling),
- TSF subset and TSFI testing, and
- Other testing

is that the TOE security functionality and TSFI are successfully tested and actually have the behaviour as specified.

7.3. Evaluator Penetration Testing

TOE Test configuration

The final TOE (version 8.25.1.20707) was tested in the abovementioned configuration.

Penetration testing approach:

The following attack scenarios have been tested:

- Try to read out the database tables which are public and available to a local attacker in order to get information about the saved user credentials.
- Try to manipulate the connection between the SQL database and the TOE in order to manipulate the role concept and get access to restricted information.

The following SFRs have been penetration tested:

FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FIA_UAU.5, FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

The remaining SFRs were analysed, but not penetration tested. Nevertheless they were covered by the functional tests conducted by the developer and the evaluator.

Conclusion

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential Basic was successful in the TOE's operational environment as defined in the ST [6] provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the configuration of the TOE as specified in the ST, chapter 1, especially chapter 1.3.2.

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 2 package including the class ASE as defined in the CC (see also part C of this report)

The evaluation has confirmed:

- for the Functionality: Product specific Security Target
Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
EAL 2

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 TOE does not include cryptographic mechanisms. Thus, no such mechanisms were part of the assessment.

10. Obligations and Notes for the Usage of the TOE

The documents 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.

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. Definitions

12.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
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
CPU	Central Processing Unit
DB	Database
EAL	Evaluation Assurance Level

ETR	Evaluation Technical Report
HDD	Hard Drive disk
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MP	MaxPatrol
OS	Operating System
PP	Protection Profile
RAM	Random Access Memory
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2. 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.

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.

13. Bibliography

- [1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
- [2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012
- [3] BSI certification: Technical information on the IT security certification of products, protection profiles and sites (BSI 7138) and Requirements regarding the Evaluation Facility for the Evaluation of Products, Protection Profiles and Sites under the CC and ITSEC (BSI 7125)
- [4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE⁸.
- [5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website
- [6] Maxpatrol Compliance and Vulnerability Management System Common Criteria Certification Security Target, BSI-DSZ-CC-0931-2015, Version 1.5, Date 29.09.2014, Positive Technologies
- [7] Evaluation Technical Report for MaxPatrol Compliance and Vulnerability Management System V8.25.1.20707, Version 3, Date 30.03.2015, TÜV Informationstechnik GmbH, (confidential document)
- [8] MaxPatrol compliance and vulnerability management system Installation guide, Checksum:
c53dfa3ad49501f23c6beb78da065ce67e7cfbd807f29aedfb49143f06f4ae49a91f7b47ebbe34a27a39d785be00bcf7885faa8a01905f904d9c0fb213f589fa, Positive Technologies
- [9] MaxPatrol compliance and vulnerability management system. Guidance Addendum, Version 1, Date 01.07.2014, Positive Technologies
- [10] Helpfile Maxpatrol_en.chm, Checksum:
ee739d9debb30b4bddd2dd5b362b6047f9dbe587824660e6d7c5cecbfc7fa691dd35b86f3154e32cd744a0fc3ff9be5daf155b8a3da42d466b567273ad9, Positive Technologies
- [11] MaxPatrol Compliance and Vulnerability Management System Administrator Guide, Checksum:
cdd266ece7485edbb7b5040fac5f0388c97241d714ceb3cb3c1e9eeda128bf44c0935d6f4c80461795066cc26a8ec2814deae2233384a86843c5fe610e060be3, Positive Technologies
- [12] MaxPatrol Compliance and Vulnerability Management System Quick Start Guide, Checksum:
595e7a71edfe94c156bef18dd9e339705fa4742896705880154963cf7ddefca36c7b3c

⁸specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2, Reuse of evaluation results

184055779e0a9655baf5d1984739e39616feb75c47f030ab2234240914, Positive Technologies

This page is intentionally left blank.

C. Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
 - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
 - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
 - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
 - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
 - the SFRs of that PP or ST are identical to the SFRs in the package, or
 - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
 - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
 - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.”

“Each assurance class contains at least one assurance family.”

“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD:	AGD_OPE.1 Operational user guidance
Guidance documents	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model

Assurance Class	Assurance Components
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE’s assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one

component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Evaluation assurance level 1 (EAL 1) - functionally tested (chapter 8.3)

“Objectives

EAL 1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL 1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL 1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL 1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL 2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL 5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL 5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL 6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL 6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL 6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL 7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL 7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary⁷

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.