Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0589-2015

for

TightGate-Pro (CC)
Version 1.4

from

m-privacy GmbH

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-0589-2015 (*)

Server Applications: Other Applications

TightGate-Pro (CC)
Version 1.4

from	m-privacy GmbH
PP Conformance:	Remote-Controlled Browsers Systems (ReCoBS), Version 1.0, 26 February 2008, BSI-CC-PP-0040-2008
Functionality:	PP conformant Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 3 augmented by ALC_CMS.4, ALC_FLR.3

SOGIS
Recognition Agreement

Common Criteria

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 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.

Common Criteria
Recognition Arrangement

Bonn, 2 December 2015

For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.

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

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 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.

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

Contents

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 Security[2]
- BSI Certification and Approval Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- 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[5] [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. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogisportal.eu.

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

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), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

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 TightGate-Pro (CC), Version 1.4 has undergone the certification procedure at BSI.

The evaluation of the product TightGate-Pro (CC), Version 1.4 was conducted by datenschutz cert GmbH. The evaluation was completed on 23 November 2015. datenschutz cert GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant is: m-privacy GmbH.

The product was developed by: m-privacy GmbH.

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 or in the CC itself.

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 is valid until 1 December 2020. Validity can be re-newed by 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, 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,

[6] Information Technology Security Evaluation Facility

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.

5. Publication

The product TightGate-Pro (CC), Version 1.4 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[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] m-privacy GmbH
Werner-Voß-Damm 62
12101 Berlin

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 Remote-Controlled Browser System (ReCoBS) which is designed to be a modular part of a security gateway to enable almost unlimited access to content on the World Wide Web (WWW) or via e-mail from a Local Computer (LC) of a user inside a Local Network (LAN). At the same time it prevents both the local information of users as well as the local computer and net devices (machines) on the LAN from (negative) effects of malware contained in active content within web pages.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Remote-Controlled Browsers Systems (ReCoBS), Version 1.0, 26 February 2008, BSI-CC-PP-0040-2008 [8].

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 3 augmented by ALC_CMS.4, ALC_FLR.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

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

TOE Security Functionality	Addressed issue
Subset information flow control	This is implemented by the XVNC Server which is supplying the TOE protocol and enforces the settings and the use of the TOE protocol. RSBAC RC provides the unbypassability.
Simple security attributes	This is implemented by the XVNC Server which is supplying the TOE protocol and enforces the settings and the use of the TOE protocol. RSBAC RC provides the unbypassability. The XVNC Server, by relaying the TOE protocol, transmits a visual representation of the WWW content. IT provides clipboard transfer according to the values of SECURITY ATTRIBUTES COPYPASTEIN AND COPYPASTEOUT set by the config administrator role. The audio content is relayed via the PulseAudio sound daemon to a proxy server (not hosted on the TOE host). The proxy server relays the audio to the LC.
Management of security attributes	The restrictive default values “off” for COPYPASTEIN and COPYPASTEOUT are installed with the mprivacytools-CC packet. The restrictive default value can only be changed from the menu system for the config administrator account.
Static attribute initialization	This is implemented by the TightGate-Pro (CC) Version 1.4 RSBAC-configuration (provided via the rsbac-policytgpro-CC packet). It allows only the VNC-Service to be accessed from the defined client IP range. The client’s IP range must be set by the config administrator (config menu).
Specification of Management	This is implemented by the config administrator menu system (config menu).
Security Roles	This is implemented by predefined, task-specific ADMINISTRATOR roles with separated duties (maint, config, backuser, update). The association of roles is done at the

TOE Security Functionality	Addressed issue
	organizational level and no user role can switch to any administrative role on the TOE host.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 1.3.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1.1. 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 3.1.

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:

TightGate-Pro (CC), Version 1.4

The following table outlines the TOE deliverables:

No	Type	Identifier / *Integrity Protection*	Release	Form of Delivery
1	SW	TightGate-Pro (CC)	Version 1.4	direct delivery from manufacturer to customer
2	DOC	Installation Handbook „TightGate-Pro, Dediziertes Remote-Controlled Browser System zum Schutz vor Gefahren aus dem Internet – Installationshandbuch, AGD-PRE“, [11] *electronic signature*	Version 1.41, 30.04.2015	download
3	DOC	Administration Handbook „TightGate-Pro, Dediziertes Remote-Controlled Browser System zum Schutz vor Gefahren aus dem Internet – Administrationshandbuch, AGDOPE“,[12] *electronic signature*	Version 2.3, 30/03/2015	download
4	DOC	User Handbook „TightGate-Pro, Dediziertes Remote-Controlled Browser System zum Schutz vor Gefahren aus dem Internet – Benutzerhandbuch“, [13] *electronic signature*	Version 2.56, 05/02/2015	download
5	SW	TOE-Client: TG-Pro-vnc_2.0.7_CC_win32.msi *SHA-256:* *e70c192045cf3fa862c9bcf21a0365b71beb853dcae8e0595f06fc44d2cf9190*	n/a	direct delivery from manufacturer to customer

No	Type	Identifier / *Integrity Protection*	Release	Form of Delivery
6	SW	TOE-Client: TG-Provnc_2.0.7_CC_win32_pw.msi *SHA-256:* *9ae61300ae1a2369c3ef91a483d34127ee63bf28c9f77c3edba2fc586107a9cf*	n/a	direct delivery from manufacturer to customer

Table 2: Deliverables of the TOE

Prior to the delivery, the TOE server is installed on the hardware selected by the customer. The hardware requirements from chapter 1.2.2.5 of the ST [6] are taken into consideration.

The delivery of the boot-medium and the TOE being installed on the TOE-Host is carried out personally by m-privacy GmbH. In addition to being delivered in person, the TOE client is also made available via secure secure download. The customer can confirm its integrity by checking the SHA-256 checksum.

The handbooks are available to the customer via download from the following address:

https://p.m-privacy.de/Dokumentation-TightGate-Pro-CC.zip

The corresponding detached signature is available via these direct links:

https://p.m-privacy.de/Dokumentation-TightGate-Pro-CC.zip.sig
https://p.m-privacy.de/Dokumentation-TightGate-Pro-CC.zip.asc

(once in binary format and once in ASCII format).

The customer can confirm the integrity of the handbooks by checking the signature. The m-privacy key "*m-privacy GmbH (m-privacy GmbH) <info@m-privacy.de>*" has the following fingerprint: *FCBA 08F2 D39E B9D7 A7AD B3C5 49E3 C159 3AE8 3223*

The link is encrypted via TLS with server authentication. The server certificate is issued to *CN=*.m-privacy.de,EMAIL=webmaster@m-privacy.de,C=DE*

by

CN=avast! Web/Mail Shield Root,O=avast! Web/Mail Shield,OU=generated by avast! antivirus for SSL/TLS scanning

and has the fingerprint:

AF987DA89A3B1A649FA18D5081DA8A709039170C

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: A role-based access control policy to control administrative access to the system, a security policy with regard to the communication between the TOE server and the TOE client. Specific information about the above-mentioned security policies can be found in section 7 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 following topics are of relevance:

- The connection between the TOE host (located in the DMZ) and devices in the LAN as well as the connection between the TOE host and the Internet are separated by a firewall (cf. Figure 1).
- It must be ensured that TOE clients on the devices (LC) within the LAN are not manipulated either by users or by software.
- The administrator must be trustworthy and competent and must not access WWW contents using this role.
- The TOE host operates an independent identification & authentication system. It must be ensured that users do not use the same credentials for logging on to the TOE host as for other devices in the LAN, e.g., on the LC.
- The IT environment, especially the TOE host, must prevent that malware on the TOE host can manipulate TSF data during normal operation.
- Programs that were started within a user's session must always be closed completely at the end of a session.
- In the IT environment, especially on the TOE host, only such programs must be available which are needed for the operation of the TOE on the TOE host.
- The IT environment must offer the possibility to initialize the TOE in time intervals to be defined and thus to restore it to a secure and known state.

Details can be found in the Security Target [6], chapter 3.2.

5. Architectural Information

The TOE is a Remote-Controlled Browser System (ReCoBS) according to [8]. It consists of three components: the TOE server, the TOE client, and the TOE protocol.

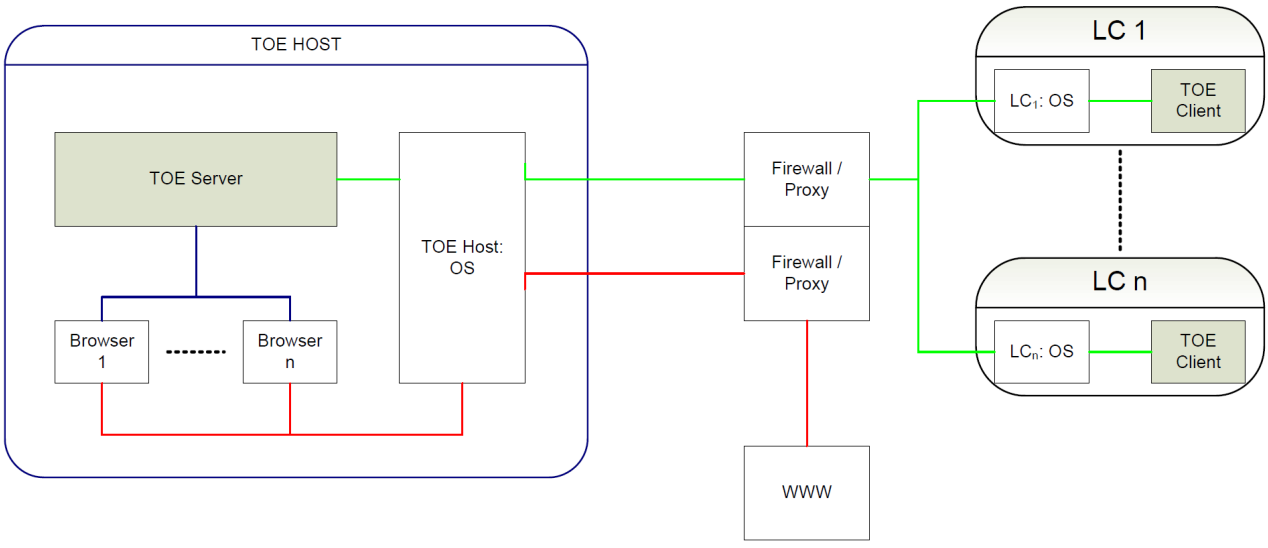

Figure 1: TOE Overview

5.1. TOE Server

The TOE server is installed in a particular environment, the TOE host, as described in chap. 1.2.2.5 [6]. The TOE server is divided into three subsystems:

1. RSBAC
2. VNC
3. Management

The subsystem “RSBAC” consists of the interplay of the kernel extension RSBAC of the TOE host OS and the associated RSBAC policy in the packet "rsbac-policy-tgprocc". RSBAC protects the system through a combination of different access control models and granular access restrictions. All of these are hard-coded and cannot be changed.

The VNC subsystem provides the TOE protocol. The TOE protocol offers the possibility of using a “clipboard function” for exchanging data between the TOE server and a TOE client. This function is controlled by this subsystem.

Subsystem Management consists of different administrative configuration menus:

1. config
2. maint
3. update
4. backuser

Each of these menus can only be accessed by the administrative role intended for it. In the “config” menu, all further settings of the TOE server are performed except for user administration. The “maint” menu serves for user administration. The “update” menu is needed for installing updates or performing a reset. The “backuser” menu offers all functions for configuring possible backup functions.

5.2. TOE Protocol

This is realized via an adapted VNC protocol.

5.3. TOE Client

This is an application that is installed on the local computer (LC) of a user. With the help of the TOE client, the user can connect to the TOE server and can access contents in the WAN with protection by the TOE. Via the VNC client menu, the user can approve or disapprove the transmission of data via the clipboard on a case-by-case basis.

The TOE Client contains three TSFI:

1. Config menu,
2. Maint menu, and
3. VNC viewer menu (interface of TOE client)

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

7.1. Test Configuration

For the test environment, the evaluators restricted themselves to a reduced set-up needed for testing the security functions of the TOE. Therefore, there is no print server and no mail server. The set-up only includes a local computer (LC) on which the TOE client is operated, the TOE server with connection to the WAN, and an attack computer (AC) for the performance of the penetration tests. The LC and the AC are connected to the TOE host via a switch.

TOE host corresponding to the hardware requirements specified in ST [6] chap. 1.2.2.5 (in the case of the testing body tests: intel NUC with the model number “D34010WYK”).

- Intel™ i3 4010U Processor (1.7 GHz Dual-Core)
- 8GB RAM
- 250GB hard drive

The TOE server, TightGate-Pro (CC) 1.4 is installed on the TOE host.

Local computer (LC) / system B: A PC on x86- with Windows 7 SP1 (32 bit) as operating system. The TOE client, TightGate-Pro (CC) 1.4, is installed on the LC via the Windows Installer (“TG-Pro-vnc_2.0.7_CC_win32.msi”).

7.2. Tests Performed by the Manufacturer

The manufacturer performed the tests in the context of the evaluation both manually and with tool support and logged them with the help of TestLink. The manufacturer has proven with the help of a mapping table that all interfaces as well as all SFRs were completely covered by the tests. To achieve this, the manufacturer defined and described test cases and assigned these to the respective requirements. All results of the manufacturer tests correspond to the expected results. Overall, the tests show that the TOE behaves as specified.

7.3. Tests Performed by the Evaluation Body

The following test methodology was applied:

- The majority of the tests performed were black-box tests that consider the behavior at the interfaces while taking into account the internal process; regarding the test parameters to be tested, equivalence classes were created.
- In addition, white-box tests were performed to check the behavior of the TOE with background knowledge about the functionality.

The tests were performed manually with tool support and were logged. Six test groups were created:

- T1: Update Process
- T2: Operation
- T3: Configuration
- T4: TOE Client Menu
- T5: TOE Reset

- T6: Vulnerability Tests

First, a reset (tests T5) was performed in order to restore the TOE to its delivery state. Then it was checked whether the requirements on the default value are fulfilled and whether the functional scope of the different roles in the delivery state is consistent with the manufacturer documentation (tests T2).

Then the TOE was configured manually on the basis of the handbooks in order to bring it into a completely operational state. While doing so, two users were created to allow later tests on the access rights to be performed. The SFR-relevant tests of the manufacturer on the “Config Menu” were repeated (tests T3).

As soon as configuration of the TOE was complete, a sniffer was started on the AC, which from then on recorded all data traffic from and to the TOE server (tests T6). Now the TOE client was started and the SFR-relevant tests on the TSFI “VNC Viewer Menu” were performed (tests T4).

Finally, the update process was checked. Here it was tested, among other things, whether a falsely signed update can be installed, and the changed version display following a successful update was checked (tests T1).

The evaluators completely repeated the SFR-related tests on the TSFI “Config Menu” and the “VNC Viewer Menu”. This ensures, on the one hand, the completeness of the checking of the SFR; on the other hand, the demand by CEM [2] for repetition of the manufacturer tests is fulfilled.

All test results corresponded to the expected results. Overall the tests show that the TOE behaves as specified.

7.4. Vulnerability Tests

In test group T6, it was checked to which extent the security functionality of the TOE can be circumvented. For this purpose, additional possibilities for attack were first sought. Then all attack points identified in the first step and the interfaces defined in the functional specification were checked with regard to vulnerabilities.

The vulnerability tests were set up systematically.

- Step 1: Identification. External port scan, internal port scan, internal vulnerability scan, network analysis, brute-force attack on the user authentication
- Step 2: Attack via rights extension
- Step 3: Attack on the separation of the user-domains
- Step 4: Attack with the help of browser extensions
- Step 5: Use of an alternative VNC viewer instead of the TOE client

All test results corresponded to the expected results. Overall the tests showed that the TOE behaves as specified. In the context of the vulnerability tests, no indication of vulnerabilities was found.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The evaluated configuration is the TightGate-Pro (CC) Version 1.4 software configured as instructed by the preparatory documentation [11], [12], [13].

For the operation of the TOE, the following non-TOE hardware/software is assumed, cf. ST [6], chap. 1.2.2.5:

The TightGate-Pro (CC) Version 1.4 server requires as a minimum the following hardware:

- Processor: 1.5ghz x86 compatible CPU(s)
- RAM: 2GB
- Storage: 20GB free
- Network: 100MBps

The TightGate-Pro (CC) Version 1.4 client requires Microsoft Windows 7 as operating system.

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 3 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_CMS.4, ALC_FLR.3 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Remote-Controlled Browsers Systems (ReCoBS), Version 1.0, 26 February 2008, BSI-CC-PP-0040-2008 [8]
- for the Functionality: PP conformant
  Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
  EAL 3 augmented by ALC_CMS.4, ALC_FLR.3

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
DMZ	Demilitarised Zone
DOS	Denial of Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LAN	Local Area Network
LC	Local Computer
PP	Protection Profile
ReCoBS	Remote Controlled Browser System
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target

TOE	Target of Evaluation
TSF	TOE Security Functionality
VNC	Virtual Network Computing
WWW	World Wide Web

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.

Malware - A programme (which might be an active content) which performs actions without explicit consent by the user under which environment it is launched. This term includes both remote controlled as well as autonomous programmes.

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 client - Program running on a LC to connect to the TOE server via the TOE protocol.

TOE host - One or several machines located in the DMZ on which the TOE server runs. The TOE host is not part of the TOE itself but forms an important part of the IT environment (namely for the TOE server). The term TOE host includes all software necessary to run the TOE server (including but not limited to the operating system) and software required for WWW access (e.g. web browsers and extensions).

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.

TOE server - Program(s) running on the TOE host to send the (audio-)visual representation of web content to the TOE client (using the TOE protocol) and transfer the user input from the TOE client (received via the TOE protocol) to the browsers running on the TOE host.

TOE transmission protocol - Set of commands and possible types of information which the TOE client can send to the TOE server combined with the set of commands and possible types of information which can be sent from the TOE server to the TOE client, cf. Section 6.1.1. The general term for the connection between the TOE server and TOE client is “TOE protocol”.

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
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012, http://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-0589-2015, Version 1.15, Date 2013-03-21, Common Criteria: Security Target for the TightGate-Pro(CC) Version 1.4, m-privacy GmbH

[7] Evaluation Technical Report, Version 1.0, Date 11.11.2015, Evaluation Technical Report – Summary, datenschutz cert GmbH, (confidential document)

[8] Remote-Controlled Browsers Systems (ReCoBS), Version 1.0, 26 February 2008, BSI-CC-PP-0040-2008

[9] Configuration list for the TOE, m-privacy GmbH, Date 24/07/2015, file: “parts_of_the_TOE_20150724.gz” (confidential document).

[10] List of sourcefiles of the TOE, m-privacy GmbH, Date 20/07/2015, file: “implementation_of_the_TOE_20150720.gz” (confidential document).

[11] Installation Handbook „TightGate-Pro, Dediziertes Remote-Controlled Browser System zum Schutz vor Gefahren aus dem Internet – Installationshandbuch, AGD-PRE“, Version 1.41, 30/04/2015

[12] Administration Handbook „TightGate-Pro, Dediziertes Remote-Controlled Browser System zum Schutz vor Gefahren aus dem Internet – Administrationshandbuch, AGD-OPE“, Version 2.3, 30/03/2015

[13] User Handbook „TightGate-Pro, Dediziertes Remote-Controlled Browser System zum Schutz vor Gefahren aus dem Internet – Benutzerhandbuch“, Version 2.56, 05/02/2015

[8] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

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: Guidance documents	AGD_OPE.1 Operational user guidance
	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 summary”

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.