Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1240-2026

for

TightGate-Pro (CC) 2.0

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-1240-2026 (*)

Proxy-Firewall

TightGate-Pro (CC) 2.0

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
valid until:	22 February 2031

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 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

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

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

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

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

Bonn, 23 February 2026

For the Federal Office for Information Security

Fabian Hodouschek
Head of Certification

L.S.

Sandro Amendola
Director-General Directorate General S

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

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

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

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

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

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

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

2. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs[3]
- Special decrees issued by the Bundesministerium des Innern (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 licensing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1 [4] [1] also published as ISO/IEC 15408

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 2 December 2025, BGBl. 2025, no. 301, p. 2

[2] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung – BSIZertV) of 02 December 2025, Bundesgesetzblatt 2025, no. 301

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

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

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates – as far as such certificates are based on ITSEC or CC – under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

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

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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

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

4. Performance of Evaluation and Certification

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

The product TightGate-Pro (CC) 2.0 has undergone the certification procedure at BSI.

The evaluation of the product TightGate-Pro (CC) 2.0 was conducted by Deutsches Forschungszentrum für Künstliche Intelligenz GmbH (DFKI GmbH). The evaluation was completed on 19 February 2026. DFKI GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and 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.

5. Validity of the Certification Result

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

- all stipulations regarding generation, configuration and operation, as given in the evaluated guidance documentation, are observed,
- the product is operated in the environment as specified and in the Security Target.

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

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

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 23 February 2026 is valid until 22 February 2031. 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,

[5] Information Technology Security Evaluation Facility

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

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

6. Publication

The product TightGate-Pro (CC) 2.0 has been included in the BSI list of certified products, which is published regularly in the listing found at the BSI Website https://www.bsi.bund.de/dok/Zertifizierung-Gesamtlisten. Further information can be obtained from BSI-Infoline +49 (0)228 9582-111.

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

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

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 TightGate-Pro (CC) 2.0 which is a workstation proxy firewall, which allows designated hosts to connect to, and use software on the server. By doing so, any potential threats are restricted to the TightGate-Pro (CC) 2.0 server, which is protected and designed to counter threats. TightGate-Pro (CC) 2.0 is designed to be used to access all WWW and e-mail content, forwarding only graphical and textual information, or the result of any executable content, without actually forwarding the code required to generate a web page.

The Security Target [5] 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 [7].

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 [5], chapter 6. They are all selected from Common Criteria Part 2. Thus the claimed set of SFRs in the ST is CC Part 2 conformant.

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

TOE Security Functionality	**Addressed issue**
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FMT_MSA.1	Management of security attributes
FMT_MSA.3(t)	Static attribute initialisation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [5], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [5], 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 [5], 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 52, 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) 2.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/ SW	TightGate-Pro (CC) 2.0 server appliance, pre-installed of specific server hardware	2.0	Courier service
2	HW (USB)	TightGate-Pro (CC) 2.0 boot media (USB)	2.0	Courier service
3	DOC	Password list with initial passwords and checklist scope of delivery	n/a	Courier service
4	SW	TightGate-Viewer (CC) 2.0, TG-Pro-vnc-CC_4.8.1_win64-all.msi	Version 4.8.1	Web site download from https://help.m-privacy.de/doku.php/tightgate-cc
5	DOC	Benutzerhandbuch für TightGate-Pro (CC) 2.0 agd_user_tightgate-pro_cc_20.pdf	Version 1.11	Web site download from https://help.m-privacy.de/doku.php/tightgate-cc
6	DOC	Administrationshandbuch für TightGate-Pro (CC) 2.0 agd-ope_tightgate-pro_cc_20.pdf	Version 1.23	Web site download from https://help.m-privacy.de/doku.php/tightgate-cc
7	DOC	Installationshandbuch für TightGate-Pro (CC) 2.0 agd-pre_tightgate-pro_cc_20.pdf	Version 1.14	Web site download from https://help.m-privacy.de/doku.php/tightgate-cc
8	SW	Digital signatures for Web site downloads	n/a	Web site download from https://help.m-privacy.de/doku.php/tightgate-cc

Table 2: Deliverables of the TOE

The TightGate-Pro (CC) 2.0 server appliance, boot media (USB), password list and checklist (scope of delivery) are delivered via a commercial courier service. The customer will be notified of the delivery in advance.

The TightGate-Viewer (CC) 2.0, the user guidance (Benutzer-, Administrations-, Installationshandbuch) and the corresponding digital signatures are delivered via web-site download. The signature verification key cc@m-privacy.de (key ID: 0xC466DE69A41EFD1B, subkey: 0x9C26225432C29B41) can be obtained using GnuPG via WKD (Web Key Directory) procedure.

The unique reference of the TOE is TightGate-Pro (CC) 2.0. TightGate-Pro (CC) 2.0 server appliance and boot media as well as the TightGate-Viewer (CC) 2.0 are labelled with the unique TOE reference. The file name of the TightGate-Viewer (CC) 2.0 refers to its individual unique version number. All parts of the user guidance are labelled with the unique TOE reference in the document title and their individual unique version number in the page footer.

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:

- Information flow control (FDP_IFC.1 and FDP_IFF.1) for the exchange of audio-visual data, keyboard/mouse events, plain-text clipboard data and (only during client startup) the contents of a clearly identified file.
- Management functionality (FMT_SMF.1, FMT_MSA.1, FMT_MSA.3(t)) regarding the rules of information flow control.
- Maintenance of security roles administrator and user (FMT_SMR.1) regarding their association with user accounts.

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 topics listed in the Security Target [5], chapter 4.2 are of relevance.

5. Architectural Information

The TOE consists of two physically separate parts: the TOE client and the TOE server. Both parts are interconnected by the TOE protocol, which is also part of the TOE itself and is not considered a TSF interface.

The TOE client (VNC-Viewer) outputs audio-visual information via loudspeaker/screen. The keyboard and mouse deliver input events to the TOE client. This input/output is not described as a TSF interface in the functional specification. It is also not mentioned in the security objectives and the SFRs. Accordingly, no subsystem for input/output has been identified. The input/output is interpreted as a non-TOE subsystem of the TOE client.

The TOE server (VNC-Server) communicates with browsers or other applications (e-mail, etc.). This input/output is not described as a TSF interface in the functional specification. It is also not mentioned in the security objectives and SFRs. Accordingly, no subsystem for input/output has been identified. The input/output is interpreted as a non-TOE subsystem of the TOE client.

The TSF subsystems are arranged hierarchically on two levels. The lower-level subsystems provide all of the security functionality. The upper-level subsystems only matter in terms of the structure of the security architecture.

The TOE protocol, as part of the TOE, is implemented by the LL-Sub VeNCrypt and LL-Sub Audio subsystems in both the TOE server (VNC-Server) and TOE client (VNC-Viewer). The Viewer Menu subsystem is implemented in the TOE client (VNC-Viewer). The menus for the various administrative roles are implemented in the TOE server (VNC-Server Management).

The LL-Sub VeNCrypt subsystem implements parts of the TOE protocol. VeNCrypt is a protocol extension of the VNC protocol used by the TOE to negotiate a TLS connection between the upper-level subsystems VNC-Server and VNC-Viewer. The VNC protocol is used to transfer visual information and the information required for its display (such as window size and position) from the VNC server to the VNC viewer, and keystrokes and mouse events from the VNC-Viewer to the VNC-Server. In addition, if enabled, plain text can be exchanged between the VNC-Server and VNC-Viewer via the clipboard (COPYPASTEOUT and COPYPASTEIN).

The LL-Sub audio subsystem implements audio transmission as part of the TOE protocol. Through the PulseAudio protocol, audio information is transmitted from the VNC-Server to the VNC-Viewer along an existing VNC connection.

The Viewer Menu Subsystem (accessible with the F8 key) allows the user to control clipboard exchange with the VNC server (COPYPASTEOUT and COPYPASTEIN).

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

Functional developer tests.

The test setup consists of a DMZ and a local network segment connected to it via a firewall. One of the network interfaces of the TOE server is located in the DMZ, the other is connected to the Internet. For the tests, a TOE client is operated in the local network segment. The TOE is tested in the evaluated configuration. All security objectives for the IT environment are met. In some tests, the TOE server is connected to a log server located in the DMZ. In addition, the following test tools are occasionally used: a network scanner, an SSH client and an RDP client.

The developer has devised a test for each SFR element and policy rule, in order to verify their enforcement. All of the observed test results corresponded to the expected results. No deviations from the SFRs have been detected.

Independent evaluator tests

An isolated network was used to test the following:

- a TOE server appliance supplied by the developer
- a running TightGate-Viewer version 4.0.7
- a running TightGate-Viewer version 4.8.1

Both the server and the client computers were located within the same network segment and were not separated by a firewall.

The interfaces tested comprise:

- Config menu

- Maint menu
- VNC viewer menu

Each interface tested provides actions necessary for enforcing the SFRs. All SFR elements and policy rules are covered by these actions. When selecting developer tests, those that check the implementation of the SFRs are chosen. All tests have been passed. No deviations from the SFRs, the functional specification or the TOE design have been found. Only the test configuration with TightGate-Viewer version 4.8.1 corresponds to the evaluated configuration. At an earlier stage, the evaluator tests were carried out with TightGate-Viewer version 4.0.7 on Windows 10. The test procedures and the results obtained can be transferred to the evaluated configuration because:

- The actions tested on TightGate-Viewer have not changed.
- TightGate-Viewer is based on an open-source product that operates across different operating systems; therefore, it only uses common functionality and does not rely on the security features of the operating system.
- The developer has performed all tests with TightGate-Viewer version 4.8.1 on Windows 11.

Vulnerability analysis

Three potential vulnerabilities have been identified and tested to verify their existence.

Two of these are related to attacks that bypass the maintenance of the administrator role, i.e. the use of administrative functions without proper authentication. The penetration tests aimed at bypassing the maintenance of the administrator role were unsuccessful. The third potential vulnerability relates to the exchange of clipboard content other than plain text. Two penetration tests revealed that TightGate-Viewer either disconnects from the TOE host or blocks illicit clipboard content types. The penetration tests have been performed with the evaluator test configuration. In order to attempt to exchange illicit clipboard content types, the TOE host has been replaced with a notebook running a specific test environment.

All penetration tests were carried out using the TightGate-Viewer user interface, with the results showing that the respective vulnerability does not exist.

8. Evaluated Configuration

The TOE can be operated in a single configuration. The TOE automatically starts up to the evaluated configuration and operating mode. During start-up, it is possible to select other operating modes of the TOE host. However, these are neither secure nor compatible with the evaluated configuration.

The TOE only operates in its evaluated configuration when all configuration settings are secure. To prevent misconfiguration of the TOE, any settings that differ from the evaluated configuration are clearly marked in the administration menus.

The TOE consists of the items in the configuration list [8].

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [6] 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 [7]
- 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.

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

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

11. Security Target

For the purpose of publishing, the Security Target [5] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
VNC	Virtual Network Computing

13.2. Glossary

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

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

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

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

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.

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

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

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

14. Bibliography

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

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

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7] https://www.bsi.bund.de/AIS

[5] Security Target BSI-DSZ-CC-1240-2026, Common Criteria: Security Target for the TightGate-Pro (CC) 2.0, Version 1.25, 2026-02-14, m-privacy GmbH

[6] Evaluation Technical Report, Evaluation TightGate-Pro (CC) 2.0 Evaluation Technical Report Summary, Version 1.1, Date 16.02.2026, including TOE Security Compendium for utilisation in the Certification Procedure, TightGate-Pro (CC) 2.0, Version 1.1, Date 16.02.2026, DFKI, (confidential documents)

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

[8] Configuration list for the TOE, Filenames TG-Pro-CC-vnc_Viewer_481_Dateiliste.odt and gen_min_parts_of_the_toe_250728.txt (confidential document)

[7] specifically

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

[9] TightGate-Pro (CC) 2.0 – Benutzerhandbuch, Version 1.11, 25.07.2023, m-privacy GmbH

[10] TightGate-Pro (CC) 2.0 – Administrationshandbuch, Version 1.23, 26.11.2025, m-privacy GmbH

[11] TightGate-Pro (CC) 2.0 – Installationshandbuch, Version 1.14, 25.07.2023, m-privacy GmbH

C. Excerpts from the Criteria

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

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

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

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report