Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0815-2013

for

LANCOM Systems Operating System LCOS 8.70 CC with IPsec VPN

from

LANCOM Systems 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-0815-2013

VPN Router Firmware

LANCOM Systems Operating System LCOS 8.70 CC with IPsec VPN

from	LANCOM Systems GmbH
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.1

Common Criteria
Recognition
Arrangement

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 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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.

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, 24 May 2013

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

Bernd Kowalski
Head of Department

L.S.

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:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- 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 technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

---

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 a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

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

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.

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. 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.

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 LANCOM Systems Operating System LCOS 8.70 CC with IPsec VPN has undergone the certification procedure at BSI.

The evaluation of the product LANCOM Systems Operating System LCOS 8.70 CC with IPsec VPN was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 13 May 2013. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: LANCOM Systems GmbH.

The product was developed by: LANCOM Systems 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,

[6] Information Technology Security Evaluation Facility

- 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.

5 Publication

The product LANCOM Systems Operating System LCOS 8.70 CC with IPsec VPN 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] LANCOM Systems GmbH
Adenauerstr. 20 / B2
52146 Würselen

This page is intentionally left blank.

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) consists of software used to construct virtual private networks (VPNs) between networks or between the TOE and a remote access client. The LANCOM Systems Operating System LCOS 8.70 CC with IPsec VPN is the operating system LCOS (software) for the LANCOM CC series routers. The TOE provides all functions to manage a secure IPsec connection. Thus temporary or mobile sites of a company, home offices, branch offices or co-locations of an enterprise or public entity can be connected to each other or to a central site at the headquarters safely by the use of the TOE at each location. Also, the TOE can manage IPsec connections from mobile users facilitating LANCOM AVC (Advanced VPN Client) software on their mobile devices. The LANCOM Advanced VPN Client is considered part of the IT environment.

The TOE implements the security functions IPsec, packet filtering, configuration management and key management.

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

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

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5. 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 Functions:

TOE Security Functions	Addressed issue
IPSEC: IPSEC.1 – IPsec Internet Key Exchange (IKE) IPSEC.2 – IPsec Encapsulating Security Payload (ESP) IPSEC.3 – IPsec Security Associations, Security Policies and Routing	The TOE in conjunction with the cryptographic acceleration engine implements IPsec protocols. Confidentiality, authenticity, and integrity are provided for IP packets protected by IPsec. The administrator defines which traffic must be protected by IPsec by configuring routes with a VPN peer as the gateway.
Packet Filtering: PACKETFILTER.1 – Packet Filtering	The TOE performs packet filtering as a part of the IP router by applying the firewall rules to IP packets traversing the IP router. The administrator defined firewall rules can either allow an IP packet to be routed, dropped or rejected.
Configuration and Management: CONFIG.1 – System Messages CONFIG.2 – Management	The TOE generates audit records to provide a log of security relevant events during TOE operation. Management and configuration of the TOE are performed on a command line interface (CLI) which can be accessed either locally via a serial configuration port, or remotely via a SSH network connection.

TOE Security Functions	Addressed issue
Remote Management: REMOTE.1	Secure Shell (SSH) is used for remote management of the TOE by the administrator. Remote management via SSH provides full access to the command line interface as it would be available via the serial console. Remote administration via SSH provides confidentiality and integrity of the management session, which is completely ensured by TOE components without use of the cryptographic acceleration engine. SSH also provides protection against replay attacks by using a unique session identifier that is bound to the key exchange process in the transport protocol. The temporary session keys are destroyed by overwriting them with zeroes when the session is closed.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 6.1.

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 3.2, 3.3, and 3.4.

The TOE requires the appropriate hardware to operate on, i.e. a LANCOM CC series router. The router hardware is outside the scope of the TOE. The list of supported hardware of the certified TOE can be found in chapter 1.5 of the ST [6]. Chapter 1.4.4 of the ST [6] gives information of product features that are explicitly excluded from the evaluated configuration and must be disabled in the configuration. Therefore, the TOE also includes two guidance documents, the preparative procedures [8] and the operational guidance [9]. The TOE must be operated in compliance with both guidance documents.

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:

LANCOM Systems Operating System LCOS 8.70 CC with IPsec VPN

The following table outlines the TOE deliverables:

No	Type	Identifier	Form of Delivery
1a	SW	Router Model: 1781-4G (CC) Identification: LC-1781-4G-8.70.0095-Rel.upx	Secure Download

No	Type	Identifier	Form of Delivery
		SHA-256 value: 95d8eed735be352de69366c688802eea33e576369b0a96bf9549b877b03c3d3e	
1b	SW	Router Model: 1781A-3G (CC) Identification: LC-1781A-3G-8.70.0095-Rel.upx SHA-256 value: d73a6536a07a0a504741443788adb7ddfbf91ae0aa1118bcc261e82961f86258	Secure Download
1c	SW	Router Model: 1781A-4G (CC) Identification: LC-1781A-4G-8.70.0096-Rel.upx SHA-256 value: e27be5f81261b0ac8b58d23aee65e33b6e9cf8a94361ffc7995164a0f1dc5c72	Secure Download
1d	SW	Router Model: 1781A (CC) Identification: LC-1781A-8.70.0095-Rel.upx SHA-256 value: 5cc9c34a058336e60bb91d77b0503e558b6d1dbdbc66921aa47146607f1eab39	Secure Download
1e	SW	Router Model: 1781EF (CC) Identification: LC-1781EF-8.70.0095-Rel.upx SHA-256 value: 888075304feb3d29b284bb9e35ba31efabfa730833a57284ffd6cd41d421da90	Secure Download
1f	SW	Router Model: 7100+ VPN (CC) Identification: LC-7100plus-8.70.0095-Rel.upx SHA-256 value: dbfd7c4c7045aaa14e572dfb500d19aa1aac67793435612ad59c662c702b1ce5	Secure Download
1g	SW	Router Model: 9100+ VPN (CC) Identification: LC-9100plus-8.70.0095-Rel.upx SHA-256 value: dcb20236335a789abbacef93203f9244568a7c7ab002c6c0e7e8ebf47cf80ff5	Secure Download
2	DOC	Preparative Procedures [8] Identification: LCOS 8.70 – Preparative Procedures.pdf SHA-256 value: 1b82f43ad013ee1475479ae74db9cb6a14f72f19dfb2cfd3f998b603096bd5fa	Secure Download
3	DOC	Operational User Guidance [9] Identification: LCOS 8.70 – Operational User Guidance.pdf SHA-256 value: 96de218b8f3f09535e9cfecd109b41e3634cf7b57358a8cc4f27387eb9320a99	Secure Download

Table 2: Deliverables of the TOE

The TOE consists of the Firmware for LANCOM CC series routers. There are seven different configurations of the TOE for different router models which can be uniquely identified by their file names and hash values given in the table above.

After installation and start-up, during normal operation, the user (i.e. the administrator) can identify the hardware platform and running firmware release (i.e. the TOE) using the command line ‘sysinfo’ command.

The firmware images and the accompanying guidance documents are downloadable after registration on the LANCOM Systems website https://www.lancom-systems.de/cc.

The TOE user/administrator can download the applicable firmware for his LANCOM CC series router and the guidance documents from the website. He has to calculate a SHA-256 checksum and compare the results with the checksums stated in this certification report.

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers IPsec for network data encryption at the IP packet level to guarantee the confidentiality, authenticity and integrity of IP packets, namely for authentication between TOE and VPN peer, confidentiality of packets, and integrity and authenticity of packets. Also, it covers packet filtering for controlled communications between two networks that are physically separated, configuration management and operation performed directly from a command line interface, including the generation of system message logs, and key management for IPsec connections as part of the IPsec implementation. Finally it also covers remote management via SSH to enable access to the command line interface functions.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance: OE.Policy, OE.Secure-Management, OE.VPN, OE.Hardware. Details can be found in the Security Target [6], chapter 4.2.

5 Architectural Information

The LANCOM Systems Operating System LCOS 8.70 CC with IPsec VPN consists of software that is used to construct virtual private networks (VPNs) between networks or the TOE and a remote access client. The TOE design implements its security functions by the following subsystems:

- Sub.VPN
- Sub.Cryptography
- Sub.Router/Firewall
- Sub.Management
- Sub.Log
- Sub.TCP/IP

- Sub.OS

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

Description of the Functional Developer Tests

The test configuration consists of a test PC, two switches for selecting the actual TOE configuration (1781-4G (CC), 1781A (CC), 1781A-3G (CC), 1781A-4G (CC), 1781EF (CC), 7100+ VPN (CC), and 9100+ VPN (CC), via WAN and LAN), the TOE itself and an IPsec gateway. The TOE configurations are installed on corresponding LANCOM CC series routers, as required in OE.Hardware of the ST [6].

The tests for the TSFIs were performed using the TOE firmware 8.70.0095 and 8.70.0096 and for some tests with a specially modified firmware.

For some of the TSFI tests an external test tool (Codenomicon Defensics) was used to run a variety of tests for each action to be tested. All other tests were implemented by the developer.

The tests of the TOE were carried out by a test tool provided by the developers. The entire developer test configuration and the test protocols were later also provided to the evaluator.

The developer used several testing approaches and several different test configurations. Many tests were performed automatically by the CC-BatchTester tool developed by LANCOM Systems. This tool starts the actual tests, which are implemented either using Python or using the Codenomicon Defensics test tool. The CC-BatchTester also shows the ordering dependencies, since the tests are organized in a tree that defines the correct execution order. When performing a test for a specific TOE configuration the tool first sets up the hardware. This makes sure, that only the actual TOE can be access by the test PC. Then, the TOEs firmware is uploaded. Third, the tests selected in the tool are executed.

Unit tests run after the firmware was built. The developer used scripts to run all or a subset of these unit tests. In order to run these tests, a development environment is needed that was set up on a virtual machine with help of the developers. The evaluator tests also included a rerun of these tests.

The communication via serial interface was tested manually. The developer specified and implemented test cases for each defined TSFI and each subsystem. Thus all subsystems are covered by several test cases and each SFR-enforcing module is covered by at least one test case.

The results of the TOE tests prove the correct implementation. All test cases were executed successfully and showed the expected result.

Description of the Independent Evaluator Tests

For the independent tests the test setup and configuration was similar to the developer tests. The developer tests were redone using the test setup provided by the developer. These tests were performed on all hardware platforms. The test execution of the developer tests is controlled by the test tool CC-BatchTester that was provided by LANCOM Systems.

The evaluators tested all TOE Security Functions. All TSFIs were tested during the independent evaluator tests. For all commands and functionality tests, test cases were specified in order to demonstrate the TOE's expected behaviour including error cases.

Tests included

- Remote administration login, serial console interface and CLI,
- Routing, firewall, and application dispatcher related tests,
- SSH connection establishment, validation of authentication schemes, and file exchange,
- ISAKMP connection establishment for both signature based and PSK authentication, including manual connection triggering,
- ESP packet related tests including SPI and padding,
- Internal data structures and file tests,
- Internal packet handling on IP, TCP, UDP and logging functionality via unit tests,
- Cryptographic functions in software and hardware,
- Checks for valid configuration,
- Port scans, fuzzing, stress test,
- Password brute force.

The evaluators have tested the TOE systematically against enhanced-basic attack potential during their penetration testing. The achieved test results correspond to the expected test results. The results of the TOE tests prove the correct implementation. All test cases were executed successfully and showed the expected result.

Description of the Penetration Tests

Publicly known vulnerabilities have been collected from CVE, textbooks and scientific publications. The applicability of each attack path has been considered for the configured TOE in its intended environment. All interfaces that the TOE configuration allows have been considered, that is Ethernet and USB. After the setup of the test environment the different attack scenarios were defined. These attack scenarios were mapped to test cases and executed in the test environment.

For testing the TOE the evaluators used the same configuration as used in the developer tests, including the hardware 1781-4G (CC), 1781A (CC), 1781A-3G (CC), 1781A-4G (CC), 1781EF (CC), 7100+ VPN (CC), and 9100+ VPN (CC).

For some penetration tests the evaluators used an additional host computer and integrated it in the trusted network of the test scenario.

The penetration tests included Timing Attack on RSA, Timing attack on AES, and Padding Oracle. It was verified that the SFRs are implemented correctly and that they cannot be bypassed, deactivated or manipulated. Direct attacks against the implementation of SFRs

including the corresponding TSFIs were considered. The TSFIs are implemented correctly. The tested TSFIs are IKE (RSA signature during DH in IKE) and SSH (RSA signature during DH in SSH, AES encryption) while independent tests covered the other TSFI.

The overall test result is that no deviations were found between the expected and the actual test results. Tests were performed according to attack potential enhanced basic.

8 Evaluated Configuration

The TOE includes only the operating system, not the hardware on which the operating system is executed, i.e. the LANCOM CC series router. In particular, the cryptographic acceleration engine in the CPU is not part of the TOE. The hardware the TOE is running on comprise the models 1781-4G (CC), 1781A (CC), 1781A-3G (CC), 1781A-4G (CC), 1781EF (CC), 7100+ VPN (CC), 9100+ VPN (CC) as identified in the ST [6] chapter 1.5. The TOE manages the hardware it is running on, in particular the various network interfaces available, and uses them to distinguish untrusted networks and trusted networks. When the TOE is in use, at least one of the network interfaces of the internetworking device will be attached to a trusted network, and at least one other interface will be attached to an untrusted network.

A set of features as described in the ST [6] chapter 1.4.4 is explicitly excluded from the evaluated configuration and must be disabled. In particular it should be mentioned that the TOE supports the PPP protocol to establish a connection to an Internet provider via, e.g., DSL. The PPP protocol is not used to provide additional security and, therefore, is not within the scope of the security evaluation. Similarly, the TOE supports the use of VLAN-Tags for Ethernet network interfaces. The use of VLAN-Tags is not used to provide additional security and, therefore, is not within the scope of the security evaluation. The evaluated configuration only supports IPv4, not IPv6. The firmware update mechanism depends on the boot-loader, which is outside the TOE scope as well.

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.

For RNG assessment the scheme interpretations AIS 20 was used (see [4]).

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

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

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target
  Common Criteria Part 2 extended

- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_FLR.1

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 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 following cryptographic algorithms are used by the TOE to enforce its security policy:

Algorithm	Bit Length	Purpose	Security Functionality	Standard of Implementation	Standard of Usage
HMAC-SHA-1	160	Digital signing and signature verification. Key derivation	IPsec Internet Key Exchange (IKE) (FCS_CKM.1, FCS_CKM.2(1)), Remote Management (FCS_COP.1, FCS_CKM.2(2))	FIPS-198-1 (198a)	RFC 2409, RFC 2104, RFC 4253
HMAC-SHA-256	256	Digital signing and signature verification. Key derivation	IPsec Internet Key Exchange (IKE) (FCS_CKM.1, FCS_CKM.2(1))	FIPS 198-1 (198a)	RFC 2409, RFC 4868
AES-CBC	128, 192, 256	Encryption and decryption of secured packets	IPsec Internet Key Exchange (IKE) (FCS_CKM.1, FCS_CKM.2(1)), Remote Management (FCS_COP.1)	AES: FIPS-197 CBC: NIST SP 800 - 38A, sec. 6.2	RFC 3602
Diffie-Hellman	2048	Diffie-Hellman key agreement	IPsec Internet Key Exchange (IKE) (FCS_CKM.1, FCS_CKM.2(1)), Remote Management (FCS_CKM.2(2))	PKCS#3	RFC 3526
RSA	2048	Authentication of the TOE. Digital signing and signature verification.	IPsec Internet Key Exchange (IKE) (FCS_CKM.2(1)), Remote Management (FCS_CKM.2(2))	PKCS#1	RFC 2409, RFC 2313, RFC 3447

Table 3: Cryptographic Algorithms used by the TOE

Please note: The HMAC-SHA-1 algorithm is implemented by the TOE because of the standards the TOE shall conform to e.g. RFC 2104.

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). According to [10] and BSI TR-02102 [11] the algorithms are suitable for their purpose as described in the table above. The validity period of each algorithm is mentioned in the official catalogue [10] and BSI TR-02102 [11] and summarized the table above.

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 for 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.

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.

The TOE includes guidance documentation (see table 2) which contains guidelines for preparation and operation of the TOE which have to be followed. The Preparative Procedures [8] and the Operational User Guidance [9] contain necessary information about the secure administration, configuration, and usage of the TOE and all security hints therein have to be considered. Namely, the use of the software random number generator requires a unique random seed with a sufficiently high entropy which has to be obtained and loaded into the TOE from a certified source of random numbers, for details see [8], chapter 1.2.3, and the objective for the operational environment "OE.Secure-Management", bullet point e) in chapter 4.2 of the ST [6].

The validity of the certificate is limited to a specific set of Hardware Routers on which the TOE is running. For a list of the allowed hardware and for more details please refer to chapter 8 of this report and to the ST [6], chapter 1.5.

The TOE will be downloadable as a firmware file at the LANCOM Systems website:

https://www.lancom-systems.de/cc

The link has to be present throughout the validity of this certificate.

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

AES Advanced Encryption Standard

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

CBC Cipher Block Chaining

CCRA Common Criteria Recognition Arrangement

CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
DH	Diffie-Hellman
DSL	Digital Subscriber Line
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
HMAC	Hash Message Authentication Code
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LAN	Local Area Network
LCOS	LANCOM Systems Operating System
OS	Operating System
PC	Personal Computer
PKCS	Public Key Cryptography Standards
PP	Protection Profile
PPP	Point-to-Point Protocol
RFC	Requests for Comments
RSA	Rivest, Shamir and Adleman, an asymmetric crypto algorithm
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SPI	Security Parameters Index
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol

TOE	Target of Evaluation
TSF	TOE Security Functionality
UDP	User Datagram Protocol
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

12.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

Protection Profile - An implementation-independent statement of security needs for a TOE type.

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 - A set of software, firmware and/or hardware possibly accompanied by guidance.

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, Revision 4, September 2012

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8].

[5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0815-2013, LANCOM Systems Operating System LCOS 8.70 CC with IPsec VPN, LANCOM Systems GmbH, Version 1.15, Release, 08.05.2013

[7] Evaluation Technical Report (ETR) for BSI-DSZ-CC-0815, LANCOM Systems Operating System LCOS 8.70 CC with IPsec VPN, Version 1.2, 10.05.2013, SRC Security Research & Consulting GmbH, (confidential document)

[8] Preparative Procedures (AGD_PRE) for LANCOM Systems Operating System LCOS 8.70 CC with IPsec VPN, LANCOM Systems GmbH, Version 1.8, Release, 11.04.2013

[9] Operational user guidance (AGD_OPE) for LANCOM Systems Operating System LCOS 8.70 CC with IPsec VPN, Version 1.10, Release, LANCOM Systems GmbH, 17.04.2013

[10] Algorithmenkatalog, Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Übersicht vom 18.02.2013

[11] Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Technische Richtline BSI TR-02102, version 2013.02, Bundesamt für Sicherheit in der Informationstechnik, Stand 09.01.2013

[8] specifically

- AIS 20, Version 2, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 31, Version 2, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- 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

Assurance Class	Assurance Components
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 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.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
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”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“Objectives

EAL1 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.

EAL1 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.

EAL1 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 EAL1 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 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 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.

EAL2 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 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 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 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL4 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. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 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 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL5 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 EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 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 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL6 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.

EAL6 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 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL7 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 EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

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.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.