Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Zertifizierungsreport

BSI-DSZ-BSZ-0013-2025

zu

LANCOM Multi-WAN SD-WAN Gateway 'LANCOM 1930EF' with LANCOM Systems Operating System 'LCOS 10.80' and IPsec VPN, Version 10.80

der

LANCOM Systems GmbH

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582- 0
bsz@bsi.bund.de
Internet: https://www.bsi.bund.de/bsz

Deutsches IT-Sicherheitszertifikat
erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-BSZ-0013-2025(*)

LANCOM Multi-WAN SD-WAN Gateway 'LANCOM 1930EF' with LANCOM Systems Operating System 'LCOS 10.80' and IPsec VPN, Version 10.80

Beschleunigte Sicherheitszertifizierung

von

LANCOM Systems GmbH

für den Geltungsbereich
Allgemeine Netzwerkkomponenten und eingebettete IP-vernetzte Geräte

fixed time certification

Das in diesem Zertifikat genannte IT-Produkt wurde von einer anerkannten Prüfstelle nach der Evaluationsmethodologie EN 17640 „Zeitlich festgelegte Cybersicherheitsevaluationsmethodologie für IKT-Produkte“ (FiT CEM) ergänzt um Anforderungen und Interpretationen des Zertifizierungsprogramms Beschleunigte Sicherheitszertifizierung (BSZ) des Bundesamtes für Sicherheit in der Informationstechnik evaluiert.
Das Zertifizierungsverfahren wurde in Übereinstimmung mit den Anforderungen und Regeln des BSI eigenen Programms zur Beschleunigten Sicherheitszertifizierung (BSZ) durchgeführt.

(*) Dieses Zertifikat gilt nur für die angegebene Version des Produkts in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport und -bescheid. Details zur Gültigkeit sind dem Zertifizierungsreport Teil A, Kap. 4 zu entnehmen.

Dieses Zertifikat ist keine generelle Empfehlung des IT-Produkts durch das Bundesamt für Sicherheit in der Informationstechnik oder einer anderen Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das IT-Produkt durch das Bundesamt für Sicherheit in der Informationstechnik oder einer anderen Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, ist weder enthalten noch zum Ausdruck gebracht.

Bonn, 16. Januar 2025
Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag

Sandro Amendola L.S.
Abteilungsleiter

Inhaltsverzeichnis

A Zertifizierung

1 Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG[1] die Aufgabe, für Produkte (Systeme oder Komponenten) der Informationstechnik Sicherheitszertifikate zu erteilen.

Die Zertifizierung eines Produkts wird auf Veranlassung des Herstellers oder eines Vertreibers – im folgenden Antragsteller genannt – durchgeführt.

Bestandteil des Verfahrens ist die technische Prüfung (Evaluierung) des Produkts gemäß den vom BSI öffentlich bekannt gemachten oder allgemein anerkannten Sicherheitskriterien.

Die Prüfung wird in der Regel von einer vom BSI anerkannten Prüfstelle oder vom BSI selbst durchgeführt.

Das Ergebnis des Zertifizierungsverfahrens ist der vorliegende Zertifizierungsreport. Hierin enthalten sind u. a. das Sicherheitszertifikat (zusammenfassende Bewertung) und der detaillierte Zertifizierungsbericht.

Der Zertifizierungsbericht enthält die sicherheitstechnische Beschreibung des zertifizierten Produkts, die Einzelheiten der Bewertung und Hinweise für den Anwender.

2 Grundlagen des Zertifizierungsverfahrens

Die Zertifizierungsstelle führt das Verfahren nach Maßgabe der folgenden Vorgaben durch:

- BSI-Gesetz[1]
- BSI-Zertifizierungs- und Anerkennungsverordnung[2]
- Besondere Gebührenverordnung BMI (BMIBGebV)[3]
- besondere Erlasse des Bundesministeriums des Innern und für Heimat
- Produktzertifizierung im BSI: Programm Beschleunigte Sicherheitszertifizierung (BSZ-Produkte) [1]
- Anerkennung von Prüfstellen im BSI: Programm im Bereich Beschleunigte Sicherheitszertifizierung (BSZ-Prüfstellen) [2]
- Anwendungshinweise und Interpretationen zum Schema für die BSZ (AIS B) [3]

Das Verfahren wurde im Geltungsbereich **„Allgemeine Netzwerkkomponenten und eingebettete IP-vernetzte Geräte“** der Beschleunigten Sicherheitszertifizierung durchgeführt.

[1] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 11 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858) geändert worden ist

[2] Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungs- und Anerkennungsverordnung - BSIZertV) vom 17. Dezember 2014, Bundesgesetzblatt Jahrgang 2014 Teil I, Nr. 61, S. 2231

[3] Besondere Gebührenverordnung BMI (BMIBGebV), Abschnitt 7 (BSI-Gesetz) vom 2. September 2019 (BGBl. I S. 1359), die zuletzt durch Artikel 1 der Verordnung vom 10. September 2021 (BGBl. I S. 4429) geändert worden ist

3 Anerkennungsvereinbarungen

Um die Mehrfachzertifizierung des gleichen Produkts in verschiedenen Staaten zu vermeiden, besteht ein Abkommen zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten der Programme CSPN (Certification de sécurité de premier niveau) und BSZ zwischen dem BSI und der französischen ANSSI (Agence nationale de la sécurité des systèmes d'information) [4]. Das Abkommen ist zunächst befristet auf zwei Jahre, d.h. bis zum 14.05.2026. Damit werden grundsätzlich alle CSPN-Zertifikate in Deutschland vom BSI und alle BSZ-Zertifikate von der ANSSI anerkannt.

Es können allerdings Zertifikate von der Anerkennung ausgenommen werden. Dies kann sowohl durch die ausstellende Seite als auch durch die anerkennende Seite geschehen.

4 Durchführung der Evaluierung und Zertifizierung

Die Zertifizierungsstelle führt für jede einzelne Evaluierung eine Prüfbegleitung durch, um einheitliches Vorgehen, einheitliche Interpretation der Kriterienwerke und einheitliche Bewertungen sicherzustellen.

Das Produkt LANCOM Multi-WAN SD-WAN Gateway 'LANCOM 1930EF' with LANCOM Systems Operating System 'LCOS 10.80' and IPsec VPN, Version 10.80 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluierung des Produkts LANCOM Multi-WAN SD-WAN Gateway 'LANCOM 1930EF' with LANCOM Systems Operating System 'LCOS 10.80' and IPsec VPN, Version 10.80 wurde von der SRC Security Research & Consulting GmbH durchgeführt. Die Evaluierung wurde am 05. Dezember 2024 abgeschlossen. Das Prüflabor ist eine vom BSI anerkannte Prüfstelle (ITSEF)[4].

Der Antragsteller ist: LANCOM Systems GmbH.

Das Produkt wurde entwickelt von: LANCOM Systems GmbH.

Die Zertifizierung wurde damit beendet, dass das BSI die Übereinstimmung mit den Kriterien überprüft und den vorliegenden Zertifizierungsreport erstellt hat.

5 Gültigkeit des Zertifizierungsergebnisses

Dieser Zertifizierungsreport bezieht sich nur auf die angegebene Version des Produkts. Die Ergebnisse der Zertifizierung gelten nur, wenn das Produkt unter den folgenden Bedingungen betrieben wird:

- Alle Auflagen hinsichtlich der Generierung, der Konfiguration und des Einsatzes des Produkts, die in diesem Report gestellt werden, werden beachtet.
- Das Produkt wird in der Umgebung betrieben, die in diesem Report und in den Sicherheitsvorgaben (Englisch: Security Target, ST) beschrieben ist.

Das Zertifikat bestätigt die Vertrauenswürdigkeit des Produkts gemäß den Sicherheitsvorgaben zum Zeitpunkt der Ausstellung. Da sich Angriffsmethoden im Laufe der Zeit fortentwickeln, ist es erforderlich, die maximale Gültigkeit des Zertifikates zu begrenzen. Dieses Zertifikat, erteilt am 16. Januar 2025, ist gültig bis 15. Januar 2027. Die Gültigkeit kann im Rahmen einer Rezertifizierung erneuert werden.

[4] Information Technology Security Evaluation Facility

Der Inhaber des Zertifikates ist verpflichtet,

1. bei der Bewerbung des Zertifikates oder der Tatsache der Zertifizierung des Produkts auf den Zertifizierungsreport hinzuweisen sowie jedem Anwender des Produkts den Zertifizierungsreport und die darin referenzierten Sicherheitsvorgaben und Benutzerdokumentation für den Einsatz oder die Verwendung des zertifizierten Produkts zur Verfügung zu stellen,
2. eine Kontaktadresse zur Meldung von potenziellen Schwachstellen durch Dritte (security@lancom.de) zu betreiben,
3. eingehende Meldungen bezüglich potenzieller Schwachstellen des Produkts unverzüglich zu prüfen und die Prüfung zu dokumentieren, hierzu gehört insbesondere die Prüfung der über die Kontaktadresse gemäß 2. gemeldeten Schwachstellen,
4. die Marktaufsicht des BSI unaufgefordert und unverzüglich nach Bekanntwerden und Bewertung über Schwachstellen des Produkts, die nach dem Zeitpunkt der Zertifizierung durch Sie oder Dritte festgestellt wurden, via Email an marktaufsicht@bsi.bund.de zu informieren. Hinweise zur sicheren Kommunikation und öffentliche Schlüssel zur Verschlüsselung der Emails finden Sie auf der Webseite des BSI unter https://www.bsi.bund.de/dok/Kontakt-MA.
   Des Weiteren müssen Sie den Anwendern des Produkts unverzüglich kostenfrei über den im Zertifizierungsreport genannten sicheren Update-Kanal eine Fehlerkorrektur und auf Wunsch des Anwenders ergänzende Informationen zur Auswirkung der Schwachstelle zur Verfügung zu stellen.

Bei Änderungen am Produkt kann die Gültigkeit des Zertifikats auf neue Versionen ausgedehnt werden. Voraussetzung dafür ist, dass der Antragsteller zur Aufrechterhaltung der Vertrauenswürdigkeit eine Rezertifizierung in Übereinstimmung mit den entsprechenden Regeln beantragt und die Evaluierung keine Abweichungen von den Sicherheitsvorgaben und weiteren Anforderungen aufdeckt.

6 Veröffentlichung

Das Produkt LANCOM Multi-WAN SD-WAN Gateway 'LANCOM 1930EF' with LANCOM Systems Operating System 'LCOS 10.80' and IPsec VPN, Version 10.80 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: https://www.bsi.bund.de/bsz).

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Hersteller des Produkts angefordert werden. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

B Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

- den Sicherheitsvorgaben des Antragstellers für den Evaluationsgegenstand (Englisch: Target of Evaluation, TOE),
- den entsprechenden Prüfergebnissen des Prüflabors und
- ergänzenden Hinweisen und Auflagen der Zertifizierungsstelle.

1 Zusammenfassung

Der Evaluierungsgegenstand (TOE) ist Multi-WAN SD-WAN Gateway.

1.1 Produktbeschreibung

Das LANCOM Multi-WAN SD-WAN Gateway ‚LANCOM 1930EF' bietet sichere VPN Standortvernetzung über unsichere Netze wie z.B. das Internet. Das Gerät verfügt über zwei Gigabit Ethernet WAN Ports und vier Ethernet LAN Ports. Eine Stateful-Firewall schützt das Netzwerk mit Intrusion Prevention und bietet Schutz gegen Denial-of-Service-Angriffe.

1.2 Produktidentifikation

Nr	*Typ*	*Identifier*	*Version*	*Auslieferungsart*
1	Hardware	Multi-WAN SD-WAN Gateway LANCOM 1930EF	A 2023-09-11 MOD A00	-
2	Software	LANCOM Systems Operating System LCOS	LCOS 10.80.0742 SU8	LANCOM Systems GmbH Download-Bereich[5]
2	Dokument	Security Target LANCOM vom 11.09.2024	1.04	Herstellerwebseite[6] / BSI-Webseite
3	Dokument	Secure User Guidance vom 10.09.2024	1.40	Herstellerwebseite[7]

Tabelle 1: Auslieferungsumfang des Evaluierungsgegenstands (TOE)

Die Software- und Hardwareversion des Produkts kann der Administrator über das Web-Interface des TOEs in Erfahrung bringen. Dafür muss er auf den Reiter Systeminformationen -> Systemdaten gehen oder Firmware -> Installierte Version. Zusätzlich wird der Name des TOE und die Version im Banner im command line interface angezeigt, wenn man sich beispielsweise mit SSH verbindet.

1.3 Sicherheitsfunktionen des Evaluierungsgegenstands

Die Werte, die durch den TOE geschützt werden, sind in den Sicherheitsvorgaben [6], Kapitel 3.3, definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und Angreifern in den Kapiteln 3.2, 3.4 und 3.5 dar. Der TOE bietet die in Tabelle 2 aufgezählten Sicherheitsfunktionen an, um die Werte vor den beschriebenen Bedrohungen zu schützen. Diese Sicherheitsfunktionen des TOE wurden in der Evaluation betrachtet.

[5] https://my.lancom-systems.de/downloads/
[6] https://www.lancom-systems.de/pdf/BSZ/LANCOM-BSZ-Security-Target-1930EF.pdf
[7] https://www.lancom-systems.de/pdf/BSZ/LANCOM-BSZ-Secure-User-Guidance-1930EF.pdf

Sicherheitsfunktionen des TOE	*Beschreibung*
SecFunc.HTTPS	Der TOE implementiert Zugriff auf das WEBconfig Management-Interface mit HTTP/1.1 [RFC 7230 ff.] über TLS 1.2/1.3 [RFC 5246/8446] (HTTPS). Die Protokolle gewähren dem Administrator sicheren Login und sicheren Zugriff auf die Management Interfaces unter Gewährleistung der Vertraulichkeit, Integrität und Authentizität der Administrator-Logindaten, der TOE-Konfiguration, der TOE-Firmware und den Monitoring-Daten, wenn diese von und zu dem TOE übertragen werden.
SecFunc.SSH	Der TOE implementiert Zugriff auf das CLI Management Interface mit SSH [RFC 4251 ff.]. Das Protokoll gewährt dem Administrator sicheren Login und sicheren Zugriff auf die Management Interfaces unter Gewährleistung der Vertraulichkeit, Integrität und Authentizität der Administrator-Logindaten, der TOE-Konfiguration und den Monitoring-Daten, wenn diese von und zu dem TOE übertragen werden.
SecFunc.SNMPv3	Der TOE implementiert Zugriff zum SNMP Management Interface mit SNMPv3 [RFC 3411 ff.]. Das Protokoll gewährt dem Administrator sicheren Login und sicheren Zugriff auf die Management Interfaces unter Gewährleistung der Vertraulichkeit, Integrität und Authentizität der Administrator-Logindaten und den Monitoring-Daten, wenn diese von und zu dem TOE übertragen werden.
SecFunc.IPsec	Der TOE implementiert IPsec VPN Verbindungen mit IPsec [RFC 4301 ff.]. Das Protokoll ermöglicht dem Nutzer sichere Datenübertragung über unsichere Netzwerke unter Gewährleistung der Vertraulichkeit, Integrität und Authentizität bei der Übertragung über nicht vertrauenswürdige remote Netzwerke (Internet).
SecFunc.IPsec.Log	Der TOE loggt erfolgreiche und nicht erfolgreiche IPsec VPN Verbindungsaufbauversuche in den TOE Monitoring Daten.
SecFunc.Firewall.Sessions	Der TOE implementiert IPv4 Firewall und Routing Dienste. Durch die Einrichtung des TOE nach SUG werden Nutzern aus vertrauenswürdigen Netzen (LAN) nicht vertrauenswürdige Netze (Internet) zu nutzen und verweigern Nutzern in nicht vertrauenswürdigen Netzen (Internet), vertrauenswürdige Netze (LAN) zu nutzen. Auch erlaubt werden Verbindungen zwischen verschiedenen Unternehmensstandorten sowie Nutzer mit vertrauenswürdigen Mobilgeräten mit IPsec VPN Verbindungen.

Sicherheitsfunktionen des TOE	*Beschreibung*
SecFunc.Firewall.DoS.IDS	Der TOE implementiert eine IPv4 Firewall mit DoS-Schutz und IDS. Der DoS-Schutz kann TCP SYN flooding, Smurf Attacken, LAND Attacken, Ping of Death Attacken, Teardrop Attacken und Bonk Attacken erkennen und darauf reagieren. Das IDS kann IP Spoofing und Portscans erkennen und darauf reagieren.
SecFunc.Firewall.Log	Der TOE loggt Login-Versuche welche von der Firewall abgelehnt wurden in den TOE Monitoring Daten.
SecFunc.Auth.AdmCrds	Der TOE authentisiert Administratoren, bevor sie Zugriff auf die Management-Interfaces WEBconfig, CLI und SNMP erhalten, anhand von Benutzernamen und Passwort oder des SSH-Schlüssels.
SecFunc.Auth.AdmPwdChrs	Der TOE erzwingt Passwort-Vorgaben für das Administrator Passwort: mind. 8 Zeichen, mit mindestens 3/4 der folgenden Vorgaben: kleine Buchstaben, große Buchstaben, Zahlen und Sonderzeichen.
SecFunc.Auth.BrtFrcCtr	Der TOE wirkt gegen Brute-Force Attacken, in dem die Login-Funktionalität eines Interfaces nach einer festgelegten Anzahl fehlgeschlagener Login-Versuche für eine festgelegte Zeit gesperrt wird.
SecFunc.Auth.AutoLogOut	Der TOE implementiert ein automatisches Log-Out des Administrators nach einer festgelegten Zeit der Inaktivität.
SecFunc.Auth.Log	Der TOE loggt erfolgreiche und nicht erfolgreiche Login-Versuche in den Monitoring Daten.
SecFunc.Mgmt.NoInet	Der TOE erlaubt keinen Zugriff auf die Management-Interfaces WEBconfig, CLI und SNMP von unsicheren Netzwerken (wie im SUG beschrieben).
SecFunc.Mgmt.Ports	Der TOE kann so konfiguriert werden, dass er TCP/UDP Ports außerhalb des Standards für die HTTPS, SSH und SNMPv3 Protokolle nutzt, um die Management Interfaces WEBconfig, CLI und SNMP Management-Oberflächen zu nutzen.

Tabelle 2: Sicherheitsfunktionen des TOE

1.4 Konfiguration des Evaluierungsgegenstands

Dieses Zertifikat gilt nur für die in den Sicherheitsvorgaben [6], Kapitel 3 beschriebene Sicherheitsproblemdefinition und in der Secure User Guidance [8] beschriebenen Konfigurationen des TOE. Insbesondere sind die folgenden Funktionen, wie in Kapitel 4 unter „Limits of Evaluation“ der Sicherheitsvorgaben [6] beschrieben, von der Evaluation ausgeschlossen und nicht vom Zertifikat abgedeckt:

- Das Produkt besitzt für Managementzwecke, bei direkter Verbindung mit dem Computer, eine serielle COM-Schnittstelle.
- Das Produkt hat eine USB Schnittstelle, welche für Managementzwecke genutzt werden kann.

- Das Produkt bietet zusätzlich IPv6 Protokolldienste.

Hinweis: Dieses Zertifikat gilt nur für die angegebene Version des Produkts in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport. Dieses Zertifikat ist keine generelle Empfehlung des IT-Produkts durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das IT-Produkt durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, ist weder enthalten noch zum Ausdruck gebracht.

1.5 Beschreibung der Einsatzumgebung

In den Sicherheitsvorgaben [6], Kapitel 2.4, wird die Einsatzumgebung des TOE beschrieben. Hierbei werden Annahmen gemacht, die beim Einsatz des TOE zu praktischen Anforderungen an die Einsatzumgebung werden, ohne die ein im Sinne des Zertifikats sicherer Betrieb nicht bestätigt ist. Hierbei sind die folgenden Punkte relevant:

- Der TOE wird nur in Umgebungen mit physischen Zugriffsbeschränkungen genutzt.
- Der Administrator hat ausschließlich für die physische Installation Zugriff auf den TOE.
- Nutzer des Gerätes haben niemals physischen Zugriff auf das Gerät.
- Für IPSec-VPN Verbindungen wird der [RFC 4301 ff.] Standard verwendet.

1.6 Dokumente

Die evaluierten Dokumente Sicherheitsvorgaben und Secure User Guidance, die in Tabelle 1 aufgeführt sind, werden zusammen mit dem Produkt zur Verfügung gestellt. Hier sind die Informationen enthalten, die zum sicheren Umgang mit dem TOE in Übereinstimmung mit den Sicherheitsvorgaben benötigt werden.

Zusätzliche Hinweise und Auflagen zum sicheren Gebrauch des TOE, die im Teil B Abschnitt 2.6 enthalten sind, müssen befolgt werden.

2 Die Evaluierung

Der TOE wurde nach der Evaluationsmethodologie EN 17640 „Zeitlich festgelegte Cybersicherheitsevaluationsmethodologie für IKT-Produkte“ (FiT CEM) evaluiert. Hierbei wurden die Anwendungshinweise und Interpretationen zum Schema BSZ (AIS B) [3] beachtet. Insbesondere wurde die AIS B4 „Anforderungen an die Evaluierung gemäß BSZ“ befolgt.

Basierend auf dem Ansatz der BSZ mit risikogetriebener Evaluierung innerhalb einer fester Evaluierungszeit wurde der Prozess der Inbetriebnahme sowie die Übereinstimmung des TOE zu der Beschreibung in den Sicherheitsvorgaben und der AIS B6 „Anforderungen an einen TOE “ überprüft. Hauptteil der Evaluierung war die Untersuchung der Widerstandsfähigkeit der Sicherheitsfunktionen mittels Penetrationstests.

2.1 Inbetriebnahme und Konfiguration

Der TOE wurde wie in AIS B4 [3] gefordert in Betrieb genommen und konfiguriert.

Der TOE kann durch die Beschreibung in den Sicherheitsvorgaben [6], Kapitel 3.2, und der Secure User Guidance [8] in die zertifizierte Konfiguration gebracht werden.

2.2 Konformität und Funktionsanalyse der Sicherheitsfunktionen

Die tatsächlichen Sicherheitsfunktionen des TOE stimmen mit den in den Sicherheitsvorgaben beschriebenen Sicherheitsfunktionen (siehe Tabelle 2) überein. Alle in AIS B6 [3] geforderten Sicherheitsfunktionen sind im TOE enthalten.

2.3 Widerstandsfähigkeit der Sicherheitsfunktionen

Der TOE wurde einem Penetrationstest unterzogen um die Widerstandsfähigkeit der Sicherheitsfunktionen zu überprüfen. Hierbei wurde untersucht, ob die in Kapitel 3.4 der Sicherheitsvorgaben [6] beschriebenen Angreifer die Sicherheitsfunktionen unter Ausnutzung von Schwachstellen brechen oder umgehen konnten. Es konnten keine ausnutzbaren Schwachstellen gefunden werden.

2.4 Ergebnis der kryptographischen Bewertung

Die Implementierung der kryptografischen Funktionen wurde nach AIS B2 [3] geprüft. Sie ist konform zu den in [3] geforderten SCES-ACM und BSI-TR-02102 Vorgaben und es konnten keine ausnutzbaren Schwachstellen gefunden werden.

Die Stärke der kryptografischen Algorithmen wurde in diesem Zertifizierungsverfahren nicht bewertet (siehe BSIG §9, Abs. 4, 2). Jedoch können kryptografische Funktionen mit einem Sicherheitsniveau unterhalb von 120 Bit nicht länger als sicher angesehen werden, ohne den Anwendungskontext zu beachten. Deswegen muss geprüft werden, ob diese kryptografischen Funktionen für den vorgesehenen Verwendungszweck angemessen sind. Weitere Hinweise und Anleitungen können der „Technischen Richtlinie BSI TR-02102“ (https://www.bsi.bund.de/dok/6615148) entnommen werden.

Die Tabelle in Anhang A in Teil C dieses Reportes gibt einen Überblick über die im TOE enthaltenen kryptographischen Funktionen und legt deren Bewertung des Sicherheitsniveaus aus kryptografischer Sicht dar. Jede kryptografische Funktion, die in der Spalte 'Sicherheitsniveau mehr als 120 Bit' ein 'Nein' enthält, erreicht nur ein Sicherheitsniveau unterhalb von 120 Bit (im allgemeinen Anwendungsfall).

2.5 Updatemechanismus

Der TOE verfügt über einen Sicheren Updatemechanismus, der gegebenenfalls notwendige Sicherheitsupdates ermöglicht. Der Prozess ist in der Weiteren Dokumentation [10] auf Seite 5 initial sowie ab Seite 9 der Secure User Guidance [8] beschrieben.

2.6 Auflagen und Hinweise zur Benutzung des TOE

Die in Tabelle 1 genannte Betriebsdokumentation enthält die notwendigen Informationen zur Anwendung des TOE und alle darin enthaltenen Sicherheitshinweise sind zu beachten. Zusätzlich sind die Anforderungen an die Einsatzumgebung des TOE aus den Sicherheitsvorgaben zu beachten, ohne die ein im Sinne des Zertifikats sicherer Betrieb nicht bestätigt ist.

Der Anwender des Produkts muss die Ergebnisse dieser Zertifizierung sowie die zeitliche Begrenzung der Gültigkeit des Zertifikats in seinem Risikomanagementprozess berücksichtigen.

Die Begrenzung der Gültigkeit der Verwendung der kryptographischen Algorithmen, wie in Teil B Abschnitt 2.4 dargelegt, muss ebenso durch den Anwender und seinen Risikomanagementprozess für das IT-System berücksichtigt werden.

3 Definitionen

3.1 Abkürzungen

AIS Anwendungshinweise und Interpretationen zum Schema

BSI Bundesamt für Sicherheit in der Informationstechnik

BSIG BSI-Gesetz

TOE Evaluierungsgegenstand (Englisch: Target of Evaluation)

LCOS LANCOM Systems Operating System

SUG Handbuch zur sicheren Benutzung (Englisch: Secure User Guidance)

ETR Evaluierungsbericht (Englisch: Evaluation Technical Report)

IT Informationstechnik (Englisch: Information Technology)

SF Sicherheitsfunktion (Englisch: Security Function)

ST Sicherheitsvorgaben (Englisch: Security Target)

TLS Transport Layer Security

USB Universal Serial Bus

VPN Virtual Private Network

IDS Intrusion Detection Services

WAN Wide Area Network

3.2 Glossar

Evaluierungsgegenstand – Untersuchtes Produkt bzw. untersuchter Teil des Produkts.

Sicherheitsvorgaben - In diesem Dokument werden Sicherheitsfunktionalität, Schnittstellen, Einsatzszenario mit Bedrohungsmodell und Umgebung des Evaluierungsgegenstands beschrieben.

3.3 Literaturangaben

[1] BSI-Zertifizierung: Verfahrensdokumentation zum Zertifizierungsprozess (BSZ- Produkte)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/BSZ-Produkte.html

[2]BSI-Zertifizierung: Verfahrensdokumentation zu Anforderungen an Prüfstellen, die Anerkennung und Lizenzierung (BSZ-Prüfstellen)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/BSZ-Pruefstellen.html

[3] Anwendungshinweise und Interpretationen zum Schema (AIS), die für den TOE relevant sind[8]
https://www.bsi.bund.de/bsz

[8] Die für diese Zertifizierung geltenden AIS B:

- AIS B1 Anforderungen an ST und IAR, Version 2.0.1, 01.03.2024
- AIS B2 Anforderungen an die Evaluierung kryptographischer Mechanismen gemäß BSZ, Version 2.0, 01.03.2024
- AIS B3 Anforderungen an die Benutzeranleitung, Version, 2.0, 01.03.2024
- AIS B4 Anforderungen an die Evaluierung gemäß BSZ, Version 2.0, 01.03.2024
- AIS B5 Anleitung zur Bestimmung des Aufwands für eine BSZ-Evaluierung, Version 2.0, 01.03.2024
- AIS B6 Anforderungen an einen TOE, Version 2.0, 01.03.2024

[4] Anerkennungsabkommen: Mutual Recognition Agreement of Cybersecurity Evaluation Certificates issued under a Fixed-time Certification Process, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/BSZ/Abkommen_Anerkennung_ANSSI_BSI.pdf

[5] Deutsche IT-Sicherheitszertifikate, periodisch aktualisierte Liste, die auch auf der Internet-Seite des BSI veröffentlicht wird, https://www.bsi.bund.de/bsz

[6] Sicherheitsvorgaben BSI-DSZ-BSZ-0013-2025, Version 1.04, 11.09.2024, Security_Target_1930EF-1.045986, LANCOM Systems

[7] Evaluierungsbericht, Version 2.1, 04.12.2024, BSZ-Evaluierungsreport, SRC Security Research Consulting GmbH

[8] SUG für den TOE, Version 1.40, 10.09.2024, Secure User Guidance for LANCOM 1930EF, LANCOM Systems

[9] Kryptografische Spezifikation, Version 1.0, Datum 04.12.2023, CRYPTO-ANNEX FOR LANCOM MULTI-WAN SD-WAN GATEWAY 'LANCOM 1930EF' WITH LANCOM SYSTEMS OPERATING SYSTEM 'LCOS 10.80' AND IPSEC VPN, LANCOM Systems

[10] Weitere Dokumentation, Version 1.0, 04.12.2023, ADDITIONAL DOCUMENTATION FOR LANCOM MULTI-WAN SD-WAN GATEWAY 'LANCOM 1930EF' WITH LANCOM SYSTEMS OPERATING SYSTEM 'LCOS 10.80' AND IPSEC VPN, LANCOM Systems

C Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

Anhang A: Übersicht und Bewertung der im TOE enthaltenen kryptographischen Funktionalitäten

Anhang A zum Zertifizierungsreport BSI-DSZ-BSZ-0013-2025 Übersicht und Bewertung der im TOE enthaltenen kryptographischen Funktionalitäten

Nr.	*Zweck*	*Kryptografische Funktion*	*Implementierungs-standard*	*Schlüsselgröße in Bit*	*Sicherheits-niveau mehr als 120 Bit*	*Bemerkungen*
	Schnittstelle WEBconfig via TLS 1.2/1.3					
1	Vertrauenswürdiger Kanal	TLS v1.2/1.3	[RFC 8446] (TLS 1.3) [RFC 5246] (TLS 1.2) [RFC 5746] (TLS-RENEGO)			
2	Authentizität	ECDSA Signatur mit SHA-2 (secp256r1, secp384r1, secp521r1)	[RFC 8446] (TLS 1.3) [RFC 5246] (TLS 1.2) [RFC 8422] (TLSECC) [RFC 4366] (TLSEXT) [ANSI X9.62] (ECDSA) [SECG SEC2] (ECC) [RFC 5280] (PKIX) [FIPS 180-4] (SHA)	256, 384, 521	Ja	
3	Authentizität	RSA Signatur (RSASSA-PKCS1-v1_5) mittels SHA-2	[RFC 5246] (TLS 1.2) [RFC 3447] (PKCS#1 v2.1) [RFC 5280] (PKIX) [FIPS 180-4] (SHA)	3072, 4096	Ja	
4	Authentisierung	ECDSA Signatur mit SHA-2 (secp256r1, secp384r1, secp521r1) (für ECDHE_ECDSA)	[RFC 8446] (TLS 1.3) [RFC 5246] (TLS 1.2) [RFC 8422] (TLSECC) [RFC 4366] (TLSEXT) [ANSI X9.62] (ECDSA) [SECG SEC2] (ECC) [RFC 5280] (PKIX) [FIPS 180-4] (SHA)	256, 384, 521	Ja	
5	Authentisierung	RSA Signatur (RSASSA-PKCS1-v1_5) mittels SHA-2 (für ECDHE_RSA)	[RFC 5246] (TLS 1.2) [RFC 8422] (TLSECC) [RFC 4366] (TLSEXT) [RFC 8017] (PKCS#1 v2.2) [RFC 5280] (PKIX) [FIPS 180-4] (SHA)	3072, 4096	Ja	

Nr.	*Zweck*	*Kryptografische Funktion*	*Implementierungs-standard*	*Schlüsselgröße in Bit*	*Sicherheits-niveau mehr als 120 Bit*	*Bemerkungen*
6	Authentisierung	RSA Signatur (RSASSA-PKCS1-v1_5) mit SHA-2 (für DHE_RSA)	[RFC 5246] (TLS 1.2) [RFC 4366] (TLSEXT) [RFC 3447] (PKCS#1 v2.1) [RFC 5280] PKIX) [FIPS 180-4] (SHA)	3072, 4096	Ja	
7	Authentisierung	Challenge-Response-Passwort Authentisierung mit SHA-256	[FIPS 180-4] (SHA)	256	Ja	
8	Schlüssel-aushandlung	ECDHE (secp256r1, secp384r1, secp521r1)	[RFC 8422] (TLSECC) [RFC 4366] (TLSEXT) [IEEE P1363] (ECDH) [SECG SEC2] (ECC)	256, 384, 521	Ja	
9	Schlüssel-aushandlung	DHE (ffdhe3072, ffdhe4096)	[RFC 8446] (TLS 1.3) [RFC 5246] (TLS 1.2) [RFC 7917] (DHE)	3072, 4096	Ja	
10	Vertraulichkeit	AES im GCM Modus	[RFC 8446] (TLS 1.3) [RFC 5246] (TLS 1.2) [RFC 5288] (TLS-AES-GCM) [RFC 5289] (TLS-AES-GCM) [RFC 5116] (AES-GCM) [FIPS 197] (AES) [SP 800-38D] (GCM)	128, 256	Ja	
11	Integrität	HMAC mit SHA-2	[RFC 8446] (TLS 1.3) [RFC 5246] (TLS 1.2) [FIPS 180-4] (SHA) [RFC 2104] (HMAC)	256, 384	Ja	
12	Zufallszahlen	Generierung von Zufallszahlen für kryptografische Algorithmen und Protokolle durch den RNG der SEC in der CPU (QorIQ T1024)	[QorIQ SEC] (RNG)	-		
	Zugriff auf die Kommandozeile (CLI) mittels SSH					

Nr.	*Zweck*	*Kryptografische Funktion*	*Implementierungs-standard*	*Schlüsselgröße in Bit*	*Sicherheits-niveau mehr als 120 Bit*	*Bemerkungen*
13	Vertrauenswürdiger Kanal	SSH	[RFC 4251] (SSH-ARCH) [RFC 4252] (SSH-USERAUTH) [RFC 4253] (SSH-TRANS) [RFC 4254] (SSH-CONNECT)			
14	Authentizität	Administrator Handlung: Abgleich des Server host key Fingerabdrucks auf dem Client	[RFC 4253] (SSH-TRANS)	-		
15	Authentizität	Administrator Handlung: Vor-Konfiguration des Administrator public key auf dem Server	[RFC 4252] (SSH-USERAUTH)	-		
16	Authentizität	Administrator Handlung: Vor-Konfiguration des Administrator Passworts auf dem Server	-	-		
17	Authentisierung	ECDSA Signatur mit SHA-2 (ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521)	[RFC 5656] (SSH-ECC) [SEC1] (ECC) [SEC2] (ECC) [ANSI X9.62] (ECDSA) [FIPS 180-4] (SHA)	256, 384, 521	Ja	
18	Authentisierung	RSA Signatur (RSASSA-PKCS1-v1_5) Mit SHA-2 (rsa-sha2- 256, rsa-sha2-512)	[RFC 8332] (SSH-AUTH-SHA2) [RFC 4253] (SSH-TRANS), [RFC 4252] (SSH-USERAUTH) [RFC 8017] (PKCS#1 v2.2) [FIPS 180-4] (SHA)	3072, 4096	Ja	

Nr.	*Zweck*	*Kryptografische Funktion*	*Implementierungs-standard*	*Schlüsselgröße in Bit*	*Sicherheits-niveau mehr als 120 Bit*	*Bemerkungen*
19	Schlüssel-aushandlung	ECDH mit SHA-2 (ecdh- sha2-nistp256, ecdh-sha2-nistp384, ecdh- sha2-nistp521)	[RFC 5656] (SSH-ECC) [SEC1] (ECC) [SEC2] (ECC) [ANSI X9.63] (ECC) [FIPS 180-4] (SHA)	256, 384, 521	Ja	
20	Schlüssel-aushandlung	DH mit SHA-2 (diffie- hellman-group-exchange-sha256)	[RFC 4419] (SSH-DH-GEX) [HAC] (DH) [FIPS 180-4] (SHA)	3072, 4096	Ja	
21	Vertraulichkeit	AES im GCM Modus	[RFC 5647] (SSH-AES-GCM) [RFC 5116] (AES-GCM) [FIPS 197] (AES) [SP 800-38D] (GCM)	128, 256	Ja	
22	Vertraulichkeit	AES im CTR Modus	[RFC 4344] (SSH-AES-CTR) [FIPS 197] (AES) [SP 800-38A] (CTR)	128, 192, 256	Ja	
23	Integrität	HMAC mit SHA-2	[RFC 6668] (SSH-SHA-2) [FIPS 180-4] (SHA) [RFC 2104] (HMAC)	256, 512	Ja	
	Zufallszahlen	Generierung von Zufallszahlen für kryptografische Algorithmen und Protokolle durch den RNG der SEC in der CPU (QorIQ T1024)	[QorIQ SEC] (RNG)	-		
	Management Interface mmittels SNMPv3					
24	Vertrauenswürdiger Kanal	SNMPv3	[RFC 3411] (SNMP-ARCH) [RFC 3412] (SNMP-MSG) [RFC 3414] (SNMP-USM) [RFC 3415] (SNMP-VACM)	-		

Nr.	*Zweck*	*Kryptografische Funktion*	*Implementierungs-standard*	*Schlüsselgröße in Bit*	*Sicherheits-niveau mehr als 120 Bit*	*Bemerkungen*
25	Authentizität	Administrator Handlung: Vor-Konfiguration der Authentisierung auf dem Server)				
26	Vertraulichkeit	AES im CFB Modus	[RFC 3826] (SNMP-AES) [FIPS 197] (AES) [SP 800-38A] (CFB)	128, 192, 256	Ja	
27	Integrität	HMAC mit SHA-2	[RFC 7860] (SNMP-SHA-2) [RFC 6234] (SHA-2) [FIPS 180-4] (SHA) [RFC 2104] (HMAC)	256, 384, 512	Ja	
28	Zufallszahlen	Generierung von Zufallszahlen für kryptografische Algorithmen und Protokolle durch den RNG der SEC in der CPU (QorIQ T1024)	[QorIQ SEC] (RNG)			
	Sichere Kommunikation über IPsec					
29	Vertrauenswürdiger Kanal	IPsec with IKEv2 and ESP	[RFC 4301] (IPsec) [RFC 7296] (IKEv2) [RFC 8247] (IKE-ALGO) [RFC 4303] (ESP) [RFC 8221] (ESP-ALGO)	-		
30	Authentizität	ECDSA Signatur mit SHA-2 (brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, secp256r1, secp384r1, secp521r1)	[RFC 7427] (IKEv2-SIGAUTH) [RFC 4754] (IKE-ECDSA) [ANSI X9.62] (ECDSA) [RFC 5280] (PKIX) [RFC 3447] (PKCS#1 v2.1) [FIPS 180-4] (SHA)	256, 384, 512	Ja	

Nr.	*Zweck*	*Kryptografische Funktion*	*Implementierungs-standard*	*Schlüsselgröße in Bit*	*Sicherheits-niveau mehr als 120 Bit*	*Bemerkungen*
31	Authentizität	RSA Signature (RSASSA- PSS) using SHA-2	[RFC 7427] (IKEv2-SIGAUTH) [RFC 4055] (RSASSA-PSS) [RFC 5280] (PKIX) [RFC 3447] (PKCS#1 v2.1) [FIPS 180-4] (SHA)	3072, 4096	Ja	
32	Authentizität	Administrator Handlung: Vor-Konfiguration der Pre-Shared Keys	[RFC 7296] (IKEv2)	-		
33	Authentisierung	ECDSA Signatur mit SHA-2 (brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, secp256r1, secp384r1, secp521r1)	[RFC 7427] (IKEv2-SIGAUTH) [RFC 4754] (IKE-ECDSA) [ANSI X9.62] (ECDSA) [RFC 5280] (PKIX) [RFC 3447] (PKCS#1 v2.1) [FIPS 180-4] (SHA)	256, 384, 512	Ja	
34	Authentisierung	RSA Signatur (RSASSA- PSS) using SHA-2	[RFC 7427] (IKEv2-SIGAUTH) [RFC 4055] (RSASSA-PSS) [RFC 5280] (PKIX) [RFC 3447] (PKCS#1 v2.1) [FIPS 180-4] (SHA)	3072, 4096	Ja	
35	Authentisierung	MAC Generierung und Verifizierung mit Pre-Shared Keys und SHA-2	[RFC 7296] (IKEv2) [FIPS 180-4] (SHA)	256, 384, 512	Ja	
36	Schlüssel-aushandlung	ECDH (brainpoolP256r1, brainpoolP384r1, brainpoolP512r1)	[RFC 6954] (IKE-ECC-BP) [RFC 5639] (ECC-BP) [EBP] (ECC Brainpool)	256, 384, 512	Ja	
37	Schlüssel-aushandlung	ECDH (secp256r1, secp384r1, secp521r1)	[RFC 5903] (IKE-ECP) [IEEE P1363] (ECDH) [SECG SEC2] (ECC)	256, 384, 521	Ja	
38	Schlüssel-aushandlung	DH	[RFC 3526] (IKE-MODP) [RFC 2631] (DH) [ANSI X9.42] (DH)	3072, 4096	Ja	

Nr.	*Zweck*	*Kryptografische Funktion*	*Implementierungs-standard*	*Schlüsselgröße in Bit*	*Sicherheits-niveau mehr als 120 Bit*	*Bemerkungen*
39	Vertraulichkeit	AES im GCM Modus	[RFC 8247] (IKE-ALGO) [RFC 5282] (IKE-AEAD) [RFC 5116] (AES-GCM) [RFC 4106] (ESP-GCM) [FIPS 197] (AES) [SP 800-38D] (GCM)	128, 192, 256	Ja	
40	Vertraulichkeit	AES im CBC Modus	[RFC 3602] (AES-CBC) [FIPS 197] (AES) [SP 800-38A] (CBC)	128, 192, 256	Ja	
41	Integrität	HMAC mit SHA-2	[RFC 4868] (HMAC-SHA-2-IPsec) [FIPS 180-4] (SHA) [RFC 2104] (HMAC)	256, 384, 512	Ja	
42	Zufallszahlen	Generierung von Zufallszahlen für kryptografische Algorithmen und Protokolle durch den RNG der SEC in der CPU (QorIQ T1024)	[QorIQ SEC] (RNG)	-		

Tabelle 3: Kryptografische Funktionen des TOE

Bemerkung: Ende des Reportes