Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1087-2026

for

VMware ESXi, Version 8.0g

from

Broadcom, Inc.

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-1087-2026 (*)

Operating System

VMware ESXi, Version 8.0g

from	Broadcom, Inc.
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.2
valid until:	24 February 2031

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 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, 25 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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - 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.

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]
- BSI Schedule of 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]

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 2 December 2025, BGBI. 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 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

- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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.

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

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. 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 VMware ESXi, Version 8.0g has undergone the certification procedure at BSI.

The evaluation of the product VMware ESXi, Version 8.0g was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 24 February 2026. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Broadcom, Inc..

The product was developed by: Broadcom, Inc..

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 in the following report 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 25 February 2026 is valid until 24 February 2031. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
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 VMware ESXi, Version 8.0g 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] Broadcom, Inc.
3421 Hillview Ave
California 94304 Palo Alto
USA

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 VMware ESXi Version 8.0g, a VMware software product implementing a hypervisor. The TOE is designed as a virtualization platform, providing the ability to implement and virtualize different workloads across multiple virtual machines (VMs) while providing isolation and efficient use of compute, storage, and network resources. This allows for implementation of cloud environments in support of wide array of various data center workloads or on-demand infrastructure.

The Security Target [5] 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.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [5], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
SF1.Security Audit	The TSF generates audit records locally for a all audit events listed in the ST [5], Table 10: Additional Auditable Events. Each audit record includes date, time, applicable subject and objective identities, the outcome of the event, and any additional information required by the TOE's conformance claims on a per-event basis.
SF2.Random Number Generation	The TOE provides random numbers for the purpose of TLS through its OpenSSL library.
SF3.User Data Protection	A Guest VM cannot access the data of another Guest VM, or transfer data to another Guest VM other than through the mechanisms described in the ST [5], chapter 6.1.3.4 FDP_IFF.1 Simple security attribute (virtual networking) when expressly enabled by an authorized user with administrator role.
SF4.Identification and Authentication	Users must be successfully identified by the TOE for all remote interfaces to the TOE. Identification and Authentication is based on a username and password, session IDs, tokens or tickets. An administrative user can import certificate trust anchors that are used for token (JWT and SAML) validation.
SF5.Security Management	The TOE has one administrator role that can perform all management functions defined in the ST [5], chapter 6.1.5.2 Specification of Management. No other user can perform management functions. The TOE has several management interfaces that can be used for that purpose.
SF6.Protection of the TSF	The TOE ensures that each virtual machine is isolated from any other virtual machines co-existing on the TOE. This isolation is provided at the virtualization layer of the TOE.
SF7.Cryptographic Support and Encrypted Channels	The TOE uses cryptography to secure data in transit between itself and its operational environment. All TOE cryptographic services are implemented by the OpenSSL cryptographic library.

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 3.2. 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], chapters 3.3 to 3.5.

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:

VMware ESXi, Version 8.0g

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW/ ISO	ESXi 8.0g Install ISO SHA-256: 66121a7158a84a36b1d6a6d6a4d01374f9e75df06291477cf171e513de42c78d	v8.0g build 25191479	Broadcom Support Portal download
2	DOC/ pdf	Installation and Operational Guidance for ESXi 8.0g SHA-256: 04cc3c3ca7c59a804ca0bfee0267cc550799c65cd8256dbf7cc9d08a171f923e	v1.0	Common Criteria Security Certification Portal
3	DOC/ pdf	Entropy Administrator Guide for ESXi 8.0g SHA-256: 3979e3483a039acac5c9df057f2acfbae9fcf68f4a9b4cc6e010a7eb6312b914	v1.0	Common Criteria Security Certification Portal
4	DOC/ zip	Evaluated Configuration Documentation Package SHA-256: 55f7810e1764adde3036c236119abd0cbe2e6b56a6e327fc911202c81b87304a	V1.0	Common Criteria Security Certification Portal

No	Type	Identifier	Release	Form of Delivery
5	DOC/ zip	VMware vSphere Management SDK SHA-256: 230dc4dbc6ddb7ed549d63cc693c75d63e32b1f089903094cb8a757bac96bc5a	8.0.0	Broadcom Developer Portal download

Table 2: Deliverables of the TOE

After downloading the deliverables from the designated Broadcom portals, the user can check the integrity and authenticity by calculating and comparing the SHA-256 value of the downloaded deliverable with the reference provided here and in the security target [5].

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: Security Audit, Random Number Generation, User Data Protection, Identification and Authentication, Security Management, Protection of the TSF and Cryptographic Support and Encrypted Channels.

Specific details concerning the above mentioned security policies can be found in Security Target [5], Chapter 7.

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.PHYSICAL: Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment. As a consequence, no local attacker can mount attacks like e.g T.UNAUTHORIZED_MODIFICATION
- OE.NETWORK: The network environment provides the ability to provide physically or logically partitioned networks
- OE.TRUSTED_ADMIN: TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner
- OE.TIME: The operational environment provides reliable time stamps to the TOE
- OE.ENTROPY: An external entropy source, such as an HSM, is provided that generates entropy that is EAL4+ certified at PTG.2

Details can be found in the Security Target [5], chapter 4.2.

5. Architectural Information

The TOE comprises the following subsystems: VMX, Virtual Machine Monitor (VMM), Networking, VMKernel Core, vmKernel Hardware, VMKernel RM CPU, VMkernel RM Memory, VMFS ObjectCache/VolumeCache/LVM, vSCSI/PSA/Software iSCSI, Userworlds, HostD, vmSyslogd, VMFS Snapshots, FileSystemSwitch, FileSystemDeviceSwitch, VMFS Tools, TLS, vmacore, Settingsd, ESXTokenD, PAM, Busybox, rhttpproxy and NFS Client.

A high level description of the IT product and its major components can be found in the Security Target [5], chapter 1.5.1.

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

All evaluated software configurations of the TOE have been tested (see Section 8).

The tests were executed on a DELL EMC PowerEdge R740xd with Intel Xeon Gold 6130 CPUs (Intel Skylake Microarchitecture).

Developer Testing Approach

Test cases are organized based on the security functions they test. This ensures that each security aspect of the system is thoroughly evaluated. Within each security function, test cases are further categorized by the Security Functional Requirements (SFRs) they affect, and then by the relevant subsystem and module.

The developer’s testing effort has been proven sufficient to demonstrate that the security functionality / TSFI perform as specified.

Evaluator Testing

The evaluator testing comprises a repetition of selected developer tests plus independently developed evaluator tests. The subset of developer’s tests contains tests to test the functionality and TSFI that is tested by the developer. It contains automatic and manual tests. The evaluator strategically selected a subset of the developer's tests as repetitions to complement the independent tests made by the evaluator, ensuring comprehensive coverage of all SFRs and TSFIs.

In the independent tests conducted by the evaluator, mindful consideration was given ensuring a whole coverage of all SFRs and TSFIs. This was achieved by thoroughly reviewing the TDS and the ST, and by strategically permutating the parameters of functions that interact with specific interfaces to trigger error conditions and validate expected failure responses. The independent tests include a vAPI Test package to intensively test the vAPI Interface. Additionally, various tests are made to test the JWT and SAML Hok Tokens. Interfaces included in the tests (including the repetition of developer test and the independent tests by the evaluator) are: TLS protocol, VIM Protocol and VIM Managed Objects (HTTPS is there also exercises by necessity), vAPI Protocol and vAPI Services, Virtual CPU and Hypercalls.

During the evaluator’s testing the TOE operated as specified.

Therefore, the TOE passed the evaluators testing. Altogether the tests confirm the TOE functionality as described in the developer documents.

Penetration Testing

The evaluation body conducted penetration testing based on functional areas of concern derived from SFRs and architectural mechanisms. These areas were prioritized with regard to various factors, e.g. attack surface, estimated flaw likelihood, developer testing coverage and detectability of flaws during developer testing.

The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential Enhanced-Basic was actually successful.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

- VMware ESXi Version 8.0g build 25191479 as identified in the first row of table 2,
- installed and configured according to the guidelines as specified in the subsequent rows in table 2,
- running on hardware and in an environment as described in chapter 7 and the guidance as defined in table 2.

There is only one evaluated configuration of the TOE.

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.

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.2 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.2

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 52, Para. 4, Clause 2). But cryptographic functionalities with

a security level of lower than 120 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The table in annex B of part D of this report gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 120 Bits*' of the following table with '*no*' achieves a security level of lower than 120 Bits (in general context) only.

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
TDS	TOE Design
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface

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-1087-2026, Version 2.0, 24 February 2026, Security Target for the VMware ESXi 8.0g, Broadcom, Inc.

[6] Evaluation Technical Report, Version 3, 24 February 2026, TÜV Informationstechnik GmbH (confidential document)

[7] Configuration list for the TOE, Version 0.08, 19 February 2026, EAL 4: Configuration List VMware ESXi 8.0g (confidential document)

[8] Guidance documentation for the TOE, Version 1.0, 13 February 2026, Installation and Operational Guidance for ESXi 8.0g, Broadcom, Inc.

[7] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

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.

Annex B: Overview and rating of cryptographic functionalities implemented in the TOE

Annex B of Certification Report BSI-DSZ-CC-1087-2026

Overview and rating of cryptographic functionalities implemented in the TOE

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits	Comments
1	Key Generation for TLS	RSA	[FIPS186-5]	3072 and more	Yes	FCS_CKM.1/RSA
2	Authentication during TLS handshake	RSA	[FIPS186-4]	3072	Yes	FCS_COP.1/RSA More information about algorithms / cipher suites can be found in ST [5], Table 13.
3	Derivation of TLS Session Keys from Shared Secret	PRF-SHA384	[FIPS180-4], [RFC2104], [RFC5246]	384	Yes	FCS_CKM.1/TLS, FCS_COP.1/PRF
4	Key Agreement of TLS Shared Secret	ECDHE	[RFC5246], [RFC8422], [SEC2], [SP800-56A-rev3]	P-256, P-384, P-521	Yes	FCS_CKM.2/TLS, FCS_COP.1/EC-DHE
5	Confidentiality and Authentication of TLS data	AES-GCM	[FIPS197], [RFC5288], [RFC5246], [RFC5116], [SP800-38D]	256	Yes	FCS_COP.1/AES
6	Integrity of Tokens	HMAC-SHA-256	[FIPS198-1]	256	Yes	FCS_COP.1/HMAC

Table 3: TOE cryptographic functionality

FIPS180-4 **Secure Hash Standard (SHS)**
Date 2015-08-04
Location https://csrc.nist.gov/pubs/fips/180-4/upd1/final

FIPS186-4 **Digital Signature Standard (DSS)**
Date 2013-07-19
Location https://csrc.nist.gov/pubs/fips/186-4/final

FIPS186-5 **Digital Signature Standard (DSS)**
Date 2023-02-03
Location https://csrc.nist.gov/pubs/fips/186-5/final

FIPS197	**Advanced Encryption Standard (AES)** Date 2023-05-09 Location https://csrc.nist.gov/pubs/fips/197/final
FIPS198-1	**The Keyed-Hash Message Authentication Code (HMAC)** Date 2008-07-16 Location https://csrc.nist.gov/pubs/fips/198-1/final
RFC2104	**HMAC: Keyed-Hashing for Message Authentication** Author(s) H. Krawczyk, M. Bellare, R. Canetti Date 1997-02-01 Location http://www.ietf.org/rfc/rfc2104.txt
RFC5116	**An Interface and Algorithms for Authenticated Encryption** Author(s) D. McGrew Date 2008-01-01 Location http://www.ietf.org/rfc/rfc5116.txt
RFC5288	**AES Galois Counter Mode (GCM) Cipher Suites for TLS** Author(s) J. Salowey, A. Choudhury, D. McGrew Date 2008-08-01 Location http://www.ietf.org/rfc/rfc5288.txt
RFC8422	**Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier** Author(s) Y. Nir S., Josefsson M., Pegourie-Gonnard Date 2018-08-01 Location http://www.ietf.org/rfc/rfc8422.txt
SEC2	**Recommended Elliptic Curve Domain Parameters** Date 2000 Location http://www.secg.org
SP800-38D	**Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC** Date 2007-11-28 Location https://csrc.nist.gov/pubs/sp/800/38/d/final
SP800-56A-Rev3	**Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography** Date 2018-04-16 Location https://csrc.nist.gov/pubs/sp/800/56/a/r3/final

Note: End of report