Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1096-2021

for

Arbit Data Diode 10 GbE

from

Arbit Cyber Defence Systems ApS

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

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1096-2021 (*)

Arbit Data Diode 10 GbE, v1.00

from	Arbit Cyber Defence Systems ApS
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 7 augmented by ALC_FLR.1

SOGIS
Recognition Agreement
for components up to
EAL 4

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, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report 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, 7 April 2021

For the Federal Office for Information Security

Sandro Amendola
Head of Division

L.S.

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

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

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

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

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

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

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

2. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- 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 licencing process (CC-Stellen) [3]

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

[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 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

[3] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 3 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 according to the rules of SOGIS-MRA, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained components above EAL 4 that are not mutually recognised in accordance with the provisions of the SOGIS MRA. For mutual recognition the EAL 4 components of these assurance families are relevant.

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

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

of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ 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 Arbit Data Diode 10 GbE, v1.00 has undergone the certification procedure at BSI.

The evaluation of the product Arbit Data Diode 10 GbE was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 17 March 2021. 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: Arbit Cyber Defence Systems ApS.

The product was developed by: Arbit Cyber Defence Systems ApS.

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 following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance 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 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-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.

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 7 April 2021 is valid until 6 Aprilg 2026. Validity can be re-newed by re-certification.

[5] Information Technology Security Evaluation Facility

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
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 Arbit Data Diode 10 GbE 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[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Arbit Cyber Defence Systems ApS
Immerkær 54
DK-2650 Hvidovre
Denmark

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 the Arbit Data Diode 10GbE Version 1.00, developed by Arbit Cyber Defence Systems ApS.

In its intended use case, the TOE contains a photodiode to convert an optical signal at its input port to an electrical signal at the output port. Additionally, the TOE implements a one-way data flow policy, i.e., information entering the TOE at its output port is not emitted at the input port in case customers follow the security requirements provided in the installation guidance document.

The TOE acts on the first level of the ISO/OSI reference model, i.e., no logical behaviour is implemented. This results in the fact that the TOE does not provide a configuration interface, return values or error messages.

The Security Target [6] and [9] 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 7 augmented by ALC_FLR.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 7. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

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

TOE Security Functionality	Addressed issue
One-Way Information Flow	The TOE implements the one-way data diode through a repeater, where a fiber optic network cable is connected to the INPUT port and a Receiver connection on the OUTPUT port. Information can only be received from the Sending network connected on the INPUT port, and no information can spill over to the INPUT port from the OUTPUT port. Information received on the INPUT port is allowed to exit through the OUTPUT port, without further processing.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapters 2.2 and 4.3.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 4.1 . 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] and [9], chapter 4.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

Arbit Data Diode 10 GbE.

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Arbit Data Diode 10GbE	v1.00	Personal hand-over of sealed SFP+ module (see below).
2	DOC	Arbit Data Diode 10GbE – Integration Guide	V1.08, 2020-10-21	Personal hand-over in paper format (see below).

Table 2: Deliverables of the TOE

Regarding delivery:

As it is stated in the Security targets [6] and [9] section 2.1.1, the “delivery of TOE and its Integration Guide shall be performed as trusted personal handover in accordance with the delivery procedure”.

Thus, delivery is conducted by the following ways:

- Announced delivery:
  The recipient knows the expected time of delivery window and forwarder company. The recipient shall accept deliveries as announced, otherwise shall contact the sender.
- Personal handover:
  The delivered items are personally handed over to the forwarder and the forwarder personally handover the delivery to the consumer. The developer shall be informed of the successful handover.
- Known forwarder:
  The respective parties know the forwarder. The identity of the forwarder shall be verified before handing over items.
- Independent delivery of TOE parts:
  TOE parts shall be delivered independently. The TOE parts may be sent by different forwarders or on different days. One forwarder shall never have the TOE and its guidance at the same time The consumer shall verify Independence of delivery before accepting the complete delivery.

Regarding identification:

The TOE and its reference are part of the Integration Guidance [11] (section 2), and the TOE itself is labelled accordingly (part of considerations of assurance family ALC_CMS).

The independent delivery of TOE parts and the correct labelling of the TOE enable consumer of secure reception of the TOE and its guidance, maintaining authenticity and integrity during delivery.

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:

The security functionality of the TOE is to implement the one-was data flow policy. While in its intended use case, the TOE converts an optical signal at its input port to an electrical signal at its output port, the TOE makes sure that no data or information is transmitted from its output port to the input port. In fact, when operated as described in the user guidance [11], the TOE is not able to emit light that contains information about any signal applied to the electrical output.

Specific details concerning the above mentioned security policy can be found in [6] and [9], chapters 2.1.2, 7.1, and 7.6.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

The Security Objective for the Operational Environment OE.INTEGRATOR requires integrators performing the installation of the TOE to be well-trained and competent in the prevention of signal leakage. Furthermore, integrators shall adhere to the guidance. In [11] section 2.2, the developer states that the integrator who is performing the installation has to apply procedures applicable to the respective operational environment such that proper protection of the TOE is maintained at all times.

The Security Objective for the Operational Environment OE.PHYSICAL requires that the TOE and its interfaces shall be physically protected from unauthorized access. In [11] section 2.2 and 2.4, the developer clearly states that no user may have physical access to the TOE. If an integrity breach is possible (identified by the means implemented by the integrator), the TOE shall not be used.

The Security Objective for the Operational Environment OE.POWER requires that the power supply of the TOE shall be 3.3V +/- 5% and that the minimum current capacity (continuous and peak-to-peak) shall be 500 mA. Guidance document [11] section 2.3.3 addresses this OE accordingly.

5. Architectural Information

Details on architectural information can be found in the Security Target [6] and [9], section 2.

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

Both the developer as well as ITSEF conducted product testing.

Regarding the developer testing:

The developer conducted tests during development of the TOE and conducted tests for each produced device:

- The development tests are suitable verify that the TSF behaves as specified in ADV_FSP, ADV_TDS, and ADV_IMP.
- The production tests are used to check that a produced product matches the expected behavior derived from the development tests.

The following TOE security functionalities were tested by the developer:

- FDP_IFC.2 Complete information flow control, and
- FDP_IFF.1 Simple security attributes.

Regarding ITSEF testing:

- Functional verification of the TOE interfaces (TSFI),
- Functional verification of the TOE design providing assurance that the product matches the implementation representation,
- Functional production tests as a sanity check of the core features of the manufactured device,
- Penetration testing.

SFRs penetration tested by the ITSEF:

- FDP_IFC.2 Complete information flow control, and
- FDP_IFF.1 Simple security attributes.

The overall ITSEF verdict is:

The penetration tests results confirm that the TOE is resistant to attackers with high attack potential in the intended operational environment.

8. Evaluated Configuration

The TOE is available in a single variant and cannot be further configured.

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 those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5.

The following guidance specific for the certification procedure was used:

- *AIS1: Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 1, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, Version 14, 2017-10-11, Bundesamt für Sicherheit in der Informationstechnik,*
- *AIS14: Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 2010-08-03, Bundesamt für Sicherheit in der Informationstechnik,*
- *AIS19: Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 2010-08-03, Bundesamt für Sicherheit in der Informationstechnik,*
- *AIS32: Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 2010-08-03, Bundesamt für Sicherheit in der Informationstechnik,*
- *AIS34: Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 2010-08-03, Bundesamt für Sicherheit in der Informationstechnik,*
- *AIS39: Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 2010-08-03, Bundesamt für Sicherheit in der Informationstechnik,*
- *AIS45: Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 45, Erstellung und Pflege von Meilensteinplänen, Version 2, 2010-08-03, Bundesamt für Sicherheit in der Informationstechnik.*

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

- All components of the EAL 7 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 thus has confirmed:

- for the Functionality: Product specific Security Target
  Common Criteria Part 2 conformant

- for the Assurance: Common Criteria Part 3 conformant
  EAL 7 augmented by ALC_FLR.1

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

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

9.2. Results of cryptographic assessment

The TOE does not include cryptographic mechanisms. Thus, no such mechanisms were part of the assessment.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered, especially the implementation guidance [11]. 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. In detail, the assumptions on the operational environment need to be taken into account by customers:

Assumption	Definition
A.INTEGRATOR	The integrator who is performing the installation of the TOE is well-trained and competent in the prevention of signal leakage, and will properly adhere to the TOE guidance.
A.PHYSICAL	The TOE and its interfaces will be physically protected from unauthorized access and mechanical, electrical, optical, radiation or any other form of physical influence.
A.POWER	Power supply to TOE shall be 3.3 V +/-5%. The minimum current capacity, both continuous and peak, shall be 500 mA.

Table 3: Assumptions on the operational environment

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 (if any) as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

For this reason the TOE includes guidance documentation (see table 2) which contains obligations and guidelines for users of the product layer on top on how to securely use this certified TOE and which (e.g. organisational measures of delivery) measures have to be implemented in order to fulfil the security requirements of the Security Target of the TOE. In the course of the evaluation of the composite product or system it must be examined if the required measures have been correctly and effectively implemented by the product layer on top.

11. Security Target

For the purpose of publishing, the Security Target [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

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
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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.

Semiformal - Expressed in a restricted syntax language with defined semantics.

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

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

TOE 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 licencing (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] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-1096-2021, Version 0.75, 21.10.2020, "Arbit Data Diode 10GbE - Security Target", Confiware ApS and Arbit Cyber Defence Systems ApS (confidential document)

[7] Evaluation Technical Report, Version 2, 2021-01-20, "ETR Summary V2 – Arbit Data Diode 1.00", TÜV Informationstechnik GmbH, (confidential document)

[8] (reference not used)

[7] See section 9.1 for details on used AIS.

[9] Security Target BSI-DSZ-CC-1096-2021, Version 1.01, 10.12.2020, “Arbit Data Diode 10GbE - Security Target Lite”, Confiware ApS and Arbit Cyber Defence Systems ApS (sanitised public document)

[10] Configuration list for the TOE, Version 0.42, 2020-12-10, “Arbit Data Diode 10GbE - Configuration List” (confidential document)

[11] “Arbit Data Diode 10GbE – Integration Guide”, Version 1.08, 2021-10-21, Confiware ApS and Arbit Cyber Defence Systems ApS

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:	Evaluation results regarding development and production environment

Annex B of Certification Report BSI-DSZ-CC-1096-2021

Evaluation results regarding development and production environment

The IT product Arbit Data Diode 10 GbE (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 7 April 2021, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.5, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.2, ALC_TAT.3)

are fulfilled for the development and production sites of the TOE. The relevant delivery related site is:

- “Arbit Hvidovre”,
  Arbit Cyber Defence Systems ApS,
  Immerkær 54,
  2650 Hvidovre – Denmark.

For all of the sites, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [9]) are fulfilled by the procedures of these sites.

Note: End of report