Swedish Certification Body for IT Security

Certification Report - Advenica DD1G Gen2

Issue: 1.0, 2026-feb-26

Authorisation: Michael Lindh Almér, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is the data diode Advenica DD1G Gen 2 with Product ID BSF-DD18605C01.

A data diode is used for sending data from one independent network to another while ensuring the networks remain physically isolated. The data diode guarantees that data can only flow in the allowed direction.

The Security Target [ST] is the basis for this evaluation. It does not claim conformance to any Protection Profile.

The TOE scope is the complete data diode, and can be uniquely identified by its label. The TOE guidance can also be uniquely identified by its document ID and version.

The TOE is delivered to customer through a secure and validated delivery process. The customer will receive customer order specific information, including the ID number of the sealed security bag. This ensures that the customer can verify that the product has not been manipulated or tampered with upon receiving the product. Shipment to customers is handled by Advenica AB.

The evaluation has been performed by Combitech AB in their premises in Växjö, Sweden and the developer's premises in Malmö, Sweden. Site-visit was performed in Malmö and Lund, Sweden. The evaluation was completed on the February 25, 2026.

The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version 2022, and the Common Methodology for IT Security Evaluation (CEM), version 2022. The evaluation conforms to evaluation assurance level EAL 4, augmented by AVA_VAN.4.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body according to ISO/IEC 17025 for Common Criteria.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports, and participated during site-visit and performed test oversight. The certifier determined that the evaluation results confirm the security claims in the Security Target (ST), the Common Methodology for evaluation assurance level EAL 4 augmented by AVA_VAN.4.

The technical information in this report is based on the Final Evaluation Report (FER) produced by Combitech AB, and the Security Target (ST).

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met. This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2024026
Name and version of the certified IT product	Advenica DD1G Gen 2, BSF-DD18605C01
Security Target Identification	DD1G Gen2, Security Target, Document number 21537, version 2.1, 2026-02-25
EAL	EAL 4 + AVA_VAN.4
Sponsor	Advenica AB
Developer	Advenica AB
ITSEF	Combitech AB
Common Criteria version	CC:2022
CEM version	CEM:2022
QMS version	2.6.1
Scheme Notes Release	22.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2026-02-26

3 Security Policy

The TOE is a hardware only data diode that ensures unidirectional Ethernet data traffic through the TOE. It is intended for installation in a network environment.

There are no dependencies to other hardware, firmware or software to use the functionality of the TOE.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes one assumption on the usage of the TOE.

- A.NO_MALICIOUS_ADMINS
  Personnel doing the installation of TOE are assumed to be authorized, trusted, and have the necessary training.

4.2 Environmental Assumptions

The Security Target [ST] makes two assumptions on the operational environment of the TOE.

- A.PHYSICAL_PROTECTION
  TOE is installed such that only authorized personnel has access.
- A.NO_BYPASS
  TOE is installed such that it forms a separation between upstream and downstream networks.

  The network is configured such that all traffic from upstream to downstream network must go through the TOE.

4.3 Clarification of Scope

The Security Target contains two threats, which have been considered during the evaluation.

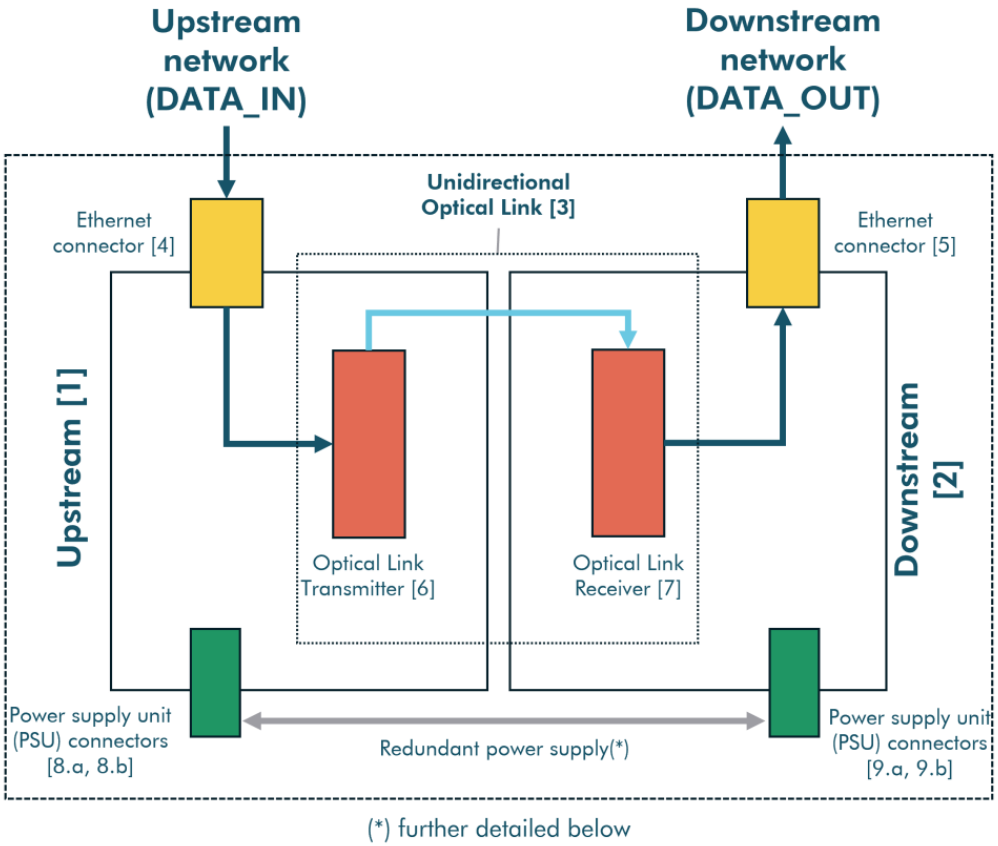
- T.LEAKAGE_VIA_DIODE
  A USER on the downstream network accidentally transmitting data through TOE to the upstream network.
- T.ATTACK_VIA_DIODE
  An ATTACKER tries to send data from downstream to upstream via the TOE with the purpose to violate resources or access data at USER_RESOURCES_US.

The Security Target contains no Organisational Security Policy (OSPs).

5 Architectural Information

The TOE is the Advenica data diode DD1G Gen 2, BSF-DD18605C01.

A data diode is used for sending data from one independent network to another while ensuring the networks remain physically isolated. The data diode guarantees that data can only flow in the allowed direction.



The TOE consists of a single device with three subsystems, denoted Upstream [1], Downstream [2], and Unidirectional Optical Link [3].

The TOE is physically connected to networks using the Upstream [4] and Downstream Ethernet connector [5] respectively. These are the only network connectors and the only offered communication ports on the TOE.

The Unidirectional Optical Link [3] is implemented using an optical fiber mounted to a transmitter [6] and receiver [7]. It provides the physical separation between the Upstream [1] and the Downstream [2] subsystems. This removes any risk of data being transferred in the reverse direction when installed correctly.

The upstream network (DATA_IN) should be configured to send all relevant network traffic through the TOE and physically ensure that all connections between the upstream and downstream (DATA_OUT) networks pass through the TOE.

Full operability of the TOE is achieved by powering the device and connecting the network interfaces.

There are several options for powering the device. By connecting to external power supply unit(s) [8,9] or via Power over Ethernet (PoE) [4,5].

The device also supports redundant power supply.

The TOE has two operational states, on and off, with no intermediate or initial states where the one-way functionality is inactive.

The TOE should be installed with visible tamper detection marking for ocular inspection to determine whether tampering has occurred. This tamper seal is already attached on delivery, but a proper visual examination of the TOE before installation is recommended.

6 Documentation

Document name	Version
Recommended_Security_Management_SecuriCDS_DD1000A_DD1G	17113v1.3
QuickGuide_DD1G_Gen_2	21350v1.0

7 IT Product Testing

7.1 Developer Testing

The developer performed tests providing full coverage and dept, including positive and negative tests. All SFRs were tested. Testing also including measuring voltage and not only network traffic.

Testing was performed within developer's premises in Malmö, Sweden. All tests were successful.

7.2 Evaluator Testing

The evaluator re-executed the developer tests within the developer's premises in Malmö Sweden. All tests were successful and no deviations were identified. No additional tests were deemed necessary.

The evaluator testing was performed on October 9, 2025.

7.3 Penetration Testing

No penetration testing was conducted, as no potential vulnerabilities were identified that could be exploited by an attacker with Moderate attack potential.

8 Evaluated Configuration

The TOE is an Ethernet-based data diode with 1 Gigabit performance and the TOE is determined by the physical borders of the box. It is intended for installation in a network environment.

There are no dependencies to other hardware, firmware or software to use the functionality of the TOE. Since the TOE is a hardware-only device, it has no communication interface for administration or configuration.

The TOE should be installed with visible tamper detection marking for ocular inspection to determine whether tampering has occurred. This tamper seal is already attached on delivery, but a proper visual examination of the TOE before installation is recommended.

All personnel doing installation and administration of the TOE should be authorized to do so, have the necessary training required to do this according to the requirements, and follow the recommended steps when doing so.

The environment in which the TOE is installed should not be accessible by unauthorized personnel to prevent the device from being tampered with, or even disconnected, since it can then no longer fulfill its security function.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Moderate.

The certifier reviewed the work of the evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators' overall verdict is PASS.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
Development	ADV	PASS
Security architecture description	ADV_ARC.1	PASS
Complete functional specification	ADV_FSP.4	PASS
Implementation representation of the TSF	ADV_IMP.1	PASS
Modular design	ADV_TDS.3	PASS
Guidance documents	AGD	PASS
Operational user guidance	AGD_OPE.1	PASS
Preparative procedures	AGD_PRE.1	PASS
Life-cycle support	ALC	PASS
Production support, acceptance procedures and automation	ALC_CMC.4	PASS
Problem tracking CM coverage	ALC_CMS.4	PASS
Delivery procedures	ALC_DEL.1	PASS
Identification of security measures	ALC_DVS.1	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well defined developer tools	ALC_TAT.1	PASS
ST evaluation	ASE	PASS
Conformance claims	ASE_CCL.1	PASS
Extended components definition	ASE_ECD.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.2	PASS
Derived security requirements	ASE_REQ.2	PASS
Security problem definition	ASE_SPD.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Tests	ATE	PASS

Assurance Class Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
Analysis of coverage	ATE_COV.2	PASS
Testing: basic design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	AVA	PASS
Methodical vulnerability analysis	AVA_VAN.4	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

CC	Common Criteria for Information Technology Security
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
CM	Configuration Management
ISO	International Organization for Standardization
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within an evaluation and certification scheme
OSP	Organisational Security Policy
PP	Protection Profile
ST	Security Target, document containing security requirements and specifications, used as the basis of a TOE evaluation
SFR	Security Functional Requirement
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

12 Bibliography

ST	DD1G Gen2 Security Target, Advenica AB, 2026-02-25, document version 2.1, FMV ID 24FMV6698-32
QG	Quick Guide, 21350, 2024, v1.0
SM	SecuriCDS DD1000A & DD1G Recommended Security Management, 17113, 2024, v1.3
CC/CEM	Common Criteria for Information Technology Security Evaluation, and Common Methodology for Information Technology Security Evaluation, CCMB-2022-11-001 through 006, document versions CC:2022/CEM:2022 rev 1

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
2.6.1	2025-10-16	No impact
2.6	2025-04-23	No impact
2.5.2	Application	Original version

A.2 Scheme Notes

Scheme Note	Version	Title	Applicability
SN-15	5.0	Testing	Compliant
SN-18	4.0	Highlighted Requirements on the Security Target	Compliant
SN-22	4.0	Vulnerability assessment	Compliant
SN-27	1.0	ST requirements at the time of application for certification	Compliant
SN-28	2.0	Updated procedures for application, evaluation and certification	Compliant
SN-31	1.0	New procedures for site visit oversight and testing oversight	Compliant