



TÜRK STANDARDLARI ENSTİTÜSÜ

BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI
CCCS CERTIFICATION REPORT



Certification Report

EAL4+(AVA_VAN.5) Evaluation of

DATAFLOWX TEKNOLOJİ A.Ş.



DATADIODEX v1.0.0

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03.0.00.00//TSE-CCCS-86

Doküman Kodu: BTBD-03-01-FR-01


Yayın Tarihi: 4.08.2015 Revizyon Tarih/No: 7.04.2023/7



BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI
CCCS CERTIFICATION REPORT

TABLE OF CONTENTS

TABLE OF CONTENTS	2
DOCUMENT INFORMATION	3
DOCUMENT CHANGE LOG	3
DISCLAIMER	3
FOREWORD	4
RECOGNITION OF THE CERTIFICATE.....	5
1 EXECUTIVE SUMMARY	6
1.1 Brief Description.....	6
1.2 Major Basic Security and Functional Attributes.....	7
1.3 Threats.....	8
1.4 Organizational Security Policies (OSPs).....	9
1.5 Assumptions.....	9
2 CERTIFICATION RESULTS.....	9
2.1 IDENTIFICATION OF TARGET OF EVALUATION / PP IDENTIFICATION	9
2.2 SECURITY POLICY.....	10
2.3 ASSUMPTIONS AND CLARIFICATION OF SCOPE.....	10
2.4 ARCHITECTURAL INFORMATION.....	10
2.5 DOCUMENTATION	10
2.6 IT PRODUCT TESTING	12
2.7 EVALUATED CONFIGURATION	12
2.8 RESULTS OF THE EVALUATION.....	14
2.9 EVALUATOR COMMENTS / RECOMMENDATIONS.....	14
3 SECURITY TARGET.....	15
4 GLOSSARY	16
5 BIBLIOGRAPHY.....	16
6 ANNEXES	17
6.1 TOE SPECIFICATIONS	17
6.2 TEST ENVIRONMENT.....	17





BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI
CCCS CERTIFICATION REPORT

Document Information

Date of Issue	06/06/2023
Approval Date	06/06/2023
Certification Report Number	21.0.03/23-003
Sponsor and Developer	Dataflowx Teknoloji A.Ş.
Evaluation Facility	Beam Teknoloji A.Ş.
TOE/ PP Name*	DataDiodeX Modules v1.0.0
Pages	17

Prepared by <i>Common Criteria Inspection Expert</i>	Göktaş İLİSU
<i>Common Criteria Candidate Inspection Expert</i>	Almila Beyza KARAKAPICI
Reviewer (Approver)	Mehmet Kürşad ÜNAL

The experts whose names and signatures are shown as above prepared and reviewed this report.

Document Change Log

Release	Date	Pages Affected	Remarks/Change Reference
1.0	06/06/2023	All	First Release

DISCLAIMER

This certification report and the IT product/PP defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 5, using Common Methodology for IT Products Evaluation, version 3.1, revision 5. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility



BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI CCCS CERTIFICATION REPORT

in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the ITCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL = Common Criteria Testing Laboratory) under CCCS' supervision.

CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by BEAM Teknoloji A.Ş., which is a commercial CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target/PP document that has been approved by the CCCS. The Security Target document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.



BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI
CCCS CERTIFICATION REPORT

This certification report is associated with the Common Criteria Certificate issued by the CCCS for DataDiodeX v1.0.0 whose evaluation was completed on May 16th 2023 and whose evaluation technical report was drawn up by BEAM Teknoloji A.Ş. (as CCTL), and with the Security Target document with version no 0.5 of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the ITCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including *EAL2*. The current list of signatory nations and approved certification schemes can be found on:

<http://www.commoncriteriaportal.org>.



BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI
CCCS CERTIFICATION REPORT

1 - EXECUTIVE SUMMARY

Developer of the IT product: Dataflowx Teknoloji A.Ş.

Evaluated IT product: DataDiodeX

IT Product Version: 1.0.0

Name of IT Security Evaluation Facility: Beam Teknoloji A.Ş.

Completion date of evaluation: 16/05/2023

Assurance Package: EAL 4+ (AVA_VAN.5)

1.1. Brief Description

The TOE provides a unidirectional data path between a source (*untrusted network*) and destination (*trusted network*) and allows information to flow from an untrusted network to a trusted network, without compromising the confidentiality of the information on the trusted network.

The TOE consists of hardware components (TX Module and RX Module) and software components (DataDiodeX Sender and DataDiodeX Receiver). The TOE components are located on the two different Application Servers.

Both of the TX Module and RX Module have two external interfaces. One external interface of these modules is connected to the PCI bus of the Application Server on which they are installed. Other external interfaces (SFP Fiber Optic Interface) of the TX Module and the RX Module are physically connected each other with as single fiber optic cable.

The connection between TX Module and RX Module allows data to flow from the Sender Application Server to the Receiver Application Server but does not allow data to flow in the reverse direction (prevents information leak from Receiver Application Server to Sender Application Server) by property of the physical implementation of TX Module and RX Module. The one-way data transmission property between TX Module and RX Module is implemented at the physical layer of the OSI reference model (no software and firmware).

DataDiodeX Sender constantly monitors specific predefined file directory in the file system. If it detects a new file that is transferred via SFTP (Secure File Transfer Protocol) to the Sender Application Server from the Untrusted Network, it immediately calculates the hash value of the file and converts the file as data packets in order to send over the UDP protocol.



BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI CCCS CERTIFICATION REPORT

All data packets and hash value of the file are forwarded according to the below order:

- ✓ From the DataDiodeX Sender to the TX Module,
- ✓ From the TX Module to the RX Module,
- ✓ From the RX Module to the DataDiodeX Receiver.

DataDiodeX Receiver receives all data packets and hash value of the file over UDP Protocol from the DataDiodeX Sender via RX Module and TX Module. And it merges all data packets and checks the integrity of the file using its hash value. According to the hash control result, the file is stored in specific predefined file directory in the file system. All stored files on the Receiver Application Server are shared with the Trusted Network.

1.2. Major Basic Security and Functional Attributes

User Data Protection: The User Data Protection function implements functionality necessary to protect the Trusted Network information. The TOE applies a set of rules (One-Way Information Flow SFP) to provide a unidirectional (One-way) data path from an untrusted network and trusted network and allows information to flow from an untrusted network to a trusted network, without compromising the confidentiality of the information on the trusted network.

1.3. Threats

Attackers: They are not TOE user and have public knowledge of how the TOE operates.

Primary Assets (User Data): The primary asset is the Trusted Network Information that must be prevented being transmitted during the communication between the untrusted network and trusted network.

T.Data_Leak: An attacker may breach the confidentiality of data on the trusted network by using a malicious software infected by attacker into devices in the trusted network with the aim of providing data leakage from the trusted network.

T.Physical_Manipulation: The hardware parts of the TOE may be subject to physical attack by an attacker, which may compromise security of the user data.





BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI
CCCS CERTIFICATION REPORT

1.4. Organizational Security Policies (OSPs)


P. Standart: TX and RX modules of TOE should be installed by NATO SDIP-29 "Installation of Electrical Equipment for the Processing of Classified Information" standard or MST 401-1(A) "Turkish Armed Forces TEMPEST Standards" standard.

1.5. Assumptions

A. Personnel: It is assumed that the personnel with authorized physical access to the TOE is well-trained and will not attempt to circumvent the TOE's security functionality.

A. Network: Apart from transmitting information through the TOE, It is assumed that there are no channels for the information to flow between the untrusted network and the trusted network.

A. Environment: It is assumed that the TOE environment provides stable network connectivity for the TOE to perform its intended function.





BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI
CCCS CERTIFICATION REPORT

2 -CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03.0.00.00//TSE-CCCS-86
TOE Name and Version	DataDiodeX v1.0.0
Security Target Title	DataDiodeX Modules Security Target
Security Target Version	0.5
Security Target Date	26/04/2023
Assurance Level	EAL 4+(AVA_VAN.5)
Criteria	<ul style="list-style-type: none">• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 5, April 2017• Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 5, April 2017• Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 5, April 2017
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 5, April 2017
Protection Profile Conformance	None

**BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI
CCCS CERTIFICATION REPORT**

Common Criteria Conformance	<ul style="list-style-type: none">• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017• Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017, conformant• Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, conformant
Sponsor and Developer	Dataflowx Teknoloji A.Ş.
Evaluation Facility	BEAM Teknoloji A.Ş.
Certification Scheme	TSE CCCS

2.2 Security Policy

P. Standart: TX and RX modules of TOE should be installed by NATO SDIP-29 "Installation of Electrical Equipment for the Processing of Classified Information" standard or MST 401-1(A) "Turkish Armed Forces TEMPEST Standards" standard.

2.3 Assumptions and Clarification of Scope

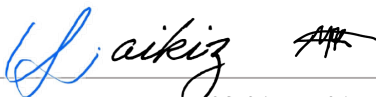
A. Personnel: It is assumed that the personnel with authorized physical access to the TOE is well-trained and will not attempt to circumvent the TOE's security functionality.

A. Network: Apart from transmitting information through the TOE, It is assumed that there are no channels for the information to flow between the untrusted network and the trusted network.

A. Environment: It is assumed that the TOE environment provides stable network connectivity for the TOE to perform its intended function.

2.4 Architectural Information

The physical scope of the TOE is a DataDiodeX Modules to be installed in two separated Application Servers (as shown in the Figure 1) and TOE Documentation.



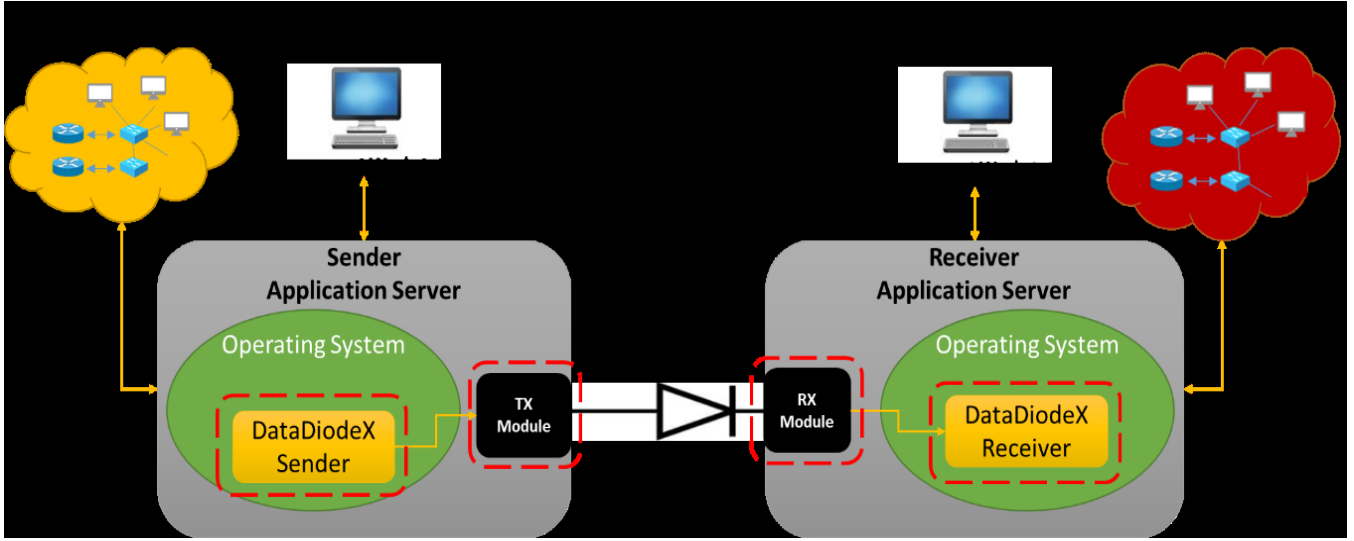
BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI
CCCS CERTIFICATION REPORT

Figure 1 DataDiodeX Modules and General TOE Environment

DataDiodeX Modules consist of:

- Hardware Modules:
 - ✓ TX Module
 - ✓ RX Module
- Software Modules:
 - ✓ DataDiodeX Sender
 - ✓ DataDiodeX Receiver

DataDiodeX Sender

- ✓ Constantly monitors specific predefined file directory in the file system to detect a new file transferred via SFTP to the Sender Application Server from the Untrusted Network
- ✓ After detection, calculates the hash value of the file and converts the file as data packets
- ✓ Sends all data packets and hash value of the file over the UDP to the DataDiodeX Receiver via TX Module and RX Module
- ✓ is configured via the LAN Interface of the Sender Application Server using the CLI commands

DataDiodeX Receiver

- ✓ Receives all data packets and hash value of the file from DataDiodeX Sender via RX Module and TX Module
- ✓ Merges the all data packets and checks the integrity of the file using its hash value

Signature

**BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI
CCCS CERTIFICATION REPORT**

- ✓ Stores the file in specific predefined file directory according to the hash control result
- ✓ is configured via the LAN Interface of the Receiver Application Server using the CLI commands

TX Module

- ✓ special Ethernet Card with customized SFP
- ✓ located in the Sender Application Server
- ✓ has only an optical transmitter
- ✓ has no external interface to receive optical signal (optical sensor)
- ✓ is implemented at the physical layer of the OSI reference model (no software and firmware).

RX Module

- ✓ special Ethernet Card with customized SFP
- ✓ has only an optical sensor
- ✓ has no an optical transmitter, therefore, it is physically not possible for data to flow from the Trusted Network to the Untrusted Network via the TOE
- ✓ is implemented at the physical layer of the OSI reference model (no software and firmware).

2.5 Documentation

Document Name	Version	Release Date
DataDiodeX Modules Security Target	v0.5	26/04/2023
DataDiodeX Operasyonel Kullanıcı Kılavuzu Dokümanı	v0.6	30/03/2023
DataDiodeX Kurulum Prosedürleri Dokümanı	v0.8	30/03/2023

2.6 IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developer. All the delivered evaluation evidences which include software, documents, etc. are mapped to the assurance families and the evaluation evidences has been established. The evaluation results are available at the final Evaluation Technical Report (ETR) of DataDiodeX Modules v1.0.0.

It is concluded that the TOE supports EAL 4+ (AVA_VAN.5). There exist 24 assurance families which are all evaluated with the methods detailed in the ETR.

- **Developer Testing:** Developer has prepared TOE Test Document according to the TOE Functional Specification documentation, TOE design documentation which includes TSF subsystems and its

**BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI
CCCS CERTIFICATION REPORT**

interactions. All SFR-Enforcing TSFIs have been tested by developer. Developer has conducted 3 functional tests in total.

- **Evaluator Testing:** Evaluator has conducted 3 developer tests. Additionally, evaluator has prepared 2 independent tests. TOE has passed all functional tests to demonstrate that its security functions work as it is defined in the ST.
- **Penetration Tests:** TOE has been tested against common threats and other threats surfaced by vulnerability analysis. As a result, 12 penetration tests have been conducted. TOE proved that it is resistant to “Attacker with High Attack Potential”.

2.7 Evaluated Configuration

Evaluated TOE configuration is composed of:

- DataDiodeX Modules v1.0.0
- Guidance Documents

Also as consistent with the minimum Hardware/ Software/ OS requirements for the TOE, the test environment presented at the ETR is composed of;

- FileZilla Client v3.63.2.1: provides data transfer to sender application server by SFTP protocol and file reception to receiver application server.

Sender Application Server Technical Specifications	
CPU	12 CPU
RAM	256 GB
Operating System	Linux (Pardus 17.5 UVD Server 64-bit)
Receiver Application Server Technical Specifications	
CPU	12 CPU
RAM	256 GB
Operating System	Linux (Pardus 17.5 UVD Server 64-bit)

Table 1 Minimum Requirements of Non-TOE hardware/software/firmware

BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI
CCCS CERTIFICATION REPORT

2.8 Results of the Evaluation

The table below provides a complete list of the Security Assurance Requirements for the TOE. These requirements consist of the Evaluation Assurance Level 4 (EAL 4) components as specified in Part 3 of the Common Criteria, augmented with AVA_VAN.5

Class Heading	Class Family	Description	Result
ADV: Development	ADV_ARC.1	Security architecture description	PASS
	ADV_FSP.4	Complete functional specification	PASS
	ADV_IMP.1	Implementation representation of the TSF	PASS
	ADV_TDS.3	Basic modular design	PASS
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance	PASS
	AGD_PRE.1	Preparative procedures	PASS
ALC: Life-Cycle Support	ALC_CMC.4	Production support, acceptance procedures and automation	PASS
	ALC_CMS.4	Problem tracking CM coverage	PASS
	ALC_DEL.1	Delivery procedures	PASS
	ALC_DVS.1	Identification of Security Measures	PASS
	ALC_LCD.1	Developer Defined Life-Cycle Model	PASS
	ALC_TAT.1	Well-Defined Development Tools	PASS
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims	PASS
	ASE_ECD.1	Extended components definition	PASS
	ASE_INT.1	ST introduction	PASS
	ASE_OBJ.2	Security objectives	PASS
	ASE_REQ.2	Derived security requirements	PASS
	ASE_SPD.1	Security problem definition	PASS
	ASE_TSS.1	TOE summary specification	PASS
ATE: Tests	ATE_COV.2	Analysis of coverage	PASS
	ATE_FUN.1	Functional testing	PASS
	ATE_DPT.1	Testing: Basic Design	PASS
AVA: Vulnerability Analysis	AVA_VAN.5	Advanced methodical vulnerability analysis	PASS

U. Aikiz

**BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI
CCCS CERTIFICATION REPORT****2.9 Evaluator Comments / Recommendations**

All guidance outlined in the Guidance Documents must be followed and all assumptions are fulfilled in order to secure usage of the TOE.

The users of the TOE should be aware of MD5 algorithm usage for integrity check during hashed files transmission.

It is also crucial that TOE should be installed in accordance with NATO SDIP-29 “Installation of Electrical Equipment for Classified Information Process” and MST 401-1(A) “Turkish Armed Forces TEMPEST Standards”. This is the core part of the operational environment OE. Standard stated at Security Target.

3 SECURITY TARGET


The security target associated with this Certification Report is identified by the following terminology:

Title: DataDiodeX v1.0.0 Security Target

Version: v0.5

Date of Document: April 26, 2023

This Security Target describes the TOE, intended IT environment, security objectives, security requirements (for the TOE and IT environment), TOE security functions and all necessary rationale.



**BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI
CCCS CERTIFICATION REPORT****4 GLOSSARY**

CCCS: Common Criteria Certification Scheme
CCMB: Common Criteria Management Board
CCRA: Common Criteria Recognition Arrangement
EAL: Evaluation Assurance Level
ITCD: Information Technologies Test and Certification Department
OSP: Organisational Security Policy
SAR: Security Assurance Requirements
SFR: Security Functional Requirements
ST: Security Target
TOE: Target of Evaluation
TSF: TOE Security Functionality
TSFI: TSF Interface

5 BIBLIOGRAPHY

- [1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017
[3] ETR v2.2 of DataDiodeX v1.0.0, Rel. Date: May 16, 2023
[4] DataDiodeX v1.0.0 Security Target, Version 0.5, Rel. Date: April 26, 2023.





BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI
CCCS CERTIFICATION REPORT

6 ANNEXES

6.1 TOE SPECIFICATIONS

TOE: DataDiodeX v1.0.0

TOE Hash (SHA256): 52762cec5275bba56e390b270c02101023d016b45e4b673e5dee939787dfd2b8

6.2 TEST ENVIRONMENT:

Hardware:

- Sender Application Server with 256 GB RAM, Linux (Pardus 17.5 UVD Server 64-bit) OS, 12 CPU
- Receiver Application Server with 256 GB RAM, Linux (Pardus 17.5 UVD Server 64-bit) OS, 12 CPU

Software:

- FileZilla Client v3.63.2.1

