Certification Report

EAL4 + (AVA_VAN.5, ADV_IMP.2, ALC_FLR.2, ALC_DVS.2) Evaluation of

DATAFLOWX TEKNOLOJİ A.Ş.

DATABROKERX CLIENT MODULE (CM) AND SERVER MODULE (SM) v1.0.0

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03.0.00.00//TSE-CCCS-103

TABLE OF CONTENTS

Document Information

Date of Issue	**31/07/2026**
Approval Date	**21/08/2026**
Certification Report Number	**21.0.03/26-003**
Sponsor and Developer	**Dataflowx Teknoloji A.Ş.**
Evaluation Facility	**BEAM Teknoloji A.Ş.**
TOE/ PP Name*	**DataBrokerX Client Module (CM) and Server Module (SM) v1.0.0**
Pages	**20**

Prepared by *Common Criteria Inspection Expert*	**Göktuğ İLISU** 
Common Criteria Candidate Inspection Expert	**Mert SEKÜ** 
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	30/07/2026	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 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.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for DataBrokerX Client Module (CM) and Server Module (SM) v1.0.0 whose evaluation was completed on July 1st 2026 and whose evaluation technical report was drawn up by BEAM Teknoloji A.Ş. (as CCTL), and with the Security Target document with version no 1.9 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.

1 - EXECUTIVE SUMMARY

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

Evaluated IT product: DataBrokerX

IT Product Version: v1.0.0

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

Completion date of evaluation: 01/07/2026

Assurance Package: EAL4 + (AVA_VAN.5, ADV_IMP.2, ALC_FLR.2, ALC_DVS.2)

1.1. Brief Description

The TOE is an *Inter-Network Protocol Breaking Solution* developed in a modular and physically separated structure to meet the inter-network real-time query-response-based communication needs of institutions with needs to isolate private networks containing sensitive data, while maintaining isolation. It guarantees uninterrupted and isolated one-way data communication for both directions at the intersections of networks with different security levels, with the system it created together with the *"DataDiodeX Modules (DataDiodeX)"*, and prevents sensitive data from a high-security network from passing uncontrolled to low-security networks.

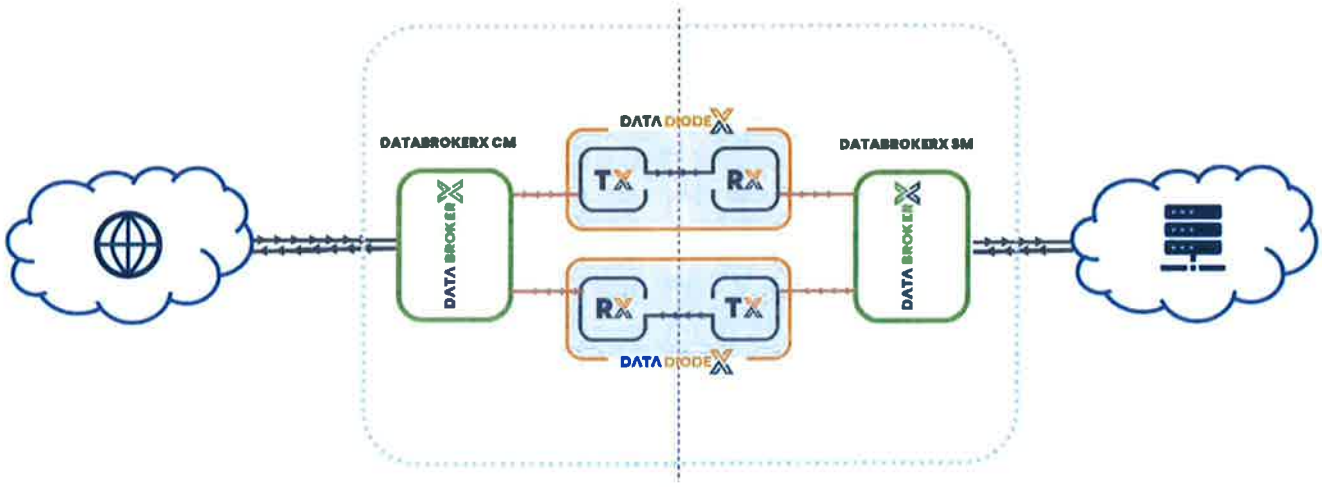

Figure 1: *DataBrokerX SM and CM modules and TOE Environment*

Even when using HTTPS, LDAPS or RDP connections, the TOE completely cuts off TCP/IP communication between networks, and transmits only the wanted queries to the services defined by the admin, with its own transmission protocol and data format. By totally making TCP/IP communication impossible between networks, it protects itself and sensitive resources against TCP/IP based attacks which

is almost all of the network security vulnerabilities relies on. TOE creates a protected environment against both attacks against itself and attacks on data transfer in between.

1.2. Major Basic Security and Functional Attributes

- The TOE protects information on the private network from being compromised by applying a set of rules to provide asynchronous and one-way data paths in both directions between the private network and target public network points.
- The TOE provides a user authentication mechanism to allow users who want to access the objects and functions of the TOE according to their access rights. For this purpose, any user who wants to access the TOE must be previously defined on the TOE.
- The TOE checks the user password whether the password quality meets the defined quality measure during user password determination.
- The TOE automatically terminates inactive sessions after a preconfigured time.
- The TOE applies an incorrect password limit to prevent brute-force attacks.
- The TOE logs all data transfer activities and stores logs in the file system.
- The TOE provides a review function for admin users and monitor users of the TOE via a Web Browser.
- Audit record loss is prevented in case the audit storage is full by overwriting the oldest stored audit records.
- TOE performs the cryptographic functions listed below:
  - ✓ TLS v1.2 protocol implementation for LDAPs, RDP, and HTTPS.
  - ✓ Cryptographic key generation,
  - ✓ Cryptographic operation (*encryption, decryption, hash calculation, and digital signature generation & verification*),
  - ✓ Key Destruction
- The TOE provides role-based access. Users have different access privileges. Various privilege levels and different accounts are supported.
- The TOE provides a secure channel that the TOE can use to communicate with remote users via a Web Browser for protection of the communicated data from modification, and disclosure.
- The TOE provides IP-based access restriction basis on a whitelist or blacklist to control the access to the SM Application Server.

1.3. Threats

Threats	Definition
T.UnAuthorized_Query	An attacker may breach the confidentiality of data on the target network by using malicious software infected by an attacker into devices in the target network with the aim of providing data leakage from the target network.
T.Physical_Manipulation	The hardware parts of the TOE may be subject to physical attack by an attacker, which may compromise the security of the user data (Target Network Information).
T.Admin_Imperson	An attacker or any monitor user may impersonate an Admin User to get admin privileges.
T.Remote_Manage	An attacker may attempt to disclose the authentication data of the Admin User (s) or Monitor User (s) transmitted via Web Browser to DataBrokerX SM_Portal or DataBrokerX CM_Portal and may attempt to modify administration session information for manipulation of the configuration of the DataBrokerX CM Services and DataBrokerX SM Services.
T.Modify_Audit	The audit log store may be full, making it impossible to record the logs of the attacker's unauthorized access attacks on the CM Application Server and the SM Application Server.

Table 1: *Threats*

The threat agents are divided into two categories:

Attackers: They are not TOE users and have public knowledge of how the TOE operates. They do not have physical access to the TOE.

Monitor Users: They have extensive knowledge of how the TOE operates, and they are assumed to possess a high skill level, and physical access to the TOE.

1.4. Organizational Security Policies (OSPs)

Policies	Definition
P.One_Way_Flow	The TOE shall provide a unidirectional (One-way) secure data path for both directions to allow real-time requests and responses between target public network points in the outside world and the private network point.
P.Secure_Access	For controlled access, the TOE shall be located in a data center or system room in closed cabinets, and physical security measures shall be taken to prevent unauthorized physical access to TOE components.
P.Management_Workstation	Anti-virus/EDR software shall be installed and updated on the workstations of the users who will access the TOE to manage or use it. The security of the operating system shall also be managed and the current patch level shall be monitored.
P.GUI_Access	Access to the TOE by the TOE users shall be controlled and authorized through the Firewall. For data traffic control, both IPS (for data filtering) and WAF shall be used. This prevents unauthorized access attempts and blocking attempts to the System's Management Interface.

Table 2: *Organizational Security Policies*

1.5. Assumptions

These assumptions are made on the operational environment in order to be able to ensure that the security functionality can be provided by the TOE. If the TOE is placed in an operational environment that does not meet these assumptions, the TOE may no longer be able to provide all of its security functionality.

Assumption	Definition
A.Personnel	*It is assumed that* the authorized person who has access to the TOE for management activities (admin user) 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 source network and the target network.
A.Environment	*It is assumed that* the TOE environment provides stable network connectivity for the TOE to perform its intended function.
A.Audit	*It is assumed that* maintained audit logs are regularly examined.
A.OS_Environment	*It is assumed that* the Operating System used as the Operational Environment of the TOE and the libraries installed on the file system (*including the web application service pa*cks) have full security updates, and *it is assumed that* OS security restrictions have been made.

Table 3: *Assumptions for the Operational Environment*

2 -CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03.0.00.00//TSE-CCCS-103
TOE Name and Version	DataBrokerX v1.0.0
Security Target Title	DataBrokerX Client Module and Server Module Security Target
Security Target Version	1.9
Security Target Date	28/06/2026
Assurance Level	EAL4 + (AVA_VAN.5, ADV_IMP.2, ALC_FLR.2, ALC_DVS.2)
Criteria	• 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

Common Criteria Conformance	• 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

Security policies are stated at Section 1.4 and detailed in Table 2.

2.3 Assumptions and Clarification of Scope

Assumptions are stated at Section 1.5 and detailed in Table 3.

2.4 Architectural Information

DataBrokerX Client Module (CM) v3.5.0		**DataBrokerX Server Module (SM) v3.5.0**	
Hardware Modules		***Hardware Modules***	
TX Module	RX Module	TX Module	RX Module
Software Modules		***Software Modules***	
CM_Application		SM_Application	
DataBrokerX CM Services	DataBrokerX CM Portal	DataBrokerX CM Services	DataBrokerX CM Portal

Table 4: *The Physical Scope of TOE*

The physical scope of the TOE is a DataBrokerX Client Module (CM) and Server Module (SM) to be installed in two separated Application Servers (as shown in the Figure 1) and TOE Documentation.

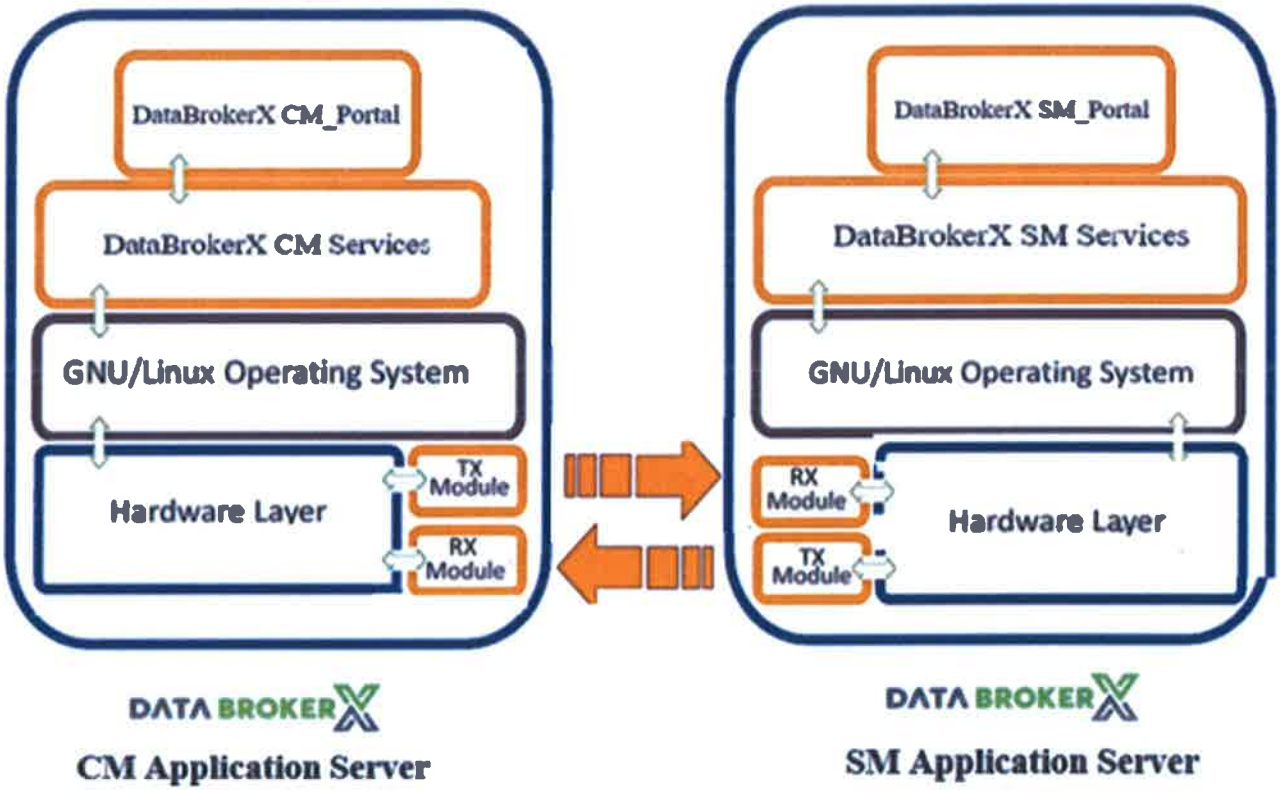

Figure 1: *DataBrokerX Client Module (CM) and Server Module (SM) Physical Scope*

DataBrokerX SM_Portal is a web-based application software used to manage and operate the SM Application Server, which is accessed using a web browser. The connection between the DataDiodeX SM_Portal and the Web Browser is established through an HTTPS connection established by using software crypto libraries. After the user authentication process, the TOE users can access the SM Application Server according to their role-based access rights. The TOE user roles (*admin and monitor*) are determined and defined during the user account creation.

DataBrokerX SM Services

- It consists of customized services to listen for requests from the private network.
- It supports three types of protocol service types (HTTP(s), LDAP(s), RDP).

- For each service running on the SM Application Server, a service is also manually created on the CM Application Server by the admin. Without a matching and correct configuration on both modules, no data transfer is possible between SM and CM modules.
- It intercepts the requests coming from the private network at the application level and sends it to the RX interface of the CM Application Server via DataDiodeX via the integrated TX interface on the SM Application Server it is working on using its propriety one way protocol.
- It receives the data messages in reply to the requests from the TX interface of the CM Application Server via the integrated RX interface on the SM Application Server it is working on and interprets them, decodes its protocol, converts the data packet to the service's protocol and then transmits the data to the client of the private network that initiated the request.

DataBrokerX CM_Portal is a web-based application software used to manage and operate the CM Application Server, which is accessed using a Web Browser. The connection between the DataDiodeX CM_Portal and Web Browser is established through an HTTPS connection established by using software crypto libraries2. After the user authentication process, the TOE users can access the CM Application Server according to their role-based access rights. The TOE user roles (*admin and monitor*) are defined and determined during the user account creation.

DataBrokerX CM Services

- It consists of a set of services that run depending on the services running on the SM Application Server, which does not have a function on its own.
- For each service running on the SM Application Server, a service is also manually created on the CM Application Server by the admin. Without a matching and correct configuration on both modules, no data transfer is possible between SM and CM modules.
- It supports three types of protocol service types (HTTP(s), LDAP(s), RDP).
- It receives the requests sent by DataBrokerX SM Services via DataDiodeX to the RX interface on the CM Application Server in its own one-way transmission protocol.
- It decodes the data which is in its own protocol delivered by DataBrokerX SM Service, gets the request data, composes the request in the desired services protocol format, executes the query or delivers the data to the configured target network point as if they were its own requests, converts the response data

into its own one way protocol and transmits the incoming replies to the RX interface of the SM Application Server via DataDiodeX over the TX interface on the CM Application Server is working.

TX Module

- ✓ Special Ethernet Card with customized SFP and
- ✓ Works in a way integrated into the host system via the PCI-e interface
- ✓ Located in both the CM Application Server and the SM 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
- ✓ Works in a way integrated into the host system via the PCI-e interface
- ✓ Located in both the CM Application Server and the SM Application Server
- ✓ Has only an optical sensor
- ✓ Has no an optical transmitter
- ✓ Is implemented at the physical layer of the OSI reference model (*no software and firmware*).

TOE Documentation consists of:

- ❖ The TOE Operational Guidance
- ❖ The TOE Preparative Procedures

All parts of the TOE including software parts and hardware parts are, installed on the Application Servers. The TOE is delivered to the customer's address by the company staff. The TOE is installed by DataBrokerX personnel. DataBrokerX customers may contact DataBrokerX support to request a copy of the guidance, which provides instructions and cautions for operating the product in its evaluated configuration.

2.5 Documentation

Document Name	Version	Release Date
DataBrokerX Client Module and Server Module Security Target	v1.9	28/06/2026
DataBrokerX TOE Architectural Analysis Document	v0.3	04/11/2024
DataBrokerX TOE Functional Specification Document	v0.4	22/03/2025
DataBrokerX TOE Design Document	v0.3	02/07/2025

DataBrokerX Operational User Guidance Document	v0.6	24/09/2025
DataBrokerX Preparational Procedures Document	v0.5	22/05/2026
DataBrokerX Configuration Management Document	v0.5	06/04/2026
DataBrokerX Configuration Elements List Document	v0.8	15/06/2026
DataBrokerX Delivery Procedures Document	v0.4	22/05/2026
DataBrokerX Development Environment Security Document	v0.4	07/04/2026
DataBrokerX Flaw Remedation Process Procedure Document	v0.1	23/03/2024
DataBrokerX Life Cycle Definition Document	v0.3	18/02/2024
DataBrokerX Development Tools and Technics Document	v0.3	18/02/2024

2.6 IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred compeletely 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 DataBrokerX Client Module and Server Module v1.0.0.

It is concluded that the TOE supports EAL 4+ (AVA_VAN.5, ADV_IMP.2, ALC_FLR.2, ALC_DVS.2). There exist 25 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 iteractions. All SFR-Enforcing TSFIs have been tested by developer. Developer has conducted 13 functional tests in total.
- **Evaluator Testing:** Evaluator has conducted 3 developer tests. Additionally, evaluator has prepared 10 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, 15 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:

- DataBrokerX Client Module (CM) and Server Module (SM) 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;

- RDP, LDAP, HTTPS Server: 10.100.30.100
- Client PC1 IP: 10.100.30.10
- Client PC2 IP: 10.100.30.11
- User information:
    - DataBrokerX-SM User: admin
    - DataBrokerX-SM User: monitor
    - DataBrokerX-CM User: admin
    - DataBrokerX-CM User: monitor

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, ADV_IMP.2, ALC_FLR.2, ALC_DVS.2.

Class Heading	Class Family	Description	Result
ADV: Development	ADV_ARC.1	Security architecture description	PASS
	ADV_FSP.4	Complete functional specification	PASS
	ADV_TDS.3	Basic modular design	PASS
	ADV_IMP.2	Complete mapping of the implementation representation of the TSF	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

Class Heading	Class Family	Description	Result
	ALC_DEL.1	Delivery procedures	PASS
	ALC_DVS.2	Sufficiency of security measures	PASS
	ALC_LCD.1	Developer Defined Life-Cycle Model	PASS
	ALC_TAT.1	Well-Defined Development Tools	PASS
	ALC_FLR.2	Flaw reporting procedures	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_IND.2	Independent testing	PASS
	ATE_DPT.1	Testing: Basic Design	PASS
AVA: Vulnerability Analysis	AVA_VAN.5	Advanced methodical vulnerability analysis	PASS

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.

It is also crucial that TOE environment shall provide stable network connectivity for the TOE to perform its intended function. This is the core part of the operational environment OE.Environment stated at Security Target.

3 SECURITY TARGET

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

Title: DataBrokerX Client Module and Server Module Security Target

Version: v1.9

Date of Document: June 28, 2026

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.

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 DataBrokerX Client Module and Server Module v1.0.0, Rel. Date: July 1, 2026

[4] DataBrokerX Client Module and Server Module Security Target, Version 1.9, Rel. Date: June 28, 2026.

6 ANNEXES

6.1 TOE SPECIFICATIONS

TOE: DataBrokerX Client Module and Server Module v1.0.0

TOE Hash (SHA256): 37a76a6b268123543fac83256328e9c81f026a36200244508a0f548e7efbb3c0

6.2 TEST ENVIRONMENT:

Hardware:

- DataDiodeX TX Server
- DataDiodeX RX Server
- DataBrokerX Client Module
- DataBrokerX Server Module
- 2 Client PC
- Servers that include RDP, LDAP, HTTPS services

Software:

- Wireshark 4.6.4