DATA FLOW	SECURITY TARGET	Document No:	
		Rev No:	1.9
		Rev Date:	28.06.2026
		Initial version:	04.09.2022

DATA BROKER

Client Module and Server Module Security Target v1.9

28.06.2026

Document History

Sürüm	Tarih	Açıklama	Değişikliği Yapan	Değişikliği Onaylayan
0.1	04.09.2022	Initial Version	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager
0.2	20.11.2022	Updated according to GR1	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager
0.3	11.12.2022	Updated according to GR1	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager
0.4	14.01.2023	Updated according to GR2	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager
0.5	07.04.2023	Updated according to GR3	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager
0.6	07.07.2023	Updated according to GR3	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager
0.7	06.08.2023	Merged TOE overview and TOE Description. Fixed typo. Changed T.Imperson name.	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager
0.8	27.08.2023	Updated Section 3.3	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager
0.9	10.09.2023	Updated Figure 3	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager
1.0	31.10.2023	Updated 1.4.1 Section. Fixed typo. Updated 1.5 Section and 6.3.1 Section.	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager
1.1	14.11.2023	Updated 2.2.2, 6.2 and 6.3.2 Section. Changed Figure 1 and 2	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager
1.2	02.02.2025	Updated according to GR19	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager
1.3	23.02.2025	Updated according to GR19	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager

1.4	22.03.2025	Updated according to GR19	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager
1.5	04.09.2025	Updated Table 11	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager
1.6	30.14.2026	Updated SFRs	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager
1.7	11.05.2026	Updated SFRs	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager
1.8	11.05.2026	Updated SFRs	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager
1.9	28.06.2026	Added Application Server Models in 1.4.3	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager

Contents

List of Tables

List of Figures

1 ST INTRODUCTION

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization.

TOE is the ***DataBrokerX Client Module (CM) and Server Module (SM)*** *and* will hereafter be referred to as the TOE ***v1.0.0*** throughout this document.

1.1 ST Organization

This ST is divided into 8 sections, as follows:

- **Section 1 ST Introduction:** Provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- **Section 2 Conformance Claims:** Provides the identification of Common Criteria (*CC*), Protection Profile, and Evaluation Assurance Level (*EAL*) package claims.
- **Section 3 Security Problem:** A security environment description in terms of assumptions, threats and organizational security policies.
- **Section 4 Security Objectives:** Identifies the security objectives that are satisfied by the TOE and its environment. It also presents the rationale for the security objectives.
- **Section 5 Extended Components:** Identifies new components (*extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)*) that are not included in CC Part 2 or CC Part 3.
- **Section 6 Security Requirements:** Presents the SFRs and SARs met by the TOE. It also presents the rationale for the security objectives.
- **Section 7 TOE Summary Specification:** Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- **Section 8 Acronyms**: Defines the acronyms used within this ST.

1.2 ST Reference

Title:	DataBrokerX Client Module and Server Module Security Target
Version:	1.9
Status:	Draft
Date:	28.06.2026
Developer:	DataFlowX Technology Corp.
Keywords:	Boundary Protection, Network Proxy, Cross Domain, Zero Trust, Network Isolation

1.3 TOE Reference

TOE Identification:	DataBrokerX Client Module (CM) and Server Module (SM)
TOE Version	v1.0.0
CC Identification:	Common Criteria for Information Technology Security Evaluations, Version 3.1R5

1.4 TOE Overview

This part of the ST describes the TOE with its intended usage, general IT features and major security features and addresses the user environment.

Today, due to cyber threats attacks that are very difficult to prevent, it has become a necessity to physically isolate private networks that contain critical information and corporate networks that are open to the Internet. Private networks had to be physically isolated regarding to the Zero Trust Architecture via a dedicated security solution, because traditional security solutions could not provide high level security. In addition, due to the need for real-time access to data, it is also an important need for these isolated networks to receive or deliver data without interruption from external resources via internet. Currently isolated private networks have no secure connection to the outside world, they cannot receive data from the Internet and other institutions.

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.

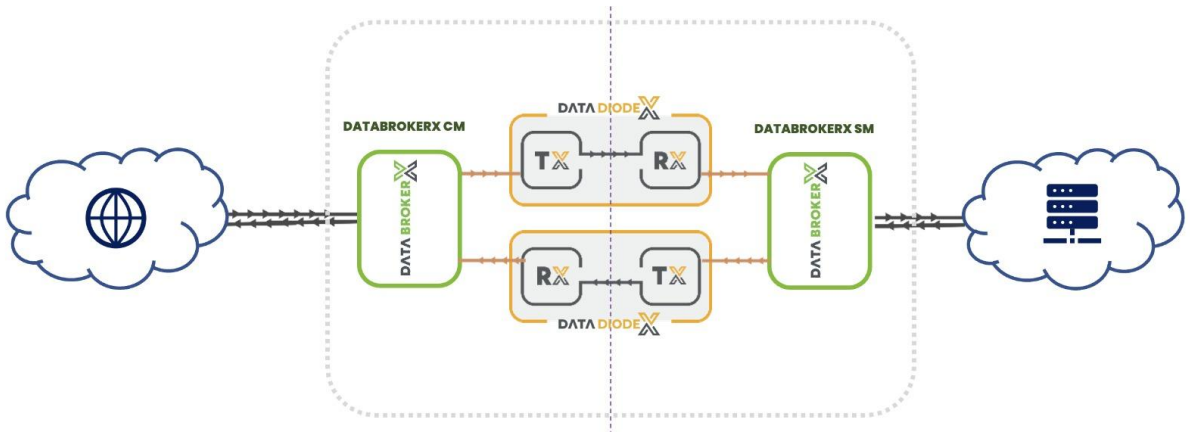

Figure 1: *DataBrokerX SM and CM modules and TOE Environment*

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.

Basically, TOE consists of two physically separate parts called the DataBrokerX Server Module (***SM***) and the DataBrokerX Client Module (***CM***). Both of these separated TOE parts are located on two separate appliances (*CM Application Server and SM Application Server*) running the GNU/Linux operating system on them. The CM Application Server and SM Application Server can be located in separate security level network cabinets and the distance between them can be many meters to comply with TEMPEST measures.

DataBrokerX SM and DataBrokerX CM perform one-way and independent (*asynchronous*) data transmissions between networks, allowing users to securely make queries and receive responses. DataBrokerX ensures that there is no two-way communication between SM and CM modules by delivering data asynchronously and independently for queries and responses without establishing a TCP/IP connection. For this purpose, both of them consist of hardware components (***TX Module and RX Module***), which are unidirectional data diode cards to ensure unidirectional transmission in both directions, and software components (***CM_Application and SM_Application***).

The TX/RX Modules on both DataBrokerX SM and DataBrokerX CM modules have two external interfaces. One external interface of these modules is connected to the PCI bus of the Application Server (*CM Application Server and SM Application Server*) on which they are installed. Other external SFP interfaces (*Fiber Optic Interface*) of the TX/RX Modules are physically connected to two different **"DataDiodeX *Modules* (*DataDiodeX*)"** with a single fiber optic cable to only send or only receive light beams in one direction.

The connection between *DataBrokerX CM - DataDiodeX* and *DataBrokerX SM - DataDiodeX* allow data to flow from the Sender to the Receiver[1] but does not allow data to flow in the reverse direction (*prevents information leak from Receiver to Sender*) 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*).

[1] *The Sender and Receiver classification changes to the defined direction of communication in Figure 1.*

1.4.1 Major Security Features of the TOE

- ✓ 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.

1.4.2 Roles of the TOE

There are two defined user roles (*Admin and Monitor*) to manage and operate the TOE. TOE Users are defined by associating them with one of these roles and their access rights on the TOE are determined by default within the scope of the roles they have defined.

Detailed description about these two roles is given below:

Admin Role: The TOE user with the admin role is called the admin user. There is only one default admin user-defined as hardcoded on the TOE but new admin users can be defined by Admin User(s). Admin Users use the TOE for only management activities including the configuration of the functional and security features.

Monitor Role: The TOE user with monitor role is called monitor user. There can be many monitor users defined on the TOE by the Admin Users. Monitor users use the TOE for only operational activities (audit log review and *dashboard monitoring*). While the passwords of the monitor users can only be changed by Admin User.

1.4.3 Non-TOE Hardware/ Software/ Firmware

Application Servers: All parts of the TOE are located in the Application Servers (*SM Application Server and CM Application Server*).

Application Server models are listed below:

DataBrokerX Small 1G	DFX-DBX-P-SM101-C-TR
DataBrokerX Small 10G	DFX-DBX-P-SM110-C-TR
DataBrokerX Medium 1G	DFX-DBX-P-MD101-C-TR
DataBrokerX Medium 10G	DFX-DBX-P-MD110-C-TR
DataBrokerX Enterprise 1G	DFX-DBX-P-EN101-C-TR
DataBrokerX Enterprise 10G	DFX-DBX-P-EN110-C-TR

The SM Application Server and the CM Application Server are physically separated from each other and powered by independent power supplies. This approach has been implemented to minimize the TEMPEST security threat. These Application Servers are generally planned to be deployed in a physically secure cabinet or data center with the appropriate level of physical access control and physical protection.

Power Supply: A component that provides power for the Application Servers (*SM Application Server and CM Application Server*).

Operating System and File System: Both the SM Application Server and the CM Application Server operate on Linux Operating System. File System stores the required configuration and log files that are read and generated by the SM Application and the CM Application.

Management Workstation: It is any PC running an operating system on it that can establish a TCP/IP connection. It is used to manage and operate the SM Application and the CM Application via the LAN Interface of the SM Application Server and the CM Application. The TOE management and operational functionalities provided by *DataBrokerX CM_Portal* and *DataBrokerX SM_Portal* are accessed by Admin User through a Web Browser running on a Management Workstation.

DataDiodeX: DataDiodeX is positioned around the DataBrokerX devices. DataBrokerX provides the secure data exchange feature via a one-way path for both directions between a target public network point and private networks with the support of DataDiodeX.

Devices in Networks: Devices in the target network and source network such as Switch, Router, and PC (*They may change depending on the deployment of the TOE in the network environment).*

Private Network Point: Any network point within the Private network that wants to use DataBrokerX SM services.

Public Network Point: A network point open to the Internet that DataBrokerX CM services attempt to access on demand.

1.4.4 TOE Type

The TOE operates and manages two Application Servers of the ***Boundary Protection Devices and Systems*** type. It is a collection of embedded application software and hardware modules installed on the Application Servers that act as a unidirectional (one-way) gateway for both directions at the physical network layer.

1.4.5 Operational Environments of the TOE

For the deployment of the TOE are given below in order to understand the use of TOE more clearly.

The TOE and the TOE environment are placed in such a way as to allow the real-time query needs of a high-security network to be made securely from the Internet.

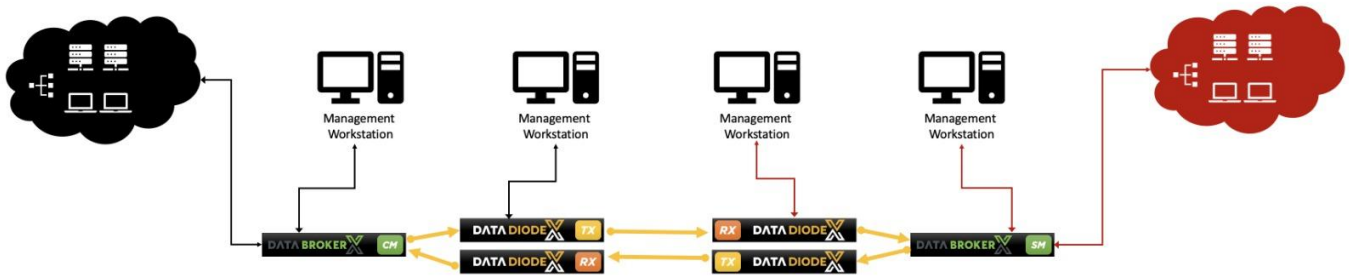

Figure 2: *Topology 3 for the deployment of the TOE*

The outgoing and incoming data are delivered independently. Different data paths are used for request and response data. Relation between request and response is not in network layer but bindings are calculated on DataBrokerX_SM module of TOE.

1.4.6 Minimum System Requirements for Non-TOE Environment

❖ **Application Servers**

- ***CPU:*** 4 Core 8 Threads 2.6Ghz Processor
- ***RAM:*** 64 GB
- ***OS:*** Debian 10
- ***Storage:*** 128 GB Hard Disk
- ***Operating temperature:*** 0°C ~ 40°C
- ***PSU:*** 240V AC 50-60hz

1.5 TOE Description

This part of the ST describes the physical and logical scopes of the TOE as an aid to the understanding security capabilities of the TOE and to the separation of the TOE from non-TOE entities.

1.5.1 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.

DataBrokerX Client Module (CM) v3.5.0 consist of below parts:

- Hardware Modules
  - TX Module
  - RX Module
- Software Modules
  - CM_Application
    - ✓ *DataBrokerX CM Services*
    - ✓ *DataBrokerX CM_Portal*

DataBrokerX Server Module (SM) v3.5.0 consist of below parts:

- Hardware Modules
  - TX Module
  - RX Module
- Software Modules
  - SM_Application
    - ✓ *DataBrokerX SM Services*
    - ✓ *DataBrokerX SM_Portal*

DataBrokerX Client Module (*CM*) and Server Module (*SM*) consists of the components (*framed in yellow*) shown in Figure 3.

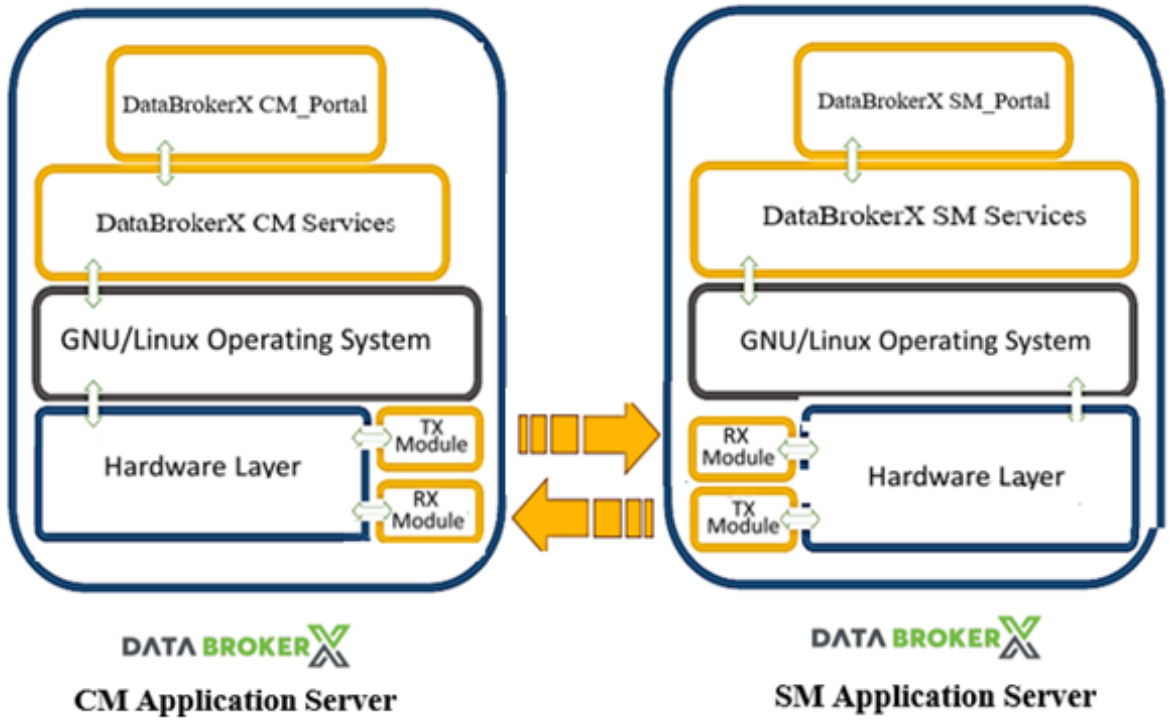

Figure 3: *The Physical Scope of the TOE*

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[2]. 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 libraries[2]. 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.

[2] *Software crypto libraries are within the scope of the DataBrokerX CM_Portal/ DataBrokerX SM_Portal and they consist of a number of sub-libraries that implement the individual crypto algorithms (symmetric encryption, public key cryptography and key agreement, certificate handling, cryptographic hash functions) and SSL/TLS protocols.*

- ✓ 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 it is working on.

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.

1.5.2 Logical Scope of TOE

This section describes the logical security features of the TOE.

Table 1- *Logical Scope of TOE*

TOE Security Function	Description
User Data Protection	The User Data Protection function implements functionality necessary to protect the private network during access to the target public network points that can be accessible through internet. The TOE applies a set of rules to provide a unidirectional (One-way) data path for both directions between the private network and the target public network points and allows real-time requests and responses between target public network points in the outside world and private network, without compromising the confidentiality of the information on the private network.
Private Network Isolation	DataBrokerX_SM and DataBrokerX_CM modules both use asynchronous and one way transmission to deliver data to the other side of the network. While DataBrokerX_CM is only capable to execute queries or deliver data packets to the preconfigured network endpoints, DataBrokerX_SM **does not have a capability** to execute query and/or fetch a response from an application or server and deliver the message to the DataBrokerX_CM as a result. With the physically separation of modules, requiring administrative access on both modules to establish a service connection and lack of capability to query and deliver response on DataBrokerX_SM module, TOE provides isolation of the private network where DataBrokerX_SM module placed and makes it unaccessable from public network while still allowing data connectivity.
Identification and Authentication	Both DataBrokerX SM and DataBrokerX CM, the TOE parts provide 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. During user password determination, the user password is checked whether the password quality meets the defined quality measure. Users who want to access the TOE for management and operational activities are authenticated *(with a unique user name and user password*) themselves to the TOE via Web Browser. The TOE does not allow any operation without logging in with the correct username, password.

	To prevent brute-force attacks, an incorrect password limit are applied. When the user authentication failure has been met three values, it does not allow further user authentication attempt for 5 minutes. In addition, inactive sessions are automatically terminated after a preconfigured time.
Audit	Configuration changes, user defining activities and successful/unsuccessful TOE user login/log out are logged with date and time information, type information of the event, the information whether the event was successful or failed. The TOE provides reliable time stamps to record the accurate date and time for audit records. All logs for each day are stored in the file system at both sides. These logs can be viewed by admin users and monitor users via a Web Browser. The TOE also overwrite the oldest stored audit records to prevent new audit record loss in case the audit storage is full.
Cryptographic Support	Both DataBrokerX SM and DataBrokerX CM, software crypto libraries perform all cryptographic operations listed below: TLS protocol implementation ○ *TLS v1.2 for HTTPS connection with Web Browser for both sides,* ○ *TLS v1.2 for LDAPs, RDP and HTTPS connection requests getting from private network to SM Services,* ○ *TLS v1.2 for LDAPs, RDP and HTTPS connection requests sending from CM services to target public network point that can be accessible through internet.* ➢ Cryptographic key generation, ➢ Cryptographic operation (*encryption, decryption, hash calculation and digital signature generation & verification*), Key destruction
Security Management	The TOE provides management functions for managing security attributes and the behavior of the security function. TSF data and TSF management access attempts of all users who are authenticated with "username" and "password" is restricted. All TOE users are associated with roles (*Admin and Monitor*) by the TOE. Role based access is used only through DataBrokerX SM_Portal and DataBrokerX CM_Portal. Users have different access privileges. Various privilege levels and different accounts are supported.

	The TOE ensures that the function behavior about the filter rules is disabled/enabled and modified only by Admin Users.
Access Control	The TOE provides IP based access restriction basis on whitelist or blacklist to control the access listening HTTP(s), LDAP(s), RDP services on SM Application Server.
Trusted Channel	The TOE provides a secure channel that the TOE can use to communicate with remote user via Web Browser for protection of the communicated data from modification, disclosure.

2 CONFORMANCE CLAIMS

2.1 CC Conformance Claim

This ST claims conformance to

- ❖ Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017, (CC Part 1)
- ❖ Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017, (CC Part 2)
- ❖ Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017, (CC Part 3)

as follows

- Part 2 conformant
- Part 3 conformant

- ❖ The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017, [CEM] has to be taken into account.

2.2 PP and Package Claim

2.2.1 Protection Profile (PP) Claim

This ST does not claim conformance to any protection profile.

2.2.2 Package Claim

This ST is conforming to assurance package EAL4 augmented with AVA_VAN.5, ADV_IMP.2, ALC_FLR.2 and ALC_DVS.2 defined in CC part 3.

2.3 Conformance Rationale

This ST does not claim conformance to any protection profile. Thus, this section is not applicable.

3 SECURITY PROBLEM DEFINITION

3.1 Threats Agents

This section identifies the threats to the assets against which protection is required by the TOE or by the security environment.

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.

3.2 Assets

Assets protected by the TOE consist of two categories: TSF data and User Data. Detailed descriptions of TOE assets are given below:

Primary Assets (User Data):

Private Network Information: The data belonging to this network can be modified, compromise confidentiality by uncontrolled data (*virus, trojan and any other malware type*) coming from the internet.

Private Network Assets: The computer systems connected to this network can be compromised by a threat actor or unauthorized user having access on internet network.

Secondary Assets (TSF Data): The secondary assets are listed below:

- ***Authentication Data:*** This asset consists of the user names and passwords used to protect security-relevant TOE settings.
- ***Cryptographic Data:*** This asset consists of:
  - SM-Side assets
    - Server TLS certificate (*including RSA Public key*) that is used to send to the Web Browser on the Management Workstation by DataBrokerX SM_Portal during the TLS handshake.
    - TLS RSA Private Key that is used for signature during the TLS handshake with Web Browser.
    - Root certificate used for verification of the integrity of the TLS certificate during the TLS handshake with Web Browser.
    - Server TLS certificate (*including RSA Public key*) used for TLS handshake with Private Network Point in case of using DataBrokerX SM services that require secure connection (*https and LDAPs*).

- RSA Private Key used signing operation by DataBrokerX SM Services in case of using DataBrokerX SM services that require secure connection (*https and LDAPs*).
- TLS session keys used to protect the TLS data traffic both Web Browser connections and DataBrokerX SM Services connections

➢ CM-Side assets

- Server TLS certificate (*including RSA Public key*) that is used to send by DataBrokerX CM_Portal to the Web Browser on the Management Workstation during the TLS handshake.
- TLS RSA Private Key that is used for signature during the TLS handshake with Web Browser.
- Root certificate used for verification of the integrity of the TLS certificate during the TLS handshake with Web Browser.
- Root certificates (*containing RSA Public key*) used for TLS handshake that DataBrokerX CM Services will establish with the **Public Network Points** to be accessible in the event that DataBrokerX SM services that require secure connections (*https and LDAPs*) are used.
- TLS session keys used to protect the TLS data traffic both Web Browser and Public Network Points connections.

❖ ***Audit Data:*** Audit Data is generated by the TOE (*both SM-side and CM-side*), for actions and events to detect any compromise of the security or address an issue in troubleshoot.

❖ ***Configuration Data:*** These data are the data entered by the Admin User to set the TOE settings via the Web Browser.

3.3 Threats

This section identifies the threats to the assets.

Table 2- *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.

3.4 Organizational Security Policies

The Organizational Security Policies identified in the following subsections are addressed by the TOE and the environment of the TOE.

The Organizational Security Policies for the operational environment are given in Table 3.

Table 3- *Organizational Security Policies*

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.

3.5 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.

The assumptions for the operational environment are given in Table 4.

Table 4- *Assumptions for the Operational Environment*

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.

4 SECURITY OBJECTIVES

The security objectives identify the responsibilities of the TOE and its environment, in meeting the security needs.

4.1 Security Objectives of the TOE

The TOE must satisfy the following objectives of the TOE.

Table 5- *Security Objectives of the TOE*

Objective	Definition
O.Authorized_Query	TOE must prevent any data that would compromise the confidentiality of information via unauthorized queries from entering the private network at the time of real-time communication. In addition, it must prevent malicious software that has infected the private network through user error from unauthorized querying of the outside world from the private network.
O.One_Way_Flow	The TOE must provide a set of rules to provide a unidirectional (One-way) secure data path for both directions between the private network point and the target public network points and allow real-time requests and responses between target public network points in the outside world and the private network without compromising the confidentiality of the information on the private network.
O.User_Authentication	The TOE must uniquely identify all TOE users and authenticate the claimed identity before granting a user access to TOE management or operational features, and take measures to prevent brute force attacks.
O.User_Privilege	The TOE must ensure that the TOE users can only access permitted security or operational functionalities.
O.Secure_Comm	The TOE must establish a secure connection to communicate with a Web Browser running on the Management Workstation.

O.Key_Managment	The TOE must provide the means for secure management of cryptographic keys used for key agreement, key generation, encryption/ decryption, and destruction of the keys.
O.Audit_Gen	The TOE must record auditable events, including audit function start-up/shutdown and user activities such as login/logout, and configuration changes, with accurate dates and timestamps. The TOE must provide authorized user with the ability to review, filter and sort the audit records.
O.Audit_Protect	If the audit trail is full, the TOE must replace the oldest audit records that have been stored.

4.2 Security Objectives of the Operational Environment

The TOE's IT environment must satisfy the following objectives.

Table 6- *Security Objectives for the Operational Environment*

Objective	Definition
OE.Physical_Security	The TOE and its interfaces shall be physically protected from unauthorized access and mechanical, electrical, optical, radiation, or any other form of physical influence.
OE.Personnel	The authorized person who has access to the TOE for management activities (admin user) shall be well-trained and will not attempt to circumvent the TOE's security functionality.
OE.Network	Apart from transmitting information through the TOE, there shall be no channels for the information to flow between the source network and the target network.
OE.Environment	TOE environment shall provide stable network connectivity for the TOE to perform its intended function.
OE.Audit	***It has to be ensured that*** appropriate audit logs stored on the both receiver-side and sender-side shall be regularly examined.
OE.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.
OE.Management_Workstation	Anti-virus 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.

OE.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.
OE.OS_Environment	The Operating System used as the Operational Environment of the TOE, the libraries installed on the file system (*including the web application service packs*) shall have full security updates and OS security restrictions shall be made.

4.3 Security Objective Rationale

This section provides rationale tables for the existence of each threat, policy statement, and assumption that compose the Security Target.

Table 7: *Objectives Mapping for Threats, Assumptions and OSPs*

	T.UnAuthorized_Query	T.Physical_Manipulation	T.Admin_Imperson	T.Remote_Manage	T.Modify_Audit	A. Personnel	A.Network	A.Environment	A.Audit	A.OS_Environment	P.One_Way_Flow	P.Secure_Access	P.Management_Workstation	P.GUI_Access
O.Authorized_Query	✓													
O.One_Way_Flow											✓			
O.User_Authentication			✓											
O.User_Privilege			✓											
O.Secure_Comm				✓										
O.Key_Managment				✓										
O.Audit_Gen			✓											
O.Audit_Protect			✓		✓									
OE.Physical_Security		✓												
OE.Personnel						✓								
OE.Network	✓						✓							
OE.Environment								✓						
OE.Audit									✓					
OE.OS_Environment										✓				
OE.Secure_Access												✓		
OE.Management_Workstation													✓	
OE.GUI_Access														✓

4.3.1 Security Objectives Rationale Relating to Threats

The following table describe the rationale for the threat to security objectives mapping.

Table 8: *Security Objectives Rationale for Threats*

Threats	Objectives	Rationale
T.UnAuthorized_Query	**O.Authorized_Query**	***O.Authorized_Query*** counters this threat by ensuring that only authorized real-time query and response are able to send/exit form/to private network.
	OE.Network	***OE.Network*** ensures that there are no channels for the information to flow between the source network and the target network, apart from transmitting information through the TOE.
T.Physical_Manipulation	**OE. Physical_Security**	***OE.Physical_Security*** ensures that the TOE and its interfaces are physically protected from unauthorized access and mechanical, electrical, optical, radiation or any other form of physical influence.
T.Admin_Imperson	**O.User_Authentication**	***O.User_Authentication*** uniquely identifies and authenticates all TOE Users (*monitor and admin users*). For an attacker or monitor user to impersonate an admin user, the they must know the admin user's identity and authentication data. To prevent brute force attacks, accounts are disabled for a certain time on repetitive authentication failure.
	O.User_Privilege	***O.User Privilege*** ensures that the TOE users can manage and operate the TOE according to the access privileges.
	O.Audit_Gen	***O. Audit_Gen*** provides a means of recording security relevant events.

	OE.Audit	***OE.Audit*** allows authorized users to detect when impersonation attacks (*e.g. brute force password guessing*) occur.
T.Remote_Manage	**O.Secure_Comm**	**O.Secure_Comm** counters this threat by ensuring that data is transferred securely between the TOE and a Web Browser running on the Management Workstation.
	O.Key_Management	***O.Key_Management*** counters this threat by providing secure cryptographic key management to enable cryptographic exchanges between the TOE and Web Browser.
T.Modify_Audit	**O.Audit_Protect**	***O.Audit_Protect*** counters this threat by overwriting the oldest stored audit records if the audit trail is full.

4.3.2 Security Objectives Rationale Relating to Assumptions

The following table describes the rationale for the assumption to security objectives mapping.

Table 9: *Objectives Rationale for Assumptions*

Assumptions	Objectives	Rationale
A. Personnel	**OE.Personnel**	***OE.Personnel*** upholds this assumption by ensuring that admin user who has access to the TOE for management activities is well-trained and is not attempt to circumvent the TOE's security functionality.
A.Network	**OE.Network**	***OE.Network*** upholds this assumption by ensuring that there are no channels for the information to flow between the source network and the target network, apart from transmitting information through the TOE.
A.Environment	**OE.Environment**	***OE.Environment*** upholds this assumption by ensuring that TOE environment is provide stable network connectivity for the TOE to perform its intended function.
A.Audit	**OE.Audit**	***OE.Audit*** upholds this assumption by ensuring that appropriate audit logs stored on the both receiver-side and sender-side are regularly examined.
A.OS_Environment	**OE.OS_Environment**	***OE.OS_Environment*** upholds this assumption by ensuring that the Operating System used as the Operational Environment of the TOE and libraries installed on the file system (*including web application service packs*) have full security updates and operating system security restrictions are enforced.

4.3.3 Security Objectives Rationale Relating to Policies

The following table describes the rationale for OSPs to security objectives mapping.

Table 10: *Objectives Rationale for OSPs*

Security Policies	Objectives	Rationale
P.One_Way_Flow	**O.One_Way_Flow**	***O.One_Way_Flow*** fulfils this Security Policies by ensuring that the TOE is provide one-way secure data path for both directions.
P.Secure_Access	**OE.Secure_Access**	***OE.Secure_Access*** fulfills these Security Policies by requiring the location of the TOE in a controlled environment for controlled access, and by taking physical security measures to prevent unauthorized physical access to the TOE.
P.Management_Workstation	**OE.Management_Workstation**	***OE.Management_Workstation*** fulfils this Security Policies by providing security controls of the computer from which the TOE is accessed.
P.GUI_Access	**OE.GUI_Access**	***OE.GUI_Access*** fulfils this Security Policies by ensuring that the TOE access network interface is monitored and managed to prevent unauthorized access by external systems.

5 EXTENDED COMPONENTS DEFINITION

There are no extended SFRs and extended SARs for this TOE.

6 SECURITY REQUIREMENTS

6.1 Security Functional Requirements

This part of the ST defines the detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE. The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in Section 8.1 of Common Criteria Part1 [17]. The following operations are used in the ST.

- The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and removed are ~~crossed out.~~
- The **selection** operation is used to select one or more options provided by the CC instating a requirement. Selections having been made are denoted as underlined text.
- The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments are denoted by *italicized* text.
- The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

6.1.1 Class FAU: Security Audit

6.1.1.1 FAU_GEN.1 - Audit data generation

Hierarchical to: No other components.

Dependencies: [FPT_STM.1 Reliable time stamps] **fulfilled** by FPT_STM.1

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified[3] level of audit; and

c) *User defining activities and successful/unsuccessful TOE user (admin or monitor) login/log out, and configuration changes.* [4].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, ~~subject identity (if applicable)~~, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ~~PP/~~ST, *no other audit-relevant information*[5].

6.1.1.2 FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: [FAU_GEN.1 Audit data generation] **fulfilled** by FAU_GEN.1.

FAU_SAR.1.1 The TSF shall provide *all users*[6] with the capability to read *auditable events*[7] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

[3] *[selection, choose one of: minimum, basic, detailed, not specified]*
[4] *[assignment: other specifically defined auditable events]*
[5] *[assignment: other audit relevant information]*
[6] *[assignment: authorised users]*
[7] *[assignment: list of audit information]*

6.1.1.3 FAU_STG.4 - Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss.

Dependencies: [FAU_STG.1 Protected audit data storage] **not fulfilled but justified** by FAU_STG.1

FAU_STG.4.1 The TSF shall overwrite the oldest stored audit records[8] and *none*[9] if the audit trail is full.

Justification: *Due to the functionality limitations of the TOE, audit logs cannot be deleted by anyone, both authorized and unauthorized. There is no need for FAU_STG.1 as there is no interface for delete and modify operations.*

Application Note 1: *Because of the overwriting the oldest stored audit records, previous audit record is erased. Those responsible for the operation of the TOE must examine the audit storage regularly (see OE.Audit). Detailed information will be given in TOE Operational Guide.*

[8] *[selection, choose one of: "ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"]*

[9] *[assignment: other actions to be taken in case of audit storage failure]*

6.1.2 Class FCS: Cryptographic Support

6.1.2.1 FCS_CKM.1/AES-GCM for TLS - Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] **fulfilled** by FCS_COP.1/AES-GCM for TLS and [FCS_CKM.4 Cryptographic key destruction] **fulfilled** by FCS_CKM.4

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *EC Diffie-Hellman Key-Agreement for TLS 1.2 protocol* [10] and specified cryptographic key sizes *256 bits*[11] that meet the following: *RFC 5246*[12].

6.1.2.2 FCS_COP.1/HASH Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] **not fulfilled** but justified.
[FCS_CKM.4 Cryptographic key destruction] **not fulfilled** but justified.

Justification: *SHA-384 hash function does not use a key so there is neither need to create nor need to destroy.*

FCS_COP.1.1 The TSF shall perform *hash value calculation*[13] in accordance with a specified cryptographic algorithm *SHA-384*[14] and cryptographic key sizes *none*[15] that meet the following: *FIPS 180-4*[16].

6.1.2.3 FCS_COP.1/AES-GCM for TLS - Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] **fulfilled** by FCS_CKM.1/AES-GCM for

[10] *[assignment: cryptographic key generation algorithm]*
[11] *[assignment: cryptographic key sizes]*
[12] *[assignment: list of standards]*
[13] *[assignment: list of cryptographic operations]*
[14] *[assignment: cryptographic algorithm]*
[15] *[assignment: cryptographic key sizes]*
[16] *[assignment: list of standards]*

	TLS; [FCS_CKM.4 Cryptographic key destruction] **fulfilled** by FCS_CKM.4
FCS_COP.1.1	The TSF shall perform *encryption and decryption for TLS/SSL connection*[17] in accordance with a specified cryptographic algorithm *AES in GCM*[18] and cryptographic key sizes 256 *bits*[19] that meet the following: *FIPS PUB 197 and NIST SP 800-38D*[20].

6.1.2.4 FCS_COP.1/TLS_SIGN Cryptographic encryption operation

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] **not fulfilled** but justified. [FCS_CKM.4 Cryptographic key destruction] **not fulfilled** but justified.
Justification:	*The RSA private key needed to perform the cryptographic operation is stored securely in encrypted form. Therefore, FCS_CKM.1 and FDP_ITC.1 SFRs are not required.* *RSA private key is needed to signature operation in all TLS connection. Therefore, FCS_CKM.4 is not required as it is not possible to recover again if the key is destroyed.*
FCS_COP.1.1	The TSF shall perform *signing*[21] in accordance with a specified cryptographic algorithm *RSA*[22] and cryptographic key sizes *2048 bits*[23] that meet the following: *RFC 3447*[24].

6.1.2.5 FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] **fulfilled** by FCS_CKM.1/AES-GCM for TLS

[17] *[assignment: list of cryptographic operations]*
[18] *[assignment: cryptographic algorithm]*
[19] *[assignment: cryptographic key sizes]*
[20] *[assignment: list of standards]*
[21] *[assignment: list of cryptographic operations]*
[22] *[assignment: cryptographic algorithm]*
[23] *[assignment: cryptographic key sizes]*
[24] *[assignment: list of standards]*

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *cryptographic zeroization*[25] that meets the following: *FIPS 140-2 zeroization requirements*[26].

[25] *[assignment: cryptographic key destruction method]*
[26] *[assignment: list of standards]*

6.1.3 Class FDP: User Data Protection

6.1.3.1 *FDP_IFC.1/HTTP(s) Subset Information Flow Control*

Hierarchical to: No other components

Dependencies: FDP_IFF.1 Simple security attributes **fulfilled** by FDP_IFF.1/HTTP(s)

FDP_IFC.1.1 The TSF shall enforce the *HTTP(s) Service SFP*[27] on

Subjects: Public Network Point and Private Network Point

Information: HTTP protocol data

Operations: Proxy and Control[28]

6.1.3.2 *FDP_IFC.1/LDAP(s) Subset Information Flow Control*

Hierarchical to: No other components

Dependencies: FDP_IFF.1 Simple security attributes **fulfilled** by FDP_IFF.1/LDAP(s)

FDP_IFC.1.1 The TSF shall enforce the *LDAP(s) Service SFP*[29] on

Subjects: Public Network Point and Private Network Point

Information: LDAP protocol data

Operations: Proxy and Control[30]

6.1.3.3 *FDP_IFC.1/RDP Subset Information Flow Control*

Hierarchical to: No other components

Dependencies: FDP_IFF.1 Simple security attributes **fulfilled** by FDP_IFF.1/RDP

FDP_IFC.1.1 The TSF shall enforce the *RDP Service SFP*[31] on

Subjects: Public Network Point and Private Network Point

Information: RDP protocol data

Operations: Proxy and Control[32]

---

[27] *assignment: information flow control SFP*

[28] *assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*

[29] *assignment: information flow control SFP*

[30] *assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*

[31] *assignment: information flow control SFP*

[32] *assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*

6.1.3.4 FDP_IFC.2 Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes **fulfilled** by FDP_IFF.1/ONE-WAY for BOTH DIRECTION

FDP_IFC.2.1 The TSF shall enforce the *One-Way Information Flow for Both Directions SFP*[33] on

Subjects: Public Network Point and Private Network Point

Information:

- *Any optical signal carrying information to be transferred by DataBrokerX SM Services for real-time request to the Public Network Point through the Interface between the TX Module of SM and DataDiodeX.*
- *Any optical signal carrying information to be received by DataBrokerX SM Services for real-time response from the Public Network Point through the Interface between the RX Module of SM and DataDiodeX*
- *Any optical signal carrying information to be received by DataBrokerX CM Services for real-time request to the Public Network Point through the Interface between the RX Module of CM and DataDiodeX.*
- *Any optical signal carrying information to be transferred by DataBrokerX CM Services for real-time response through the interface between the TX Module of CM and DataDiodeX.*[34]

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

[33] *[assignment: information flow control SFP]*

[34] *[assignment: list of subjects and information]*

6.1.3.5 FDP_IFF.1/ONE-WAY for BOTH DIRECTION Simple Security Attributes

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control **fulfilled** by FDP_IFC.2

FMT_MSA.3 Static attribute initialization **not fulfilled** but justified

Justification: *The TOE configuration is static and has no concept of manageable security attributes. Therefore, this dependency SFR is not required, nor meaningful.*

FDP_IFF.1.1 The TSF shall enforce the *One-Way Information Flow for Both Directions SFP*[35] based on the following types of subject and information security attributes:

Subjects: Public Network Point and Private Network Point

Information:

- *Any optical signal will be transferred by DataBrokerX SM Services for real-time request to the Public Network Point through the Interface between the TX Module of SM and DataDiodeX.*
- *Any optical signal will be received by DataBrokerX SM Services for real-time response from the Public Network Point through the Interface between the RX Module of SM and DataDiodeX.*
- *Any optical signal will be received by DataBrokerX CM Services for real-time request to the Public Network Point through the Interface between the RX Module of CM and DataDiodeX.*

Subject Attributes: Target Network and Source Network

Information Attributes: Request Information and Response Information[36].

[35] *[assignment: information flow control SFP]*

[36] *[assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]*

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *no security attribute-based rules*[37].

FDP_IFF.1.3 The TSF shall enforce the *none*[38].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules:

i. *Any information attempting to exit from the SFP Fiber Optic Interface of the TX Module of the SM and attempting to enter to the DataDiodeX.*

ii. *Any information coming from the DataDiodeX in order to enter the SFP Fiber Optic Interface of the RX Module of SM*

iii. *Any information attempting to exit from the SFP Fiber Optic Interface of the TX Module of the CM and attempting to enter to the DataDiodeX.*

iv. *Any information coming from the DataDiodeX in order to enter the SFP Fiber Optic Interface of the RX Module of CM*[39].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:

i. *Any information attempting to leave through the SFP Fiber Optic Interface of the RX Module of CM.*

ii. *Any information attempting to leave through the SFP Fiber Optic Interface of the RX Module of SM.*

iii. *Any information attempting to enter to the SFP Fiber Optic Interface of the TX Module of the SM.*

iv. *Any information attempting to enter to the SFP Fiber Optic Interface of the TX Module of the CM.*[40]

[37] *[assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]*

[38] *[assignment: additional information flow control SFP rules]*

[39] *[assignment: rules, based on security attributes that explicitly authorise information flows].*

[40] *[assignment: rules, based on security attributes that explicitly deny information flows].*

6.1.3.6 FDP_IFF.1/HTTP(s) Simple Security Attributes

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control **fulfilled** by FDP_IFC.1

FMT_MSA.3 Static attribute initialization **not fulfilled** but justified

Justification: *HTTP protocol data is static and has no concept of manageable security attributes. Therefore, this dependency SFR is not required, nor meaningful.*

FDP_IFF.1.1 The TSF shall enforce the *the HTTP(s) Service SFP*[41] based on the following types of subject and information security attributes:

Subjects: Public Network Point and Private Network Point

Information: HTTP Protocol data

Subject attributes: IP address, DataBrokerX SM Side and DataBrokerX CM Side

Information attributes: HTTP Request and HTTP Response[42]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *no security attribute-based rules*[43]

FDP_IFF.1.3 The TSF shall enforce the *none*[44].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: *none*[45].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: *If the IP address of Private Network Point is included in blacklist defined by the Admin User, the HTTP request is rejected*[46].

[41] *[assignment: information flow control SFP]*

[42] *[assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]*

[43] *[assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]*

[44] *[assignment: additional information flow control SFP rules]*

[45] *[assignment: rules, based on security attributes that explicitly authorise information flows].*

[46] *[assignment: rules, based on security attributes that explicitly deny information flows].*

6.1.3.7 FDP_IFF.1/LDAP(s) Simple Security Attributes

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control **fulfilled** by FDP_IFC.1

FMT_MSA.3 Static attribute initialization **not fulfilled** but justified

Justification: *LDAP Protocol Data is static and has no concept of manageable security attributes. Therefore, this dependency SFR is not required, nor meaningful.*

FDP_IFF.1.1 The TSF shall enforce the *the LDAP(s) Service SFP*[47] based on the following types of subject and information security attributes:

Subjects: Public Network Point and Private Network Point

Information: LDAP Protocol data

Subject attributes: IP address, DataBrokerX SM Side and DataBrokerX CM Side

Information attributes: LDAP Request and LDAP Response[48]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *no security attribute-based rules*[49]

FDP_IFF.1.3 The TSF shall enforce the *none*[50].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: *none*[51].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: *If the IP address of Private Network Point is included in blacklist defined by the Admin User, the LDAP request is rejected*[52].

[47] *[assignment: information flow control SFP]*

[48] *[assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]*

[49] *[assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]*

[50] *[assignment: additional information flow control SFP rules]*

[51] *[assignment: rules, based on security attributes that explicitly authorise information flows].*

[52] *[assignment: rules, based on security attributes that explicitly deny information flows].*

6.1.3.8 FDP_IFF.1/RDP Simple Security Attributes

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control **fulfilled** by FDP_IFC.1

FMT_MSA.3 Static attribute initialization **not fulfilled** but justified

Justification: *RDP Protocol Data is static and has no concept of manageable security attributes. Therefore, this dependency SFR is not required, nor meaningful.*

FDP_IFF.1.1 The TSF shall enforce the *the RDP Service SFP*[53] based on the following types of subject and information security attributes:

Subjects: Public Network Point and Private Network Point

Information: RDP Protocol Data

Subject attributes: IP address, DataBrokerX SM Side and DataBrokerX CM Side

Information attributes: RDP Request and RDP Response[54]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *no security attribute-based rules*[55]

FDP_IFF.1.3 The TSF shall enforce the *none*[56].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: *none*[57].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: *If the IP address of Private Network Point is included in blacklist defined by the Admin User, the RDP request is rejected*[58].

[53] *[assignment: information flow control SFP]*

[54] *[assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]*

[55] *[assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]*

[56] *[assignment: additional information flow control SFP rules]*

[57] *[assignment: rules, based on security attributes that explicitly authorise information flows].*

[58] *[assignment: rules, based on security attributes that explicitly deny information flows].*

6.1.4 Class FMT: Security Management

6.1.4.1 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles **fulfilled** by FMT_SMR.1

FMT_SMF.1 Specification of Management Functions **fulfilled** by FMT_SMF.1

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete, *and define*[59] the *data described in the table below* to *the authorized identified roles in the table below*[60].

Table 11- *Management of TSF data*

TSF Data	*Define*	*Query*	*Modify*	*Delete*
Audit Data	*N/A*	*Admin* *Monitor User*	*X*	*X*
Monitor User Account	*Admin*	*Admin*	*Admin*	*Admin*
Monitor User Password	*Admin*	*X*	*Admin*	*X*
Admin Account	*Admin*	*Admin*	*Admin*	*Admin*
Admin Password	*Admin*	*X*	*Admin*	*X*

[59] *[selection: change_default, query, modify, delete, clear, [assignment: other operations]]*

[60] *[assignment: list of TSF data] to [assignment: the authorised identified roles]*

6.1.4.2 FMT_MOF.1/FLOW_RULE Management of security functions behavior

Hierarchical to: No other components.

Dependencies: [FMT_SMR.1 Security roles] **fulfilled** by FMT_SMR.1

[FMT_SMF.1 Specification of Management Functions] **fulfilled** by FMT_SMF.1

FMT_MOF.1.1 The TSF shall restrict the ability to disable, enable and modify the behaviour of [61] the function *filter rules*[62] to *Admin*[63].

6.1.4.3 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

For Admin User on the SM Side:

- *Dashboard*
- *System Configuration*
  - *User Management*
- *HTTP Services*
  - *Http Services*
  - *Security Filters*
  - *SSL Certificates*
- *LDAP Services*
  - *LDAP Services*
  - *LDAP Certificates*
- *RDP Services*
  - *RDP Services*
  - *RDP Certificates*
- *Reporting*
  - *Audit Logs*

For Admin User on the CM Side:

- *System Configuration*
  - *User Management*
- *HTTP Services*
  - *Http Services*
  - *Security Filters*
- *LDAP Services*
  - *LDAP Services*
- *RDP Services*
  - *RDP Services*

[61] *[selection: determine the behaviour of, disable, enable, modify the behaviour of]*

[62] *[assignment: list of functions]*

[63] *[assignment: the authorised identified roles].*

- *Reporting*
  - *Audit Logs*

6.1.4.4 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification **fulfilled** by FIA_UID.2 which is hierarchic to FIA_UID.1
FMT_SMR.1.1	The TSF shall maintain the roles *Admin and Monitor*[64]
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.1.5 Class FTA: TOE Access

6.1.5.1 FTA_SSL.3 TSF-initiated termination

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_SSL.3.1	The TSF shall terminate an interactive session after *25 minutes.*

6.1.6 Class FPT: Protection of the TSF

6.1.6.1 FPT_STM.1 Reliable Time Stamps

Hierarchical to:	No other components
Dependencies:	No dependencies
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.

Application Note 2: *The TOE gets the reliable time stamps from the RTC in the Application Servers, Real-time clocks of the Application Servers are updated from a trusted NTP server.*

[64] *[assignment: the authorised identified roles]*

6.1.7 Class FIA: Identification and Authentication

6.1.7.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: [FIA_UAU.1 Timing of authentication] **fulfilled** by FIA_UAU.2 which is hierarchic to FIA_UAU.1

FIA_AFL.1.1 The TSF shall detect when *3 times* unsuccessful authentication attempts occur related to *user authentication.*

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall *not allow new authentication attempt for 5 minutes*.

6.1.7.2 FIA_UID.2 User Identification before any action

Hierarchical to: FIA_UID.1.

Dependencies: No dependencies

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.7.3 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1.

Dependencies: [FIA_UID.1 Timing of identification] **fulfilled** by FIA_UID.2 which is hierarchic to FIA_UID.1

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.7.4 FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet *length of 12 case-sensitive characters and must contain at least one characters from upper case letters, lower case letters, numbers and non-alphanumeric symbols.*

6.1.8 Class FTP: Trusted Path/Channels

6.1.8.1 FTP_TRP.1 Trusted Path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification, disclosure.

FTP_TRP.1.2 The TSF shall permit remote users to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial user authentication.

6.2 Security Assurance Requirements

For the evaluation of the TOE and its development and operating environment, are those taken from the Evaluation Assurance Level (*EAL4*) and augmented by taking the following component: AVA_VAN.5, ADV_IMP.2, ALC_FLR.2 and ALC_DVS.

The security assurance requirements are listed in Table 11 below.

Table 12- *Security Assurance Requirements Table*

Assurance Classes	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV.IMP.2 Complete mapping of the implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance Documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life Cycle Support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DVS.2 Sufficiency of security measures
	ALC_TAT.1 Well-defined development tools
	ALC_DEL.1 Delivery procedures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_FLR.2 Flaw reporting procedures
ASE: Security Target Evaluation	ASE_INT.1 ST Introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability Assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

Table 13- *Security Functional Requirements Rationale*

Objective	SFRs	Rationale
O.Authorized_Query	FDP_IFC.1/HTTP(s) Subset Information Flow Control	This requirement meets the objective by ensuring that any information flow in the TOE is covered by the "*HTTP(s)* Services *SFP*".
	FDP_IFF.1/ HTTP(s) Simple security attributes	This requirement meets the objective by ensuring the http data transfer for both directions between the CM Application Server and SM Application Server is broken and controlled.
	FDP_IFC.1/LDAP(s) Subset Information Flow Control	This requirement meets the objective by ensuring that any information flow in the TOE is covered by the "*LDAP(s)* Services *SFP*".
	FDP_IFF.1/ LDAP(s) Simple security attributes	This requirement meets the objective by ensuring the LDAP data transfer for both directions between the CM Application Server and SM Application Server is broken and controlled.
	FDP_IFC.1/RDP Subset Information Flow Control	This requirement meets the objective by ensuring that any information flow in the TOE is covered by the "*RDP* Services *SFP*".
	FDP_IFF.1/ RDP Simple security attributes	This requirement meets the objective by ensuring the RDP data transfer for both directions

		between the CM Application Server and SM Application Server is broken and controlled.
O.One_Way_Flow	FDP_IFC.2 Complete information flow control	This requirement meets the objective by ensuring that any information flow in the TOE is covered by the "*One-Way Information Flow for Both Directions SFP*".
	FDP_IFF.1/ONE-WAY for BOTH DIRECTIONS Simple security attributes	This requirement meets the objective by ensuring the one-way data transfer for both directions between CM Application Server. and SM Application Server.
O.User_Authentication	FIA_SOS.1 Verification of Secrets	This requirement meets the objective by requiring a mechanism to verify that secrets meet a minimum level of security.
	FIA_UAU.2 User authentication before any action	This requirement meets the objective by requiring all TOE users to authenticate before any other TSF-mediated actions are performed.
	FIA_UID.2 User identification before any action	This requirement meets the objective by requiring all TOE users to identify before any other TSF-mediated actions are performed.
	FTA_SSL.3 TSF-initiated termination	This requirement meets the objective by ensuring the TOE provides a protection,

		automatically terminating sessions after a period of user inactivity.
	FIA_AFL.1 Authentication failure handling	This requirement meets the objective by ensuring that the TOE provides a protection by limiting the number of unsuccessful authentication attempts before imposing a timeout on that user account.
O.User_Privilege	FMT_MTD.1 Management of TSF data	This requirement meets the objective by ensuring the TOE provides the function so authorized users can manage the TSF data.
	FMT_SMR.1 Security Roles	This requirement meets the objective by ensuring that the TOE associates users with roles (*Admin and Monitor User*) to provide access to TSF management functions and TSF data.
	FMT_MOF.1/FLOW_RULE Management of security functions behavior	This requirement meets the objective by ensuring that the function behaviour about the filter rules is disabled/enabled and modified only by Admin Users.
	FMT_SMF.1 Specification of Management Functions	This requirement meets the objective by ensuring that the TOE provides the admin user with the ability to manage the security functions of the TSF.
O.Secure_Comm	FCS_COP.1/AES-GCM for TLS Cryptographic operation	This requirement meets the objective by ensuring that the TOE provides the cryptographic encryption and decryption operation with AES Algorithm *(in*

		GCM Mode) for secure TLS (*TLSv1.2*) communication.
	FCS_COP.1/TLS_SIGN Cryptographic operation	This requirement meets the objective by ensuring that the TOE provides the cryptographic digital signature generation operation with RSA Algorithm for secure TLS (TLSv1.2) communication between the TOE and a Web Browser on the Management Workstation.
	FCS_COP.1/HASH Cryptographic operation	This requirement meets the objective by ensuring that the TOE provides the cryptographic hashing operation with SHA384 Algorithm for secure TLS (*TLSv1.2*) communication.
	FTP_TRP.1 Trusted Path	This requirement meets the objective by ensuring that the TOE establishes and maintains a trusted communication by using TLS protocol (*TLSv1.2*).
O.Key_Managment	FCS_CKM.1/AES-GCM for TLS Cryptographic key generation	This requirement meets the objective by ensuring that the TOE generate cryptographic AES keys as a result of the handshake message of the TLSv1.2 protocol.
	FCS_CKM.4 Cryptographic key destruction	This requirement meets the objective by ensuring that the cryptographic keys are destroyed.

O.Audit_Gen	FAU_GEN.1 Audit Data Generation	This requirement meets the objective by ensuring that the TOE generates and records auditable events, including audit function start-up/shutdown and user login/logout activities, logout ,and configuration changes, with accurate dates and timestamps.
	FAU_SAR.1 Audit review	This requirement meets the objective by ensuring that the TOE provides the ability to review logs for to support management of the audit facilities.
	FPT_STM.1 Reliable Time Stamps	This requirement meets the objective by ensuring that the TOE ensures that a date and time stamp is recorded with the audit record.
O.Audit_Protect	FAU_STG.4 Prevention of audit data loss	This requirement meets the objective by ensuring that the TOE prevents the audit data loss by overwriting the oldest stored audit records.

6.3.2 Security Assurance Requirements Rationale

As the DataBrokerX Client Module (CM) and Server Module (SM) (TOE) allow secure access to the public internet network point from an isolated private network, attackers can be highly motivated to manipulate the designed system. Considering the advantages that attackers will gain as a result of hacking the system, attackers can accept the necessary costs and carry out attacks. Therefore, potential customers expect the TOE to have maximum security assurance level to protect itself advance attacks. For these reasons, EAL4 + AVA_VAN.5, ADV_IMP.2, ALC_FLR.2 and ALC_DVS.2 security assurance level has been chosen.

EAL4 is the highest level at which it is likely to be feasible to retrofit to an existing product line. The underlying EAL4 assurance level is augmented by AVA_VAN.5 (*Advanced methodical vulnerability analysis*).

The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential.

By using the component ALC_FLR.2, it is possible to respond to security flaw complaints from TOE users in a suitable manner and to identify the right recipient of corrective updates.

ADV_IMP.2's selection offers a higher level of assurance for the TOE's implementation, particularly in terms of the lack of unexpected functionality.

The selection of ALC_DVS.2 ensures that the development environment is protected against tampering, and that the security measures applied throughout the development lifecycle are sufficient to maintain the integrity of the TOE.

7 TOE SUMMARY SPECIFICATION

7.1 TOE Security Functionality

This chapter provides a description of the Security Functionality of the TOE, which show how the TOE meets each Security Functional Requirement.

The Security Functionalities of the TOE are:

- Security Audit
- Cryptographic Support
- Trusted Channel
- User Data Protection
- User Identification and Authentication
- Security Management

The following section explains how the security functions are implemented.

7.1.1 Security Audit

It generates an audit record of events (*configuration changes, user defining activities and successful/unsuccessful TOE user (admin or monitor) login/log out)*.

These records contain the following information:

- success or failure of the event
- type of event
- date and time provided from the Real Time Clock (*RTC*)

The RTC is updated from a trusted NTP server. The TOE gets the reliable time stamps from the RTC in the Application Servers.

Audit records for each day are stored in the file system automatically and are displayed in a human-readable format. The TOE provides all users with the capability to read auditable events to view from the audit records. If the audit storage is full, it overwrites the oldest stored audit records.

7.1.2 User Identification and Authentication

The TOE requires Admin and Monitor User to be successfully identified and authenticated before allowing any management activities of the TOE according to the access rights. When the user authentication failure has been met by three values, it does not allow further TOE User authentication failure for 5 minutes.

The password requirements for the TOE are defined below:

Length	➢ Minimum 12
Case sensitive	Yes
Valid characters	a-z A-Z 0-9 ! @ # % ^ * + = { } : . , _ ~ / \ - [ ]
Mix	Must contain at least one characters from upper case letters, lower case letters, numbers and non-alphanumeric symbols.

After the authentication is successful, the user interface of the DataBrokerX CM_Portal and DataBrokerX SM_Portal is opened according to the administrator access rights. The TOE will terminate an authenticated interactive session after 25 minutes.

7.1.3 Cryptographic Support

It supports communication (*via any Web Browser*) between remote users and TOE to protect TSF data such as authentication data and configuration data.

Protection of the communication channel between the *Web Browser* and DataBrokerX CM_Portal and DataBrokerX SM_Portal is provided by TLS v1.2 Protocol with and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 cipher suites for key establishment and for message authentication.

- The SHA-384 algorithm is used to get the hash value of the message to be signed.
- The message authentication during the key agreement process is provided by the RSA signature algorithm (*FCS_COP.1/TLS_SIGN*).
- The EC Diffie-Hellman algorithm is used for key generation during the key agreement process.
- The AES Algorithm with 256 bits key in GCM Mode is used for encryption/decryption operation during TLS Session.

The TOE destroys cryptographic keys in accordance with FIPS 140-2 zeroization requirements.

7.1.4 User Data Protection

All parts of the TOE are located in the Application Servers (*SM and CM*). Both the SM Application Server and CM Application Server are entirely independent, each with its own independent power and network interfaces, each enclosed in an enclosure that does not admit

electrical or optical signals via any other than the described interfaces. The SM Application Server is only connected to the Private Network and is not connected to the Public Network. Conversely, the CM Application Server is connected only to the Public Network.

The SM Application Server and CM Application Server are connected each other with via two DataDiodeX. The SM Application Server and CM Application Server are connected to the DataDiodeX via Fiber Optic Cable. This ensures that all data flowing through the TOE must flow through the fiber-optic cable and are thereby covered by the *One-Way Information Flow for Both Directions SFP.*

These SFPs contain the following rules:

- The TOE explicitly authorizes an information flow based on the following rules:
  - Any information attempting to exit from the SFP Fiber Optic Interface of the TX Module of the SM and attempting to enter to the DataDiodeX
  - Any information coming from the DataDiodeX in order to enter the SFP Fiber Optic Interface of the RX Module of SM
  - Any information attempting to exit from the SFP Fiber Optic Interface of the TX Module of the CM and attempting to enter to the DataDiodeX
  - Any information coming from the DataDiodeX in order to enter the SFP Fiber Optic Interface of the RX Module of CM.
- The TOE explicitly denies an information flow based on the following rules:
  - Any information attempting to leave through the SFP Fiber Optic Interface of the RX Module of CM.
  - Any information attempting to leave through the SFP Fiber Optic Interface of the RX Module of SM.
  - Any information attempting to enter to the SFP Fiber Optic Interface of the TX Module of the SM.
  - Any information attempting to enter to the SFP Fiber Optic Interface of the TX Module of the CM.

The TOE also enforces the *HTTP(s) Service SFP, LDAP(s) Service SFP and RDP Service SFP* on Public Network Point and Private Network Point. If the IP address of Private Network Point is included in blacklist defined by the Admin User, the all requests (*RDP, HTTP and LDAP*) are rejected

7.1.5 Security Management

It provides the Admin User the capability to manage the TOE. In this context, the following management functions are performed by Admin User in this scope:

- On the SM Side:
  - *Dashboard*
  - *System Configuration*
    - *User Management*
  - *HTTP Services*
    - *Http Services*
    - *Security Filters*
    - *SSL Certificates*
  - *LDAP Services*
    - *LDAP Services*
    - *LDAP Certificates*
  - *RDP Services*
    - *RDP Services*
    - *RDP Certificates*
  - *Reporting*
    - *Audit Logs*
- On the CM Side:
  - *System Configuration*
    - *User Management*
  - *HTTP Services*
    - *Http Services*
    - *Security Filters*
  - *LDAP Services*
    - *LDAP Services*
  - *RDP Services*
    - *RDP Services*
  - *Reporting*
    - *Audit Logs*

It associates users with roles (*Admin and Monitor User*) to provide access to TSF management functions and TSF data.

The management access permissions are shown on the Web Bowser according to the administrators' privileges after Admin User is authenticated.

It ensures that the function behavior about the filter rules is disabled/enabled and modified only by Admin Users.

It restricts the ability to query, modify, delete, and define the data described in Table 11 to the authorized identified roles in Table11.

7.1.6 Trusted Channel

The trusted channel function guarantees a secure channel that the TOE can use to communicate with remote users via Web Browser. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

cipher suite can be selected during TLS v1.2 handshake process remote users via any Web Browser for key establishment and for message authentication.

7.2 TOE Summary Specification Mapping

Mapping of portions of the TOE security functionality to the Security Functional Requirements of the TOE are provided the following table.

Table 14- *Mapping of SFRs and the TOE Security Functionality*

	Security Audit	Cryptographic Support	User Data Protection	User Identification and Authentication	Security Management	Trusted Channels
FAU_GEN.1	✓					
FAU_SAR.1	✓					
FAU_STG.4	✓					
FCS_CKM.1/AES-GCM for TLS		✓				
FCS_CKM.4		✓				
FCS_COP.1/HASH		✓				
FCS_COP.1/AES-GCM for TLS		✓				
FCS_COP.1/TLS_SIGN		✓				
FDP_IFC.1/HTTP(s)			✓			
FDP_IFC.1/LDAP(s)			✓			
FDP_IFC.1/RDP			✓			
FDP_IFC.2			✓			
FDP_IFF.1/ONE_WAY for BOTH DIRECTION			✓			
FDP_IFF.1/HTTP(s)			✓			
FDP_IFF.1/LDAP(s)			✓			

	Security Audit	Cryptographic Support	User Data Protection	User Identification and Authentication	Security Management	Trusted Channels
FDP_IFF.1/RDP			✓			
FIA_AFL.1				✓		
FIA_UID.2				✓		
FIA_UAU.2				✓		
FIA_SOS.1				✓		
FMT_MTD.1					✓	
FMT_MOF.1/FLOW_RULE					✓	
FMT_SMF.1					✓	
FMT_SMR.1					✓	
FPT_STM.1	✓					
FTA_SSL.3				✓		
FTP_TRP.1		✓				✓

8 Acronyms

EAL	Evaluation Assurance Level
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
NTP	Network Time Protocol
LDAP	Lightweight Directory Access Protocol