SECURITY TARGET WDP MX

Document Revision History

Version	Date	Notes
1.0	07.06.2021	Initial Version
1.01	19.12.2023	Rework – Initial Version
1.1	12.06.2024	Rework to current state
1.11	14.06.2024	Minor changes
1.2	28.08.2024	Reduction of Scope
E01	14.11.2024	Changes to versioning scheme. Starting at release E01. Added Guidance documentation references.
E02	19.02.2025	Changes after evaluation of ALC
E03	27.02.2025	Changes for AGD
E04	25.03.2025	Adjusted document version numbers and hashes
E05	10.04.2025	Small adjustment in version numbers and hashes
E06	16.04.2025	Small adjustment in version numbers and hashes
E07	23.05.2025	Small adjustment in version numbers and hashes

		Clarification of Access Control SFRs New Assumption regarding logical administrative access Removed Default user from scope Fixed mistake in System-Control operation
E08	11.06.2025	Fixed minor mistake in system overview figure More precise statement in OE.Set-Up Fix typos and formatting
E09	13.06.2025	Changed file names of some manuals

Table of Contents

1 ST Introduction 5

1.1 ST reference 5

1.2 TOE reference 5

1.3 TOE overview 5

1.4 TOE description 6

1.4.1 TOE components 6

1.4.2 TOE user roles 8

1.4.3 Physical scope of the TOE 8

1.4.4 Logical scope of the TOE 12

2 Conformance Claim 13

2.1 CC Conformance Claim 13

2.2 PP Claim 13

2.3 Package Claim 13

3 Security Problem Definition 14

3.1 Assets and Definitions 14

3.1.1 Assets 14

3.1.2 Subjects 14

3.1.3 Operations 15

3.2 Threats 16

3.3 Organisational Security Policies (OSPs) 16

3.4 Assumptions 16

4 Security Objectives 17

4.1 Security Objectives for the TOE 17

4.2 Security Objectives for the Environment 17

4.3 Security Objective Rationale 19

4.3.1 T.Access_Control 19

4.3.2 T.Unauth 19

4.3.3 P.Password_Policy 20

4.3.4 A.Backend_Access 20

5 Extended Components Definitions 21

6 Security Requirements 22

6.1 Security Functional Requirements (SFRs) 22

6.1.1 User Authentication and Management 22

6.1.2 Access Control 23

6.2 Security Assurance Requirements (SARs) 25

6.3 Security Requirements Rationale 26

6.3.1 Security Functional Requirements Rationale 26

6.3.2 Security Assurance Requirements Rationale 27

7 TOE Summary Specification 28

7.1 SM.1 User identification and authentication 28

7.2 SM.2 Access control for source systems, user data and TOE data 28

8 Glossary 28

9 Bibliography 29

10 Annex A - Hash values for Guidance documentation 30

1 ST Introduction

1.1 ST reference

Title:	Security Target WDP MX
Version:	E09
Date:	13.06.2025
Sponsor:	WEY Group AG (short: WEYTEC)
Developer:	WEY Group AG
Certification-ID:	BSI-DSZ-CC-1253

1.2 TOE reference

TOE name:	WEYTEC distributionPLATFORM
TOE name short:	WDP MX
TOE version:	1.4.1

1.3 TOE overview

The TOE is the WEYTEC distributionPLATFORM developed by WEYTEC. The type of the TOE is a smart and secure *KVM (keyboard, video, mouse) solution* that provides users with flexible access to computers and information sources – even across multiple sites. The WDP MX integrates different components within a single, independent IP network. With the unique smartTOUCH keyboard, users stay focused on their tasks and can customize their view of, control over and interaction with relevant sources. It is also possible to use the WDP MX with “regular” keyboards instead of the smartTOUCH. In this setup it is also possible to use the WDP MX with a smartUX Receiver. The WDP MX is designed for 24/7 operations.

The WDP MX in version 1.4.1 as in scope of this Security Target consists of the following, uniquely identifiable components (the respective version numbers are given in section 1.4.3):

- Transmitter IPR Tx in one or more of the following configurations
  - IP Remote II DP (24872TDP-MX)
  - IP Remote III 4K (24873T-MX)
  - IP Remote IV (24874T-MX)
- Transmitter IPR USB Tx in the following configuration
  - IP Remote USB II SFP Transmitter (24877T-MX)
- Receiver IPR Rx in one or more of the following configurations
  - IP Remote II DP (24872RDP-MX)
  - IP Remote III 4K (24873R-MX)
  - IP Remote IV (24874R-MX)
- Receiver IPR Rx smartUX in one or more of the following configurations
  - IP Remote III 4K smartUX (24873RUX-MX)
  - IP Remote IV smartUX (24874RUX-MX)
- Receiver IPR USB Rx in the following configuration
  - IP Remote USB II SFP Receiver (24877R-MX)
- Control Application
- Configuration Server
- EventStore
- smartTOUCH in one or more of the following configurations

- smartTOUCH (22003BK-MX)
- smartTOUCH Flex (22002-MX)

Some TOE components are operated in the frontend (IPR Tx, IPR Rx, smartTOUCH). A single TOE usually contains multiple up to several hundreds of these components. The remaining components (Control Application, Configuration Server, EventStore) form the TOE backend. Each component is contained once in one instance of the backend, however multiple instances of the backend are possible for redundancy and business continuance reasons.

To be operational, the WDP MX needs the following non-TOE components:

- Network Switches
- Source Systems (see Glossary for definition)
- Workstation HW (i.e. Monitors, Input devices like keyboard, mouse)
- WDP MX servers, a server cluster for the backend components running Windows Server 22
- A Database with a Database Management System
- Multiple WEYTEC chassis to mount the IPR TXs and IPR RXs as well as other WEY devices with the correct formfactor like ultraFLEX Mini PCs that are used for our WDP MX Servers

Please note that the non-TOE components, especially the server cluster and the database, are also provided by WEYTEC and especially the TOE installation is performed by WEYTEC field engineers or people who obtained the same training and have to follow the same procedures. If the customer wants to use their own workstation HW or source systems, this is also possible.

The security features provided by the WDP MX are:

- User identification and authentication
- Logical access control to source systems, user data and TOE data

1.4 TOE description

In a world where work processes are increasingly digitized, automated, and monitored, the amount of information we manage is expanding exponentially.
Manual operator tasks are shifting towards data oversight, controlling and intervention activities. And as human beings, we need tools to help us observe and respond to deviations in data streams, immediately and accurately.

This support can be provided by the WEYTEC distributionPLATFORM (WDP), a signal distribution system which presents all the relevant information from any system or source in real time to selected individuals or teams.

So that those held responsible can operate systems conveniently and ergonomically, making workflows and critical systems more resilient and secure.

1.4.1 TOE components

The TOE consists of multiple components which are described further in the following sections.

1.4.1.1 Transmitter

A transmitter is a hardware device in combination with a firmware using a proprietary communication protocol. A Source System is connected to a transmitter by connecting its keyboard, mouse, video, audio and USB port to it. The transmitter will compress the received signals of the Source System into a data stream, to make it routable to an arbitrary receiving unit. (Receiving units can be other TOE components at the workplace.) The transmitter will as well receive signals through the data stream and forward it to the Source System to make it remotely controllable from the WDP user's workplace.

Which transmitters and related sources are available per WDP-user is configured within the WDP MX User Configuration.

1.4.1.2 Receiver

A receiver is a hardware device in combination with a firmware using a proprietary communication protocol. It receives a data stream provided by a transmitter. It decompresses the contained signals to provide them to a workplace. The receiver also sends input data back to the transmitter to provide those to the Source System. This can be keyboard, mouse, USB or audio data.

1.4.1.3 Control application

The control application is a software which runs on the WDP MX servers. It is the central part the system through which the WDP-user's authorization and his access permissions are checked. The control application sends out commands to the TOE components that should be connected to each other, like transmitters and receivers.

1.4.1.4 Configuration server

The configuration server is a software which runs on the WDP MX servers. It administers all configuration data which is used by the control application. These are the WDP users and Console users account data as well as the configuration data of the devices of the system.

1.4.1.5 EventStore

The EventStore is a third-party software which is used to communicate configuration changes between the different WDP MX servers to keep the data synchronised across all servers.

1.4.1.6 SmartTOUCH

The smartTOUCH is a hardware device in combination with a firmware. It is the user interface at the workplace, through which the system is operated by the WDP-user. It consists of a keyboard with a touchscreen, allowing users to switch sources and work on the sources they are authorized to access.

The smartTOUCH flex as well is a hardware device in combination with a firmware. It also is a user interface at the workplace, through which the system is operated by the WDP-user. It consists of a touchscreen to which an external keyboard and mouse can be attached to.

An IP Remote Receiver with smartUX functionality can also be used as a user interface at the workplace, through which the system is operated by the WDP-user. A keyboard and mouse can be attached to this IP Remote Receiver. Instead of a touchscreen, an on screen display is shown at the monitor which allowes to switch sources and work on the sources they are authorized to access.

The smartTOUCH / smartTOUCH flex / smartUX is communicating with the control application. E.g. the login credentials are sent to it and verified for correctness. The control application will send information about the users access rights back to the smartTOUCH wich will display the corresponding UI elements on the touch screen for them.

The smartTOUCH / smartTOUCH flex / smartUX can also act as a receiver. It can receive video, audio and USB data and can send audio, keyboard, mouse, and USB data back to a transmitter.

1.4.2 TOE user roles

The TOE manages multiple user roles which are described within the following table.

Role name	Description
WDP-user	This role is assigned to users of the smartTOUCH / smartTOUCH flex / smartUX component after a successful login.
System-Reader	This is the least-privileged role a Console-User can be assigned to. A System-Reader can only perform Read-operations via the API. A System-Reader can access the list of User data and User Configuration and display the configuration of the WDP MX Console.
System-Observer	This role is assigned to Console-Users who are higher privileged than a System-Reader. A System-Observer can perform all actions a System-Reader can, and additionally can remotely log-out WDP-Users and has full access to the Connection States.
System-Controller	This role is assigned to Console-Users who are higher privileged than a System-Observer. A System-Controller can perform all actions a System-Observer can, and additionally can add, change and delete WDP-Users including their User passwords and can modify the User Configuration.
System-Configurator	This role is assigned to Console-Users who are higher privileged than a System-Controller. A System-Configurator can perform all actions a System-Controller can, and additionally can change the configuration of the system (i.e. add/change/delete Transmitters with their connected Source Systems, Receivers and smartTOUCH). Also, the System-Configurator can create, upload and download backups.
System-Administrator	This role is the highest-privileged role a Console-User can be assigned to. A System-Administrator can perform all actions a System-Configurator can, and additionally can add/change/delete Console-Users including their User passwords as well as configure the server settings and database in the TOE environment. The System-Administrator can also switch the WDP Control and restore Backups.
Device Admin	This role is assigned to users connecting to the TOE components via the Device GUI. As the Device GUI is out of scope for this certification, so is this user role. It is only listed for completeness sake.

1.4.3 Physical scope of the TOE

The WDP MX is a system consisting of different hardware components including the respective firmware and software components. The TOE also includes the respective guidance documents.

TOE component		Configurations	Version	Delivered Format	Description
Transmitter	IPR Tx	IP Remote II DP	HW: 24872TDP-MX, Revision V1 FW: 2.1.2	HW+FW	The IPR Tx (or Transmitter) consists of HW with respective firmware and connects customer Source System with the remaining TOE components. They are mounted in dedicated WEYTEC chassis, which have between 1 and 16 slots. Each Source System needs an IPR Tx. One TOE installation can contain hundreds of IPR Tx. All stated configurations are in scope of this evaluation and a single TOE can combine any mix of these configurations.
		IP Remote III 4K	HW: 24873T-MX, Revision V1 FW: 2.3.2	HW+FW	
		IP Remote IV	HW: 24874T-MX, Revision V1 FW: 2.2.2	HW+FW	
	IPR USB Tx	IP Remote USB II SFP Transmitter	HW: 24877T-MX, Revision V1 FW: 2.0.1	HW+FW	The IPR USB Tx (or Transmitter) consists of HW with respective firmware and connects customer Source Systems with the remaining TOE components. They are mounted in dedicated WEYTEC chassis, which have between 1 and 16 slots. Source System can be connected to an IPR USB Tx. One TOE installation can contain multiple devices. All stated configurations are

TOE component		Configurations	Version	Delivered Format	Description
					in scope of this evaluation and a single TOE can combine any mix of these configurations.
Receiver	IPR Rx	IP Remote II DP	HW: 24872RDP-MX, Revision V1 FW: :2.1.2	HW+FW	The IPR Rx (or Receiver) consists of HW with respective firmware and provides the interface of the TOE to user workstations (i.e. Monitors, Input devices) and are like the counterparts of the IPR Tx. Like the IPR Tx they are mounted in a WEYTEC chassis next to the WDP-User workspaces. One TOE installation can contain hundreds of IPR Rx. All stated configurations are in scope of this evaluation and a single TOE can combine any mix of these configurations.
		IP Remote III 4K	HW: 24873R-MX, Revision V1 FW: 2.3.2	HW+FW	
		IP Remote IV	HW: 24874R-MX, Revision V1 FW: 2.2.2	HW+FW	
	IPR Rx smartUX	IP Remote III 4K smartUX	HW: 24873RUX-MX, Revision V1 FW: 2.3.2	HW+FW	The IPR Rx smartUX is a specific configuration of the IPR Rx and offers additional functionality to control the workstation. This is comparable to smartTOUCH. The difference is that instead of a touch display, this content is visualized on an On Screen Display (OSD) on the connected monitor. Enabling or disabling the smartUX does not change the TOE functionality, but merely provides an additional interface for WDP-Users.
		IP Remote IV smartUX	HW: 24874RUX-MX, Revision V1 FW: 2.2.2	HW + FW	
	IPR USB Rx	IP Remote USB II SFP Receiver	HW: 24877R-MX, Revision V1 FW: 2.0.1	HW+FW	The IPR USB Rx (or Receiver) consists of HW with respective firmware and provides an interface of the TOE for user workstations (i.e. Input devices) and are like the counterparts of the IPR USB Tx. Like the IPR USB Tx they are mounted in a WEYTEC chassis next to the WDP-User workspaces. One TOE installation can contain multiple devices. All stated configurations are in scope of this evaluation and a single TOE can combine any mix of these configurations.
Control Application		interface enabled/disabled (25602)	1.4.1.10306	SW	The Control Application is the heart of the TOE controlling most operation including access control and user control. It interacts with all devices (IPR Tx, IPR Rx and smartTOUCH) and controls the state and operations. It can be accessed and managed from the Configuration Server via the EventStore and a direct connection. A TOE set-up consists of three WDP MX Server backend (for redundancy reasons) which are synchronized via the EventStores.
Configuration Server		25603	1.4.7.10373	SW	The Configuration Server provides the management interface for the TOE backend. It communicates with the Control Application via the EventStore. It is also connected to the (non-TOE) database. A TOE set-up consists of three WDP MX Server backend (for redundancy reasons) which are synchronized via the EventStores.
EventStore		25604	23.10.1.0	SW	The EventStore organizes the message flow in the backend, i.e. between Control Application and Configuration Server. A TOE set-up consists of three WDP MX Server backend (for redundancy reasons) which are synchronized by a proprietary logic.
smartTOUCH		smartTOUCH	HW: 22003BK-MX, Revision V1 FW: 2.2.2	HW+FW	A smartTOUCH is a user interface which replaces a complete workstation. It has a touch display and a keyboard (hardware keyboard on the smartTOUCH, virtual keyboard on the smartTOUCH Flex). Additional input devices like a mouse or keyboard can be connected to it. It can operate similar as a IPR Rx, i.e. exchanging data immediately with IPR Tx, or it can connect to the Control Application via the WEY Protocol.
		smartTOUCH Flex	HW: 22002-MX, Revision V1 FW: 2.2.2	HW+FW	

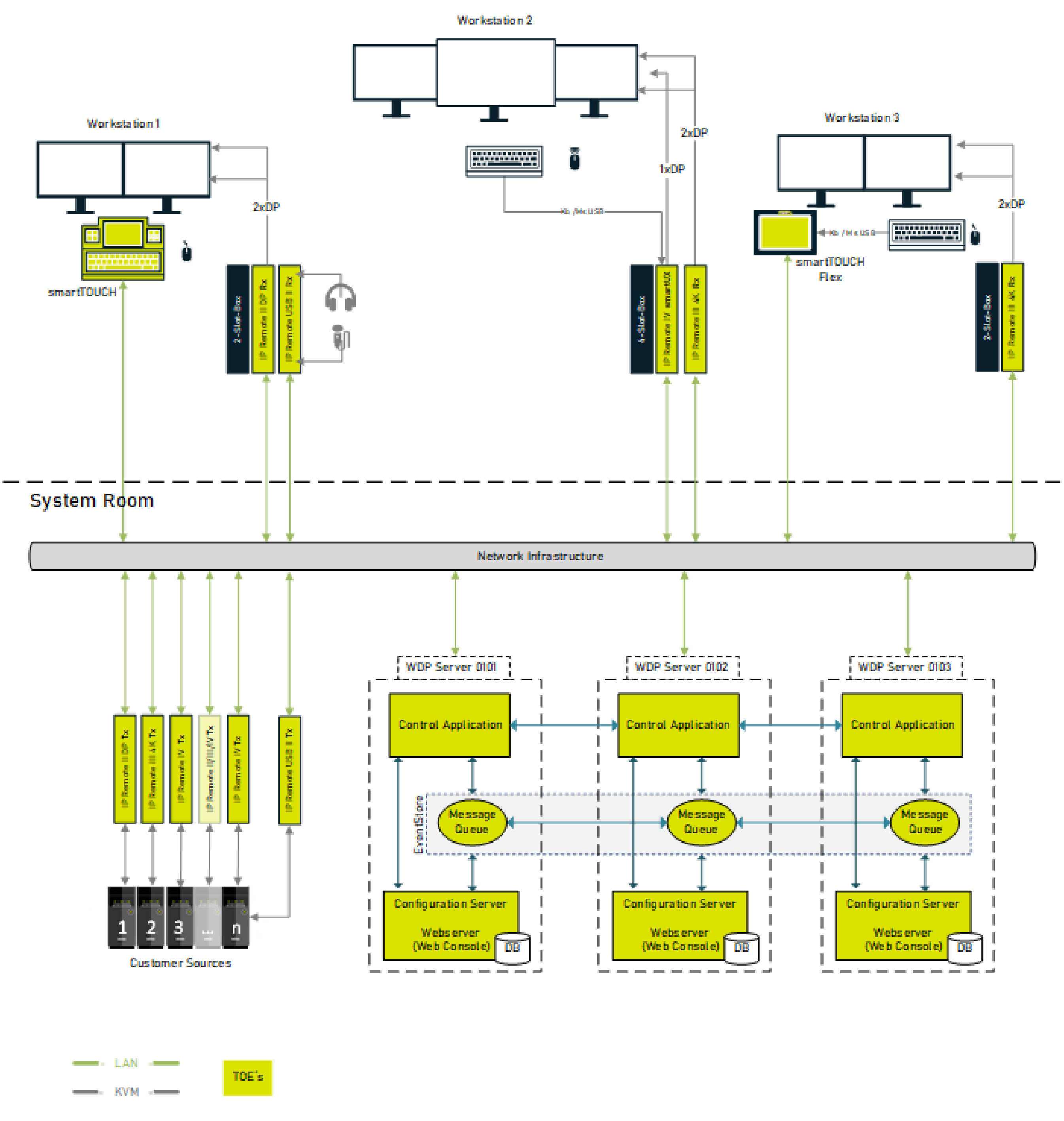
TOE component	Configurations	Version	Delivered Format	Description
Manual for IP Remote II DP (MX)	MAN24872DP-MX_E_CC.pdf	E25	Download	User guidance for the IPR Tx and IPR Rx, Configuration IP Remote II DP
Manual for IP Remote III 4k (MX)	MAN24873-MX_E_CC.pdf	E26	Download	User guidance for the IPR Tx and IPR Rx, Configuration IP Remote III 4k
Manual for IP Remote IV (MX)	MAN24874-MX_E_CC.pdf	E28	Download	User guidance for the IPR Tx and IPR Rx, Configuration IP Remote IV
Manual for IP Remote USB II SFP (MX)	MAN24877-MX_E_CC.pdf	E24	Download	User Guidance for the IPR USB Tx and IPR USB Rx Configuration IP Remote USB II SFP
Manual for WDP Configuration Server	MAN25603_E_1.4.1.pdf	E11.2	Download	User guidance for the Configuration Server
Manual for smartTOUCH	MAN22003BK-MX_E_CC.pdf	E10	Download	User guidance for the smartTOUCH
Manual for smartTOUCH Flex	MAN22002-MX_E_CC.pdf	E09	Download	User guidance for the smartTOUCH Flex
User Guidance Rest API	User_Guidance_Rest API.pdf	E04	Download	User guidance for the REST API of the Configuration Server
GUIDANCE DOCUMENTATION AGD_PRE	AGD_PRE-Dokument.pdf	E05	Download	Instructions for verification of the TOE
ANWENDUNGSHANDBUCH	Anwendungshandbuch WDP MX.pdf	E03	Download	Further guidance on how to use a complete WDP MX System
Notes on certified operation	Notes on certified operation.pdf	E06	Download	Additional remarks to be followed in a certified use

All HW and SW is being shipped to the customer together with essential non-TOE parts like the chassis, HW for the server cluster and the database. At customer side the TOE is set-up by WEYTEC field engineers or experts who have passed the same trainings (compare A.Set-Up). Once completely set-up and tested the TOE is handed over to the customer. All manuals are available electronically on a dedicated WEYTEC extranet[1] accessible by the customer.

The following graphic provides an exemplary visualization of a TOE set-up with a three WDP MX Servers as backend.

[1] All manuals can be downloaded from https://my.weytec.com by authorized customers

Workplaces


Workstation 2
Workstation 1
Workstation 3
2xDP
1xDP
2xDP
2xDP
Kb /Ms USB
Kb /Ms USB
smartTOUCH
smartTOUCH Flex
2-Slot-Box
IP Remote II DP Rx
IP Remote USB II Rx
4-Slot-Box
IP Remote IV smartUX
IP Remote III 4K Rx
2-Slot-Box
IP Remote III 4K Rx
System Room
Network Infrastructure
IP Remote II DP Tx
IP Remote III 4K Tx
IP Remote IV Tx
IP Remote II/III/IV Tx
IP Remote IV Tx
IP Remote USB II Tx
1
2
3
...
n
Customer Sources
WDP Server 0101
WDP Server 0102
WDP Server 0103
Control Application
Control Application
Control Application
EventStore
Message Queue
Message Queue
Message Queue
Configuration Server
Webserver (Web Console)
DB
Configuration Server
Webserver (Web Console)
DB
Configuration Server
Webserver (Web Console)
DB
LAN
KVM
TOE's

1.4.4 Logical scope of the TOE

The logical scope of the TOE includes the following features:

- User identification and authentication
  The WDP MX requires users to be identified and authenticated before allowing any security relevant operations. Different user types and roles are managed by different WDP MX components like Control Application, Configuration Server and Devices. The Configuration Server can be reached via a REST-API (Also called Web-console in this document).
- Access control for source systems, user data and TOE data
  The WDP MX implements different access control mechanisms which restrict operations to authenticated users in the correct role or with explicit permissions set to them. Therefore, the WDP MX protects especially all source systems as well as personal user data against unauthorized access.

The following features of the TOE are explicitly out of scope for this certification:

- Administration of a TOE device via its respective Device GUI
- Web Interface of the control application and configuration server
- Implementation of TLS channels
- Encryption within the WEYTEC protocol
- Direct Mode of the smartTOUCH and smartUX Receiver
- Login with “Default user”

2 Conformance Claim

2.1 CC Conformance Claim

This Security Target claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2022-11-001, Version CC:2022, Revision 1, November 2022 [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2022-11-002, Version CC:2022, Revision 1, November 2022 [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2022-11-003, Version CC:2022, Revision 1, November 2022 [3]
- Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements; CCMB-2022-11-005, Version CC:2022, Revision 1, November 2022 [6]

as follows:

- CC Part 2 conformant (all SFRs used in this Security Target are defined in [2]).
- CC Part 3 conformant (all SARs used in this Security Target are defined in [3]).

2.2 PP Claim

This Security Target does not claim conformance to any Protection Profile.

2.3 Package Claim

The Security Target claims to conformance to the SAR package **EAL2**.

3 Security Problem Definition

This section defined all assets, subjects, operations and security attributes which will further be used throughout this Security Target.

It also names the threats (T.xxx) which are being countered by the WDP MX as well as the security policies (P.xxx) implemented by the WDP MX. Finally, it lists the assumptions (A.xxx) made for the TOE environment.

3.1 Assets and Definitions

3.1.1 Assets

Asset	Description
User data	The user data is information on the WDP-Users and Console-Users including the username, actual name, role and user organization. The confidentiality of User data is protected by the TOE against unauthorized disclosure and modification.
User password	The user password is the password used by WDP-Users, Console-Users and Device Admins used to authenticate themselves against the TOE. The confidentiality and integrity of User passwords is protected by the TOE against unauthorized disclosure or modification.
User Configuration	The User Configuration contains mappings between WDP-Users, available Source System and allowed Resource-Use operations. The User Configuration also includes a setting for one WDP-User to be another WDP-Users substitute. The User Configuration is protected by the TOE against unauthorized disclosure and modification.
Device Configuration data	Device Configuration data is a configuration of Transmitters, Receivers, smartTOUCH devices and the WDP Control allowing to enable or disable the encryption between these subjects. The Device Configuration data is protected by the TOE against unauthorized disclosure and modification.

3.1.2 Subjects

Subject	Description
WDP-User	A WDP-User can log in to the TOE via smartTOUCH or via the IPR smartUX and can use all assigned resources of the WDP according to his user-profile. A WDP-User can also change his own User password. As there is only a single role this is also called WDP-user.
Console-User	A Console-User can log in to the TOE via the REST-API of the Configuration Server and can assume one of multiple roles (System-Administrator, System-Configurator, System-Controller, System-Observer or System-Reader). Console-Users can access system information or perform functional changes of the TOE defined by their role.
Device Admin	A Device Admin can log in to a Transmitter, Receiver or smartTOUCH via local access or remotely using the Device GUI and can manage the users on this device and set the Device Configuration data.
Transmitter	A Transmitter or Tx is a subsystem of the TOE which is physically attached to Source Systems and connected via network to the other parts of the TOE.

Subject	Description
Receiver	A Receiver or Rx is a subsystem of the TOE which is connected via network to the other parts of the TOE.
smartTOUCH	A smartTOUCH is a subsystem of the TOE which is connected via network to the other parts of the TOE. It consists of a Receiver combined with a screen and possibly a keyboard in a single Hardware.
WDP Control	The WDP Control is a subsystem of the TOE which is connected via network to the other parts of the TOE. It is part of the backend and runs on the server cluster.

3.1.3 Operations

Operation	Description
System-Read	A Console-User reads the list and usage of Source Systems, reads the list of User data and reads the User Configuration.
System-UserLogout	A Console-User logs-out a WDP-User.
System-Control	A Console-User adds, changes or deletes WDP-Users including their User passwords and modifies the User Configuration.
System-Configure	A Console-User changes the HW configuration of the system (i.e. add/change/delete Transmitters with their connected Source System, Receivers and smartTOUCH) as well as performs system SW updates and switches between WDP Control.
System-Administrate	A Console-User adds/changes/deletes Console-Users including their User passwords as well as configures the server settings and database in the TOE environment.
Resource-Use	A WDP-User (in role WDP-user) controls Source Systems and/or view data from Source System.
ChangePW	A WDP-User or Console-User changes the value of their own User password.

Security attributes

Security attribute	Attribute of	Description
Authenticated	WDP-User, Console-User	After successful authentication a WDP-User, Console-User or Device Admin will obtain the security attribute authenticated until logout.
Permission	WDP-User	A Permission is a security attribute of a WDP-User allowing him to perform Resource-Use which is stored and managed in the User Configuration. It can be set individually for single WDP-Users or for WDP-User groups.

3.2 Threats

T.Access_Control

An attacker gains access to the Web-Console of the TOE and reads or manipulates User Configuration, User password, User data or Device Configuration data.

T.Unauth

Attackers or WDP-Users without Permission are performing Resource-Use on Source Systems, therefore bypassing the access control rules defined in User Configuration.

3.3 Organisational Security Policies (OSPs)

P.Control_Room

The organisation using the TOE must ensure that users bring no external devices with network capabilities into the control room.

Additionally, the organisation must ensure that all network infrastructure components (i. e. switches) are located within the secure System Room.

P.Secure_Transmission

If TSF data is transmitted over insecure networks (e.g. between multiple sites of a TOE operator), the operator has to make sure appropriate and effective security measures (e.g. protection via a VPN connection) are taken to prevent modification and disclosure of the transferred TSF data.

P.Password_Policy

The administrators shall choose a password policy for WDP users which enforces strong passwords. The exact guidelines shall be chosen according to an internal risk assessment process.

3.4 Assumptions

A.Backend_Access

Access to the WDP MX servers is only granted to administrators.

A.Logical_Separation

The TOE is operated in a logically separated network and has no connection to other networks of the customer. This especially means that the Source Systems (other than the WDP MX Servers themselves) have no network connections to any TOE component.

A.Passwords

Users keep their User password secret and do not share it with other persons. Console-Users with access to other users' passwords do not share or misuse these passwords.

A.Physical

The System Room in which the server cluster hosting the TOE backend (Control Application, Configuration Server, EventStore) as well as the database used by the TOE is placed, is physically protected in a way that ensures only trustworthy personnel has physical access.

A.Set-Up

The TOE is set-up and initially configured only by WEYTEC field engineers or persons which have participated the same trainings conducted by WEYTEC or their affiliates. The WEYTEC-Installer is being used to set-up the cluster for the TOE backend and the database. The TOE is set-up and connected as a WDP cluster ("WDP Verbund").

A.Trusted_Admins

Administrators (acting in the role System-Administrator) and especially users accessing the TOE via a Device GUI (therefore acting as a user in the role Device Admin) are trusted and only perform actions which do not hinder the TSF in any way.

4 Security Objectives

This chapter contains the security objectives (O.xxx) implemented by the TOE and derived from the threats and policies of the previous chapter.

It also contains the security objectives for the TOE environment (OE.xxx) which need to be fulfilled by the environment for a secure TOE operation.

Finally, it contains the Security Objectives rationale, providing a mapping and explanatory text between the previous chapter and this one.

4.1 Security Objectives for the TOE

O.Access_Control The TOE shall implement different access control mechanisms (WDP access control policy) which restrict operations to authenticated users in the correct role or with explicit permissions set to them. Therefore, the WDP MX shall protect especially all source systems as well as personal user data against unauthorized access.

O.Authenticate The TOE shall require all users to be identified and authenticated before allowing any security relevant operations. Different user types, roles and operations shall be managed by different TOE components like Control Application, Configuration Server and Devices.

4.2 Security Objectives for the Environment

OE.Control_Room The organisation using the TOE shall ensure that users bring no external devices with network capabilities into the control room.

Additionally, the organisation shall ensure that all network infrastructure components (i. e. switches) are located within the secure System Room.

OE.Logical_Separation The TOE shall be operated in a logically separated network and must have no connection to other networks of the customer. This especially means that the Source Systems (other than the WDP MX Servers themselves) shall have no network connections to any TOE component.

OE.Passwords WDP-Users, Console-Users and Device Admins keep their User password secret and do not share it with other persons. Console-Users with access to other users' passwords do not share or misuse these passwords.

OE.Physical The server cluster hosting the TOE backend (Control Application, Configuration Server, EventStore) as well as the database used by the TOE shall be physically protected in a secure environment. Only trustworthy personnel shall have physical access to the secure environment.

OE.Secure_Transmission If TSF data is transmitted over insecure networks (e.g. between multiple sites of a TOE operator), the operator shall provide appropriate and effective security measures (e.g. protection via a VPN connection) to prevent modification and disclosure of the transferred TSF data.

OE.Set-Up The TOE is being set-up and initially configured only by WEYTEC field engineers or persons which have participated the same trainings conducted by WEYTEC or their affiliates. The WEYTEC-Installer is being used to set-up the cluster for the TOE backend and the database. The TOE shall be set-up and connected as a WDP cluster ("WDP Verbund"). The initial setup shall make sure that only administrators can access the WDP MX servers.

OE.Trusted_Admins	Administrators (acting in the role System-Administrator) and especially users accessing the TOE via a Device GUI (therefore acting as a user in the role Device Admin) shall be trusted and only perform actions which do not hinder the TSF in any way. The administrators also choose a password policy for WDP users which enforces adequately strong passwords in the context of the organisation’s TOE usage.

4.3 Security Objective Rationale

The following mapping provides the relationship between the threats, policies and assumptions from chapter 3 and the objectives for the TOE and the environment in this chapter. The mapping will be further explained below.

	O.Access_Control	O.Authenticate	OE.Control_Room	OE.Logical_Separation	OE.Passwords	OE.Physical	OE.Secure_Transmission	OE.Set-Up	OE.Trusted_Admins
T.Access_Control	X	X	X		X	X			
T.Unauth	X	X	X		X		X		
P.Control_Room			X						
P.Secure_Transmission							X		
P.Password_Policy									X
A.Backend_Access								X	X
A.Logical_Separation				X					
A.Passwords					X				
A.Physical						X			
A.Set-Up								X	
A.Trusted_Admins									X

Mappings between OSP/assumptions and security objectives for the operational environment, which do not have their own subchapter below this, are simple 1-to-1 mappings and are self-explanatory.

4.3.1 T.Access_Control

OE.Physical prevents any physical access to the TOE thereby eliminating any physical attacks. OE.Control_Room further restricts the attack surface within the control room. O.Authenticate and O.Access_Control require any user to be authenticated before any TSF related action is allowed and also establish an access control between controlled subjects, objects and operations, thereby preventing attackers from accessing the threatened assets via the interfaces offered by the TOE. OE.Passwords ensures that users do not give their authentication data to other users.

4.3.2 T.Unauth

OE.Control_Room restricts the attack surface within the control room. O.Authenticate and O.Access_Control require any user to be authenticated before any TSF related action is allowed and also establish an access control between controlled subjects, objects and operations. This is further supported by OE.Secure_Transmission which prevents disclosure of data shared between parts of the TOE exposed to potentially untrusted environments. OE.Passwords ensures that users do not give their authentication data to other users.

4.3.3 P.Password_Policy

OE.Trusted_Admins requires administrators to choose a password policy for WDP users which enforces adequately strong password. How strong such a guideline has to be is dependent on the security context in which the TOE is used and thereby up to the administrators.

4.3.4 A.Backend_Access

A.Backend_Access requires the TOE and its environment, especially the WDP MX servers, to be set up in a way that only administrators can access the WDP MX servers. In the initial setup this is ensured by OE.Set-Up. OE.Trusted_Admins further ensures that administrators don’t give access to the WDP MX servers to non-administrative users.

5 Extended Components Definitions

This ST does not define any extended components.

6 Security Requirements

6.1 Security Functional Requirements (SFRs)

This section contains the SFRs, arranged into subsections based on security functionality.

Operations on the SFRs are highlighted as follows

- Assignments are <u>underlined</u>
- Selections are *italic*
- Refinements are **bold**
- Iterations are marked with a unique identifier added to the Component ID

Furthermore, the original text from CC Part 2 is given in footnotes.

6.1.1 User Authentication and Management

FIA_UID.2 **User identification before any action**

Hierarchical to: FIA_UID.1 Timing of identification

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.

FIA_UAU.2 **User authentication before any action**

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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.

FMT_SMR.1 **Security roles**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles <u>WDP-user, System-Administrator, System-Configurator, System-Controller, System-Observer, and System-Reader</u>[2].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

ST application note 1: The role WDP-user is assigned to any user that logs into the TOE via smartTOUCH or smartUX. The roles System-Administrator, System-Configurator, System-Controller, System-Observer and System-Reader are assigned to users that are Console-Users.

[2] [assignment: the authorised identified roles]

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: System-Control, System-Configure, System-Administrate[3].

6.1.2 Access Control

FDP_ACC.1 **Subset access control**

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the WDP access control policy[4] on the subjects WDP-User and Console-User, the objects Source System, User data, User Configuration, Device Configuration data, User password and the operations Resource-Use, System-Read, System-UserLogout, System-Control, System-Configure, System-Administrate[5].

FDP_ACF.1 **Security attribute based access control**

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the WDP access control policy[6] to objects based on the following: the subject WDP-User with security attributes Authenticated and Permission, the subject Console-Users with security attributes Authenticated and the objects Source System, User data, User Configuration, Device Configuration data, User password[7].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- WDP-Users, who are Authenticated, can perform Resource-Use on Source Systems based on Permissions set in the User Configuration.
- WDP-Users, who are Authenticated, can perform ChangePW on their own User password.
- Console-Users, who are Authenticated, can perform ChangePW on their own User password
- Console-Users, who are Authenticated and in the role System-Reader, can perform System-Read.
- Console-Users, who are Authenticated and in the role System-Observer, can perform System-Read and System-UserLogout.

[3] [assignment: list of management functions to be provided by the TSF]
[4] [assignment: access control SFP]
[5] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[6] [assignment: access control SFP]
[7] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

- Console-Users, who are Authenticated and in the role System-Controller, can perform System-Read, System-UserLogout and System-Control.
- Console-Users, who are Authenticated and in the role System-Configurator, can perform System-Read, System-UserLogout, System-Control and System-Configure.
- Console-Users, who are Authenticated and in the role System-Administrator, can perform System-Read, System-UserLogout, System-Control, System-Configure and System-Administrate[8].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[9].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[10].

ST application note 2: The rules defined in element FDP_ACF.1.2 only describe who is allowed to perform actions. It does not make any statement regarding the functionality of the functions themselves.

FMT_MSA.3/ACC Static attribute initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the WDP access control policy[11] to provide *restrictive*[12] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the System-Controller, System-Configurator and System-Administrator[13] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.1/ACC Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the WDP access control policy[14] to restrict the ability to *modify, delete*[15] the security attributes Permission[16] to System-Controller, System-Configurator, System-Administrator[17].

[8] [assignment: rules governing access among
controlled subjects and controlled objects using controlled operations on controlled objects]
[9] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[10] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[11] [assignment: access control SFP, information flow control SFP]
[12] [selection, choose one of: restrictive, permissive, [assignment: other property]]
[13] [assignment: the authorised identified roles]
[14] [assignment: access control SFP(s), information flow control SFP(s)]
[15] [selection: change_default, query, modify, delete, [assignment: other operations]]
[16] [assignment: list of security attributes]
[17] [assignment: the authorised identified roles]

6.2 Security Assurance Requirements (SARs)

This Security Target claims conformance with **EAL2** as defined by CC Part 3 [3].

The relevant SARs are

- Security Target evaluation
  - ASE_INT.1
  - ASE_CCL.1
  - ASE_SPD.1
  - ASE_OBJ.2
  - ASE_ECD.1
  - ASE_REQ.2
  - ASE_TSS.1
- Guidance documents
  - AGD_OPE.1
  - AGD_PRE.1
- Development
  - ADV_ARC.1
  - ADV_FSP.2
  - ADV_TDS.1
- Life-cycle support
  - ALC_CMC.2
  - ALC_CMS.2
  - ALC_DEL.1
- Tests
  - ATE_COV.1
  - ATE_FUN.1
  - ATE_IND.2
- Vulnerability assessment
  - AVA_VAN.2

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

The following table shows all SFRs of this Security Target, their dependencies as defined in CC Part 2 [2] and the components which fulfill this requirement. For the not fulfilled dependencies a rationale is given below the table.

Component in ST	Dependencies	Fulfilled by
FIA_UID.2	No dependencies	n/a
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FMT_SMF.1	No dependencies	n/a
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3/ACC
FMT_MSA.3/ACC	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/ACC FMT_SMR.1
FMT_MSA.1/ACC	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1

The mapping below shows the relationship between the Security Objectives for the TOE (as in section 4.1) and the SFRs from section 6.1. Further explanations are provided below the table.

	FIA_UID.2	FIA_UAU.2	FMT_SMR.1	FMT_SMF.1	FDP_ACC.1	FDP_ACF.1	FMT_MSA.3/ACC	FMT_MSA.1/ACC
O.Authenticate	X	X	X	X				
O.Access_Control					X	X	X	X

O.Authenticate requires all users to be identified and authenticated before allowing any security relevant operations and to manage different user types, roles and operations. The identification and authentication is modelled in FIA_UID.2 and FIA_UAU.2 respectively. The roles can be found in FMT_SMR.1 and the management operations in FMT_SMF.1.

O.Access_Control requires different access control mechanisms to be implemented, especially protecting all source systems as well as personal user data against unauthorized access. This is immediately modelled in the WDP access control policy modelled in FDP_ACC.1 and FDP_ACF.1. The respective managing of the related security attributes and their default values are handled in FMT_MSA.1/ACC and FMT_MSA.3/ACC.

6.3.2 Security Assurance Requirements Rationale

As the predefined package EAL 2 without augmentations was chosen all dependencies are implicitly fulfilled.

This package has been chosen to demonstrate resistance against attacks with basic attack potential.

7 TOE Summary Specification

The SFRs of the TOE are implemented in three different security mechanisms, which are further described in the following subsections.

7.1 SM.1 User identification and authentication

The WDP MX requires users to be identified and authenticated before allowing any security relevant operations (FIA_UID.2 and FIA_UAU.2). Users are then associated with roles (FMT_SMR.1). This is implemented in three different TOE components. Management functions are available to some roles (FMT_SMF.1).

- WDP-Users can log in with username and password via a smartTOUCH / smartUX, a workstation connected to a Receiver. WDP-Users are always associated with the role WDP-user.
- Console-Users can log in with username and password via the Web-Console of the Configuration Server. They can be associated with one of the roles System-Reader, System-Observer, System-Controller, System-Configurator and System-Administrator. Depending on the role they can have access to one or more of the management functions System-Control, System-Configure or System-Administrate.

7.2 SM.2 Logical access control for source systems, user data and TOE data

The WDP MX implements different access control mechanisms following the WDP access control policy (FDP_ACC.1, FDP_ACF.1) which restrict operations to authenticated users in the correct role or with explicit permissions set to them. Therefore, the WDP MX protects especially all source systems as well as personal user data against unauthorized access.

- For authenticated WDP-Users the rights to perform Resource-Use on Source Systems is based on Permissions set in the User Configuration of the WDP Control. These can be managed by Console-Users performing the operation System-Control (FMT_MSA.1/ACC). The rights can be either set for user individually or for groups to which users can be assigned. By default, WDP-Users do not have any access to any Source System, this default cannot be changed (FMT_MSA.3/ACC). WDP-Users can also perform ChangePW on their own User password.
- For Console-Users the rights to perform the operations Resource-Use, System-Read, System-UserLogout, System-Control, System-Configure, System-Administrate and therefore to operate with the objects Source System, User data, User Configuration and User password is based on the role and authentication status of the Console-User. No further management of security attribute (Authenticated) is implemented. Console-Users can also perform ChangePW on their own User password

8 Glossary

Item	Description
Control Room	The control room is where the users of the WDP MX operate. It's where the smartTOUCH devices and receivers are located.
Device GUI	Local Administrators can access and configure the TOE HW devices (Transmitter, Receivers and SmartTouch) via an application called Device GUI which is installed on an external computer. This Device GUI as well as the interface it connects to, are out-of-scope for this certification.
Source System	Source systems are machines and resources like cameras under control of the user organization. They are attached to the TOE via Transmitters (Tx) and can be accessed by WDP-User based on the Permissions set in the User Configuration.
System Room	The system room is where the backend components of the TOE are installed. Note: This does not necessarily need to be one single room, but includes the complete installation of all backend components. The system room needs to be physically protected from unauthorized access.

Web Console	The web console is the REST-API of the Configuration Server, as used by Console-Users.

9 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version CC2022, Revision 1, November 2022, CCMB-2022-11-001

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version CC2022, Revision 1, November 2022, CCMB-2022-11-002

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version CC2022, Revision 1, November 2022, CCMB-2022-11-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version CC2022, Revision 1, November 2022, CCMB-2022-11-006

[5] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, Version CC2022, Revision 1, November 2022, CCMB-2022-11-004

[6] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, Version CC2022, Revision 1, November 2022, CCMB-2022-11-005

10 Annex A - Hash values for Guidance documentation

Document	SHA-256 value
Manual for IP Remote II DP (MX)	ba6a993a1581ade096c27c008ab9779d1b74387b28331d551f56389bf5ed00b0
Manual for IP Remote III 4k (MX)	63f91fc43717c4b7544efc2e23cde68d7cbe21f5a44b4bd620d05cbe909c5d90
Manual for IP Remote IV (MX)	ddae938a0ee9c5cc320751db6ff9802a6d644101d4905bdea88c009b51aaa0d6
Manual for IP Remote USB II SFP (MX)	f32bb52f5ceb7d90f4ecac2cea95013c57375b867f52257694ecc2ba7b65dd1f
Manual for WDP Configuration Server	cd4e3fe0ccc41a2374ea96687c5e522c9473ace16418a6086826316fc7049df2
Manual for smartTOUCH	54b1c8aa92c7eabef2ad2ef8c8a9ef7e652fa8184bd09258b33aa2af7642f973
Manual for smartTOUCH Flex	69aa1e6f5c7aca394118b8879b6a6fdcbcac3ac241992a50b53c23661dfbe56a
User Guidance Rest API	27c18769de9967f6a5b7e9381ce0c0f213db386277a49f1f3bacb71d82b001d9
GUIDANCE DOCUMENTATION AGD_PRE	6c590233f1c6096eff963b66791e2c6029fab55c8192c4cbaea29bd56fce80cc
ANWENDUNGSHANDBUCH	ce55dcbfd001d32dc4b1f96aa3443f09051b21b80ebf8dce32d64c8b41a6f8e3
Notes on certified operation	4666224c669a40fa5efcb530a9d02d1e97834a8656826843f1803db45e428caf