Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1253-2025

for

WEYTEC distributionPLATFORM (WDP MX) Version 1.4.1

from

WEY Group AG

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1253-2025 (*)

KVM (keyboard, video, mouse) solution

WEYTEC distributionPLATFORM (WDP MX)
Version 1.4.1

from	WEY Group AG
PP Conformance:	None.
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 2
valid until:	27 July 2030

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), CEM:2022 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), CC:2022. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement

Bonn, 28 July 2025

For the Federal Office for Information Security

Sandro Amendola
Director-General

L.S.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licensing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), CC:2022 [4] [1] also published as ISO/IEC 15408

1 Act on the Federal Office for Information Security (BSI-Gesetz – BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

2 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung – BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

3 BMI Regulations on Ex-parte Costs – Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) – dated 2 September 2019, Bundesgesetzblatt I p. 1365

- Common Methodology for IT Security Evaluation (CEM), CC:2022 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates – as far as such certificates are based on ITSEC or CC – under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under CCRA-2014 for all assurance components selected.

[4] Proclamation of the Bundesamtes für Sicherheit in der Informationstechnik vom 14. April 2023 auf https://www.bsi.bund.de

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product WEYTEC distributionPLATFORM (WDP MX), Version 1.4.1 has undergone the certification procedure at BSI. Thereby, WDP MX is the short form of the full product name WEYTEC distributionPLATFORM.

The evaluation of the product WEYTEC distributionPLATFORM (WDP MX), Version 1.4.1 was conducted by secuvera. The evaluation was completed on 25 June 2025. secuvera is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: WEY Group AG.

The product was developed by: WEY Group AG.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the evaluated guidance documentation, are observed,
- the product is operated in the environment as specified and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis. Therefore the BSI reserves the right to revoke the certificate, especially if a exploitable vulnerability of the certified product gets to known.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 28 July 2025 is valid until 27 July 2030. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

[5] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product WEYTEC distributionPLATFORM (WDP MX), Version 1.4.1 has been included in the BSI list of certified products, which is published regularly in the listing found at the BSI Website https://www.bsi.bund.de/dok/Zertifizierung-Gesamtlisten. Further information can be obtained from BSI-Infoline +49 (0)228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] WEY Group AG
Dorfstrasse 57
CH-8103 Unterengstringen
Schweiz

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The TOE is the WEYTEC distributionPLATFORM developed by WEY Group AG. 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 across multiple sites.

The Security Target [5] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [5], chapter 6.1. They are all selected from Common Criteria Part 2. Thus the claimed set of SFRs in the ST is CC Part 2 conformant.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
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).
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.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [5], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [5], chapter 3.1.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [5], chapter 3.2 - 3.4.

This certification covers the configurations of the TOE as outlined in chapter 8.

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

WEYTEC distributionPLATFORM (WDP MX), Version 1.4.1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/ SW	IPR Tx, IP Remote II DP	HW: 24872TDP-MX, Revision V1 FW: 2.1.2	delivered pre-configured by WEYTEC
2	HW/ SW	IPR Tx, IP Remote III 4K	HW: 24873T-MX, Revision V1 FW: 2.3.2	delivered pre-configured by WEYTEC
3	HW/ SW	IPR Tx, IP Remote IV	HW: 24874T-MX, Revision V1 FW: 2.2.2	delivered pre-configured by WEYTEC
4	HW/ SW	IPR USB Tx, IP Remote USB II SFP Transmitter	HW: 24877T-MX, Revision V1 FW: 2.0.1	delivered pre-configured by WEYTEC
5	HW/ SW	IPR Rx, IP Remote II DP	HW: 24872RDP-MX, Revision V1 FW: 2.1.2	delivered pre-configured by WEYTEC
6	HW/ SW	IPR Rx, IP Remote III 4K	HW: 24873R-MX, Revision V1 FW: 2.3.2	delivered pre-configured by WEYTEC
7	HW/ SW	IPR Rx, IP Remote IV	HW: 24874R-MX, Revision V1 FW: 2.2.2	delivered pre-configured by WEYTEC
8	HW/ SW	IPR Rx smartUX, IP Remote III 4K smartUX	HW: 24873RUX-MX, Revision V1 FW: 2.3.2	delivered pre-configured by WEYTEC
9	HW/ SW	IPR Rx smartUX, IP Remote IV smartUX	HW: 24874RUX-MX, Revision V1 FW: 2.2.2	delivered pre-configured by WEYTEC
10	HW/ SW	IPR USB Rx, IP Remote USB II SFP Receiver	HW: 24877R-MX, Revision V1 FW: 2.0.1	delivered pre-configured by WEYTEC
11	SW	Control Application	1.4.1.10306	delivered pre-configured by WEYTEC
12	SW	Configuration Server	1.4.7.10373	delivered pre-configured by WEYTEC
13	SW	EventStore	23.10.1.0	delivered pre-configured by WEYTEC
14	HW/ SW	smartTOUCH	HW: 22003BK-MX, Revision V1 FW: 2.2.2	delivered pre-configured by WEYTEC

No	Type	Identifier	Release	Form of Delivery
15	HW/ SW	smartTOUCH Flex	HW: 22002-MX, Revision V1 FW: 2.2.2	delivered pre-configured by WEYTEC
16	DOC	Manual for IP Remote II DP (MX), MAN24872DP-MX_E_CC.pdf, Part No. 24872xxxx-MX, [7]	E25 SHA256: ba6a993a1581ade096c27c008ab9779d1b74387b28331d551f56389bf5ed00b0	PDF download
17	DOC	Manual for IP Remote III 4k (MX), MAN24873-MX_E_CC.pdf, Part No. 24873xxxx-MX, [8]	E26 SHA256: 63f91fc43717c4b7544efc2e23cde68d7cbe21f5a44b4bd620d05cbe909c5d90	PDF download
18	DOC	Manual for IP Remote IV (MX), MAN24874-MX_E_CC.pdf, Part No. 24874xxxx-MX, [9]	E28 SHA256: ddae938a0ee9c5cc320751db6ff9802a6d644101d4905bdea88c009b51aaa0d6	PDF download
19	DOC	Manual for IP Remote USB II SFP (MX), MAN24877-MX_E_CC.pdf, Part No. 24877T-MX / 24877R-MX, [10]	E24 SHA256: f32bb52f5ceb7d90f4ecac2cea95013c57375b867f52257694ecc2ba7b65dd1f	PDF download
20	DOC	Manual for WDP Configuration Server, MAN25603_E_1.4.1.pdf, Part No. 25603, [11]	E11.2 SHA256: cd4e3fe0ccc41a2374ea96687c5e522c9473ace16418a6086826316fc7049df2	PDF download
21	DOC	Manual for smartTOUCH, MAN22003BK-MX_E_CC.pdf, Part No. 22003BK-MX, [12]	E10 SHA256: 54b1c8aa92c7eabef2ad2ef8c8a9ef7e652fa8184bd09258b33aa2af7642f973	PDF download
22	DOC	Manual for smartTOUCH Flex, MAN22002-MX_E_CC.pdf, Part No. 22002-MX, [13]	E09 SHA256: 69aa1e6f5c7aca394118b8879b6a6fdcbcac3ac241992a50b53c23661dfbe56a	PDF download

No	Type	Identifier	Release	Form of Delivery
23	DOC	User Guidance Rest API, User_Guidance_Rest API.pdf, [14]	E04 SHA256: 27c18769de9967f6a5b7e9381ce0c0f213db386277a49f1f3bacb71d82b001d9	PDF download
24	DOC	GUIDANCE DOCUMENTATION, AGD_PRE, AGD_PRE-Dokument.pdf, [15]	E05 SHA256: 6c590233f1c6096eff963b66791e2c6029fab55c8192c4cbaea29bd56fce80cc	PDF download
25	DOC	ANWENDUNGSHANDBUCH, Anwendungshandbuch WDP MX.pdf, [16]	E03 SHA256: ce55dcbfd001d32dc4b1f96aa3443f09051b21b80ebf8dce32d64c8b41a6f8e3	PDF download
26	DOC	Notes on certified operation, Notes on certified operation.pdf, [17]	E06 SHA256: 4666224c669a40fa5efcb530a9d02d1e97834a8656826843f1803db45e428caf	PDF download

Table 2: Deliverables of the TOE

The TOE is produced at the WEYTEC headquarters in Unterengstringen, Switzerland.

If a customer out of Switzerland orders the TOE, the TOE will be shipped first to the local WEYTEC entity. Afterwards the TOE will be assembled, installed and configured. If a customer in Switzerland orders the TOE, the TOE will directly be assembled, installed and configured in Unterengstringen.

After the assembling, installation and configuration a factory acceptance test is performed. If the factory acceptance test is passed, the system will be disassembled and shipped to the customer.

The system will be assembled again at the customers' site by WEYTEC technicians or persons who have participated the required training conducted by WEYTEC or their affiliates. Afterwards a site acceptance test is performed with the customer. If the site acceptance test is passed, the TOE is handed over to the customer. During the acceptance test an acceptance protocol is written.

During the whole process parcels are sent with DHL, pallets with destinations within Europe with DSV and with destinations outside of Europe with Kühne & Nagel.

The manuals are published on the developer's web page protected via TLS1.2 and TLS1.3 on the WEYTEC platform https://my.WEYTEC.com.

The developer describes in chapter 2.4 "How to get Firmware edition of hardware components" and 2.5 "How to get the version numbers of the WDP MX software components" of the "GUIDANCE DOCUMENTATION AGD_PRE" [15] how to identify the version numbers of the TOE components.

Furthermore, the user is able to verify the authenticity of the manuals with SHA256 checksums written in in the Security Target [5] in “Annex A - Hash values for Guidance documentation” and in Table 2 above.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. The Security Functional Requirements are described in the Security Target [5], chapter 6.1.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The objectives which have to be met by the the environment are described in the Security Target [5], chapter 4.2.

5. Architectural Information

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.

WDP MX in version 1.4.1 consists of the different, uniquely identifiable components as mentioned in table 2.

Some TOE components are operated in the frontend (IPR Tx, IPR Rx, smartTOUCH). A single TOE usually contains multiple 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.

For details please read chapter 1.4.3 and 1.4.4 of the Security Target [5].

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

The TOE configuration consists of the components as listed in table 2.

The following non-TOE components are required:

- Network Switches.

- Source Systems, i.e. machines and resources like cameras under control of the user organization.
- 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 the WDP MX Servers.

The developer performed functional tests of the TOE focusing on the functionality and usability of TOE while covering various TSFIs of the TOE. The expected results of the developer tests are well defined and cover the specific areas specified for each test. All actual test results are as expected by the developer.

The Independent Evaluator Tests were performed in the ITSEF using the TOE in version 1.4.1 in a logically and physically separated network within the laboratory of the ITSEF. The TOE in this network was accessible via the TOE receiver and smartTOUCH components. The TOE was delivered by a WEYTEC technician to the ITSEF and assembled in a separate network in the laboratory of the ITSEF. The assembling was attended by a member of the ITSEF the whole time. Afterwards a site acceptance test was performed to check the TOE components and to explain the functionalities of the TOE to the ITSEF. To verify the test results of the developer, a sampling strategy was used in which the test objectives of the developer tests were analysed. During the performed tests all claimed SFRs written in the Security Target were tested. The test results have not shown any deviations between the expected test results and the actual test results.

The evaluator has done an independent vulnerability analysis. As a result additionally vulnerability tests have been designed. The penetrations test configuration correlates with the TOE configuration described in the Security Target. If all operational measures required by the developer are applied, no attack scenario with basic attack potential was actually successful in the TOE’s operational environment as defined in the ST.

8. Evaluated Configuration

This certification covers the configurations of the TOE as described in the previous chapter 7 and in chapter 1.4.3 and 1.4.4 of the Security Target [5]. The TOE consists of the components listed in the configuration list in chapter 2 of [18] and of the component versions as listed in table 2 above.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [6] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 2 package including the class ASE as defined in the CC (see also part C of this report)

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target
  Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
  EAL 2

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The TOE does not include cryptographic mechanisms. Thus, no such mechanisms were part of the assessment.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

As described in the Security Target [5] in Chapter 1.4.4 “Logical scope of the TOE” 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”.

There should be regularly performed inspections of the TOE configuration. During those inspections also the user, profile and group access rights should be examined.

11. Security Target

For the purpose of publishing, the Security Target [5] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None.

13. Definitions

13.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FW	Firmware
HW	Hardware
IP	Internet Protocol
IPR	IP Remote
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MX	Multiplexer
PP	Protection Profile
Rx	Receiver
SAR	Security Assurance Requirement
SFP	Small Form-factor Pluggable
SFR	Security Functional Requirement
ST	Security Target
SW	Software
TLS	Transport Layer Security
TOE	Target of Evaluation

TSF	TOE Security Functionality
Tx	Transmitter
USB	Universal Serial Bus
WDP	WEYTEC distributionPLATFORM

13.2. Glossary

Augmentation – The addition of one or more requirement(s) to a package.

Collaborative Protection Profile – A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension – The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal – Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal – Expressed in natural language.

Object – A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package – named set of either security functional or security assurance requirements

Protection Profile – A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target – An implementation-dependent statement of security needs for a specific identified TOE.

Subject – An active entity in the TOE that performs operations on objects.

Target of Evaluation – An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality – Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation/CC
ISO-Version:
ISO 15408:2022, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements
https://www.iso.org/standard/72891.html
https://www.iso.org/standard/72892.html
https://www.iso.org/standard/72906.html
https://www.iso.org/standard/72913.html
https://www.iso.org/standard/72917.html
CCRA-Version:

CC:2022 R1, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirement
https://www.commoncriteriaportal.org

[2] Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology
ISO-Version:
ISO 18045:2022: Information technology Security techniques Methodology for IT security evaluation
https://www.iso.org/standard/72889.html
CCRA-Version:
CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
https://www.commoncriteriaportal

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licensing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7]
https://www.bsi.bund.de/AIS

[5] SECURITY TARGET WDP MX, BSI-DSZ-CC-1253, Version E09, 13.06.2025, WEY Group AG

[6] Evaluation Technical Report - SUMMARY for WEYTEC distributionPLATFORM, BSI-DSZ-CC-1253, Version: 2, Date: 24.06.2025, secuvera GmbH (confidential document)

[7] Manual for IP Remote II DP, Part No. 24872xxxx-MX, Version: E25, Date: 30.10.2024, WEY Group AG

[8] Manual for IP Remote III 4K, Part No. 24873xxxx-MX, Version: E26, Date: 13.03.2025, WEY Group AG

[9] Manual for IP Remote IV, Part No. 24874xxxx-MX, Version: E28, Date: 13.03.2025, WEY Group AG

[10] Manual for IP Remote USB II SFP, Part No. 24877T-MX / 24877R-MX, Version: E24, Date: 23.05.2024, WEY Group AG

[11] MANUAL FOR WDP CONFIGURATION SERVER, Part No. 25603, Version: E11.2, Date: 09.05.2025, WEY Group AG

[12] Manual for smartTOUCH, Part No. 22003BK-MX, Version: E10, Date: 27.02.2025, WEY Group AG

[13] Manual for smartTOUCH Flex, Part No. 22002-MX, Version: E09, Date: 21.02.2025, WEY Group AG

[7] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

[14] User Guidance Rest API, Version: E04, Date: 21.03.2025, WEY Group AG

[15] GUIDANCE DOCUMENTATION AGD_PRE, Version: E05, Date: 21.03.2025, WEY Group AG

[16] ANWENDUNGSHANDBUCH, Version: E03, Datum 10.04.2025, WEY Group AG

[17] Notes on certified operation, Version, E06, Date: 20.05.2025, WEY Group AG

[18] Configuration list for the TOE: LIFECYCLE DOCUMENTATION, Version: E08, Date: 13.06.2025, WEY Group AG (confidential document)

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria in its CCRA Documents can be followed:

- On conformance claim definitions and descriptions refer to CC:2022 part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC:2022 Part 3 chapter 6.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CCRA CC:2022 Part 5.
- On the assurance class ASE for Security Target evaluation refer to CC:2022 Part 3 chapter 9
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC:2022 Part 3 chapters 7 to 15
- The table 1 in CC:2022 part 5, Chapter 4.2 summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published as the CCRA Version at
https://www.commoncriteriaportal.org/cc/index.cfm

The CC are published as the ISO/IEC Version at
https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report