Agenzia per la Cybersicurezza Nazionale

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti ISO/IEC 15408 Common Criteria (CC) CC:2022 Release 1

Certificato n. *(Certificate No.)*	10/2026
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/CCL/05/2025/RC, v1.0
Decorrenza *(Date of 1st Issue)*	13 febbraio 2026
Nome e Versione del Prodotto *(Product Name and Version)*	Holley's Smart Meters: model DDSD285/DDSY283SR version D285WI0036002503:20-X33-11VS1.0, model DTSD545/DTSY541 version D545WI0036002503:20-X042-11V1.1
Sviluppatore *(Developer)*	Holley Technology Ltd.
Tipo di Prodotto *(Type of Product)*	Altre categorie – Smart meter
Livello di Garanzia *(Assurance Level)*	EAL4+ (ALC_FLR.3) conforme a CC Parte 3
Conformità a PP *(PP Conformance)*	Nessuna
Funzionalità di sicurezza *(Conformance of Functionality)*	TDS specifico per il prodotto, CC Parte 2 estesa

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR
(CCRA recognition for components up to EAL2 and ALC_FLR only)

Riconoscimento SOGIS MRA per componenti fino a EAL4
(SOGIS MRA recognition for components up to EAL4)

Roma, 13 febbraio 2026

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

[ORIGINAL SIGNED]

Il prodotto IT (*Information Technology*) identificato nel presente certificato è stato valutato presso un LVS (Laboratorio per la Valutazione della Sicurezza) accreditato e abilitato/approvato utilizzando la Metodologia Comune per la Valutazione di Sicurezza della Tecnologia dell'Informazione CEM:2022 revisione 1 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione CC:2022 revisione 1. Questo certificato si applica solo alla versione e al rilascio specifici del prodotto nella sua configurazione valutata e unitamente al Rapporto di certificazione completo. La valutazione è stata condotta in conformità alle disposizioni dello Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004) e le conclusioni dell'LVS nel Rapporto di Fine Valutazione sono coerenti con le evidenze addotte. Il presente Certificato non costituisce un sostegno o promozione del prodotto IT da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosca o dia effetto a questo certificato, e nessuna garanzia del prodotto IT, da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosce o dà effetto a questo certificato, è espressa o implicita.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using Common Methodology for Information Technology Security Evaluation CEM:2022 release 1 for conformance to *Common Criteria for Information Technology Security Evaluation CC:2022 release 1. 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. The evaluation has been conducted in accordance with the provisions of the National scheme for the evaluation and certification of the security in the sector of information technology (Prime Ministerial Decree of 30 October 2003 - Official Journal no. 93 of 27 April 2004) 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 Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product, by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.*

Organismo di Certificazione della Sicurezza Informatica

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Holley's Smart Meters: model DDSD285/DDSY283SR version D285WI0036002503:20-X33-11VS1.0, model DTSD545/DTSY541 version D545WI0036002503:20-X042-11V1.1

OCSI/CERT/CCL/05/2025/RC

Version 1.0

13 February 2026

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	13/02/2026

2 Table of contents

3 Acronyms

3.1 National scheme

DPCM	Decreto del Presidente del Consiglio dei Ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Agreement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other acronyms

AMI	Advanced Metering Infrastructure
ECDSA	Elliptic Curve Digital Signature Algorithm
FAN	Field Area Network

HDLC	High-Level Data Link Control
HES	Head End System
HLMCS	Holley Meter Communication System
LMN	Local Management Network
NMS	Network Management System
PCB	Printed Circuit Board
Wi-SUN	Wireless Smart Utility Network

4 References

4.1 Normative references and national Scheme documents

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, November 2022, CC:2022 Revision 1 CCMB-2022-11-001

[CC2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, November 2022, CC:2022 Revision 1 CCMB-2022-11-002

[CC3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, November 2022, CC:2022 Revision 1 CCMB-2022-11-003

[CC4] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, November 2022, CC:2022 Revision 1 CCMB-2022-11-004

[CC5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, November 2022, CC:2022 Revision 1 CCMB-2022-11-005

[CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2014

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, November 2022, CC:2022 Revision 1 CCMB-2022-11-006

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 agosto 2023

[NIS4] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Gestione nel tempo delle garanzie di prodotti certificati, versione 1.1, 21 agosto 2023

[SOGIS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3, January 2010

4.2 Technical documents

[AGD] Holley Technology Ltd, Holley's Smart Meters: DDSD285, DDSY283SR, DTSD545 and DTSY541 AGD Documentation, Version 1.6, 2026-01-21

[ETRv2] Evaluation of Holley's Smart Meters: DDSD285, DDSY283SR, DTSD545 and DTSY541, WONSECEVSM-029_ETR_v2, CCLab – The Agile Cybersecurity Laboratory, Version: v2, 7 November 2025

[ETRv4] Evaluation of Holley's Smart Meters: DDSD285, DDSY283SR, DTSD545 and DTSY541, WONSECEVSM-029_ETR_v4, CCLab – The Agile Cybersecurity Laboratory, Version: v4, 23 January 2026

[PP] Protection Profile for Smart Meter Minimum Security requirements, CEN/CLC/ETSI_SMCG/Sec/00156/DC, Version 1.0, 2019-10-30

[ST] Holley Technology Ltd, Holley's Smart Meters: DDSD285, DDSY283SR, DTSD545 and DTSY541 Security Target, Version 1.9, 2026-01-21

5 Recognition of the certificate

5.1 European recognition of CC certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT -Products. A higher recognition level for evaluations beyond EAL4 is provided for IT -Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under SOGIS-MRA for all claimed assurance components up to EAL4.

5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] was ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all claimed assurance components up to EAL2 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the "**Holley's Smart Meters: model DDSD285/DDSY283SR version D285WI0036002503:20-X33-11VS1.0, model DTSD545/DTSY541 version D545WI0036002503:20-X042-11V1.1**", in the following also referred to as "**Holley's Smart Meters: DDSD285, DDSY283SR, DTSD545 and DTSY541"**, developed by Holley Technology Ltd.

The Target of Evaluation (TOE) are smart meters, which are devices for measuring and recording energy consumption, widely used in residential electricity, commercial electricity and industrial fields. Holley's single phase and three phase smart meters not only have traditional energy metering functions, but also integrate a variety of advanced functions, such as data storage, event monitoring, rate management, remote Wi-SUN communication, local Optical Port and RS485 communication.

The Developer clarified that out of four smart meters in the TOE name, the TOE comprises actually two distinct smart meters (ref. section 1.3 of [ST]). Namely, for business purposes a single phase meter has been assigned two different names (DDSD285 and DDSY283SR) for distribution in different markets. Likewise, a three phase meter has been assigned two different names (DTSD545 and DTSY541) for distribution in different markets. The single phase meter (DDSD285 and DDSY283SR) is identified by the software version D285WI0036002503 and the hardware version 20-X33-11VS1.0, while the three phase meter (DTSD545 and DTSY541) is identified by the software version D545WI0036002503 and the hardware version 20-X042-11V1.1.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the and Scheme Information Notes [NIS1, NIS2, NIS3, NIS4]. The Scheme is operated by the Italian Certification Body "Organismo di Certificazione della Sicurezza Informatica (OCSI)", established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC version CC:2022 Release 1 for the assurance level EAL4, augmented with ALC_FLR.3 according to the information provided in the Security Target [ST] and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3] and [CC5]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product named "**Holley's Smart Meters DDSD285, DDSY283SR, DTSD545 and DTSY541**" to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should also review the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Holley's Smart Meters: model DDSD285/DDSY283SR version D285WI0036002503:20-X33-11VS1.0, model DTSD545/DTSY541 version D545WI0036002503:20-X042-11V1.1
Security Target	Holley Technology Ltd, Holley's Smart Meters: DDSD285, DDSY283SR, DTSD545 and DTSY541 Security Target, Version 1.9, 2026-01-21 [ST]
Evaluation Assurance Level	EAL4, augmented with ALC_FLR.3
Developer	Holley Technology Ltd.
Sponsor	Zhejiang Wangan Technology Co., Ltd.
LVS	CCLab – The Agile Cybersecurity Laboratory (Debrecen site)
CC version	CC:2022 Release 1
PP conformance claim	None
Evaluation starting date	24 February 2025
Evaluation ending date	7 November 2025

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled, and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description it is possible to refer to the Security Target [ST].

The target of evaluation (TOE) is a smart electric energy meter delivered with models for single phase and three phase devices. DDSD285 and DDSY283SR are single-phase meters, and DTSD545 and DTSY541 are three-phase meters. Holley's single phase and three phase smart meters are electrical

energy metering devices with the function of real-time monitoring and user electricity consumption recording. Compared with traditional electric meters, Holley's single phase and three phase smart meters not only support two-way communication but also transmit electricity consumption data to power companies in real time and receive relevant instructions and information.

Holley's single phase and three phase smart meters communicate with users via local (direct) or network interfaces, including configuration data, operating parameters, metrologically certified data, keys, and other non-TSF parts.

TOE core security functions include:

- ensure the confidentiality, authenticity and integrity of data.
- ensure the secure transmission of information flows.

The security functions of Holley's single phase and three phase smart meters are designed to ensure that the user's electricity consumption data is stored and transmitted safely, ensuring that only authorized and trusted AMI systems or maintenance personnel can access the meter. Effectively prevents meter data from being maliciously tampered with, avoiding potential losses to users and power systems.

For a detailed description of the TOE, refer to section 1.5 of the Security Target [ST].

7.3.1 TOE architecture

Smart electric energy meters are devices for measuring and recording energy consumption, widely used in residential electricity, commercial electricity and industrial fields. Holley's single phase and three phase smart meters not only have traditional energy metering functions, but also integrate a variety of advanced functions, such as data storage, event monitoring, rate management, remote Wi-SUN communication, local Optical Port and RS485 communication. Through built-in software and hardware systems, a high degree of intelligent and automated management is achieved.

Figure 1 illustrates the TOE architecture:

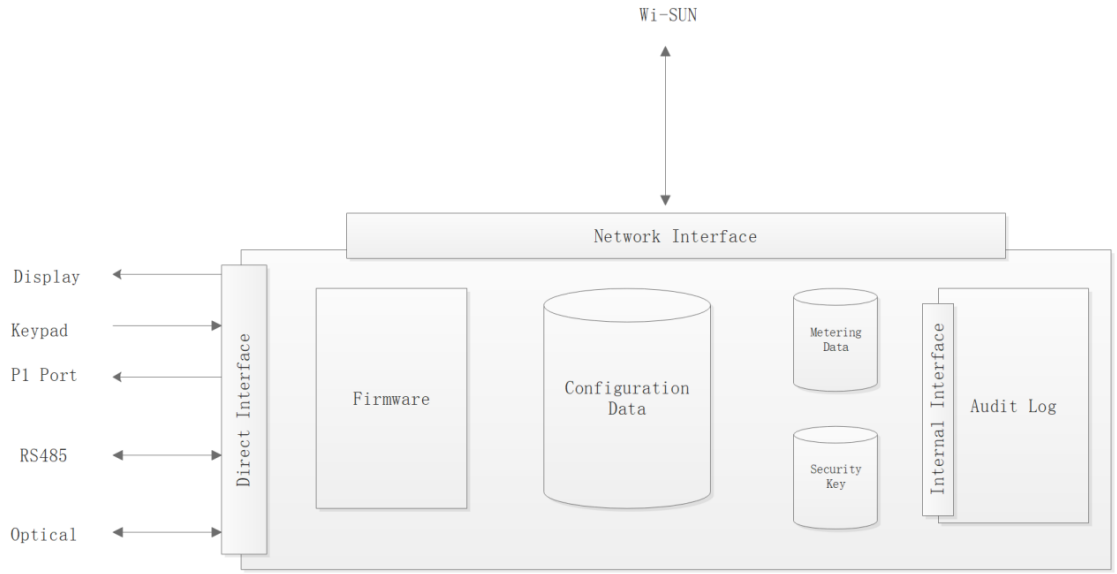

Figure 1 - TOE Architecture

Components of Figure 1 are described in Table 1.

Components	Description
Firmware	It is used to store firmware and backup of updated firmware required for Holley's single phase and three phase smart meters operation, ensuring normal operation of equipment and support firmware update.
Configuration Data	Store the parameter data of Holley's single phase and three phase smart meters to maintain normal operation, including real-time clock (RTC) and other operating parameters to ensure stable operation of the equipment.
Metering Data	Record electricity consumption, instantaneous quantity and demand and other metering data of Holley's single phase and three phase smart meters to provide accurate electricity consumption information for users and systems.
Security Key	Store all cryptographic key data (including Master key, Global Authentication key, Global Encryption key, Global Broadcast key, Client Public Key, Server Private Key, and Server Public Key) in Holley's single phase and three phase smart meters to ensure the security of equipment data and access control.
Audit Log	Record all monitoring and operation logs generated by Holley's single phase and three phase smart meters operation to provide complete historical data for fault diagnosis and operation trail.
Direct Interface	Includes local display, human-computer interaction and maintenance interfaces: Display : Display metrologically certified data of Holley's Single Phase and Three Phase Smart Meters. Keypad: Switch the display item, reset the demand of Holley's Single Phase and Three Phase Smart Meters. P1 Port : Transmit meter data to the user display unit. RS485 : Used for local maintenance and configuration operations. Optical Port : Used for local data reading and maintenance.
Network Interface	The AMI system is connected through the network to support the transmission of Holley's single phase and three phase smart meters data and remote operation.

Table 1 - Components of TOE Architecture

Holley's single phase and three phase smart meters can automatically measure and record power consumption and send the data to the power company via communication technology (Wi-SUN). Generally, Holley's single phase and three phase smart meters are installed in residential homes, commercial buildings or industrial sites to measure and record power consumption. These meters can not only be connected to the local power grid but also communicate bidirectionally with the power company, transmitting power consumption data and receiving instructions such as relay control and

power outage notifications. They also have real-time monitoring, time-of-use billing and fault detection functions, helping users optimize energy usage and improving the operational efficiency of the power company.

This section primarily addresses the physical and logical components of the TOE that are included in the evaluation.

TOE refers to the whole electric energy meter product, including the following key parts:

Hardware

- Meter body: the core part responsible for measuring electric energy, including the metering unit, circuit board, etc.
- Module body: usually refers to the additional function module, i.e. Wi-SUN communication module.

Software

- Includes embedded software, implementing the functional logic, data processing, communication protocol, etc. of the meter.

Structural

- Dust- and water-resistant, usually with a specific degree of protection (e.g. IP65 or higher).
- Designed to prevent external environmental factors (such as moisture, dust) from affecting the hardware to ensure long-term stable operation.
- Prevent external damage through structural optimization, such as anti-disassembly design, application of impact-resistant materials, etc.

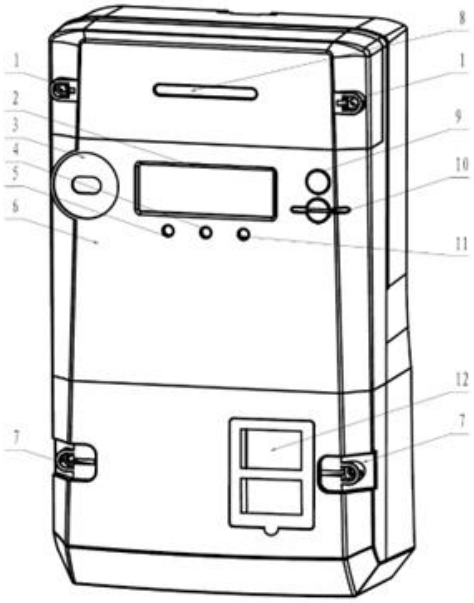

Figure 2 - Meter appearance

No.	Description
1	Module cover & Screws
2	LCD display
3	Optical communication port
4	Alarm LED
5	Active pulse LED
6	Meter cover & Nameplate
7	Terminal cover & Screws
8	Module status LEDs
9	Scroll button
10	Config button (Sealable)
11	Reactive pulse LED
12	P1 port (RJ12)

Table 2 - Meter appearance description

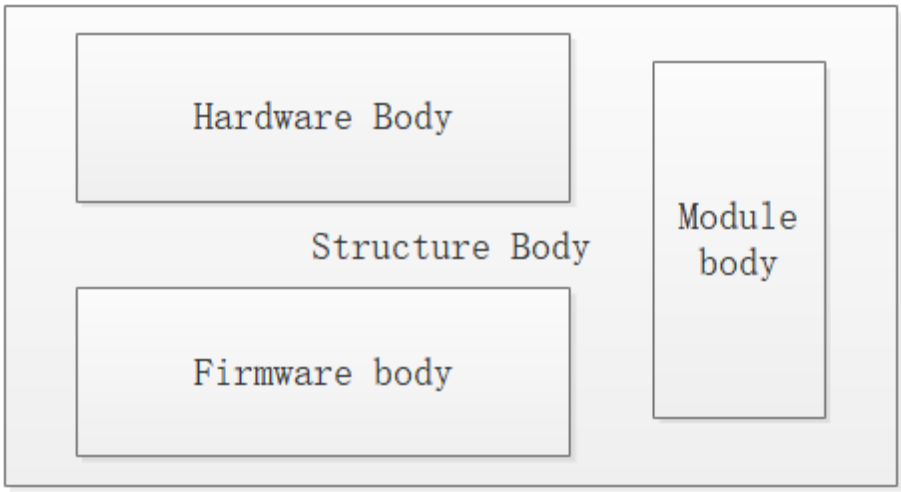

Figure 3 - Meter components

Components	Description
Hardware Body	The core hardware part of Holley's single phase and three phase smart meters, including metering chips, circuit boards, power supply units, etc., is used to achieve electricity measurement and basic operation functions.
Firmware Body	The core software system of Holley's single phase and three phase smart meters operation, including operation logic, metering algorithm and function module, is responsible for the normal operation and data processing of the equipment.
Structure Body	The case and internal support structure of Holley's single phase and three phase smart meters provide physical protection and fixation and layout of components.
Module Body	The communication module (including software and hardware) of Holley's single phase and three phase smart meters is used to realize the connection with external systems, such as wireless communication module or wired interface module.

Table 3 - Meter components description

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in sections 3 and 4 of the Security Target [ST].

For a detailed description of the TOE Security Functions, consult section 1.5.5 and Chapter 8 of the Security Target [ST].

The major security features of the TOE are summarised in the following:

- ***Message Security***

When other devices communicate with Holley's single phase and three phase smart meters, both parties must authenticate to ensure the security and legitimacy of the communication.

Holley's Single Phase and Three Phase Smart Meters use identity authentication and message encryption to ensure confidentiality, integrity and tamper-resistance of transmitted information.

- Authentication: Both parties authenticate each other's identity through security mechanisms (ECDSA based on ECC256) to prevent unauthorized devices from accessing the communication network.
- Information encryption: AES-GCM-128 is used for information encryption to ensure that data is protected from eavesdropping and tampering with during transmission, while providing integrity verification functions.

This mechanism can effectively prevent man-in-the-middle attack and data forgery and ensure the security of Holley's single phase and three phase smart meters communication.

- ***TSF Protection***

  Holley's single phase and three phase smart meters will activate the corresponding protection mechanism to ensure the normal operation of the meter and timely alarm notification when encountering faults or physical tampering.

  Anti-replay mechanism is implemented to prevent malicious users from reusing previously successfully executed requests.

  The data in Holley's single phase and three phase smart meters will be stored in two independent storage units at the same time, ensuring that even if one piece of data is damaged, the other is still available. If an error occurs in a certain piece of data, it can be directly recovered from the backup block to ensure the integrity and availability of the data. Each piece of data is equipped with verification information to verify whether the data is correct. When reading or processing data, data errors can be found through the verification mechanism, and data errors can be quickly located and repaired without external intervention. Even if a piece of data is damaged, the normal operation of the system can still be guaranteed through backup.

  Holley's single phase and three phase smart meters will detect firmware, random number generator and functional modules during startup and after reset to ensure normal operation of the meter.

  Reliable timestamps are provided to provide trusted time for audit generation.

- ***Audit***

  Holley's single phase and three phase smart meters can record security events, including access control events, electric larceny events, grid monitoring events, parameter configuration events, other energy meter operation security events, to achieve a complete log of energy meters; each type of event record timestamp, event type, event ID, etc.; use structured format, unify time format, and archive and storage by event type; complete logs facilitate system analysis of user behaviour or grid status.

  At the same time, the access control authority of audit records is defined, including reading, modifying and deleting operations. In addition, Holley's single phase and three phase smart meters set a cap on the storage of audit records, and when the number of logs exceeds a predefined storage limit, the system automatically overwrites the oldest audit records, ensuring that new records are saved and important events are continuously tracked.

- ***Authentication & Authorisation***

  Authentication is used to verify whether the identity of the user or system is legitimate. The goal is to ensure that the party communicating is indeed who it claims to be. Access to data, parameters, and logs must be authorized by the client. Permissions can be controlled through access tokens (such as OAuth) or other authentication mechanisms.

  Holley's single phase and three phase smart meters use ECDSA based on ECC256 (ECC Key Pair Generation) for mutual authentication for enhanced security. The client and the server exchange authentication messages using AES-GCM-128 encryption and ensure that the messages are not tampered with through authentication labels. When the number of authentication times exceeds the preset number of times, the user is restricted from continuing authentication until the preset time expires.

  After authentication, encryption is used to protect the data access path according to the permission policy to avoid unauthorized access. This combination provides reliable authentication and access control assurance for secure communication, while ensuring re-authentication after a preset period of time to ensure security.

- ***Data Protection***

  Data access in Holley's single phase and three phase smart meters will go through a strict authentication mechanism. Only the subject who has passed the authentication mechanism can access the energy meter data. In addition, different permissions are set for different subjects, and only subjects with corresponding permissions can read or modify the data. Holley's single phase and three phase smart meters have four independent operable interfaces, and different subjects can access the data through different interfaces. However, when accessing data, the subject using the interface needs to be authenticated to access the data to avoid data leakage. In addition, when using the interface for data transmission, the data will be encrypted using an encryption algorithm to prevent data leakage or tampering caused by transmission in plain text.

  Holley's single phase and three phase smart meters can ensure that after some sensitive data is released, any previous content of the data is unusable, avoiding the reuse of sensitive data after release.

- ***Underlying Cryptography***

  The data and information of Holley's single phase and three phase smart meters are encrypted with AES-GCM-128 to protect the real-time readings, historical data and other information from larceny, to ensure that the data has not been tampered with during transmission, to prevent unauthorized equipment from forging the data. No duplication during each encryption is guaranteed, to ensure that even if the same data information is informed, there will not be the same encryption result. Keys are regularly rotated to prevent key leakage.

A detailed description of the TOE security functionality is provided in section 8 of the Security Target [ST].

7.4 Documentation

The guidance documentation specified in "Annex A – Guidelines for the secure usage of the product" is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration, and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in section 8.2 of this report.

7.5 Protection Profile conformance claims

No conformance to Protection Profile is claimed even though security requirements and evaluation conduct have been derived from the Protection Profile for Smart Meter Minimum Security requirements, CEN/CLC/ETSI_SMCG/Sec/00156/DC, Version 1.0, dated October 30th, 2019 (Ref. [PP]).

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3] and are from EAL 4 assurance package, augmented with the CC part 3 component ALC_FLR.3.

All the SFRs have been selected or derived by extension from CC Part 2 [CC2]. The following extended components are described in section 5 of [ST]: FAU_ARP.2, FPT_TSU.1, FPT_BST.1 and FPT_TNN.1.

It is possible to refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab – The Agile Cybersecurity Laboratory (Debrecen site).

The evaluation was completed on 7 November 2025, with the issuance by the LVS of the approved Evaluation Technical Report in version 2 of the ETR ([ETRv2]). Following some editorial updates to the evaluation documentation a final version 4 of the ETR ([ETRv4]) was acquired. The Certification Body has then issued the certification report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in "Annex B – Evaluated configuration".

Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; there is a probability, however small, that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to regularly check the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETRv2] issued by the LVS CCLab – The Agile Cybersecurity Laboratory (Debrecen site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE named "Holley's Smart Meters DDSD285, DDSY283SR, DTSD545 and DTSY541" meets the requirements of Part 2 and 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4 augmented with ALC_FLR.3 with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in "Annex B – Evaluated configuration".

Table 4 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL4 augmented with ALC_FLR.3 (augmentation in *italics* in Table 4).

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Modular design	ADV_TDS.3	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass
Delivery procedures	ALC_DEL.1	Pass
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass

Assurance classes and components		Verdict
Well-defined development tools	ALC_TAT.1	Pass
Systematic flaw remediation	*ALC_FLR.3*	*Pass*
Test	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Focused vulnerability analysis	AVA_VAN.3	Pass

Table 4 - Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in section 6 (Statement of Certification).

Potential customers of the product “Holley’s Smart Meters DDSD285, DDSY283SR, DTSD545 and DTSY541” are suggested to properly understand the specific purpose of the certification by reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the “Security Objectives” specified in section 4 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all Assumptions described in section 3.5 of the Security Target [ST] shall be satisfied.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, “Annex A – Guidelines for the secure usage of the product” includes a number of recommendations relating to delivery, installation, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([AGD]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE delivery

After receiving Holley's single phase and three phase smart meters provided by the manufacturer, the customer should power up and start the equipment and read the software version number and software check code of Holley's single phase and three phase smart meters through the PC software to confirm whether it is consistent with the information provided by the manufacturer. At the same time, the customer is required to verify the functions of Holley's single phase and three phase smart meters through the PC software to ensure that it is consistent with the performance and specifications described in the guide (Ref. [AGD]).

In addition, Holley's single phase and three phase smart meters are disassembled by sampling to check whether the PCB version number is consistent with the information provided. After the above verification steps, the customer can complete the acceptance of Holley's single phase and three phase smart meters.

Through the above procedures, the secure transmission of Holley's single phase and three phase smart meters firmware and configuration files from the development to the production process to the client is ensured to prevent unauthorized and illegal firmware loading and running, and Holley's single phase and three phase smart meters meeting the requirements are finally delivered safely.

9.2 Installation, configuration and secure usage of the TOE

TOE installation, configuration and operation should be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the Common Criteria guidance [AGD] contains detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure operation of the TOE in accordance with the security objectives specified in the Security Target [ST].

10 Annex B – Evaluated configuration

The Evaluators followed the preparation steps defined in the [AGD] document for the TOE being in the evaluated configuration.

The following are the TOE version numbers of Holley's single phase and three phase smart meters (section 1.3 of [ST]):

Holley's Single Phase Smart Meters: DDSD285/ DDSY283SR

TOE Software Version: D285WI0036002503

TOE Hardware Version: 20-X33-11VS1.0

Holley's Three Phase Smart Meters: DTSD545/ DTSY541

TOE Software Version: D545WI0036002503

TOE Hardware Version: 20-X042-11V1.1

The software identification is viewed by the user through the PC Software (HLMCS). The hardware version can be found by disassembling Holley's single phase and three phase smart meters and looking at the PCB.

The items described in section 10.1 "TOE operational environment" must be available before performing the installation.

10.1 TOE operational environment

Holley's single phase and three phase smart meters needs to be installed in the normal power grid, or in a laboratory connected to the standard power supply test equipment (power supply specification between 220V and 240V), Wi-SUN module is connected to the Internet through the link gateway, PC is connected to TOE via RS485 converter of RJ12 interface, or PC is connected to TOE via contactless optical port communication adapter.

The TOE located in the LMN network communicates with the Gateway through the Wi-SUN interface using the encrypted information of the HDLC/WRAPPER protocol (Figure 4).

Figure 4 – TOE operational environment

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities.

11.1 Test configuration

Testing activities have been carried out from the LVS premises.

The Evaluators verified the configuration of the test environment, including the TOE, and found it to be consistent with the guidance documentation [AGD] and the Security Target [ST].

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The developer performed extensive tests to verify the functionality of the TOE. The tests cover all Subsystems, Modules and TSFIs of the TOE.

11.2.2 Test coverage

The following aspects of the TSF are covered by the tests:

1. Message Security
2. TSF Protection
3. Audit
4. Authentication & Authorisation
5. Data Protection
6. Underlying Cryptography

The Developer provided 42 manual test cases. The Evaluators have examined the test plan presented by the Developer and verified the complete coverage of the functional requirements (SFRs) and the TSFIs described in the functional specification. The Evaluators verified that the test cases are sufficient to demonstrate the internal behaviour and the properties of the TSF.

11.2.3 Test results

The actual test results of all Developer's tests were consistent with the expected ones.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Test approach

In addition to the 42 Developer's test Evaluator created and performed 4 more independent test cases to test the TSF more in depth.

These are:

1. WONSECEVSM-TEST01: The purpose of the test was to verify whether the functions identified in [ST] section 6.2.5.2 Management of Security Functions Behaviour (FMT_MOF.1) as "Not configurable" truly cannot be configured.

2. WONSECEVSM-TEST02: The purpose of the test was to verify that load data, frozen data, and event log data were truly deleted upon a deletion request, and that after deletion, the objects identified in the FDP_RIP.1 SFR could not be accessed via at least one of the functions that would previously be used to access it.
3. WONSECEVSM-TEST03: The purpose of the test was to verify the TOE protected itself against messages that have a frame counter with the highest possible 32-bit value, and the lowest possible 32-bit value. Every message must have a higher frame counter value than the previously received one accepted by the TOE smart meter.
4. WONSECEVSM-TEST04: The purpose of this test was to verify that the TOE stores the amount of consumed power persistently, even after multiple reboots, and prolonged periods of being powered off.

The Evaluator conducted exhaustive testing on the TOE and on its functionalities and aimed with these independent tests to connect these two and observe their impact on each other.

11.3.2 Test results

All Developer's tests were run successfully, and the Evaluators verified the correct behaviour of the TSFIs and TSFs and the correspondence between expected results and achieved results for each test.

All test cases devised by the Evaluators were passed successfully and all the test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked with the TOE already used for the functional test activities and verified that the TOE and the test environment were properly configured.

The Evaluators designed the following attack scenarios:

- Replay attack.
- Manipulation of keys in the TOE.
- Power on process.
- Store the blocking condition.
- Interface examination.
- Brute force attack.
- Manipulating or guessing the Smart Meter's Random Number Generator (RNG).
- Change the "allowed failed attempts" value on the TOE.
- Insecure remote Wi-SUN communication.

The Evaluators has concluded that the TOE is resistant to "Enhanced-basic" attack potential in its intended operating environment. No exploitable or residual vulnerabilities were identified.