



# *Agenzia per la Cybersicurezza Nazionale*



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) ve.3.1 rel. 5

**Certificato n.** 08/2025  
(Certificate No.)

**Rapporto di Certificazione** OCSI/CERT/CCL/11/2024/RC, v 1.0.  
(Certification Report)

**Decorrenza** 29 ottobre 2025  
(Date of 1<sup>st</sup> Issue)

**Nome e Versione del Prodotto** Wasion aMeter100 and aMeter300 Smart Energy Meters  
(Product Name and Version)

**Sviluppatore** Wasion Limited Group  
(Developer)

**Tipo di Prodotto** Altre categorie – Smart meter  
(Type of Product)

**Livello di Garanzia** EAL3+ (ALC\_FLR.3) conforme a CC Parte 3  
(Assurance Level)

**Conformità a PP** Protection Profile for Smart Meter Minimum Security requirements. Version: 1.0, date: 2019-10-30  
(PP Conformance)

**Funzionalità di sicurezza** Funzionalità conformi a PP, CC Parte 2 estesa  
(Conformance of Functionality)



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, 29 ottobre 2025

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 Metodologia Comune per la Valutazione di Sicurezza della tecnologia dell'Informazione versione 3.1 revisione 5 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5. 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 version 3.1 release 5 for conformance to Common Criteria for Information Technology Security Evaluation version 3.1 release 5. 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.*



*Agenzia per la Cybersicurezza Nazionale*

*Servizio Certificazione e Vigilanza*



Organismo di Certificazione della Sicurezza Informatica

## **Certification Report**

# **Wasion aMeter100 and aMeter300 Smart Energy Meters**

OCSI/CERT/CCL/11/2024/RC

Version 1.0

29 October 2025

## 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	29/10/2025

## 2 Table of contents

1	Document revisions .....	3
2	Table of contents .....	4
3	Acronyms.....	6
3.1	National scheme.....	6
3.2	CC and CEM.....	6
3.3	Other acronyms.....	6
4	References .....	8
4.1	Normative references and national Scheme documents .....	8
4.2	Technical documents .....	8
5	Recognition of the certificate .....	10
5.1	European recognition of CC certificates (SOGIS-MRA).....	10
5.2	International recognition of CC certificates (CCRA).....	10
6	Statement of certification.....	11
7	Summary of the evaluation.....	12
7.1	Introduction.....	12
7.2	Executive summary .....	12
7.3	Evaluated product .....	12
7.3.1	TOE architecture .....	13
7.3.2	TOE security features.....	15
7.4	Documentation.....	18
7.5	Protection Profile conformance claims.....	18
7.6	Functional and assurance requirements .....	18
7.7	Evaluation conduct .....	18
7.8	General considerations about the certification validity .....	19
8	Evaluation outcome .....	20
8.1	Evaluation results.....	20
8.2	Recommendations.....	21
9	Annex A – Guidelines for the secure usage of the product .....	22
9.1	TOE delivery .....	22
9.2	Installation, configuration, and secure usage of the TOE.....	24
10	Annex B – Evaluated configuration .....	25
10.1	TOE operational environment .....	25
11	Annex C – Test activity .....	26

11.1	Test configuration .....	26
11.2	Functional tests performed by the Developer .....	26
11.2.1	Testing approach .....	26
11.2.2	Test coverage.....	26
11.2.3	Test results.....	26
11.3	Functional and independent tests performed by the Evaluators .....	26
11.3.1	Test approach .....	26
11.3.2	Test results.....	27
11.4	Vulnerability analysis and penetration tests .....	27

## 3 Acronyms

### 3.1 National scheme

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

### 3.2 CC and CEM

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

### 3.3 Other acronyms

<b>COSEM</b>	Companion Specification for Energy Metering
<b>DLMS</b>	Device Language Message Specification
<b>FW</b>	Firmware



<b>GPRS</b>	General Packet Radio Service
<b>HDLC</b>	High-Level Data Link Control
<b>I2C</b>	Inter-Integrated-Circuit
<b>MCU</b>	Micro Controller Unit
<b>MPMS</b>	Meter Parameter Management System
<b>OS</b>	Operating System
<b>OSM</b>	Other Service Module
<b>RTC</b>	Real Time Clock
<b>SPI</b>	Serial Peripheral Interface
<b>UART</b>	Universal Asynchronous Receiver-Transmitter

## 4 References

### 4.1 Normative references and national Scheme documents

- [CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017
- [CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017
- [CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017
- [CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2014
- [CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017
- [LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004
- [LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004
- [LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004
- [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
- [SOGIS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3, January 2010

### 4.2 Technical documents

- [AGDv1.5] AGD Documentation WASION aMeter100 and aMeter300 Smart Energy Meters Evaluation Assurance Level (EAL): EAL3 augmented with ALC\_FLR.3, version: v1.5, date: 2025-05-19
- [B-Book] Blue Book Edition 15 - COSEM Interface Classes and OBIS Object Identification System DLMS UA 1000-1 Ed. 15, 2021-12-23

- [DSMR P1] P1 Companion Standard Dutch Smart Meter Requirements, Date: February 26th, 2016, Version: 5.0.2.
- [ETRv2] Evaluation Technical Report Evaluation of Wasion aMeter100 and aMeter300 Smart Energy Meters Evaluation Assurance Level EAL3 augmented with ALC\_FLR.3 based on ISO/IEC 18045:2008 Information technology - Security techniques - Methodology for IT security evaluation, WASIONEVAL-039\_ETR\_v2, 2025-08-01.
- [IEC 62056-21] Electricity metering – Data exchange for meter reading, tariff and load control – Part 21: Direct local data exchange, IEC 62056-21 First edition 2002-05.
- [IEC 62056-46] Electricity metering Data exchange for meter reading, tariff and load control Part 46: Data link layer using HDLC protocol, IEC 62056-46 First edition 2002-02.
- [IEC 62056-47] Electricity metering – Data exchange for meter reading, tariff and load control – Part 47: COSEM transport layers for IPv4 networks, IEC 62056-47 First edition 2006-11.
- [OLv1.2] Hungary Object list v1.2 20250507.xlsx, version: 1.2, Received: 2025-05-07.
- [SM-MSR-PP] Protection Profile for Smart Meter Minimum Security requirements. Version: 1.0, date: 2019-10-30, Authors: Ad-Hoc Group Privacy & Security of the CEN/CENELEC/ETSI Coordination Group on Smart Meters.
- [ST] Security Target WASION aMeter100 and aMeter300 Smart Energy Meters Evaluation Assurance Level (EAL): EAL3 augmented with ALC\_FLR.3, version: v1.6, date: 2025-05-19.
- [UMv1.0] WASION aMeterx00 Smart Energy Meter User Manual Version: V1.0 (aMeterx00 Smart Energy Meter User Manual.pdf)

## **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 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 8 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 product “**Wasion aMeter100 and aMeter300 Smart Energy Meters**”, developed by Wasion Group Limited.

The TOE takes digital medium as information exchange media. The TOE can realize remote communication and control via CAT-1/CAT M1 module. It also supports DLMS/COSEM specification to achieve interconnection with the master station. The meter includes measurement unit, display unit, button input, real-time clock unit, infrared communication, remote communication, load switch and other auxiliary equipment. Wasion Smart Meter includes two types of devices based on the metrology. Different power supply needs different metrological systems. The aMeter100 is a single-phase, while the aMeter300 is a three-phase smart meter.

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 Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. 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 also review 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 3.1 Revision 5 for the assurance level EAL3 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 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 “Wasion aMeter100 and aMeter300 Smart Energy Meters” 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

<b>TOE name</b>	Wasion aMeter100 and aMeter300 Smart Energy Meters
<b>Security Target</b>	Security Target WASION aMeter100 and aMeter300 Smart Energy Meters Evaluation Assurance Level (EAL): EAL3 augmented with ALC_FLR.3., v1.6, 2025-05-19 [ST]
<b>Evaluation Assurance Level</b>	EAL3 augmented with ALC_FLR.3
<b>Developer</b>	Wasion Group Limited
<b>Sponsor</b>	Wasion Group Limited
<b>LVS</b>	CCLab - The Agile Cybersecurity Laboratory (Budapest site).
<b>CC version</b>	3.1 Rev. 5
<b>PP conformance claim</b>	Protection Profile for Smart Meter Minimum Security requirements. Version: 1.0, date: 2019-10-30, Authors: Ad-Hoc Group Privacy & Security of the CEN/CENELEC/ETSI Coordination Group on Smart Meters [SM-MSR-PP].
<b>Evaluation starting date</b>	21 June 2024
<b>Evaluation ending date</b>	6 August 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 further details refers to [ST].

The TOE (Wasion aMeter100 and aMeter300 Smart Energy Meters) is a smart meter; it is an electronic device that records information such as consumption of electric energy, voltage levels, current, and power factor. Smart meters communicate the information to the consumer for greater clarity of consumption behavior, and electricity suppliers for system monitoring and customer billing.

It is possible to consult sections 1.3 and 1.4 of the Security Target [ST] for a more detailed description of the TOE.

### 7.3.1 TOE architecture

The TOE includes two types of devices based on the metrology. Different power supply needs different metrological systems. The aMeter100 is a single-phase, while the aMeter300 is a three-phase smart meter.

In the following Figure 1 is presented the high-level TOE architecture highlighting the TOE interfaces.

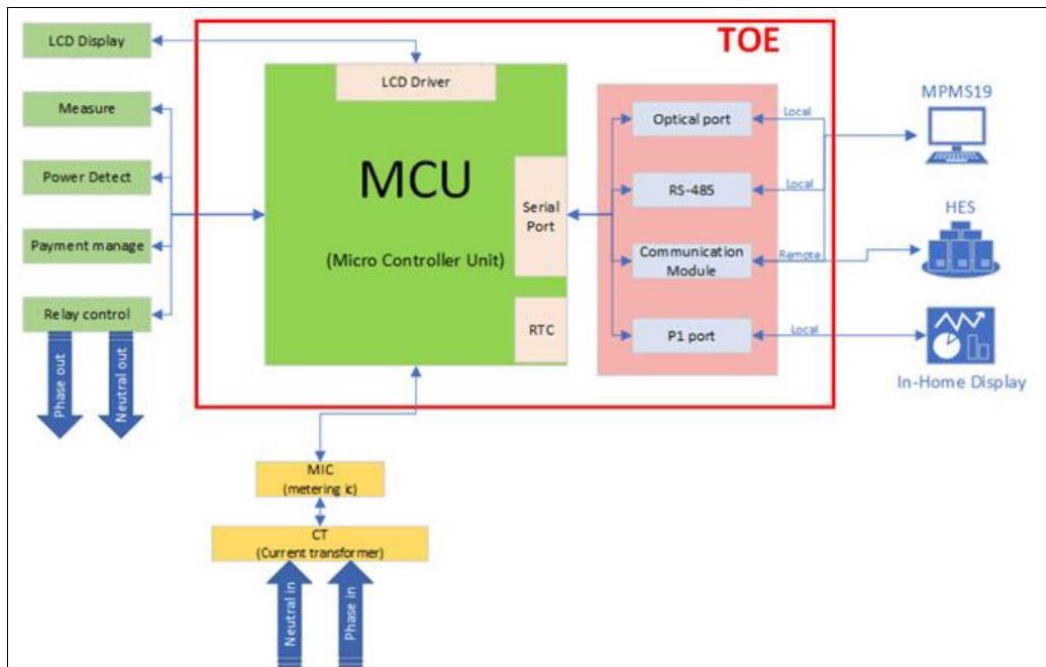


Figure 1 – TOE Architecture

The TOE has following interfaces:

- Optical port, which can support direct HDLC ([IEC 62056-46]) or Mode E of [IEC 62056-21].
- RS-485 port, which can support direct HDLC ([IEC 62056-46]).
- Communication Module (CAT-1/CAT M), which can support [IEC 62056-47].
- P1 port, which can support Mode D of [IEC 62056-21], physical connector pin assignment of passive mode according to DSMR 5.0.2 [DSMR P1].

The TOE is divided into the subsystem/module/TSFI level as per Table 1.

Subsystem	Module	TSFI
MCU (Micro Controller Unit)	RTC	--
	Serial Port	Optical port RS-485 Communication Module P1 port
	LCD Driver (SFR-noninterfering)	--

Table 1 - TOE Boundary (Subsystems, Modules and TSFIs)

The Event Log, Security, Push and Firmware Upgrade functionalities are provided by the subsystem itself.

- **MCU (Micro Controller Unit):** A single chip that integrates a CPU, memory (ROM, RAM), I/O ports, Timers, Serial communication interfaces (UART, SPI, I2C, etc.), and other peripheral device controllers. Mainly used for data calculation, process processing, and functional control.
- **RTC (Real-Time Clock):** The RTC provides the local time for every time related record or function.
- **Serial Port:** The serial port corresponds to the UART port inside of MCU, which can communicate bi-directionally (two ways) and has a configurable baud rate. The typical baud rate is 9600bps, and some ports can reach 115200bps. The Serial Port module used to receive request command messages transmitted from communication ports (Optical, RS-485, Communication Module, etc.), and to respond to them after parsing the received request command messages. For example, reading energy data, billing log, load profile, event log of TOE, manage and configure parameters and configurations of TOE, transmission of image packages when operate a firmware upgrade, and other usage scenarios.
- **LCD Driver:** Meter equipped a non-reflective and support photograph ability and readability under various lighting conditions. Operating and storage temperature from -40°C to 70°C, and its service life is for 20 years. The symbol for LCD is shown in the following Figure 2.

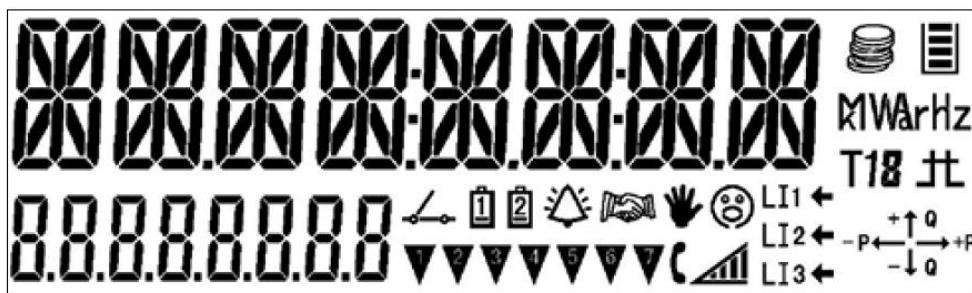


Figure 2 – Symbol for LCD display

It can be found from the symbol figure of LCD screen that is used a segmented type of LCD. The LCD datasheet describes that need uses 8 COM ports and 34 segments as the driving form. Therefore, an LCD driver is needed to control the operation of this segmented type of LCD, this determine whether each segment should be light on or off.



### 7.3.2 TOE security features

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

For a detailed description of the TOE Security Functions, consult section 1.3.3 and Chapter 7 of the Security Target [ST].

The major security features are the following:

- Real-Time Clock.
- Event Log.
- Security.
- Push.
- Firmware Upgrade.
- Meter Communications.

Security functionalities are summarized in the following sections.

#### 7.3.2.1 Real-Time Clock

The RTC provides the local time for every time related record or function. The MCU has built-in real-time clock module, which uses 32768Hz crystal oscillator as clock source to calculate. The accuracy of the clock can reach 0.5 s/d at 25 °C after modification. There is an independent power supply for the RTC module. It is powered from the main supply in normal operation mode and powered by battery during power failure period.

#### 7.3.2.2 Event Log

The TOE has advanced logging capabilities. Logging is performed using OBIS codes. Log entries can be divided into the following groups:

- *General Information:* The logs found here are mainly information related to the incoming and outgoing power supply. The logs generated here can be easily interpreted if one or more phases are not working in the TOE system. It also records how long there was no power and when the error occurred.
- *Standard Event Log:* The logs here are information about the TOE, such as turning the TOE on and off. If the time changes or the TOE experiences a problem over time, it will indicate this here. The TOE contains a battery, if its voltage drops below 2.9V for 1 minute, it will also indicate that it needs to be replaced. It also records the clearing of the Error and Alarm registers. If any problem occurs, these registers are set, and the administrator manually clears them at the end of the error. If the TOE detects any problem such as RAM, NV memory, Watchdog, FW verification fails, key exchange, random number generation or event log clearing it is also logged here.
- *Fraud Detection Log:* If the TOE detects any attack, it will be reported here. The TOE can detect if the terminal is removed or replaced. Also, it detects if a strong magnet is placed near the TOE or authentication error and replays attack appears.
- *Communication Log:* If someone connects to the TOE on any of the protocols, it will be recorded here.

- *Disconnect Control Log*: The TOE can interrupt the further supply of incoming power. It does it using the disconnecter. This can be done locally or remotely. The TOE logs these and the elapsed time.
- *Power Quality Log*: The TOE can also monitor the quality of the incoming power. If any incoming phase is providing too little or too much power, it logs it. Furthermore, it detects asymmetry in the phase.
- *Power Failure Management*: It records the power failures in all phases and their duration.

### 7.3.2.3 Security

The TOE support one security context. The security context is configured by its security setup object. In this security setup object, the global unicast key is related to the “Administrator/Operator/Reader Client association”. The attributes “security\_suite” can be configured:

- If “security\_suite” set to 0, then AES-GCM-128 authenticated encryption and AES-128 key wrap will be supported.
- If “security\_suite” set to 1, then AES-GCM-128 authenticated encryption, ECDSA P-256 digital signature, ECDH P-256 key agreement, SHA-256 hash and AES-128 key wrap will be supported.

The TOE uses Security\_suite 0 (AES-GCM-128 for authenticated encryption) during building association and HLS5 GMAC Authentication and requires a re-authentication when after a period of 3 minutes from the previous successful authentication. In addition to these, only the Administrator and Operator roles can delete the event logs, so no unauthorized deletion is possible. Also, only these two roles have the rights to modify the meter clock.

COSEM models the utility meter as a server application used by client applications that retrieve data from, provide control information to, and instigate known actions within the meter via controlled access to the COSEM objects. The clients act as agents for third parties i.e., the business processes of energy market participants. [OLv1.2] contains all the relevant COSEM objects according to the TOE. Every object has its own attributes defined in the [B-Book]. The object model indicates the available operations for every object and attribute to every user role (Access rights). There are 3 operations connected to the objects’ attributes and access rights:

- GET: read the attribute
- SET: set/modify the attribute
- ACTION: perform an action, e.g., the relay object can be connected or disconnected remotely.

The COSEM object model is stored in the code flash of the TOE. The object model is defined as read-only data in the firmware, and the modification of the object model is only available through a firmware upgrade.

### 7.3.2.4 Push

The registration operation is the meter announcement at the management level when the meter is installed on the field for the first time. For the wireless WAN devices, the registration is performed with the means of push operation by pressing button 5 seconds. This registration is required after the TOE is in its secure operational state, and this registration is related to the electricity service provider’s network.

Push Setup – On Alarm: some of the events can trigger alarms. If one of these events occurs, the corresponding flag in the alarm registers are set and an alarm is then raised via communication channel. All alarm flags in the alarm registers remain active until the alarm registers are cleared. Each

bit in the alarm registers represents a different alarm. If the bit is set (logical 1) the alarm (corresponding to position of the set bit) was recorded. The value in the Alarm Registers is a summary of all active and inactive alarms at that time. Depending on the capabilities of the system and the policy of the utility, not all possible alarms are wanted. Therefore, the Alarm Filters can be programmed to mask out unwanted alarms. The structure of the filter is the same as the structure of the Alarm Registers. To mask out unwanted alarms the corresponding bits in Alarm Filters should be set to logical 0.

#### 7.3.2.5 *Firmware Upgrade*

The meter supports local update via local communication port (IR or RS-485) or remote ports (GPRS) and adopts DLMS to upgrade meter's firmware. The firmware update for the meter and its communication module could be executed remotely via the system administrator or the manufacturer's system, as per data protection regulations or locally, using the local communication port (IR or RS-485). This process involves encrypted and key-protected updates and remote parameterization, ensuring the authentication and DSO seal remain intact. The firmware update must only be possible after the authenticity of the firmware update has been verified and if the version number of the new firmware is higher to the version of the installed firmware. This verification process is done by the TOE after successfully receiving the firmware image. After the TOE has found everything in order and created the logs then it performs a firmware upgrade. It's crucial that the firmware update does not affect the stored data, change the device's measuring capabilities, or render the existing driver unsuitable for remote reading operations. Administrator and Supervisor (Operator) are allowed to upgrade the firmware with separate keys.

#### 7.3.2.6 *Meter Communications*

The TOE has four communication ports/modules:

- *Communication Module*: With the Communication Module the TOE is accessible using its IP address and TCP/IP protocol. The manufacturer-based configuration and parameterization tool, the MPMS, provides the possibility to connect to the TOE directly, using its IP address and a designated port. MPMS first authenticates the user then the proper symmetric keys are required to be loaded to the software for authentication and encryption, then the communication can be started.
- *Optical port*: Meters have an optical port, which can support direct HDLC or Mode E ([IEC 62056-21]). The Optical port is implemented according the DLMS/COSEM standard, which means that the communication is always secured by the AES-128-GCM symmetric encryption keys. Every message is authenticated, and the authorization of the sender is always under control. After 10 times of authentication failure the TOE will reject every message from the same address for 60 minutes.
- *RS-485*: Meters have an RS-485 port, which can support direct HDLC. The RS-485 Interface is implemented according the DLMS/COSEM standard, which means that the communication is always secured by the AES-128-GCM symmetric encryption keys. Every message is authenticated, and the authorization of the sender is always under control. After 10 times of authentication failure the TOE will reject every message from the same address for 60 minutes.
- *P1 port*: P1 port is a read only interface. The meter has only one P1 port, the baud rate for the communication is 115200bps, using [IEC 62056-21] mode D. The P1 port connector type is RJ12. The Metering System holds a female connector, the OSM (Other Service Module) connects via standard RJ12 male plug. This interface is a one-way communication, and the

TOE only sends non-sensitive information, so the communication doesn't need a secured channel.

The P1 port provides the following information for the customer:

- Equipment identifier.
- Currently active tariff.
- Relay status.
- Actual meter energy reading of electricity meter.
- Measured data: Voltage, Current, Power, Power Factor, Frequency.
- Active power limitation threshold.
- The message for the user.

## 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

The Security Target [ST] claims strict conformance to the following Protection Profile (PP).

- Protection Profile for Smart Meter Minimum Security requirements. Version: 1.0, date: 2019-10-30, Authors: Ad-Hoc Group Privacy & Security of the CEN/CENELEC/ETSI Coordination Group on Smart Meters [SM-MSR-PP].

## 7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

All the SFRs have been selected or derived by extension from CC Part 2 [CC2].

Security Target [ST] provides a 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 Provisional Guideline [LGP3] and 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].

Furthermore, all specific assurance activities required by the Protection Profile for Smart Meter Minimum Security requirements [SM-MSR-PP] have been carried out.

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

The evaluation was completed on August 6<sup>th</sup>, 2025, with the delivery by LVS of the Evaluation Technical Report v2 [ETRv2], which was approved by the Certification Body on September 1<sup>st</sup>, 2025. Then, the Certification Body issued this 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 (lower as the assurance level increases), 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 v2 [ETRV2] issued by the LVS CCLab - The Agile Cybersecurity Laboratory (Budapest site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE “Wasion aMeter100 and aMeter300 Smart Energy Meters” meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL3 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 2 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 EAL3 augmented with ALC\_FLR.3 (augmentations are represented in italics in Table 2).

Assurance classes and components		Verdict
<b>Security Target evaluation</b>	<b>Class ASE</b>	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
<b>Development</b>	<b>Class ADV</b>	Pass
Security architecture description	ADV_ARC.1	Pass
Functional specification with complete summary	ADV_FSP.3	Pass
Architectural design	ADV_TDS.2	Pass
<b>Guidance documents</b>	<b>Class AGD</b>	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
<b>Life cycle support</b>	<b>Class ALC</b>	Pass
Authorisation controls	ALC_CMC.3	Pass
Implementation representation CM coverage	ALC_CMS.3	Pass
Delivery procedures	ALC_DEL.1	Pass
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
<i>Systematic Flaw remediation</i>	<i>ALC_FLR.3</i>	<i>Pass</i>

Assurance classes and components		Verdict
<b>Test</b>	<b>Class ATE</b>	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
<b>Vulnerability assessment</b>	<b>Class AVA</b>	Pass
Vulnerability analysis	AVA_VAN.2	Pass

Table 2 - 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 “Wasion aMeter100 and aMeter300 Smart Energy Meters” 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 for the Operational Environment” specified in section 4 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all Assumptions and Organizational Security Policies described in section 3.3 and 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, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE (user manuals [UMv1.0], and CC guidance [AGDv1.5]).



## 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

The [AGDv1.5] contains the information presented in Table 3 about the firmware versions.

Type	aMeter100	aMeter300
<b>Hardware version</b>	DDZ101-aMeter100(GTEU)V1.0	DTZ341-aMeter300(GTEU)V1.0
<b>Firmware version of part 1</b>	aM100-L-A3480100	aM300-L-B3480100
<b>Checksum of firmware part 1</b>	9B9810DB	4BB5D82A
<b>Firmware version of part 2</b>	aM100-N-A3480100	aM300-N-B3480100
<b>Signature of firmware part 2</b>	2AF03FF8E659A69643A55B6A9 B7D37FB519A680372551413261 7FFE0B25CAB604E3AF34E380 375754E0B3AC1EEDC6E98143 7DF08101E609488FA13C353E7 77C2	7C44B87C6AA5287B442439685 E7CC78FECB8BD8915047141A DB3DD17540421E1495CA7299 C900F36628AC4CE9B45C81B9 87DA82659BC6C6B2BD783BC9 A5B48DA
<b>Firmware version of part 3</b>	Wasion-aMeter-BOOT-V1.0- 20231125	Wasion-aMeter-BOOT-V1.0- 20231125
<b>Checksum of firmware part 3<sup>1</sup></b>	N.A.	N.A.

Table 3 - TOE versions from [AGDv1.5]

According to [AGDv1.5] section 3.2, the installation process of the meter includes the following steps:

- 1) Take out the meter from the box and remove the packaging.
- 2) Install the hook of meter and the antenna of communication module.
- 3) Open the terminal cover screw and remove the terminal cover.
- 4) Wire the power line to meter terminal block according to wiring diagram.
- 5) Close the terminal cover and tighten the screw.
- 6) Install the terminal cover seal.
- 7) Power on and check the meter working state.

<sup>1</sup> The BootLoad part of the firmware cannot be changed after manufacturing, because it is burned into the main board, so there is no checksum for firmware part 3.

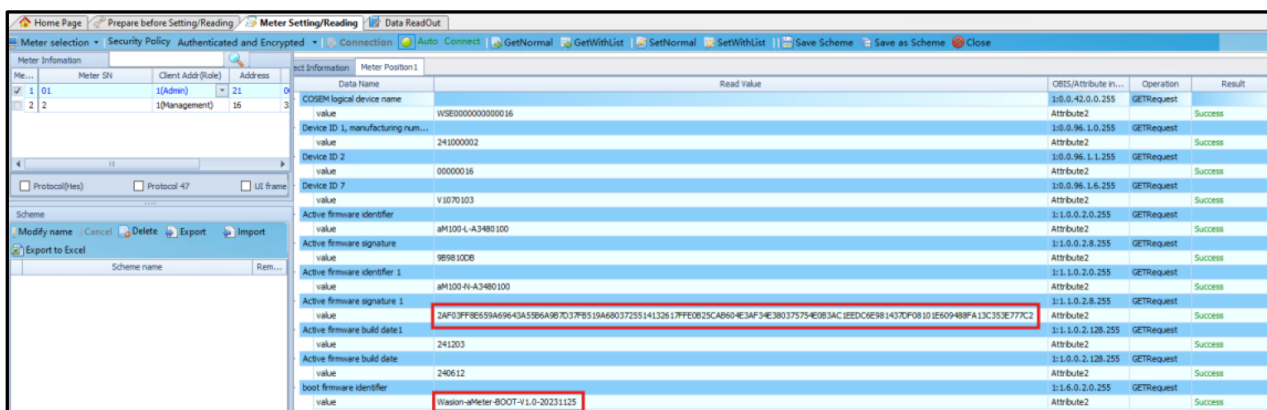


The TOE is always delivered with pre-installed firmware, but the installation can be verified. During the start-up process, the meter shows the version of the firmware on the LCD display (Figure 3), and the visible version can be compared to the one in the Order Specification to validate that the correct version of the firmware is running on the TOE.



Figure 3 – aMeter100 and Firmware indication (left side) aMeter300 and Firmware indication (right side)

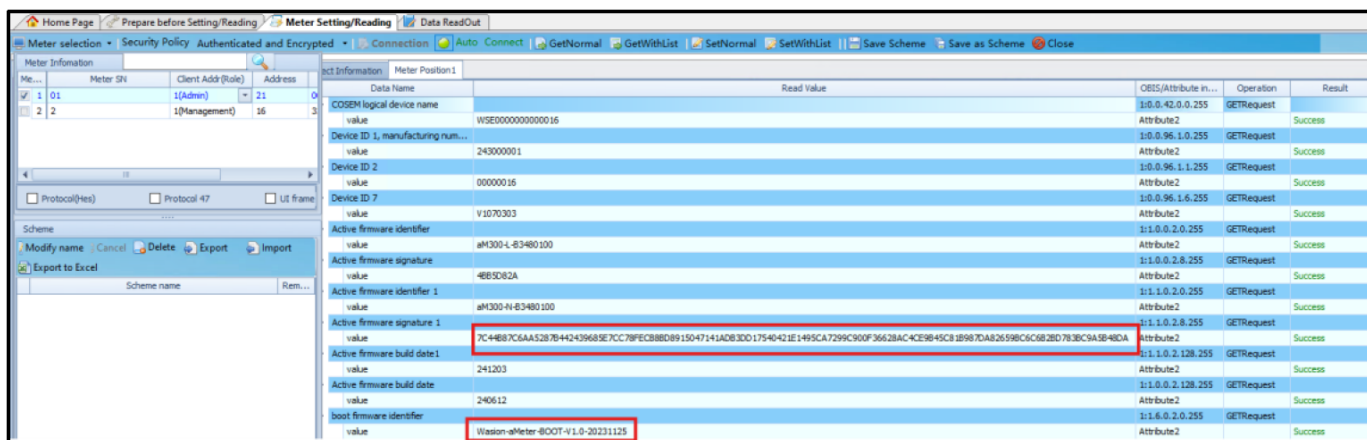
The customer can also connect the TOE devices with the provided MPMS application and verifies the firmware details such as in Figure 4 for the aMeter100.



Attribute Name	Read Value	Operation	Result
COSEM logical device name	WSE00000000000016	GETRequest	Success
Device ID 1, manufacturing num...	241000002	GETRequest	Success
Device ID 2	00000016	GETRequest	Success
Device ID 7	V1070103	GETRequest	Success
Active firmware identifier	aM100-L-43480100	GETRequest	Success
Active firmware signature	9898100B	GETRequest	Success
Active firmware identifier 1	aM100-L-43480100	GETRequest	Success
Active firmware signature 1	2AF03FF8E59A69643A556A87D37F8519A6803725514132617FE0B25CA604E3AF34E380375754E0B3AC1EE0C6E961437CF08101E609488FA13C353E77C2	GETRequest	Success
Active firmware build date 1	241203	GETRequest	Success
Active firmware build date	240612	GETRequest	Success
boot firmware identifier	Wasion-aMeter-BOOT-V1.0-20231125	GETRequest	Success

Figure 4 - Version details collected from aMeter100

The same firmware verification can be done with the aMeter300 (Figure 5)



Attribute Name	Read Value	Operation	Result
COSEM logical device name	WSE00000000000016	GETRequest	Success
Device ID 1, manufacturing num...	243000001	GETRequest	Success
Device ID 2	00000016	GETRequest	Success
Device ID 7	V1070303	GETRequest	Success
Active firmware identifier	aM300-L-63480100	GETRequest	Success
Active firmware signature	4B83D62A	GETRequest	Success
Active firmware identifier 1	aM300-L-63480100	GETRequest	Success
Active firmware signature 1	7C44B87C6A5A5287B442439683E7CC78FEC8BD8915047141AD83DD17540421E1495CA7299C90F3662BAC4CEB45C81B987CA82659B6C682BD783C9A9B4BD4	GETRequest	Success
Active firmware build date 1	241203	GETRequest	Success
Active firmware build date	240612	GETRequest	Success
boot firmware identifier	Wasion-aMeter-BOOT-V1.0-20231125	GETRequest	Success

Figure 5 - Version details collected from aMeter300

## **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 [AGDv1.5] 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 Evaluator has followed the preparation steps for the TOE defined in [AGDv1.5] and [UMv1.0] for the evaluated configuration.

The evaluated configuration of the TOE includes the items listed in Table 3.

For more details, please consult section 1.4 of the Security Target [ST] and [AGDv1.5].

### **10.1 TOE operational environment**

The LVS reproduced the operational environment consistent with [ST], [AGDv1.5] and [UMv1.0].

## **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 at LVS premises.

The Evaluators verified the configuration of the test environment, including the TOE, and found it to be consistent with the AGD documentation [AGDv1.5] and the Security Target [ST].

### **11.2 Functional tests performed by the Developer**

#### **11.2.1 Testing approach**

The Developer provided 34 test cases, the first half of the test cases are covering specific functions on each TSFI and additionally tamper protection, upgrade or key generation.

The second half is the implementation of the test cases described in [SM-MSR-PP] section 6.4.1.7. (Protection Profile).

#### **11.2.2 Test coverage**

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 correct 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**

Before initiating the testing activity, the Evaluators verified that the TOE was configured correctly.

Evaluator executed all the 34 test cases. These covered the corresponding refinements of the protection profile [SM-MSR-PP] and other TOE functionalities too.

The Evaluator already examined that the Developer's testing effort was to cover the whole TSF according to the [SM-MSR-PP]. Since no security feature is missing from the Developer's testing effort, the Evaluator created three additional test cases where further investigation was needed. The Evaluator created 3 more additional test cases based on the Developer tests to verify the TOE with additional inputs:

- Further test the audit capabilities of the TOE.
- To validate the TOE's behavior with respect to privilege management.
- Examine and check some of the parameters has to be set to operate the TOE accordingly.

### 11.3.2 Test results

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

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

### 11.4 Vulnerability analysis and penetration tests

The Evaluators conducted vulnerability analysis and penetration testing activities using [SM-MSR-PP] as a basis for the applied methodology.

A search on public vulnerabilities on TOE and TOE components (e.g. hardware) has been conducted. The analysis confirmed that there are no public vulnerabilities exploitable with the TOE implementation and configuration.

The Evaluators conducted penetration testing activities on the same instance of the TOE configured for functional and independent tests.

The following attack scenarios were verified:

- Frame Counters Unenforced (Lack of Replay Protection).
- Manipulation of Global unicast key.
- Absence of service mode or safe mode accessible during power up process.
- Store blocking conditions after powering off.
- Examination of active interfaces.
- Brute Force (local RS-485 port).
- Manipulating or guessing the Smart Meter's Random Number Generator.
- Protection from manipulation of users lockout.

The Evaluators could then conclude that the TOE is resistant to a basic attack potential in its intended operating environment. No exploitable or residual vulnerabilities have been identified.