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. *(Certificate No.)*	01/2026
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/CCL/05/2024/RC, v 1.1.
Decorrenza *(Date of 1st Issue)*	8 gennaio 2026
Nome e Versione del Prodotto *(Product Name and Version)*	Sanxing SX601/S12U26 and SX631/S34U28 Smart Energy Meters
Sviluppatore *(Developer)*	Ningbo SANXING Smart Electric Co., Ltd.
Tipo di Prodotto *(Type of Product)*	Altre categorie – Smart meter
Livello di Garanzia *(Assurance Level)*	EAL3+ (ALC_FLR.3) conforme a CC Parte 3
Conformità a PP *(PP Conformance)*	Protection Profile for Smart Meter Minimum Security requirements. Version: 1.0, date: 2019-10-30
Funzionalità di sicurezza *(Conformance of Functionality)*	Funzionalità conformi a PP, 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, 26 gennaio 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 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.*

Organismo di Certificazione della Sicurezza Informatica

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

SANXING SX601/S12U26 and SX631/S34U28 Smart Meters

OCSI/CERT/CCL/05/2024/RC

Version 1.1

26 January 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	08/01/2026
1.1	OCSI	Editorial revision	26/01/2026

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
AES	Advanced Encryption Standard
AES-GCM	Advanced Encryption Standard - Galois/Counter Mode

APDU	Application Protocol Data Unit
API	Application Program Interface
ARM	Advanced RISC Machine
COSEM	Companion Specification for Energy Metering
CRC	Cyclic Redundancy Check
DLMS	Device Language Message Specification
GMAC	Message authentication code in Galois/Counter Mode
GPRS	General Packet Radio Service
HES	Head-End System
HHU	Hand-Held Unit
LN	Logical Name
LTE-M	Long-Term Evolution Machine Type Communication
OS	Operating System
PRNG	Probabilistic random number generator
QSCD	Qualified Signature Creation Device
RISC	Reduced Instruction Set Computer
TLS	Transport layer Security

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

[NIS4] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 4/23, versione 1.1, 21 agosto 2023

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

4.2 Technical documents

[ETRv3] "Evaluation of SANXING SX601 1 phase and SX631 3 phase Smart Meter" Evaluation Technical Report, date 2025-10-03, Version 3, CCLab Software laboratory.

[ETRv4] "Evaluation of SANXING SX601 1 phase and SX631 3 phase Smart Meter" Evaluation Technical Report, date 2025-11-13, Version 4, CCLab Software laboratory.

[SX631] Smart Meter User Manual Model S34U28, date: 2024-07, version: v1.5

[SX601] Smart Meter User Manual Model S12U26, date: 2025-02, version: v1.6

[SM-MSR] 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

[AGD] AGD Documentation SANXING SX601 and SX631 Smart Meters, date 2025-11-04, version 1.7

[ST] Security Target, SANXING SX601 and SX631 Smart Meters - Evaluation Assurance Level (EAL): EAL3 augmented with ALC_FLR.3 – date: 2025-11-04, version 2.0 (PUBLIC)

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 up to EAL4 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 claim assurance components up to EAL2 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the product "SANXING SX601/S12U26 1-phase and SX631/S34U28 3-phase Smart Meter", developed by Ningbo SANXING Smart Electric Co., Ltd.

The TOE is the SX601 and SX631 family of Smart Meters designed for measuring and monitoring energy parameters.

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 and 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 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 "SANXING SX601/S12U26 1-phase and SX631/S34U28 3-phase Smart Meter" 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	SANXING SX601 1 phase and SX631 3 phase Smart Meter SX601 • Hardware version: S12U26 S15.Y4.J0 M12 • Metrological FW version: V0.03.10 • Application FW version: E.S12U26.HU.007179.V1.00.33 SX631 • Hardware version: S34U28 S38.Y2.J0 M11 • Metrological FW version: V0.10.10 • Application FW version: E.S34U28.HU.007178.V1.00.33
Security Target	Security Target SANXING SX601 and SX631 Smart Meters Evaluation Assurance Level (EAL): EAL3 augmented with ALC_FLR.3, Ningbo SANXING Smart Electric Co., Ltd., version 2.0, November 04th 2025. [ST]
Evaluation Assurance Level	EAL3 augmented with ALC_FLR.3
Developer	Ningbo SANXING Smart Electric Co., Ltd
Sponsor	Ningbo SANXING Smart Electric Co., Ltd
LVS	CCLab Software Laboratory (Budapest site).
CC version	3.1 Rev. 5
PP conformance claim	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 Strict conformance
Evaluation starting date	27 May 2024
Evaluation ending date	3 October 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 refer to the Security Target [ST].

The TOE "SANXING SX601/S12U26 1-phase and SX631/S34U28 3-phase Smart Meter" is an electronic device that tracks how much electricity the user uses and sends this information directly to electricity provider for monitoring and billing purposes. Smart meters allow for two-way communication between hosting premises and the electricity company. This means smart meters not only record electricity use in detail but also provide information on when and how the users use energy.

The SX601 and SX631 family is designed for measuring and monitoring energy parameters. The name of the 1phase Smart Meter is SX601, and the 3phase is SX631. The TOE can be programmed and configured locally through 2 interfaces, which are the optical interface (P0) and the RS-485 interface. The TOE also has remote access. through cellular network. It supports the following standards: GPRS/4G, LTE-M. The meter does not measure its own consumption.

There are 2 types of devices, the only difference between them is the metrological part of the meters. SX601 is a 1-phase and SX631 is a 3-phase smart meter. The two devices are otherwise equal.

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

7.3.1 TOE architecture

TOE architecture and physical boundaries are illustrated in Figure 1. As anticipated, there are 2 types of devices, the only difference between them is the metrological part of the meters. SX601 is a 1-phase and SX631 is a 3-phase smart meter. The two devices are otherwise equal. In particular, the firmware has two parts: metrological part and application part. The metrological part of the firmware is separated from all other firmware modules. The application part implements all the application functions except the functions in metrological area. For example, communication process, event log, display, tariff etc.

Type	Hardware version	Metrological FW version	Metrological FW version CRC	Application FW version	Application FW version CRC
SX601	S12U26 S15.Y4.J0 M12	V0.03.10	F289	E.S12U26.HU.007179.V1. 00.33	3CD3
SX631	S34U28 S38.Y2.J0 M11	V0.10.10	A434	E.S34U28.HU.007178.V1. 00.33	B3DC

Table 1 – SX601 and SX631 firmware identification

Table 1 indicates SX601 and SX631 differences and uniquely identifies their firmware.

A checksum generated with CRC16 is used to verify that the firmware version has not changed at startup.

Firmware integrity protection relies on two main measures:

1. Anti-tampering measures (see [ST] section 7.4.1);
2. Digital signature protected firmware updates (see [ST] section 7.6[1]).

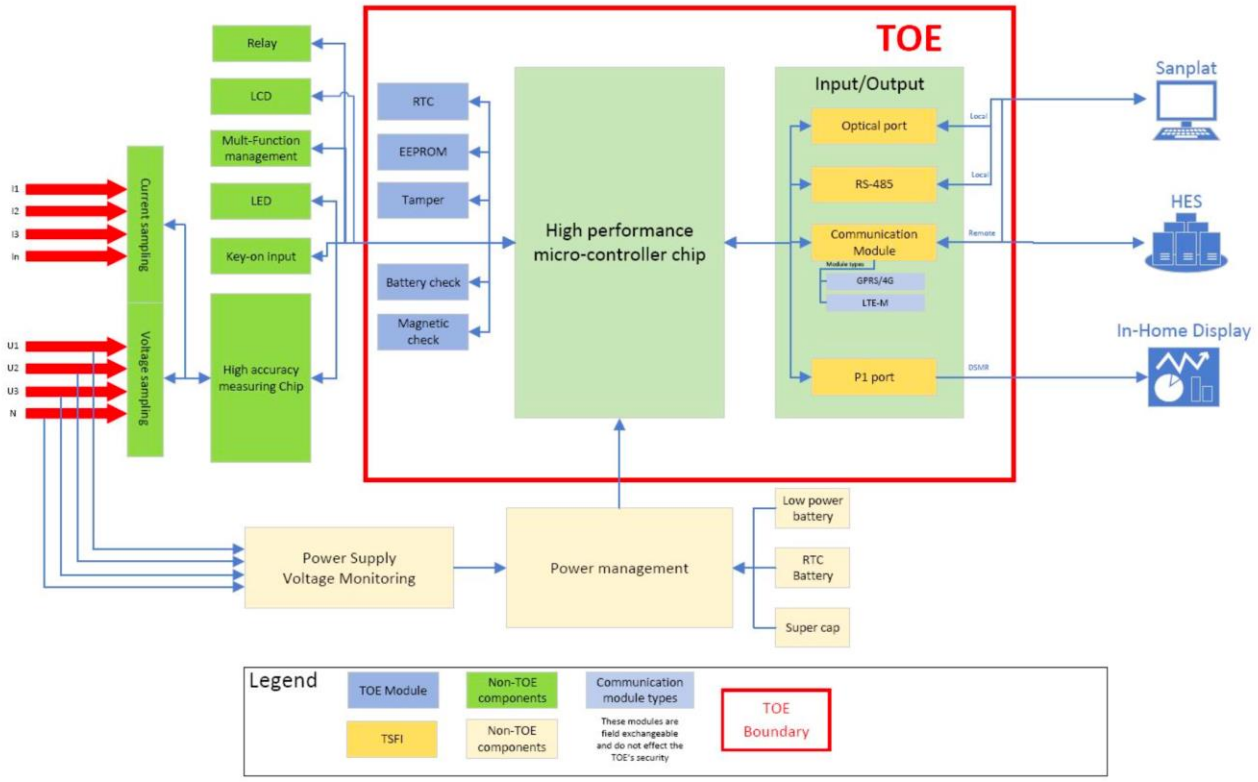

Figure 1 – TOE architecture and physical boundaries

The High-performance micro-controller chip subsystem is the main processing unit of the TOE. The subsystem does not have any direct TSFIs, but it is using the I/O subsystem's TSFIs through the I/O subsystem.

The Input/Output subsystem contains all the communication modules. These modules are responsible for the interactions with the users of TOE (configuration, data read, parametrization, etc.).

The I/O subsystem contains 4 interfaces without individual modules. The additional interfaces directly connected to the subsystem are the following:

- Communication Module. Remote systems (e.g. HES for remote reading/control of smart meters) communicates with the ARM system through this module. The TOE supports several types of communication modules, such as GPRS/4G, LTE-M. Module parameters can be set by proprietary software (Sanplat) locally and also remotely through a DC and Gateway. The module can support

[1] For firmware upgrades the firmware package is always protected by a digital signature and an AES_GCM_128 tag.

both eSIM and SIM card. Communication module supports upgrade locally, by optical interface, and remotely via radio interfaces.

- Optical port. It can support bi-directional communication with HHU or PC software. The optical port on the meter cover has a Metallic ring inside. This interface complies with IEC 62056-21MODEE and IEC 62056-46.
- RS-485. It can support bi-directional communication with HHU or PC software. This interface complies with TIA/EIA-485-A and IEC 62056-46. The baud rate for the communication is 9600 bps.
- P1 port. The P1 port is a read-only interface, meaning you can only receive data from it and cannot send commands to the meter. The meter has a single P1 port, which communicates at a speed of 115200 bps and uses IEC 62056-21 mode D. The connector for the P1 port is an RJ12 type. The metering system has an RJ12 female socket, and external devices (such as the OSM, or Other Service Module) connect to it using a standard RJ12 male plug.

Real-Time Clock (RTC): the RTC provides the local time for every time related record or function. All the functions where a reliable time is required like event logs and alarm messages are using the times tamp from the RTC module.

EEPROM: secure storage is a reserved space in EEPROM which is cryptographically protected. In the secure storage the TOE stores all the necessary global encryption, authentication, and master keys.

Tamper: the TOE has several solutions implemented for physical tamper detection, and it is sealed in several points to prevent undetectable activities.

Open cover detection: there are 2 outer covers, the module, and the terminal cover, which are protected with seals in the first place, and there are physical switches (buttons) under the terminal cover. If the TOE is assembled, if any of the covers or housing is removed the corresponding switch will pop up and the tamper will be detected.

Pull out module detection: the module is secured to the module cover. There is a single pin on the communication module for detection. When the module is in place, the output level is high, when the module is unplugged, the output level is low.

Battery check: the purpose of this module is indicating battery replacement to avoid clock invalidation. The battery check module communicates with the Communication Module. If the battery capacity is low, it will ask the actual time and date for the timestamp and send the gathered information the High-performance micro-controller chip to create an event log entry with appropriate event description (what happened) and timestamp.

Magnetic check: the module detects magnetic interference around the TOE. The TOE has a built-in hall sensor that detects the changes in the magnetic field. When the external magnetic field interference occurs, the hall sensor will output a low level (digital 0) and an alarm will be sent immediately, and an even log entry is recorded.

TOE case is shown in Figure 2. There is a LCD display and 2 push-buttons. The 2 buttons perform two different functions, the first button's function is to scroll the information on the LCD display, the second button's function is to reconnect the circuit breaker. The second button is sealable, so its pressing can be traced.

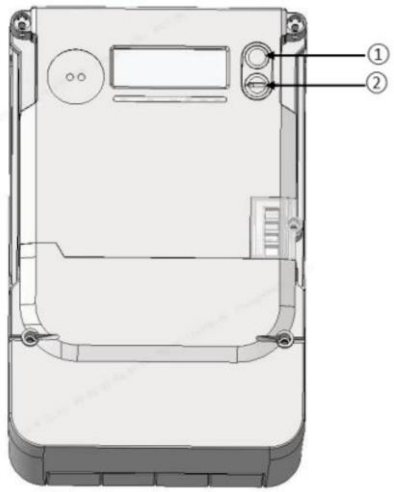

Figure 2 – TOE case

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 summarized in the following sections.

7.3.2.1 Local data security

The meter has sealed screws to prevent unauthorized access and support serial device detections. After establishing the serial port connection signals exposed by the serial port can be set for device detection.

There are two different set of seal protection. First set protects terminal cover while the second protects meter cover. If seals are tampered with and either of the terminals is removed, then the corresponding events are recorded in the fraud event log. In case of terminal cover open, the dedicated counter (Cover opening counter) is incremented as well.

There are three separate switches that detect if the terminal cover, the meter cover, or the front cover have been opened or closed. Data access security is controlled by the “Association LN” object. Each COSEM server, or logical device, can allow connections from different clients, each with its own role and specific access rights. There are six access roles supported with different keys: management, technician, reader, pre-established, public and upgrade. Each access level has different authentication keys. Data transport security relies on applying cryptographic protection to xDLMS APDUs. This is achieved via several security mechanisms. The first mechanism is incorporated in application association request with the COSEM application context. When the meter receives the frame counter value in the data frame sent by the client is less than or equal to the frame counter value recorded in the meter, the meter will refuse communication and record corresponding events. A security suite defines which cryptographic algorithm is used to keep messages secure (see below).

7.3.2.2 Communication security

Table 2 summarizes TOE encryption capabilities for secure communications.

Security suite ID	Suite name	Authenticated encryption	Digital signature	Key agreement	Hash	Key transport
0	AES-CGM	AES-CGM-128	-	-	-	AES key wrap 128 bit
1	ECDSA-AES-CGM-128-SHA-256	AES-CGM-128	ECDSA with P-256	-	SHA-256	AES key wrap 128 bit
2		AES-CGM-256	ECDSA with P-384	-	SHA-384	AES key wrap 128 bit

Table 2 - DLMS/Cosem security suite configurations

Even though the TOE can work in the above-mentioned security suites, only Security Suite 0 is part of the evaluation.

The TOE will be delivered with unique passwords and keys to the customer, which will be loaded by the manufacturer. The common method is to use PGP encryption, before the transmission of the corresponding file, share their public keys with each other, and then decrypt with their private keys; The channel for transferring files can be via email, or can add security by setting up a dedicated VPN.

Push messages: DLMS messages can be sent automatically ('pushed') to a destination without needing a direct request. A push message is sent whenever a specific trigger event occurs, such as:

- Reach the scheduled time
- The value of local monitoring exceeds the threshold
- Local events (such as power failure, power on, push button, meter cover opening, etc.)

Push messages are both authenticated and encrypted.

7.3.2.3 Firmware upgrade

The TOE:

- Support broadcast upgrade and point-to-point upgrade.
- Support continuous upgrade after communication interruption.
- If some upgrade packages fail to be transmitted, supplementary transmission of these upgrade packages is supported.
- Support locally and remotely
- The meter action digital signature mechanism for FW integrity is based on message encryption.

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].

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] have been carried out.

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

The evaluation was completed on 3 October 2025 with the issuance by LVS of the Evaluation Technical Report v3 [ETRv3], which was approved by the Certification Body on November 4th 2025 Then, the Certification Body issued this Certification Report. Evaluation Technical Report v4 [ETRv4] was finally issued following a new version of the ST.

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 v3 [ETRv3] issued by the LVS CCLab Software Laboratory (Budapest site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "SANXING SX601/S12U26 1-phase and SX631/S34U28 3-phase Smart Meter" 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 3 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 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
Functional specification with complete summary	ADV_FSP.3	Pass
Architectural design	ADV_TDS.2	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
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
Systematic Flaw remediation	*ALC_FLR.3*	*Pass*

Assurance classes and components		Verdict
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
Vulnerability analysis	AVA_VAN.2	Pass

Table 1 - 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 "SANXING SX601/S12U26 1-phase and SX631/S34U28 3-phase Smart Meter" 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 described in section 3.2 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 [SX601] and [SX631], CC guidance [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

For the physical delivery of electricity smart meters, before delivery, the delivery parameters will be confirmed with the customer, such as electricity meter parameters to be configured, how to package the electricity meter, what stickers are needed, the size of the packaging, the size of the pallet, etc. After reaching an agreement and confirmation with the customer, delivery will be carried out according to the demand via a courier delivery.

When the customer receives the product, physical and procedural checks shall be done in accordance with user manuals ([SX601] and [SX631]) and CC guidance [AGD]. The hardware acceptance procedures can be found in [AGD] section 3.1.1.

The documents or software upgrade packages will be delivered with unique passwords and keys to the customer. The firmware is always preloaded upon delivery.

The SHA-256 hash values corresponding to the delivered documents will be summarized in a table and sent to the customer. The customer will be able verify the integrity of the files through the corresponding hash value.

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 has followed the preparation steps for the TOE defined in [AGD], [SX631] and [SX601] for the evaluated configuration.

The evaluated configuration of the TOE includes the following items:

Type	Hardware version	Metrological FW version	Metrological FW version CRC	Application FW version	Application FW version CRC
SX601	S12U26 S15.Y4.J0 M12	V0.03.10	F289	E.S12U26.HU.007179.V1. 00.33	3CD3
SX631	S34U28 S38.Y2.J0 M11	V0.10.10	A434	E.S34U28.HU.007178.V1. 00.33	B3DC

Table 5 – SX601 and SX631 evaluated configuration

For more details, please consult sect. 1.4 of the Security Target [ST] and [AGD].

10.1 TOE operational environment

The LVS reproduced the test environment consistent with [ST], [AGD] [SX631] and [SX601].

The Evaluator's test environment is represented in Figure 3.

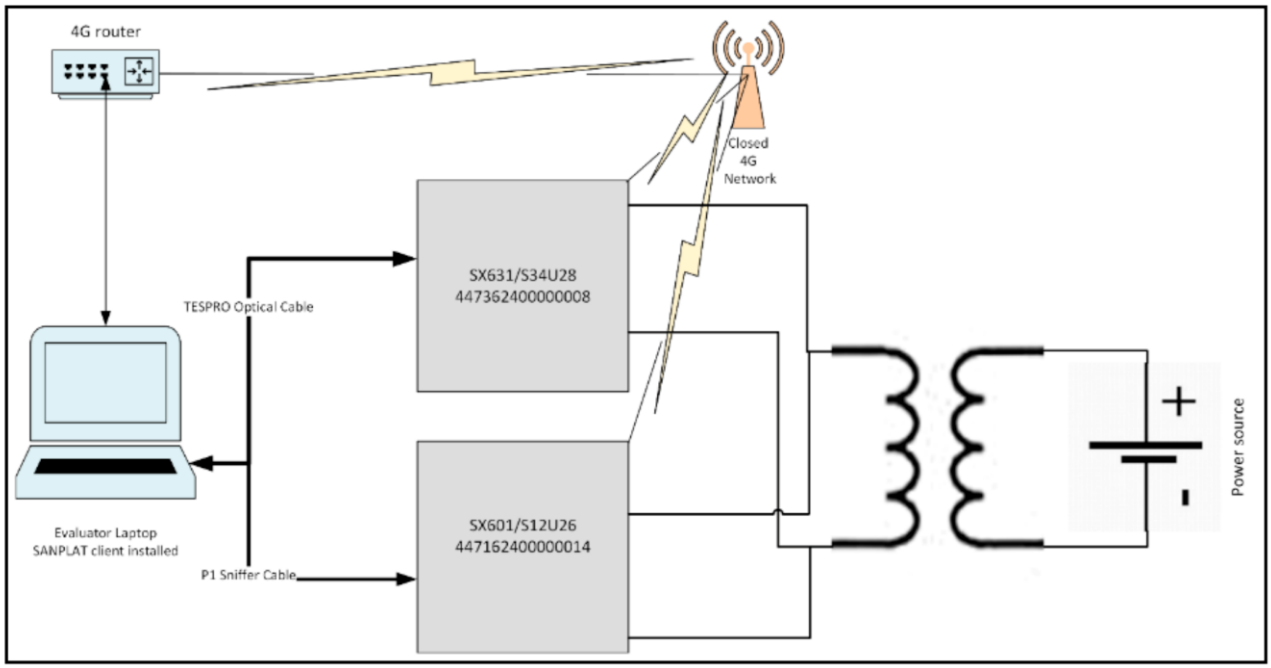

Figure 3 – TOE operational environment

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 AGD documentation [AGD] and the Security Target [ST].

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer used a very detailed testing approach, covering the functionalities of the TOE with manual tests. Namely, different test cases were designed, for the general purpose of guaranteeing each security function and aspect of the TSF was tested and verified.

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 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.

The Evaluators verified that the developer's testing covered the entire TSF, as required by the Protection Profile (PP). Since the developer's tests covered all security features, the Evaluators only needed to create four additional test cases for areas that required further investigation. These four test cases were based on the developer's tests and were designed to test the TOE with extra inputs:

TEST1 - The TOE will reject every message from the same address for 60 seconds after 3 times of authentication failure. When the freeze time ends, the user is able to authenticate.

TEST2 - To verify that the integrity of the messages exchanged through wireless networks is also secured with the symmetric encryption and the frame counter protects the TOE from replay attack.

TEST3 - To verify that the public client of the TOE is able to read only allowed basic parameters and the reading and writing of other parameters is not possible.

TEST4 – The TOE will accept firmware updates only from the "Upgrade" role.

11.3.2 Test results

All Developer's tests were run successfully; the Evaluators verified the correct behaviour 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-SMR] as a basis for the applied methodology.

A search on public vulnerabilities on TOE and TOE components (e.g. OS) have 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 testing.

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.