Holley Technology Ltd.

Security Target

Holley's Smart Meters：DDSD285, DDSY283SR, DTSD545 and DTSY541

Evaluation Assurance Level (EAL): EAL 4 augmented with ALC_FLR.3

TOE Reference:	Holley's Smart Meters: DDSD285, DDSY283SR, DTSD545 and DTSY541
Version	V1.9
Date	2026-1-21
Classification:	PUBLIC

Version history

The following table contains the changes made to the different versions of the ST.

Version	Date	Author	Description
V 1.0	2024-12-24	Holley Technology Ltd.	The first version of the Security Target.
V1.1	2025-01-06	Holley Technology Ltd.	Refinement of the content of the Audit Generation Component and addition of appendices related to the description of audit events.
V1.2	2025-01-23	Holley Technology Ltd.	Modify 1.3 TOE Reference to standardise TOE names throughout the text.
V1.3	2025-02-10	Holley Technology Ltd.	Add a document cover page.
V1.4	2025-02-24	Holley Technology Ltd.	Review the full text and modify the nonconformities.
V1.5	2025-05-16	Holley Technology Ltd.	Amendments based on ASE 1st analysis cycle.
V1.6	2025-07-02	Holley Technology Ltd.	Amendments based on ASE 2nd analysis cycle.
V1.7	2025-08-18	Holley Technology Ltd.	Update the firmware package version number in section 1.3.
V1.8	2025-12-15	Holley Technology Ltd.	Update the document version and adjust the description.
V1.9	2026-1-21	Holley Technology Ltd.	Update section 1.3.

Table of Contents

1. ST introduction

1.1 Introduction

The main purpose of smart meters is to ensure data security while increasing the transparency of consumers (end users) about their energy consumption. Through the analysis of users' electricity consumption behavior, it helps users optimize their electricity consumption habits, so as to reduce energy consumption and use costs.

In addition to data processing functions, smart meters can also generate smart tariff, providing network operators and consumers with efficient energy control methods. Through smart meters, users' electricity consumption data can be recorded, processed, and transmitted, so higher requirements for data protection and security are put forward.

The target of evaluation (TOE) defined in this document is a smart meter with models of Holley's Single Phase and Three Phase Smart Meters. 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 modern electrical energy metering devices with the functions 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. This document describes the security objectives of Holley's Single Phase and Three Phase Smart Meters, and the 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 and that only authorized and trusted AMI System or maintenance personnel can access the meter. It can effectively prevents meter data from being maliciously tampered with, avoiding potential losses to users and power systems.

1.2 ST Reference

Title:	Holley's Smart Meters: DDSD285, DDSY283SR, DTSD545 and DTSY541 SECURITY TARGET
Version:	V1.9
Date:	2026.1.21
Author:	Holley Technology Ltd.
CC-Version:	CC:2022 Release 1
Evaluation Assurance Level:	EAL 4 augmented with ALC_FLR.3
Keywords:	Smart Metering, Security Target, Meter, ST
PP Based:	This ST is based on the Protection Profile for Smart Meter Minimum Security requirements[1].

1.3 TOE Reference

The unique reference to TOE is shown in Table 1.

TOE Full Name	Holley's Smart Meters：DDSD285, DDSY283SR, DTSD545 and DTSY541
TOE Version	Single Phase Meter 1 - DDSD285 TOE Software Version: D285WI0036002503 TOE Hardware Version: 20-X33-11VS1.0 Single Phase Meter 2 - DDSY283SR TOE Software Version: D285WI0036002503 TOE Hardware Version: 20-X33-11VS1.0 Three Phase Meter 1 - DTSD545

	TOE Software Version: D545WI0036002503 TOE Hardware Version: 20-X042-11V1.1 Three Phase Meter 2 - DTSY541 TOE Software Version: D545WI0036002503 TOE Hardware Version: 20-X042-11V1.1
TOE Short Name	Holley's Single Phase and Three Phase Smart Meters
TOE Developer	Holley Technology Ltd.

Table 1：TOE reference

For single-phase meters DDSD285, DDSY283SR and three-phase meters DDSD285, DDSY283SR, they have a unique TOE identifier: Holley's Smart Meters: DDSD285, DDSY283SR, DTSD545 and DTSY541. The current meter type (e.g., DDSD285, DDSY283SR, DTSD545, or DTSY541) will be clearly labeled on Holley's Single Phase and Three Phase Smart Meters cover. Single-phase meters are labeled as DDSD285 or DDSY283SR, while three-phase meters are labeled as DTSD545 or DTSY541. Users can view the firmware identifier in the PC Software (HLMCS). The hardware version can be found on the internal PCB, which requires disassembling Holley's Single Phase and Three Phase Smart Meters.

The method by which a unique reference to the TOE is created/generated is shown below:

Holley's Smart Meters：DDSD285
Software Version: D285WI0036002503
Hardware Version: 20-X33-11VS1.0

Holley's Smart Meters：DDSY283SR
Software Version: D285WI0036002503
Hardware Version: 20-X33-11VS1.0

Holley's Smart Meters：DTSD545
Software Version: D545WI0036002503
Hardware Version: 20-X042-11V1.1

Holley's Smart Meters：DTSY541
Software Version: D545WI0036002503
Hardware Version: 20-X042-11V1.1

Note:

For business purposes, Single Phase Meter has two different names (DDSD285 and DDSY283SR) on different markets. Despite the different names, they refer to the same TOE and they are identical. The same goes for Three Phase Meter. Three Phase Meter has two different names (DTSD545 and DTSY541) on different markets. Despite the different names,

they refer to the same TOE and they are identical.

Single Phase Meter and Three Phase Meter adopt the same functional design and safety architecture. The main software differences lie in the sampling of voltage and current signals: Single Phase Meter only samples the voltage and current of one phase, while Three Phase Meter needs to sample the voltage and current of phases A, B, and C simultaneously. These sampling differences are further reflected in the metrologically certified data of metering, the logs of power grid quality monitoring, and the displayed data. Moreover, due to the different numbers of sampling channels, there are also corresponding differences in the hardware design of the mainboard between Single Phase Meter and Three Phase Meter.

TOE comprises all meter hardware (including external communication interfaces), software, and the physical meter casing. The precise hardware boundaries of the TOE are detailed in Section 1.5.6.

The customer will receive guidance document with the TOE:

- Holley Technology Ltd Holley's Smart Meters: DDSD285, DDSY283SR, DTSD545 and DTSY541 AGD Documentation[16]

1.4 Specific terms

Various vocabularies exist in the area of Smart Grid, Smart Metering, and Home Automation. Further, the Common Criteria has its own vocabulary. This table clarifies the primary terminology used in this Security Target and is intended to prevent misinterpretation.

Term	Meaning
Administrator	Entity that has a level of trust with respect to all policies implemented by the TSF – see [2]. The Administrator role is referred to in SFRs in section 6.3 as a generic terms for a privileged role that has access to sensitive operations affecting the configuration and operation of the meter.
AMI **Advanced Metering Infrastructure**	Infrastructure which allows two way communications be-tween the Head-End System and the meter(s) and may be linked to other in-house devices.
Assurance	Grounds for confidence that a TOE meets the SFRs – see [2].
Consumer	End user of the metered quantity (electricity, gas, water or thermal energy)
Critical Event	An event that can take place in a smart meter and that is particularly significant for supply or security of the meter.

	(The critical events for a meter conformant with this Protec-tion Profile are defined as part of FAU_ARP.2 in section 6.3.6.1.)
Digital Signature	A cryptographic digital signature applied to data in order to al-low verification of its integrity and authenticity.
Direct Interface	An interface to the meter that does not involve access from external networks (WAN, Neighbourhood Network or Local Network).
EM	Electromagnetic
EU	European Union
Evaluator	The person or group that carries out a security evaluation of the TOE, using the criteria in [2], [3] and [4] and the associated methodology in [6].
External Entity	See 'User'.
Firmware	Executable code of a meter that is stored in hardware and that cannot be updated except via a secure update process (for the purposes of this Protection Profile the relevant up-date process is defined in FPT_TSU.1, see section 6.3.4.6).
Hand-Held Terminal Unit	Portable device for reading and programming equipment or meters at the consumer's premises or at the access point – see [8]
Local Network	Data communication network providing access to local (in-house/building) devices and / or other local networks – see [8].
MAC Message Authentication Code	A cryptographic checksum on message data, used to provide assurance that the sender of a message is who they claim to be and that the message is in the form originally sent (subject to the assumption that a cryptographic key is known only to the sender and the receiver).
Message	The term 'message' is generally used in this Security Target to refer to application-level messages. The minimum requirements in [7] that are the source for this Protection Profile require that security is implemented at the application-level, independent of protections that might be provided by the communication protocol.
Meter data	Meter readings that allow calculation of the quantity of electricity, gas, water or thermal energy consumed over a period. Meter data thus may include daily and monthly meter readings, interval readings and actual meter register values. Other readings and data may also be included (such as quality data,

	events and alarms) – see [8].
Metrology	Non TSF part of the TOE that converts a physical property in a digital signal. These functions are governed by the requirements of the Measuring Instruments Directive 2004/22/EC (MID)
MID	Measuring Instruments Directive 2014/32/EU
Neighbourhood Network	Data communication network providing access to several premises and / or other neighbourhood networks – see [8]
Operational Interfaces	Interfaces required for normal operation of the meter (all other accessible interfaces are disabled)
PP **Protection Profile**	Implementation-independent statement of security needs for a TOE type – see [2].
Role	The entitlement of a party to execute a set of one or more commands associated with the role name. (Note that this is different to the definition in [2], but con-sistent with the interpretation and refinement of "role" in this Security Target.)
SAR **Security Assurance Requirement**	A description of how the TOE is to be evaluated, using the standardised language of [4] – see section A.9.2 of [1].
SFR **Security Functional Requirement**	A translation of the security objectives for the TOE into a set of standardised functional requirements drawn from [3] (or as extended components, cf. section 8.3 of [2]) – see section A.9.1 of [2].
Sensor	Device that translates a physical property in an electric signal. A sensor can be a non TSF part of the TOE, or mounted exter-nally, for example a current transformer or a temperature sensor on a water return pipe.
Service Technician	Users who carry out any local installation, commissioning, maintenance or diagnostic activities on a meter. These activi-ties may be carried out over direct or network interfaces and service technicians may need access to privileged functions.
SM-CG	Smart Meters Coordination Group A joint advisory body, combining expertise and resources from the European Standardization Organizations (CEN, CENELEC and ETSI), that provides a focal point concerning smart meter-ing standardisation issues.
ST **Security Target**	Implementation-dependent statement of security needs for a specific identified TOE – see [2].

TOE **Target of Evaluation**	A set of software, firmware and/or hardware possibly accom-panied by guidance – see [2].
TSF **TOE Security Functionality**	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs – see [2].
TSF Data	Data for the operation of the TSF upon which the enforce-ment of the requirements relies – see [2].
User	Human or IT entity interacting with the TOE from outside of the TOE boundary (based on [2]).
WAN **Wide Area Network**	extended data communication network connecting a large number of communication devices over a large geographical area – see [8]
Wi-SUN	Wireless Utility Networks is a series of standard wireless communication networks based on IEEE 802.15.4 standards [9].
RS485	A commonly used serial communication standard called Recommended Standard 485. It was formulated by the Electronic Industries Association (EIA) and is mainly used for multi-point differential signal transmission, which has the advantages of strong anti-interference ability, long transmission distance, and support for multi-device communication [10].
P1 port	This interface is based on NEN-EN-IEC 62056-21 (electrical metering-data exchange for meter readings, tariff and load control-Part 21: direct local data exchange, 2002-05). The standard contains physical properties and protocol definitions of interfaces [11].
Optical port	Optical port is a contactless data communication interface, often used for data reading and configuration of smart meters and other equipment. It generally complies with international standard IEC 62056-21 (formerly IEC 61107), ensuring compatibility of data transmission between different devices [11].
ECDSA	Elliptic Curve Digital Signature Algorithm [12].
ECC256	A specific curve that uses a 256-bit key in Elliptic Curve Cryptography (ECC) [13].
VPN	A means of communication that realizes security, encryption, and privacy through a public network (such as the Internet) [14].
DLMS	Device Language Message Specification is an open standard used as a communication protocol between electrical energy

	metering equipment (such as smart meters) and other equipment (such as data acquisition systems or remote management systems) [15].
Client	In Device Language Message Specification **(**DLMS), the client refers to some logical roles in communication, such as Public, Administrator, Operator, Technician, etc.
Server	In Device Language Message Specification **(**DLMS), the server refers to the electric energy meter.
GUEK **Global Unicast Encryption Key**	GUEK is an encryption key used in message communication, mainly used to ensure the security of data in transmission and prevent data leakage and tampering..
GAK **Global Authentication Key**	GAK is a key used for identity authentication and message integrity verification in communications. It is mainly used to ensure the authenticity of the identities of both parties in communication, prevent unauthorized devices or users from communicating, and verify the integrity of messages during transmission to prevent data from being tampered with or forged.
HLMCS **Holley Meter Communication System**	For local or simulated remote communication between PC and Holley's Single Phase and Three Phase Smart Meters

Table 2：Vocabulary

See [2] for other Common Criteria abbreviations and terminology.

1.5 TOE Overview

1.5.1 Overview of TOE

Smart 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.

The following diagram illustrates the TOE architecture:

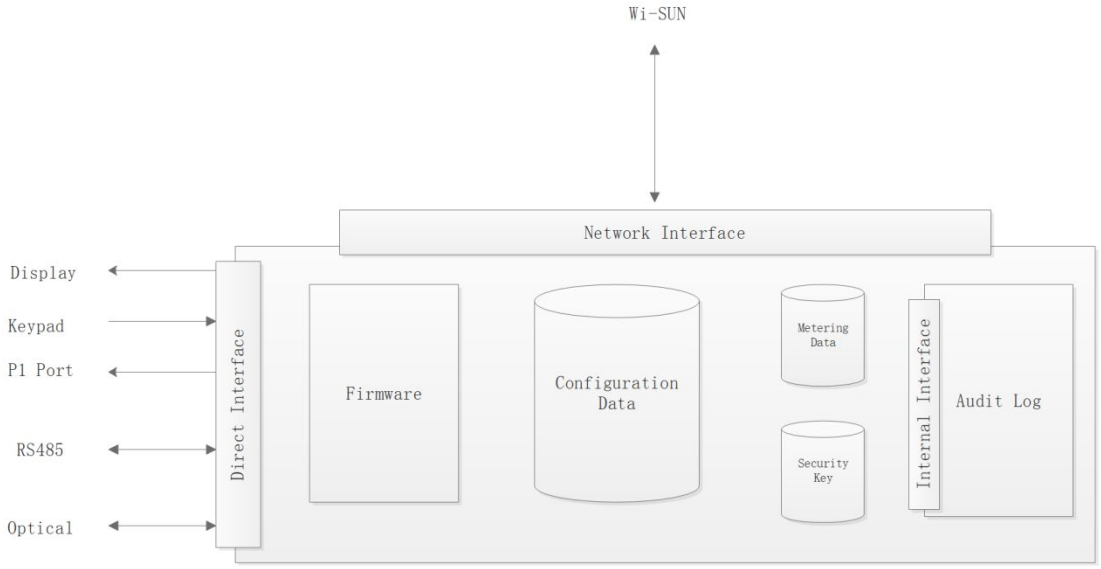


Figure 1：TOE Architecture

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 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 3：Components of TOE Architecture

1.5.2 Requirements on the operational environment of the TOE

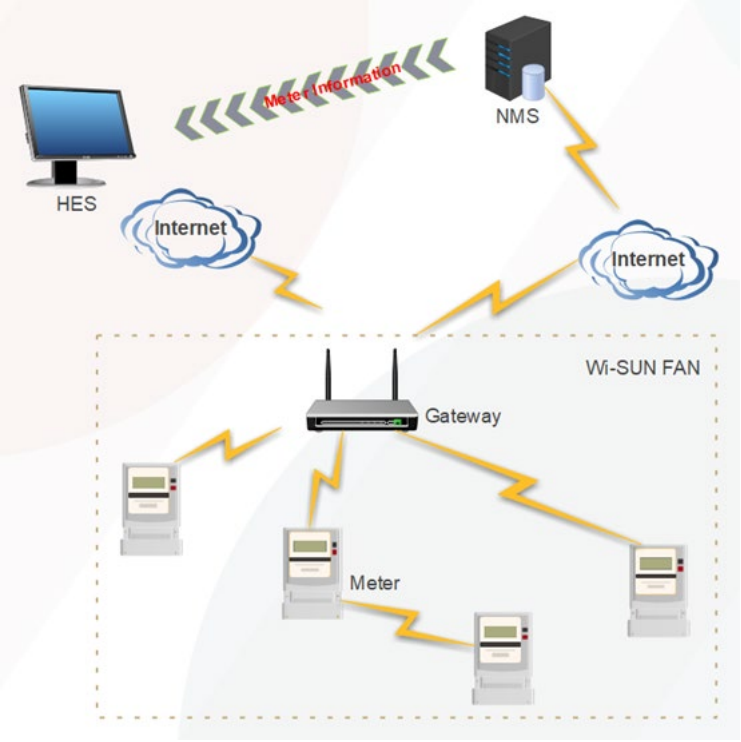


Figure 2： Requirements on the operational environment of the TOE

While requirements for the operating environment do not impact the TOE's security functionality, it is prudent to consider measures that ensure the availability of all services provided by the TOE.

Therefore, Holley's Single Phase and Three Phase Smart Meters shall be installed in a standard power grid, or the laboratory shall connect them to a standard AC power supply test equipment (specification: 220V–240V). Communication shall be established via one of the following interfaces: Wi-SUN module connected to the Internet through a link gateway; PC connected to the TOE via an RS-485 converter with an RJ12 interface; PC connected to the TOE via a 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.

1.5.3 TOE description

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 can communicate bidirectionally with the power company, and can transmit power consumption data and receive instructions such as relay control and power outage notifications. They also have functions of real-time monitoring, time-of-use billing, and fault detection, helping users optimize energy usage and improving the operational efficiency of the power company.

The following are the main functional modules and descriptions of Holley's Single Phase and Three Phase Smart Meters:

Electricity metering function
Accurately measure active and reactive power, supports time-of-use metering for peak/off-peak billing, and is capable of measuring both forward/reverse active power and four-quadrant reactive power for comprehensive energy data. It features a built-in microcontroller for extensive electricity consumption data storage.

Measurement and monitoring function
Measure voltage, current, frequency, power factor and instantaneous power in real time to monitor the operating status of the power grid.

Event recording function
Record significant events, including logs of grid connection monitoring, remote/local operations, and physical damage caused by human intervention or environmental factors. For each recorded event, the meter captures and stores the precise time stamp, its occurrence status,

and its resolution status.

Clock function

The built-in high-precision clock module provides a time reference and supports automatic calibration and power-failure maintenance.

Tariff Period function

Multi-tariff billing is supported, and time-sharing electricity statistics are performed according to preset time periods, which meet the requirements of time-of-use electricity price policies.

Freeze function

Freeze(such as daily freezing and monthly freezing) electrical energy data according to preset time periods, which facilitates the statistical analysis of power companies.

Load recording function

Regularly record the load curve data, including active and reactive loads, to analyze the user's electricity consumption behavior.

Security protection function

Provide password protection, permission management, tamper-proof design, and encryption of critical data to ensure data security.

Button function

The button interface enables the user to navigate display pages, perform local relay closure operations, and execute settlement functions via the local display. This provides a convenient and intuitive human-machine interaction experience, facilitating status monitoring and operational control.

Alarm function

Provide a sound and light alarm or a remote notification function to prompt abnormal power consumption behavior (such as overload and voltage loss). When abnormal conditions are detected, such as overload, voltage loss, reverse phase sequence, etc., the meter will issue an alarm in time.

Display function

An LCD or LED display provides clear, real-time visibility of key parameters including active/reactive power, voltage, current, and time, offering an intuitive and user-friendly interface.

Communication function

The data is transmitted to the server of the power company through communication technology

to realize remote monitoring and management. A variety of communication interfaces (such as RS485, Wi-SUN, Optical, P1, etc.) are supported to achieve remote data acquisition and control.

Signal output
Pulse output or status signal interface is provided to work with other devices.

Breaker opening and closing function
Support remote or local control circuit breaker to open or close operation, realizing power control and management.

Demand measurement function
Measure and record the maximum demand value and occurrence time of user electricity to meet power demand management.

Electric larceny-proof function
By monitoring and recording various abnormal operations, such as illegal opening of meter cover and terminal cover, magnetic interference, etc., the protection against potential electric larceny is realized. These functions usually monitor and prevent illegal operation by logging and timely reporting to ensure the security and stability of the meter.

1.5.4 TOE type

A smart electric energy meter (smart meter) is an energy metering device with advanced measurement, data processing, and communication functions, which is used to measure, record, and manage the use of electricity in real time. Smart meters not only can accurately measure the consumption of electrical energy, but also have functions such as data transmission, remote monitoring, and two-way communication. It can be interconnected with other equipment and systems (such as energy management systems, smart grids, etc.).

Smart electric energy meter is an important part of a modern power metering system, which can not only improve the accuracy and efficiency of power metering, but also provide more flexible and intelligent power management means for power companies and users. It promotes the development of smart grid and energy management.

1.5.5 TOE logical boundary

1.5.5.1 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 employed for encrypting information, safeguarding data against eavesdropping and tampering during transmission, and simultaneously providing integrity verification.

This mechanism can effectively prevent man-in-the-middle attacks and data forgery, and can ensure the security of Holley's Single Phase and Three Phase Smart Meters communication.

1.5.5.2 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.

An 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.

A reliable time stamping mechanism supplies a trusted time source for audit generation.

1.5.5.3 Audit

Holley’s Single Phase and Three Phase Smart Meters log security events, which encompass access control, electric larceny events, grid monitoring, parameter configuration, and other operational security events. Each event record includes a time stamp, event type, and event ID. Logs are stored in a structured format with unified time stamps and archived by event type. This comprehensive logging enables system analysis of user behavior and grid status.

Access-control permissions are defined for audit records, including read, modify, and delete operations. It also implements a storage-capacity limit for audit logs. Once the predefined log-count threshold is reached, the system automatically overwrites the oldest records, ensuring that new logs are retained and critical events remain continuously tracked.

1.5.5.4 Authentication & Authorisation

Authentication confirms the legitimacy of a user's or system's claimed identity, ensuring that each communicating party is verified as genuine. Access to data, parameters, and logs must be explicitly authorized by the client, with permissions enforced via access tokens (e.g., OAuth) or equivalent authentication mechanisms.

Holley’s Single Phase and Three Phase Smart Meters use ECDSA based on ECC256 (ECC Key Pair Generation) for mutual authentication to enhance security. The client and the server exchange authentication messages using AES-GCM-128 encryption to 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 so as to ensure security.

1.5.5.5 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 before accessing the data to avoid data leakage. In addition, when using the interface for data transmission, the data will be encrypted with 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.

1.5.5.6 Underlying Cryptography

Data and information in Holley's Single Phase and Three Phase Smart Meters are protected by AES-GCM-128 encryption, which provides confidentiality and integrity for real-time readings, historical data, and other sensitive information. The authenticated-encryption mode prevents data tampering during transmission and blocks unauthorized devices from forging data. Each encryption operation uses a unique nonce, ensuring that identical plaintext never produces the same ciphertext. Keys are regularly rotated to mitigate the risk of key compromise.

1.5.6 TOE physical boundary

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

Hardware part:

- 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, Wi-SUN communication module.

Software part:

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

Structural part:

- 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.

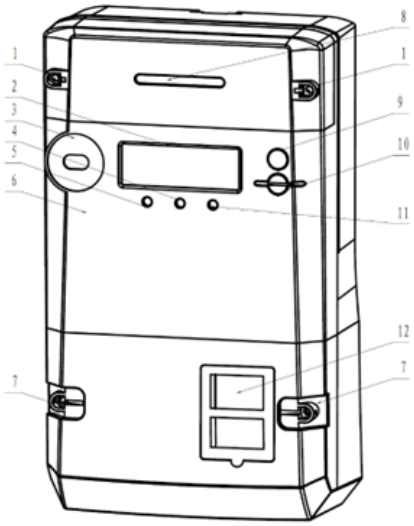


Figure 3：Meter Appearance

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 4：Meter Appearance Description

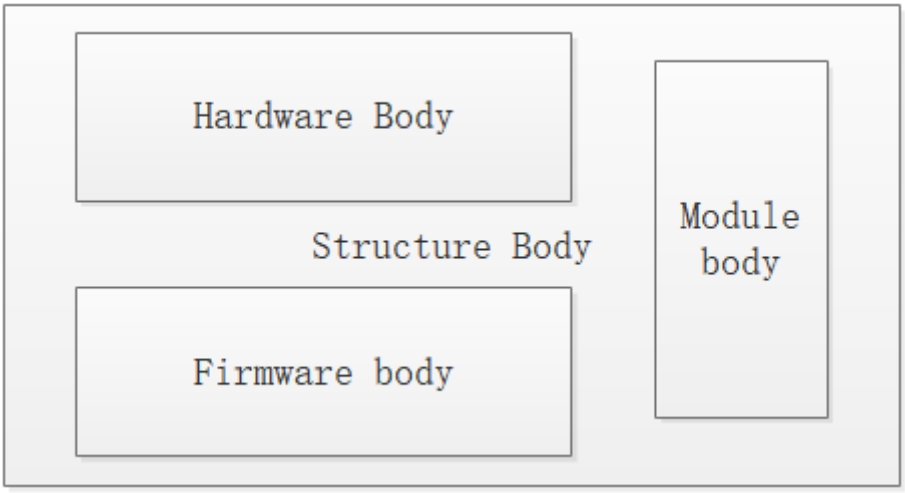


Figure 4：Meter Components

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.. It 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. It 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 . It provides physical protection for components while ensuring their secure positioning and organized layout.
Module Body	The communication module (including software and hardware) of Holley’s Single Phase and Three Phase Smart Meters. It is used to realize the connection with external systems, such as wireless communication module or wired interface module.

Table 5：Meter Components Description

Following successful testing and verification in Holley's production workshop, the smart meters are dispatched via Holley's designated logistics partner. Transport vehicles are equipped with GPRS tracking, and the delivery note includes the vehicle license plate number and driver's signature. Upon loading, the cargo is secured with corresponding seal numbers for integrity control.

Upon shipment, each package of smart meters includes a packing list and a unique sealing number. Upon receipt, customers should verify that the contents match the packing list and inspect the packaging integrity. After removing the meter cover, the printed information on the PCB board can be reviewed to confirm the hardware version. To verify the firmware version,

select the "Meter Firmware" option in the PC Software interface and click "Read" to retrieve the TOE's firmware version number. The PC Software version itself is displayed on its login interface.

1.5.7 TOE life-cycle

The life cycle of the product can be divided into the following stages：

1. Requirements analysis stage: Collect and sort out user requirements, clarify product functional objectives and performance indicators, analyze market trends and technical feasibility to provide a basis for subsequent design.
2. Product design stage: According to the requirements analysis results, determine the functional modules, technical architecture and user experience solutions of the product, and form detailed design documents, including hardware, software, and appearance design.
3. Product development stage: Carry out product research and development according to the design plan, including hardware manufacturing and software development. And realize the initial development of the product.
4. Testing and verification stage: Test the products comprehensively, including functional, performance, safety and reliability testing, to verify whether design requirements are met.
5. Product release stage: Confirm that the design and function of the product meet expectations, and prepare for formal external release.
6. Production stage: Carry out mass production to ensure product quality consistency and supply chain stability, and to prepare for market supply.
7. Installation and commissioning stage: Install the product into the actual use environment and conduct commissioning to ensure that the installation is correct and the product can work normally.
8. Formal operation stage: The product enters normal use, with user services and follow-up operation/ maintenance support provided. Configuration of operational parameters for Holley’s Single Phase and Three Phase Smart Meters will be finalized after product release, and executed solely by authorized personnel in a controlled environment to maintain product security and stability.

2. Conformance Claims

2.1 CC Conformance Claims

This ST has been developed using CC:2022 Release 1. This ST is CC:2022 Release 1, part 2[3] extended due to the use of FAU_ARP.2, FPT_TSU.1, FPT_BST.1 and FPT_TNN.1. This ST is CC:2022 Release 1 part 3[4] conformant; no extended assurance components have been defined.

2.2 PP Claim

This ST is based on the Protection Profile for Smart Meter Minimum Security requirements [1].

2.3 Conformance claim rationale

This ST is based solely on the Smart Meter PP [1].

The security problem definition (SPD) of this ST complies with the security problem definition in the Smart Meter PP [1], as this security target is based on the Smart Meter PP [1] and adds no other threats, assumptions and organisational security policies.

The security objectives of this ST comply with the security objectives in the Smart Meter PP [1], as this security target is based on the Smart Meter PP [1] and adds no other security objectives.

The security requirements of this ST comply with the security requirements in the Smart Meter PP [1], as this security target is based on the Smart Meter PP [1] and adds no other security requirements. Since the ST complies with CC:2022 Release 1 [CC], but the PP is based on CC v3.1 R5, the following adjustments need to be made:

1. Based on the PP's claimed compliance with CC v3.1 R5, the security functional component FAU_STG.1 is changed to FAU_STG.2. The updated FAU_STG.2 corresponds to the component in CC:2022 Release 1, with no change in functionality.

2. Based on the PP's claimed compliance with CC v3.1 R5, the security functional component FAU_STG.3 is changed to FAU_STG.4. The updated FAU_STG.4 corresponds to the component in CC:2022 Release 1, with no change in functionality.

3. Based on the PP's claimed compliance with CC v3.1 R5, the security functional component FCS_CKM.6 is added. The updated FCS_CKM.6 corresponds to the component in CC:2022 Release 1, with no change in functionality.

4. Based on the PP's claimed compliance with CC v3.1 R5, the security functional component FCS_CKM.4 is deleted. The updated corresponds to the component in CC:2022 Release 1, with no change in functionality.

5. Based on the PP's claimed compliance with CC v3.1 R5, the security functional extended component FCS_RNG.1 is deleted. The update corresponds to the component in CC:2022 Release 1, with no change in functionality.

Since the EAL was increased for the Security Target, there are some changes in the security assurance requirements:

1. Upgrade ADV_FSP.3 in PP to ADV_FSP.4;

2. Add ADV_IMP.1;

3. Upgrade ADV_TDS.2 in PP to ADV_TDS.3;

4. Upgrade ALC_CMC.3 in PP to ALC_CMC.4.

5. Upgrade ALC_CMS.3 in PP to ALC_CMS.4;

6. Add ALC_TAT.1;

7. Upgrade AVA_VAN.2 in PP to AVA_VAN.3.

2.4 Package Claim

This Security Target claims an assurance package EAL4 augmented by ALC_FLR.3 as defined in CC:2022 Release 1 Part 5[5] for product certification.

3.Security Problem Definition

3.1 Assets

The assets that Holley's Single Phase and Three Phase Smart Meters need to protect are listed below.

3.1.1 User Data

Asset	Description	Need for Protection
meter data	Power data, instantaneous data (including voltage, current, power, power factor) and other data	Integrity Authenticity
consumer log data	load record, daily settlement data, monthly settlement data, event record	Integrity Authenticity Confidentiality（For privacy reasons）
parameter data	Communication parameters, event parameters, load parameters, demand parameters, settlement parameters, etc.	Confidentiality Integrity
client data	The client ID supported by Holley's Single Phase and Three Phase Smart Meters. The client uses this ID to interact with the corresponding key.	Authenticity

Table 6：User Data Description

3.1.2 TSF Data

Asset	Description	Need for Protection
configuration data	Configuration data of Holley's Single Phase and Three Phase Smart Meters, such as parameter data for TOE to maintain normal operation, including RTC, security key data, event parameters, freezing parameters, metering parameters and other operating parameters.	Integrity Authenticity Confidentiality
firmware	Firmware update downloaded by the TOE,	Integrity

update	used to update Holley's Single Phase and Three Phase Smart Meters firmware.	Authenticity
firmware	Firmware of the Holley's Single Phase and Three Phase Smart Meters	Integrity Authenticity
encryption key	Key required for Holley's Single Phase and Three Phase Smart Meters operation	Integrity Authenticity Confidentiality
random number generator	The random number involved in the Holley's Single Phase and Three Phase Smart Meters encryption process	Integrity Authenticity
secure access serial number	The frame number management of the data frame will be involved in the encrypted communication process of Holley's Single Phase and Three Phase Smart Meters. The frame number is an important part to ensure that the data frames can be received and processed in the correct order, and it is also used to detect and correct possible errors.	Integrity Authenticity
metrologically certified data	Holley's Single Phase and Three Phase Smart Meters' metrologically certified data such as electricity, demand, instantaneous quantity.	Integrity Authenticity
interface configuration	Configure Wi-SUN network parameters.	Integrity Authenticity Confidentiality
audit logging	Recording of event logs during operation.	Integrity Authenticity
meter time	Time displayed by Holley's Single Phase and Three Phase Smart Meters.	Integrity Authenticity
alarm event configuration data	Holley's Single Phase and Three Phase Smart Meters can issue alerts for different event types.	Integrity Authenticity
time stamp	Holley's Single Phase and Three Phase Smart Meters provide reliable time stamp, synchronizing the RTC function time of the main chip.	Integrity Authenticity

Table 7：TSF Data Description

3.2 External Entities and Threat Agents

The external entities that interact with the TOE are as follows:

Entities	Description
direct user	Users that physically interact with the meter either via the LCD screen of Holley's Single Phase and Three Phase Smart Meters, or through a separate component connected via RS485 or Optical port.
network user	Connected to the head-end system via Wi-SUN connectivity, enabling the head-end to read or set meter data and parameters through the interface.
The following is the materialization of the above two types of users.	
AMI System	AMI System (Advanced Metering Infrastructure) is an important part of power grid management system. It is responsible for remote acquisition and monitoring of various data of power grid, including metering data, operation state and load information of power meter. It also provides data support and intelligent control for power grid operation and user management.
PC Software	The local communication software of Holley's Single Phase and Three Phase Smart Meters is an application program installed on PC (computer) or HHU (handheld terminal). It directly communicates with Holley's Single Phase and Three Phase Smart Meters through Operator. It realizes equipment configuration, data reading and maintenance, etc. It ensures efficient management and operation of Holley's Single Phase and Three Phase Smart Meters.

Table 8：Entities Description

Permission classification	Operation properties of permissions
Public	Authorized person, organization and consumers that own meter data can access meter data locally. This role does not require authentication.
Administrator	Administrator holds the highest permission including read and write permission to Holley's Single Phase and Three Phase Smart Meters. Administrator can access the data of Holley's Single Phase and Three Phase Smart Meters remotely and locally, configure the parameters of Holley's Single Phase and Three Phase Smart Meters, etc. Any communication initiated under the Administrator role requires authentication.
Operator	Operator holds the most permissions to the meter. This role can access

	meter data both remotely and locally, configure and modify parameters (excluding cryptographic keys). Any communication initiated under the Operator role requires authentication.
Technician	Technician who performing any installation, commissioning, maintenance or diagnostic activities on the meter holds partial permissions to the meter, including accessing Holley's Single Phase and Three Phase Smart Meters data and parameters through local communication, and configuring network parameters. Any communication initiated under the Technician role requires authentication.

Table 9：Permission classification Description

Threat agents are defined as individuals or groups that interact with the TOE through the same interfaces and methods identical to those available to the Direct User and Network User roles described above.

3.3 Threats

The following sections define the threats to Holley's Single Phase and Three Phase Smart Meters. The attacker described in each threat (i.e.,"threat agent") is an unauthorized subject: the attacker can appear as a completely unknown user or as one of the legitimate external entities in Section 3.2 (but in this case, the attacker will not have access to authentication or authorization data for the user or remote entity).

3.3.1 T.NetworkDisclosure Unauthorised data disclosure via network access

An attacker gains access via a network interface to data that requires protection of confidentiality (this is defined according to the policies implemented in the TOE, but typically includes private and secret keys, reference authentication/authorisation data such as unencrypted password or PIN values, and personal data such as consumption and financial data held on the meter). Access might be gained either from intercepting messages in transit to or from the TOE, or by executing a command (without authorisation) to remotely access data stored in the TOE.

3.3.2 T.DirectDisclosure Unauthorised data disclosure via direct access

An attacker gains access to data that requires protection of confidentiality (defined according to the policies implemented in the TOE, as described for T.NetworkDisclosure). Access might be gained either from intercepting messages in transit to or from the TOE, or by executing a command (without authorisation) via a direct interface to access data stored in the TOE (noting that, in additional to any network interfaces a direct attacker will also be able to use any other interfaces present on the meter, such as the display and keypad). In addition, the attacker might attempt unauthorised physical access to the meter by accessing internal interfaces and components (e.g. to access memory directly, without using the intended interfaces).

3.3.3 T.NetworkDataMod Unauthorised data modification via network access

An attacker gains access via a network interface to data in a way that enables unauthorised modification of data that is intended to require prior authorisation for modification (this is defined according to the policies implemented in the TOE). Such data might include meter data, configuration data (including the meter time) or other operating parameters (e.g. such as whether the meter is operating in credit or prepayment mode). Access might be gained from modifying, replaying or forging messages in transit to or from the TOE, or by executing a command (without authorisation) to remotely modify data stored in the TOE.

3.3.4 T.DirectDataMod Unauthorised data modification via direct access

An attacker gains access to data in a way that enables unauthorised modification of data that is intended to require prior authorisation for modification (defined according to the policies implemented in the meter). The scope of such data is defined as for T.NetworkDataMod. Access might be gained from modifying, replaying or forging messages in transit to or from the TOE, or by executing a command (without authorisation) via a direct interface to modify data stored in the TOE (noting that, in additional to any network interfaces a direct attacker will also be able to use any other interfaces present on the meter, such as the display and keypad). In addition, the attacker might attempt unauthorised physical access to the meter by accessing internal interfaces and components (e.g. to access memory directly, without using the intended

interfaces).

3.3.5 T.Malfunction Asset compromise due to TOE malfunction

The TOE may develop a fault that causes some other security property to be weakened or to fail causing the energy supply to be disabled. Where other security properties are weakened, this could affect any of the data assets and could result in any of the other threats being realised.

3.4 Organizational Security Policies(OSPs)

The TOE shall comply with the following organisational security policies.

3.4.1 P.Logging Logging security events

The TOE shall maintain a log of security events, and shall protect the log against unauthorized modification.

Application Note 1

This log is required to assist in diagnosis of faults, determination or confirmation of the meter state, and investigation of suspicious events.

3.4.2 P.Alarms Alarms sent for critical events

The TOE shall send an alarm message to a defined destination when any of a defined list of critical events occur. The alarm shall be sent at or before the meter's next default communication opportunity.

When any event in the defined critical information list occurs, the TOE stores alarm information to nonvolatile memory. Alarm records shall be obtained when the system periodically reads tasks.

Application Note 2

The specific destinations and events are not specified in the Protection Profile but are defined by the ST author[1].

[1] The definition of the events is required in FAU_ARP.2.

Note：
Key information：Modem cover open、 Magnetic influence、 Terminal cover open、 Meter cover open、Battery low、Watchdog reset、Random number generator failure、The network status has changed、Key replacement、Authentication failed.

3.5 Assumptions

3.5.1 A.ExternalData Protection of data outside TOE control

Where copies of data protected by the TOE are managed outside of the TOE, the relevant external applications and other entities must provide appropriate protection for that data.

3.5.2 A.AuditSupport Audit data review

The audit trail generated by the TOE will be collected, maintained and reviewed by an appropriate external audit role according to a defined audit procedure for the AMI.

Application Note 3

The audit trail consists of the log of security events recorded by the TOE.

3.5.3 A.InspectionSupport Meter integrity inspections

Each particular scheme for deployment and operation of an AMI will include measures (based on risk-analysis) to deter tampering with the meter and to support appropriate inspections of meter integrity.

Application Note 4

The term "scheme for deployment and operation of an AMI" applies to individual AMIs with distinct sets of standards, architecture definitions, and operational policies and authorities. The scheme is the point at which policies for activities such as inspections will be defined and enforced.

3.5.4 A.UniqueSubjectIDs Subjects have unique identifiers

External subjects will use unique identifiers in their interactions with the TOE. (Note that this requirement is derived from Requirement E in [7].)

4. Security Objectives

This section identifies and defines the security objectives for Holley's Single Phase and Three Phase Smart Meters and its operational environment.

4.1 Security Objectives for the TOE

The following security objectives describe security properties to be implemented by the TOE.

4.1.1 O.Authorisation Authorisation for access to TOE data and functions

The TOE shall check the authorisation of any direct or network entity requesting access to its data and functions, and shall grant or deny access based on the result of that check. The TOE shall respond to repeated, consecutive, unsuccessful authorisation attempts by temporarily denying all further authorisation requests for a defined period of time. Successful authorisation attempts shall expire after a defined period of time.

4.1.2 O.Messages Message protection

The TOE shall conduct all data exchanges in manner that provides security over the entire path between the TOE and the message originator/recipient (where the message recipient is the intended final receiver). The data exchange shall include protection against at least replay, unauthorised disclosure, unauthorised modification and forgery of authentic messages. The protection shall be independent of the underlying communication protocol.

4.1.3 O.DataAtRest Stored data protection

The TOE shall protect stored data against unauthorised disclosure and modification according to a defined policy for the types of data.

4.1.4 O.Crypto Approved cryptographic mechanisms

The TOE shall implement protection mechanisms using documented cryptographic mechanisms, random bit generation, and key management techniques, based on approved open standards.

Application Note 5

The authority for approval of the cryptographic standards is determined by the AMI scheme(s) in which the meter is intended to be used. It is intrinsic to this approval that it represents confirmation of the use of appropriate cryptographic parameters (e.g. algorithms, modes, initialisation values, key lengths).

4.1.5 O.Interfaces Non-operational interfaces disabled

The TOE shall disable any interfaces that are not required for normal operation of the meter. The method of disabling such interfaces shall prevent them from being used to compromise the other TOE security objectives.

4.1.6 O.Resilience Resilience against failures

The TOE shall start-up and recover from failures in a defined and secure way.

4.1.7 O.SecureUpdate Updates protected using digital signature

The TOE firmware shall be updatable only via a secure update function, using digital signature to protect the integrity and authenticity of the update.

Application Note 6

The term "firmware" is used in this security target to describe any executable software or firmware present in the meter. The secure update function applies to all firmware in the TOE that can be updated.

4.1.8 O.Logging Security event logging

The TOE shall maintain a log of security events and shall protect the log against unauthorised modification.

4.1.9 O.Alarms Alarms for critical events

The TOE shall send an alarm message to a defined destination when any of a defined list of events occur. The alarm shall be sent at or before the meter's next default communication

opportunity.

4.2 Security Objectives for the Operational Environment

The following security objectives relate to the TOE environment.

4.2.1 OE.ExternalData Protection of data outside TOE control

Where copies of data protected by the TOE are managed outside of the TOE, the relevant external applications and other entities shall provide appropriate protection for that data.

4.2.2 OE.AuditSupport Audit data review

The audit trail generated by the TOE shall be collected, maintained and reviewed by an appropriate external audit role according to a defined audit procedure for the AMI.

4.2.3 OE.InspectionSupport Meter integrity inspections

The scheme for deployment and operation of an AMI shall include measures (based on risk-analysis) to deter tampering with the meter and to support appropriate inspections of meter integrity.

4.2.4 OE.UniqueSubjectIDs Subjects have unique identifiers

External subjects shall use unique identifiers in their interactions with the TOE. (Note that this requirement is derived from Requirement E in [7].)

5. Extended Component Definitions

5.1.1 Security Event Alarm (FAU_ARP.2)

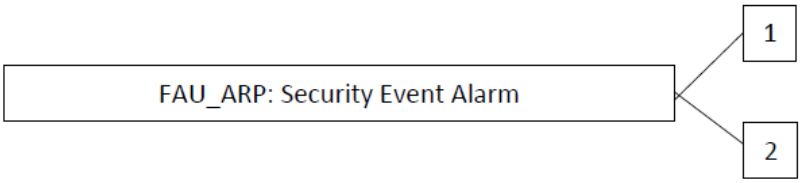
This component extends the existing family FAU_ARP in [3], adding a different type of alarm that, unlike FAU_ARP.1, is not tied directly to the audit log. Note that elements of definition

that are relevant only to FAU_ARP.1 are not repeated here.

Family behaviour

This family defines the response to be taken in case of detected events indicative of a potential security violation.

Component levelling:



Management: FAU_ARP.2

There are no management activities defined by default.

Audit: FAU_ARP.2

There are no actions defined to be auditable by default.

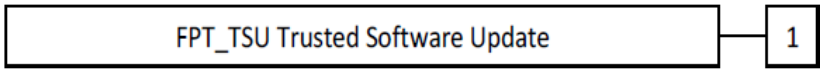
FAU_ARP.2	*Security Event Alarm*
Hierarchical to:	No other components.
Dependencies:	No dependencies
FAU_ARP.2.1	The TSF shall send an alarm message to the indicated destination for the following events: [assignment: *list of events and destination for the alarm for each event*].
FAU_ARP.2.2	The TSF shall include within each alarm message at least the following information: a) Date and time of the event; b) Type of event.
FAU_ARP.2.3	The TSF shall include the following additional alarm information: [assignment: *list of alarm messages and associated additional information*].
FAU_ARP.2.4	The TSF shall send alarms according to the following timing rules: [assignment: *rules that specify when an alarm must be sent relative to the detection of the event*].

5.1.2 Trusted Software Update (FPT_TSU.1)

Family behaviour

Components in this family address the requirements for trusted software/firmware update of the TSF.

Component levelling:



Management: FPT_TSU.1

There are no management activities defined by default.

Audit: FPT_TSU.1

There are no actions defined to be auditable by default.

FPT_TSU.1	*Trusted Software/Firmware Update*

Hierarchical to: No other components

Dependencies: FCS_COP.1

FPT_TSU.1.1 The TSF shall provide [assignment: *list of authorised roles*] the ability to query [selection, one of: *the currently executing version of the TOE software/firmware*, *the currently executing and the most recently downloaded versions of the TOE software/firmware*].

FPT_TSU.1.2 The TSF shall provide means to authenticate and verify the integrity of software/firmware updates to the TOE prior to installing those updates, using a digital signature mechanism that meets the following: [assignment*: mechanism specification*].

FPT_TSU.1.3 The TSF shall provide means to verify the following additional properties of software/firmware updates to the TOE prior to installing those updates: [assignment*: list of additional properties*].

FPT_TSU.1.4 The TSF shall provide [assignment: *list of authorised roles*] the ability to activate updates to TOE software/firmware.

Application Note 7

In FPT_TSU.1.1 the version currently executing may not be the same as the version most recently downloaded, since a downloaded version may not yet have been activated.

The cryptographic operations used to implement the digital signature mechanism in FPT_TSU.1.2 must be specified in iterations of FCS_COP.1.

Examples of the properties specified in FPT_TSU.1.3 might be ensuring that the update is intended for the TOE type or instance, or ensuring that the update is a later version than the currently executing version.

Activation in FPT_TSU.1.4 results in the updated software/firmware being executed.

If the TOE does not support the querying of the currently executing version then it is legitimate to complete the assignment of the list of roles in FPT_TSU.1.1 with 'None', and in this case the SFR element is treated as trivially satisfied.

5.1.3 Basic TSF Self Testing (FPT_BST.1)

The extended component defined here is a simplified version of FPT_TST.1 in [3].

Family behaviour

Components in this family address the requirements for self-testing the TSF at selected times for correct operation.

Component levelling:

Management: FPT_BST.1

There are no management activities defined by default.

Audit: FPT_BST.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

• Indication that TSF self test was completed.

FPT_BST.1	*Basic TSF Self Testing*
	Hierarchical to: No other components.
	Dependencies: No dependencies.
FPT_BST.1.1	The TSF shall run a suite of the following self-tests [selection: *during initial start-up (on power on), periodically during normal operation, at the request of the authorised user, at the conditions [assignment:*

conditions under which self-tests should occur] to demonstrate the correct operation of the TSF: [assignment: *list of self-tests run by the TSF*].

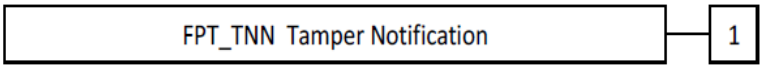
5.1.4 Tamper Notification (FPT_TNN.1)

The extended component defined here has some similarities with FPT_PHP.2 in [3], but states an active tamper detection requirement more suitable for devices such as smart meters.

Family behaviour

Components in this family address requirements for notification of defined tamper scenarios on identified elements of the TOE. This contrasts with FPT_PHP.1 and FPT_PHP.2 in the definition of specific tamper scenarios to be addressed, and the ability to notify using an identified interface rather than to a particular user or role.

Component levelling:



Management: FPT_TNN.1

There are no management activities defined by default.

Audit: FPT_TNN.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- detected tampering events.

FPT_TNN.1 *Tamper notification*

Hierarchical to: No other components.

Dependencies: None

FPT_TNN.1.1 The TSF shall monitor [assignment: *list of TSF devices/elements for which active detection is required*] and notify [assignment: *designated user(s), role(s), or interface(s)*] when physical tampering of the following types has occurred: [assignment: *list of physical tampering scenarios*].

Application Note 8

The second assignment ('designated user, role, or interface'), describes the way in which notification is conveyed, via communication with a specific subject or else by using a particular interface (or both). The use of an interface could include, for example, a light on a device panel, the sending of a particular alarm message, or the recording of a particular log entry. In the case of a log entry, the content of the log entry should be described using an appropriate FAU SFR, and the protection of the log against modification (cf. FAU_STG.2) associated with the tamper event should be described in the TOE Summary Specification.

Application Note 9

A physical random number generator (RNG) produces the random number by a noise source based on physical random processes. A non-physical true RNG uses a noise source based on non-physical random processes like human interaction (key strokes, mouse movement). A deterministic RNG uses a random seed to produce a pseudorandom output. A hybrid RNG combines the principles of physical and deterministic RNGs where a hybrid physical RNG produces at least the amount of entropy the RNG output may contain and the internal state of a hybrid deterministic RNG output contains fresh entropy but less than the output of RNG may contain.

6. Security Requirements

6.1 Typographical Conventions

This chapter describes the security functions and assurance requirements that TOE must meet. These requirements include the functional components of CC:2022 Release 1 Part 2[3] and the assurance components defined for EAL4+ in CC:2022 Release 1 Part 3[4].

The following marks are used:

- Refinement operation (**in bold**): Used to add detail to requirements, thereby further limiting requirements. If a word is deleted from the original text, the refinement is indicated by the ~~**deleted bold text**~~.
- Selection operation (use an underline): Used to select one or more options provided by [CC] when describing the requirements.
- Assignment operation (*in italics*): Used to assign a specific value to an unspecified parameter, such as the password length.
- Iteration operation: identified by the suffix in the SFR name (e.g., FDP_IFC.2/FW).

6.2 Security Functional Requirements

The following table lists the required components of the security functions implemented by Holley's Single Phase and Three Phase Smart Meters EAL4+.

User Data Protection	
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1/Msgs	Subset information flow control
FDP_IFF.1/Msgs	Simple security attributes
FDP_IFC.2/Int	Complete information flow control
FDP_IFF.1/Int	Simple security attributes
FDP_IFC.1/Keys	Simple security attributes
FDP_IFF.1/Keys	Subset information flow control
FDP_RIP.1	Subset residual information protection
Cryptographic Support	
FCS_CKM.1	Cryptographic key generation
FCS_CKM.6	Timing and event of cryptographic key destruction
FCS_COP.1/message encryption and decryption	Cryptographic operation
FCS_COP.1/key wrap	Cryptographic operation
FCS_COP.1/firmware signature verification	Cryptographic operation
FCS_RNG.1	Random number generation
Identification and authentication	
FIA_UAU.6	Re-authenticating
FIA_AFL.1	Failure with preservation of secure state
Protection of the TSF	
FPT_FLS.1	Failure with preservation of secure state
FPT_TNN.1	Tamper notification
FPT_BST.1	Basic TSF Self Testing
FPT_RPL.1	Replay detection
FPT_STM.1	Reliable time stamps
FPT_TSU.1	Trusted update
Security Management	
FMT_SMR.1	Security roles
FMT_MOF.1	Management of Security Functions Behaviour
FMT_MTD.1/Audit	Management of TSF data
FMT_MTD.1 /Time	Management of TSF data
Security Audit	
FAU_ARP.2	Security Event Alarm

FAU_GEN.1	Audit data generation
FAU_SAR.1 – refined	Audit review
FAU_SAR.2 – refined	Restricted audit review
FAU_STG.2	Protected audit data storage
FAU_STG.4	Action in case of possible audit data loss
Trusted Channel	
FTP_ITC.1	Inter-TSF trusted channel

Table 10：Security Functional Components

The individual security functional requirements are specified in the sections below.

6.2.1 Cryptographic Support

6.2.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1 Cryptographic key generation

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] FCS_CKM.3 Cryptographic key access[FCS_RBG.1 Random bit generation, or FCS_RNG.1 Random number generation]FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECC Key Pair Generation* and specified cryptographic key sizes *256bit* that meet the following: *NIST Special Publication 800-56A Revision 3*.

Application Note 10

The Security Target must include an iteration of FCS_CKM.1 for each cryptographic key that is generated in the meter and supports other parts of the TSF (e.g. message protection (see FDP_IFF.1/Msgs in section 6.2.2.4)). The ST author identifies where the random bit generator specified by FCS_RNG.1 is used for key generation.

If the meter does not generate any keys then the ST author completes all of the assignments with 'None' and addresses the import of keys using the rules in FDP_IFF.1/Keys (see also the requirements for description of security-related activities in the manufacturing environment as part of the refinements to ALC_DVS.1 in section 6.3.1.6). Where this import relies on a secure channel the ST author also adds a secure channel SFR to describe this channel (see the discussion of secure channel SFRs in Application Note 17).

6.2.1.2 Timing and event of cryptographic key destruction(FCS_CKM.6)

FCS_CKM.6 Timing and event of cryptographic key destruction

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.6.1 The TSF shall destroy *Master key,Global Authentication key,Global Encryption key,Global Brodacast key,Server Private Key,Server Public Key,Client Public Key* when *Replace the currently used key for security purposes*.

FCS_CKM.6.2 The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method *Overwrite the storage area/RAM* that meets the following: *NIST Special Publication 800-57 Part 1 Revision 5*.

Application Note 11

The Security Target must specify the method(s) of secure destruction of all private and secret keys that it holds (whether they were generated internally or received from some other source). If necessary then more than one iteration of FCS_CKM.6 may be included to describe different standards for secure deletion. The 'list of standards' in the final assignment may be met in the Security Target by simply providing a description of the action taken to destroy the keys rather than referencing an external standard.

6.2.1.3 Cryptographic operation (FCS_COP.1/ message encryption and decryption)

FCS_COP.1/ message encryption and decryption Cryptographic operation

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation , or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.3 Cryptographic key access

FCS_COP.1.1/message encryption and decryption The TSF shall perform *encryption/decryption*] in accordance with a specified

cryptographic algorithm *AES-GCM-128* and cryptographic key sizes *128 bits* that meet the following: *NIST SP 800-38D*.

Note: The random number generated by the algorithm is *encrypted* and exchanged before the communication is established, and the information is encrypted during the entire communication process.

6.2.1.4 Cryptographic operation (FCS_COP.1/Key wrap)

FCS_COP.1/key wrap Cryptographic operation

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation , or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.3 Cryptographic key access

FCS_COP.1.1/key wrap The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *AES key wrap* and cryptographic key sizes *128 bits* that meet the following: *RFC3394*.

Note: Encrypt the replaced master key (making the replaced key ciphertext).

6.2.1.5 Cryptographic operation (FCS_COP.1/Firmware Signature Verification)

FCS_COP.1/ firmware Signature Verification Cryptographic operation

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation , or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.3 Cryptographic key access

FCS_COP.1.1/ firmware Signature Verification The TSF shall perform *signature/verification* in accordance with a

specified cryptographic algorithm *ECDSA based on ECC256* and cryptographic key sizes *private key: 256 bits, public key: 512 bits* that meet the following: *FIPS 186-5*.

Note: Before the communication is established, random numbers are signed through this algorithm and the signature of the firmware is exchanged and updated.

Standard	Key algorithm	Key length	Operation	Note
NIST SP 800-38D	AES-GCM-128	128 bit	Encryption/ decryption	The algorithm encrypts information throughout the communication process.
FIPS 186-5	Based on the ECDSA of ECC256(ECC Key Pair Generation)	Private key: 256 bit Public key: 512 bit	Signature/ verification	Before communication is established, random numbers are signed by the algorithm and signatures of upgraded firmware are exchanged.
RFC3394	AES key wrap	128 bit	Encryption/ decryption	Encrypt the replaced key (making the replaced key ciphertext).

Table 11：Cryptographic Operation Description

Application Note 12

The Security Target must include an iteration of FCS_COP.1 for each cryptographic operation that supports message protection (see FDP_IFF.1/Msgs in section 6.2.2.4). For example, separate iterations would be used to describe the cryptographic functions used for digital signature (e.g. to support authentication and authorisation mechanisms), and for confidentiality. In addition, iterations of FCS_COP.1 must be included for each cryptographic operation used to support trusted update (see FPT_TSU.1 in section 0) — examples here would include digital signature, confidentiality, and also any separate hash mechanism used to protect the update.

Approved cryptographic standards are determined by the relevant authority for an AMI.

6.2.1.6 Random number generation (FCS_RNG.1)

FCS_RNG.1 Random number generation

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a hybrid physical random number generator that implements: *1. generate random numbers exchanged by both parties during communication; 2. generate random numbers needed for the electric meter's digital signature private key*.

FCS_RNG.1.2 The TSF shall provide *32bits* that meet *NIST Special Publication 800-90A Revision 1* .

Application Note 13
A physical random number generator (RNG) – also referred to as a random bit generator (RBG) – produces the random number by a noise source based on physical random processes. A deterministic RNG uses a random seed to produce a pseudorandom output. A hybrid RNG combines the principles of physical and deterministic RNGs where a hybrid physical RNG produces at least the amount of entropy the RNG output may contain and the internal state of a hybrid deterministic RNG output contains fresh entropy but less than the output of RNG may contain.

The ST author describes the ways in which random numbers generated according to FCS_RNG.1 are used by the TOE in the TOE Summary Specification. Examples of such uses would be generation of cryptographic keys or challenges.

6.2.2 User Data Protection

6.2.2.1 Complete access control (FDP_ACC.2)

FDP_ACC.2 Complete access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1 The TSF shall enforce the *Meter Data SFP* on
(1) subjects: all ***(Public, Administrator, Operator, Technician)***
(2) *objects: metrologically certified data, credentials, meter configuration, Load Profile Data, Freeze Data, Event Log*

and all operations among subjects and objects covered by the SFP.

Application Note 14

The ST author describes and explains the specific implementation of the controlled objects, including 'metrologically certified data', 'credentials', and 'meter configuration' in the Security Target and this is also described and explained in the operational guidance for the meter with reference to the actual terminology and names of objects in that particular meter (cf. refinement of AGD_OPE.1 in section 0).

Objects	Description
Metrologically Certified Data	Energy: accumulated value of consumer electricity consumption, including active and reactive electricity
	Instantaneous Values: instantaneous value of current electricity consumption, including voltage, current, power, frequency, power factor, etc.
	Demand: user's current power consumption; average value over a period of time; configurable for 1-60 minutes
Credentials	Symmetric encryption password (AES-GCM-128), public key of client digital signature, private key of server digital signature, public key (ECDSA) and all operations between the subject and object covered by SFP.
Meter Configuration	Parameter data for TOE to maintain normal operation, including RTC, safety key data, and other operating parameters.
Load Profile Data	Load Profile Recorder 1: Energy of timed frozen TOE; configurable for 1-60 minutes.
	Load Profile Recorder 2: instantaneous values of timed frozen TOE; configurable for 1-60 minutes.
Freeze Data	Monthly Billing：Freeze user data in TOE every month.
	Daily Billing：Freeze user data in TOE every day.
Event Log	Some monitoring logs generated by TOE itself, including serious events, physical damage events, other events, etc.

Table 12：Objects description (FDP_ACC.2)

Subject	Object	Interface	Operation
Public	objects listed above	Optical RS485 Wi-SUN	The role can only read the data specified above (other than credentials) but cannot modify any of that data.
Administrator	objects listed above	Optical RS485 Wi-SUN	Under the role: The above data other than credentials can be read.

			Metrologically certified data cannot be cleared. Load Profile Data/Freeze Data/Event Log can be cleared. Configuration parameters can be changed. Credentials can be modified.
Operator	objects listed above	Optical RS485 Wi-SUN	Under the role: The above data other than credentials can be read. Load Profile Data/Freeze Data/Event Log can be cleared. Load Profile Data/Freeze Data/Event Log can be cleared. Configuration parameters (except for security key data) can be changed. Credentials can be not modified.
Technician	objects listed above	Optical RS485 Wi-SUN	Under the role: The above data other than credentials can be read. No data can be cleared. Only network-related operating data can be configured. Credentials can be not modified.

Table 13：Complete access control description (FDP_ACC.2)

Meter Data SFP:

Meter data SFP passes strict identity authentication, so that object data such as metrologically certified data, credentials, meter configuration, Event_Log, Freeze Data, and Load Profile Data are limited to specific subjects for reading and modification. In addition, interfaces that restrict subject access to object data are specific interfaces (Optical, RS485, and Wi-SUN).

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

6.2.2.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1 Security attribute based access control

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

FDP_ACF.1.1 The TSF shall enforce the *Meter Data SFP* to objects based on the following:

(1) Metrologically certified data (e.g., consumption/generation measurements)

(2) Credentials

(3) Meter configuration

(4) *Subject: Public, Administrator, Operator, Technician*

Object: Metrologically certified data、*Load Profile Data*、*Freeze data*、*Event Log*、*Meter configuration parameters*、*credentials*

Security attributes: identity authentication (ECDSA based on ECC256), access rights, data encryption, data integrity protection， *TOE interfaces (RS485, Optical and Wi-SUN)*.

Application Note 15

Authorisation of a subject for access to the objects in FDP_ACF.1.1 is defined in the rules in the other elements of FDP_ACF.1 below – these exclude rules for accesses via messages which are separately described in FDP_IFF.1/Msgs. The rules therefore apply, for example, to the meter's user interface. The rules describe the role- and/or identity-based access controls to objects that are used to enforce appropriate protection based on a risk analysis.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *Public can only read the above data other than credentials, but can't modify any of the data;*

Administrator can read the above data other than credentials, clear Load Profile Data/Freeze Data/Event Log data, modify configuration parameters, modify credentials but cannot clear metrologically certified data;

Operator can read the above data other than credentials, clear Load Profile Data/Freeze Data/Event Log data, modify configuration parameters(except for security key data), but cannot clear metrologically certified data and modify credentials;

Technician can read the above data other than credentials and configure network-related operational data, but cannot clear any data, and modify credentials.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *None*.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *All entities except Administrators cannot modify credentials;*

Administrator and Operator cannot clear metrologically certified data;

Technician cannot clear any data.

Application Note 16

Note that the security policy for access to cryptographic keys is described separately in FDP_IFF.1/Keys. In most cases it is expected that the keys will be accessed via messages (and therefore will be subject to FDP_IFF.1/Msgs as well as FDP_IFF.1/Keys); however if non-message interfaces also provide access to keys then there may also be relevant rules included in FDP_ACF.1 and FDP_IFF.1/Keys.

6.2.2.3 Subset information flow control (FDP_IFC.1) – Messages

FDP_IFC.1/Msgs Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1/Msgs The TSF shall enforce the *Messages SFP* on

(1) subjects: all

(2) information: messages

(3) operations: send, receive.

Role	Interface	Message type
Public	Optical RS485 Wi-SUN	Block-transfer-with-get Get Selective Access Multiple-references
Administrator	Optical RS485 Wi-SUN	Block-transfer-with-get Block-transfer-with-set Get Set Multiple-references Selective Access Action

		Data-Notification
Operator	Optical RS485 Wi-SUN	Block-transfer-with-get Block-transfer-with-set Get Set Multiple-references Selective Access Action
Technician	Optical RS485 Wi-SUN	Block-transfer-with-get Block-transfer-with-set Get Set Multiple-references Selective Access Action

Table 14：Role、Interface and message type (FDP_IFC.1/Msgs)

Message type	Description
Block-transfer-with-get	This message type is used by the client to get large amounts of data from the server, and is usually used for the transmission of large amounts of data. It sends data to the client in stages through "block transfer". The client uses this type of message to request the device to send one or more data blocks, each containing a certain size of data.
Block-transfer-with-set	This message type is similar to Block-transfer-with-get, but this message type is used to send a large amount of data to the server. The data is transmitted to the server for set or configuration by blocking.
Get	This message type is used to request the server to provide specific data items. The client sends a GET request to the device, asking for the current state or value of a specific object.
Set	This message type is used to set data to the server. The client sends commands to the server via Set messages to modify some configuration or state of the device.
Multiple-references	This message type allows clients to request multiple data items for multiple objects at once. It improves communication efficiency by including multiple data references in a message.
Selective Access	This message type allows the client to selectively access the data in the server, and supports precise access control of specific data objects or attributes.

Action	This message type is used to request the server to perform certain operations or actions. Unlike data reading and configuration modification, messages of Action type are usually used to trigger the server to execute some specific functions or control commands. **Note:** The Action message type is used for credential replacement.
Data-Notification	This message type allows the server to actively send notifications of data updates or status changes to the client. Unlike the traditional request-response model, the server actively pushes data, usually when the state changes or the data reaches a certain threshold.

Table 15：Message type description(FDP_IFC.1/Msgs)

Note: The messages in the message type list contain object data of the FDP_ACF.1 component and security event alerts described in FAU_ARP.2(Section 6.3.6.1). The Administrator's Action message includes sending and importing of keys, but the Operator's and Technician's Action do not include that.

Message SFP:

For sending and receiving messages, authentication of the client and server is required, and RS485, Optical, and Wi-SUN can be restricted for sending and receiving messages. In addition, encryption algorithms are used to encrypt messages during transmission and reception to prevent malicious modification of messages.

Note: The P1 port of Holley's Single Phase and Three Phase Smart Meters can only send data out, and cannot receive data.

6.2.2.4 Simple security attributes (FDP_IFF.1) - Messages

FDP_IFF.1/Msgs Simple security attributes

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1/Msgs The TSF shall enforce the *Messages SFP* based on the following types of subject and information security attributes: *message type: Block-transfer-with-get, Block-transfer-with-set, Get, Set, Multiple-references, Selective Access, Action, Data-Notification;*

Security attributes: authentication (ECDSA based on ECC256), Anti-

replay, access rights, message encryption, message integrity protection, TOE interface (RS485, Optical, and Wi-SUN)).

FDP_IFF.1.2/Msgs The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *Public can receive Block-transfer-with-get, Get, Selective Access, Multiple-references messages through RS485, Optical, and Wi-SUN;*

Administrator, Operator and Technician can receive and send Block-transfer-with-get, Block-transfer-with-set, Get, Set, Multiple-references, Selective Access and Action messages through RS485, Optical, and Wi-SUN. Identity authentication will be performed when sending and receiving messages. Message encryption will be performed during sending and receiving (AES-GCM-128, AES Key Wrap);
Only the Administrator can receive Data-Notification messages through RS485, Optical, and Wi-SUN;
Except for Public, the other subjects can send and receive the object data in FDP_ACF.1 through RS485, Optical, and Wi-SUN. Message encryption measures will be carried out during the transmission of the data;
Public can receive object data in FDP_ACF.1 through RS485, Optical, and Wi-SUN;
When the Administrator can transmit the key through RS485, Optical, and Wi-SUN, the key will be encrypted (AES Key Wrap) to prevent the key from being leaked.

FDP_IFF.1.3/Msgs The TSF shall enforce the **following additional information flow control rules**: *None*.

FDP_IFF.1.4/Msgs The TSF shall explicitly authorise an information flow based on the following rules: *None.*

FDP_IFF.1.5/Msgs The TSF shall explicitly deny an information flow based on the following rules:

(1) Message received from a source that is not authorised to send messages of that type;

(2) *None*.

Application Note 17

The ST must describe the types of messages and the policy for protection of each message type using this SFR. In most cases the rules for message types can probably be expressed using FDP_IFF.1.1 and FDP_IFF.1.2 only, in which case the assignments in FDP_IFF.1.3, FDP_IFF.1.4 and FDP_IFF.1.5 can be completed with 'none' (in the case of FDP_IFF.1.5 the 'none' can be omitted, leaving only rule (1)).

The operations referred to in FDP_IFF.1.2/Msgs are those defined in FDP_IFC.1/Msgs, and the messages covered by the operations and rules include security event alarms as described in FAU_ARP.2(section 6.2.6.1).

The term "authorisation measures" in FDP_IFF.1.2 means measures that determine whether or not a source is authorised to provide certain message types to the meter (note that this may overlap with authorisation of sources of imported keys in FDP_IFF.1.2/Keys and with authentication in FIA_UAU.6 and FIA_AFL.1). In general, these authorisation rules would be expected to use the roles defined in FMT_SMR.1 (section 6.2.5.1). The authorisation measures stated in these rules might, for example, define an implementation of role-based permissions to limit certain message types to energy suppliers or network operators. Although no specific authorisation measures are stated in this PP, it is expected that every meter conformant to this PP will define some authorisation measures in its ST, and this is expressed by the general 'deny' rule in FDP_IFF.1.5/Msgs.

An example of a rule that could be stated in FDP_IFF.1.2/Msgs would be "All commands, responses and alarms in the 'Critical' group (as defined in <reference>) shall be discarded without effect unless the digital signature (as defined in <reference>) is valid and belongs to a role that is authorised to issue the message according to <reference>" – in this case references would be given (in the SFR or using application notes in the ST) to the definition of the 'Critical' message group, the format and creation of the digital signature, and the definition of permitted messages for each role.

The rules expressed in FDP_IFF.1/Msgs must make clear how the access controls over types of data defined in FDP_ACF.1 are implemented for message processing (cf. the refinement of ADV_ARC.1 in section 0). The references might be to other rules listed in the SFR, or to external documents, however it is important that the references define unambiguous rules that can therefore be tested (cf. the refinement of ATE_IND.2 in section 0).

The rules must cover all available combinations of messages and interfaces over which they can be sent. Thus, for example, a message that can be received from any of the Local Network, Neighbourhood Network, or WAN, must specify the protection applicable to each of the interfaces. At the level of direct interfaces this would include interfaces such as using inter-PAN on a ZigBee TOE to communicate directly with a device such as a hand-held terminal unit.

The ST author may introduce additional iterations of FDP_IFF.1/Msgs (e.g. appending the name of the interface or protocol as the iteration name) in order to specify separate rules applicable to each interface.

Rules governing authorised access to objects other than via messages are given in FDP_ACF.1. As part of the refinement of ADV_FSP.4 in section 2 the evaluator checks that the rules given in the Meter Data SFP (FDP_ACF.1), Messages SFP (FDP_IFF.1/Msgs), and the Keys SFP (FDP_IFF.1/Keys) are unambiguous and completely cover the interfaces, operations and data provided by the TOE.

The ST author describes the protection specified for messages in terms of cryptographic operations defined in iterations of FCS_COP.1 (see section 0).

Where the protection of messages is based on a secure channel rather than by protecting each individual message (noting that security measures are required to be implemented at the application layer and not to depend on the lower layer protocols, as checked in the refinements to ADV_FSP.4 in section 2) then the ST author should consider adding an SFR to describe the secure channel used (e.g. FDP_ITC.1 or FTP_ITC.1).

Note that if the TOE receives random bits that support SFRs (e.g. for generation of keys, nonces or salts), or if it receives keys rather than generating its own, then the rules in FDP_IFF.1/Msgs must include the specification of the secure channel(s) used to transmit the random bits and/or keys. In the case of receiving random bits and/or keys from other AMI components, these rules s should be supported by inclusion of a secure channel SFR (such as FDP_ITC.1 or FTP_ITC.1) in the Security Target.

6.2.2.5 Complete information flow control (FDP_IFC.2) – Interfaces

FDP_IFC.2/Int Complete information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1/Int The TSF shall enforce the *Interfaces SFP* on

(1) subjects: all

(2) information: all communication

and all operations that cause that information to flow to and from subjects covered by the SFP.

Role	Interface	Message type
Public	Optical RS485 Wi-SUN	Block-transfer-with-get Get Selective Access Multiple-references
Administrator	Optical RS485 Wi-SUN	Block-transfer-with-get Block-transfer-with-set Set Multiple-references

		Selective Access Action Data-Notification
Operator	Optical RS485 Wi-SUN	Block-transfer-with-get Block-transfer-with-set Get Set Multiple-references Selective Access Action
Technician	Optical RS485 Wi-SUN	Block-transfer-with-get Block-transfer-with-set Get Set Multiple-references Selective Access Action

Table 16：Role、Interface and message type (FDP_IFC.2/Int)

Note: The messages in the message type list contain object data of the FDP_ACF.1 component and security event alerts described in FAU_ARP.2(Section 6.2.6.1). The Administrator's Action message includes sending and importing keys, but the Operator's and Technician's Action do not include.

Interface SFP:

Only authenticated subjects (ECDSA based on ECC256) can use the above four interfaces. Messages are encrypted when communicating with the interface.

FDP_IFC.2.2/Int The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

6.2.2.6 Simple security attributes (FDP_IFF.1) - Interfaces

FDP_IFF.1/Int Simple security attributes

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1/Int The TSF shall enforce the *Interfaces SFP* based on the following types

of subject and information security attributes: *Optical, RS485, P1, Wi-SUN, Display, and Keypad*.

FDP_IFF.1.2/Int The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation **only via the following interfaces**: *for each enabled interface presented, a statement of the operational use of the interface*.

Interface	**Purpose**	**Link layer Protocol**	**Application layer protocol**	**Baud Rate**
Optical	Local communication	IEC62056-21E to HDLC	DLMS	9600bps
RS485	Remote communication	HDLC	DLMS	9600bps
P1 Port	Local communication	DSMR 5.0.2	DSMR 5.0.2	115200bps
Wi-SUN	Remote communication	WRAPPER(TCP)	DLMS	9600bps
Display	Display metrologically certified data	/		/
Keypad	Switch the display item, reset the demand	/		/

Table 17：Interface and related protocol

- local optical interface:

  Optical interface enables a bi-directional local communication for data readout and parameterization.

  Physical properties of the optical interface are implemented according to the IEC 62056-21E standard.

  The local meter data exchange is performed via a hand-held unit (HHU) or a PC using optical probe. Maximum baud rate of optical interface is limited to 9600bps.
- P1: Customer interface port allows the consumers to use in-home displays and other devices to monitor and optimize their energy consumption. The interface provides a unidirectional data flow from the meter, as well as 5V power that can be used to power a connected device. It is physically a standard RJ12 connector, with default data rate

115200bps. The protocol is based on DSMR standard.

- RS485 Remote communication port: RS485 interface enables a bi-directional local communication for data readout and parameterization. Physical properties of the interface are implemented according to the HDLC standard. The communication rate is configurable from 1200bps to 9600bps, with a default setting of 9600bps.
- Wi-SUN module Remote communication port: The meter supports plug-in communication module with Wi-SUN. The module is powered directly from the meter. And the communication default data rate is 9600bps.

FDP_IFF.1.3/Int The TSF shall enforce the **following additional information flow control rules**: *None*.

FDP_IFF.1.4/Int The TSF shall explicitly authorise an information flow based on the following rules: *None*.

FDP_IFF.1.5/Int The TSF shall explicitly deny an information flow based on the following rules:
(1) any interface other than those in FDP_IFF.1.2/Int is disabled.

Application Note 18

The purpose of this SFR is to ensure that If the device has interfaces other than those supporting normal operation (and that are therefore not necessarily governed by the access control rules in FDP_IFF.1/Msgs or other SFRs – e.g. debug interfaces or other interfaces intended for use during manufacturing), then these interfaces are disabled for normal operation. FDP_IFF.1.1/Int therefore lists the available operational interfaces (i.e. those required for normal operation), and FDP_IFF.1.5/Int requires that all other accessible interfaces are disabled. Note that these operational interfaces are defined at the level of protocols and available commands, and not simply at a general level such as WAN, Neighbourhood Network or Local Network. A refinement of ADV_TDS.3 in section 6.4.1.4 requires that the disabled interfaces and their methods of disablement are documented and examined by the evaluators. Methods of disabling the interfaces may be physical (e.g. based on manufacturing actions) or logical (e.g. by requiring authentication of at least the same strength as for FIA_UAU.6 or for support of other protection mechanisms over messages (FDP_IFF.1/Msgs), meter data (FDP_ACF.1) or keys (FDP_IFF.1/Keys)).

The Functional Specification describes the interfaces that are presented by the TOE). Some of these interfaces are used for the normal operation of the meter, and all others are disabled: this is identified by the ST author in FDP_IFF.1.2/Int. Note that 'normal operation' of the meter here includes any interfaces that require authentication and that may be limited to specific roles (e.g. administration or maintenance roles). For the disabled interfaces, the Functional Specification describes the method(s)by which these interfaces are disabled – including both physical and logical methods as appropriate. This is supported by the analysis of design

elements and testing of the post-installation state required by the refinements of the assurance requirements in section 6.3.1.

6.2.2.7 Subset information flow control (FDP_IFC.1) – Keys

FDP_IFC.1/Keys Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1/Keys The TSF shall enforce the *Keys SFP* on

(1) subjects: ***Administrator***

(2) information: keys **** Master key, Global Authentication key, Global Encryption key, Global Broadcast key, Client public key +***

(3) operations: send, import.

Key SFP:

Key types include Master key, Global Authentication key, Global Encryption key, Global Broadcast key, Client public key, Server private key, and Server public key.

When the client entity imports keys (Master key, Global Authentication key, Global Encryption key, Global Broadcast key, Client public key) into the electricity meter, the client entity's identity will be verified (based on ECDSA of ECC256). Meanwhile, the interface for key import is restricted to RS485, Optical, and Wi-SUN. During the key import process, the keys will be encrypted (AES Key Wrap). Additionally, the smart meter will export the Server public key to the client entity for the client's identity verification of the server.

After the meter is produced, the Client public key will be imported into the meter. If the Client public key needs to be updated, when importing the new Client public key into the meter, the previous Client public key should be used to verify the client's identity.

Key type：

- Master key: To renew all GUEK/GAK keys and the Master Key itself.
- Global Authentication key: To authenticate the interaction messages between client and server.
- Global Encryption key: To encrypt messages exchanged between client and server.
- Global Broadcast key: To encrypt messages broadcasted from client to server.
- Client Public Key: To verify the digital signature generated by the client's private key.
- Server Private Key: To generate a digital signature to prove that the source of the message is the server and that the data has not been tampered with.

- Server Public Key: To verify the digital signature generated by the server's private key, or to encrypt messages (only the server can decrypt them).

Note:
Client refers to the client subject role (Public, Administrator, Operator, Technician), which can exist in the AMI System and the PC Software. Public role do not require authentication, so Public role have no Client Public Key.
Server refers to DDSD285, DDSY283SR, DTSD545 and DTSY541.

6.2.2.8 Simple security attributes (FDP_IFF.1) – Keys

FDP_IFF.1/Keys	Simple security attributes
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1.1/Keys	The TSF shall enforce the *Keys SFP* based on the following types of subject and information security attributes: *Key type: Master key, Global Authentication key, Global Encryption key, Global Broadcast key, Client public key, Server public Key;* *Security attributes: authentication (ECDSA based on ECC256), access rights, key encryption, TOE interface (RS485, Optical, and Wi-SUN).*
FDP_IFF.1.2/Keys	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *Only Administrator can send and import keys(Master key, Global Authentication key, Global Encryption key, Global Brodacast key, Client public key) through TOE interface (RS485, Optical, and Wi-SUN), and the keys will be encrypted during sending and importing (AES Key Wrap);* *When it is necessary to replace the signature public-private key pair of the power meter, the client body needs to export the Server public key of Holley's Smart Meters：DDSD285, DDSY283SR, DTSD545 and DTSY541 to the client body after authentication, and the key will be encrypted with AES-GCM-128 in the process of exporting.*

FDP_IFF.1.3/Keys The TSF shall enforce the **following additional information flow control rules**: *None*.

FDP_IFF.1.4/Keys The TSF shall explicitly authorise an information flow based on the following rules: *None*.

FDP_IFF.1.5/Keys The TSF shall explicitly deny an information flow based on the following rules:

(1) A key received from a source that is not authorised to provide keys of that type shall be rejected;

(2) No read access shall be provided to plaintext private or secret keys stored in the meter;

(3) None.

Application Note 19

The ST describes the types of keys and the policy for protection of each key type using this SFR. In most cases the rules for key types can probably be expressed using FDP_IFF.1.1 and FDP_IFF.1.2 only, in which case the assignments in FDP_IFF.1.3, FDP_IFF.1.4 and FDP_IFF.1.5 can be completed with 'none'.

The operations referred to in FDP_IFF.1.2/Keys are those defined in FDP_IFC.1/Keys.

The term "authorisation measures" in FDP_IFF.1.2 means measures that determine sources that are authentic and authorised to provide keys to the meter (note that this may overlap with authorisation of sources of particular message types in FDP_IFF.1.2/Msgs and with authentication in FIA_UAU.6 and FIA_AFL.1). In general these authorisation rules would be expected to use the roles defined in FMT_SMR.1 (section 6.2.5.1). Although no specific authorisation measures are stated in this PP, it is expected that every meter conformant to this PP will define some authorisation measures in its ST, and this is expressed by the general 'deny' rule in FDP_IFF.1.5/Keys.

Examples of rules that could be stated in FDP_IFF.1.2/Keys would be "All public keys generated in the TOE are exported in the form of a certificate signing request", and "Public keys for eternal entities shall only be imported into the TOE in the form of a public key certificate validated as defined in <reference>and received from a source authenticated as defined in <reference> and where the source has a role that is authorised to issue the key according to <reference>". In this case the references might be to other rules listed in the SFR, or to external documents, however it is important that the references define unambiguous rules that can therefore be tested (cf. the refinement of ATE_IND.2 in section 0).

The 'deny' rule in FDP_IFF.1.5/Keys item (2) ensures that there is no way to read unencrypted secret or private keys over any interface of the TOE.

The import rules must cover all relevant secret, private and public keys.

Requirements for the documentation of keys are included in the refinements of ADV_FSP.4 and ADV_TDS.4 in section 6.3.1.

6.2.2.9 Subset residual information protection (FDP_RIP.1)

FDP_RIP.1 Subset residual information protection

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from the following objects: *metrologically certified data, credentials, Freeze Data, Event Log, meter configuration*.

Application Note 20

Note that destruction of cryptographic keys is also s subject to the requirements of FCS_CKM.6.

The objects listed in FDP_RIP.1.1 include those objects that are subject to the access control rules in FDP_ACF.1. 'Deallocation of the resource' means that the objects are made unavailable as soon as a deletion or replacement of the object takes place.

6.2.3 Identification and authentication

6.2.3.1 Re-authenticating (FIA_UAU.6)

FIA_UAU.6 Re-authenticating

Dependencies: No dependencies.

FIA_UAU.6.1 The TSF shall re-authenticate **authenticate and re-authenticate** the user **for access to data** under the conditions *defined in the Re-authentication Table*.

ID	Data	Authentication for initial access	Re-authentication
(I)	*All user data and TSF data defined in 3.1 Assets*	*Identity authentication (identity authentication mechanism is shown in the figure below), corresponding interfaces: Optical, RS485, Wi-SUN*	After a period of *1min(local)/ 3min* (remote) from the previous successful authentication

Table 18：Re-authentication Table

This SFR requires user authentication for access to all types of data held on the TOE. If necessary,different types of data with different authentication methods and re-authentication times, may be specified using separate rows in the Re-authentication Table, provided that all types of data are covered by the complete set of rows.

This SFR also covers authentication over all available interfaces: separate rows in the Re-authentication Table may also be used to distinguish interfaces and the types of data they give access to).

If the period of time for reauthentication is configurable then the roles that are able to configure this are specified in FMT_MOF.1.

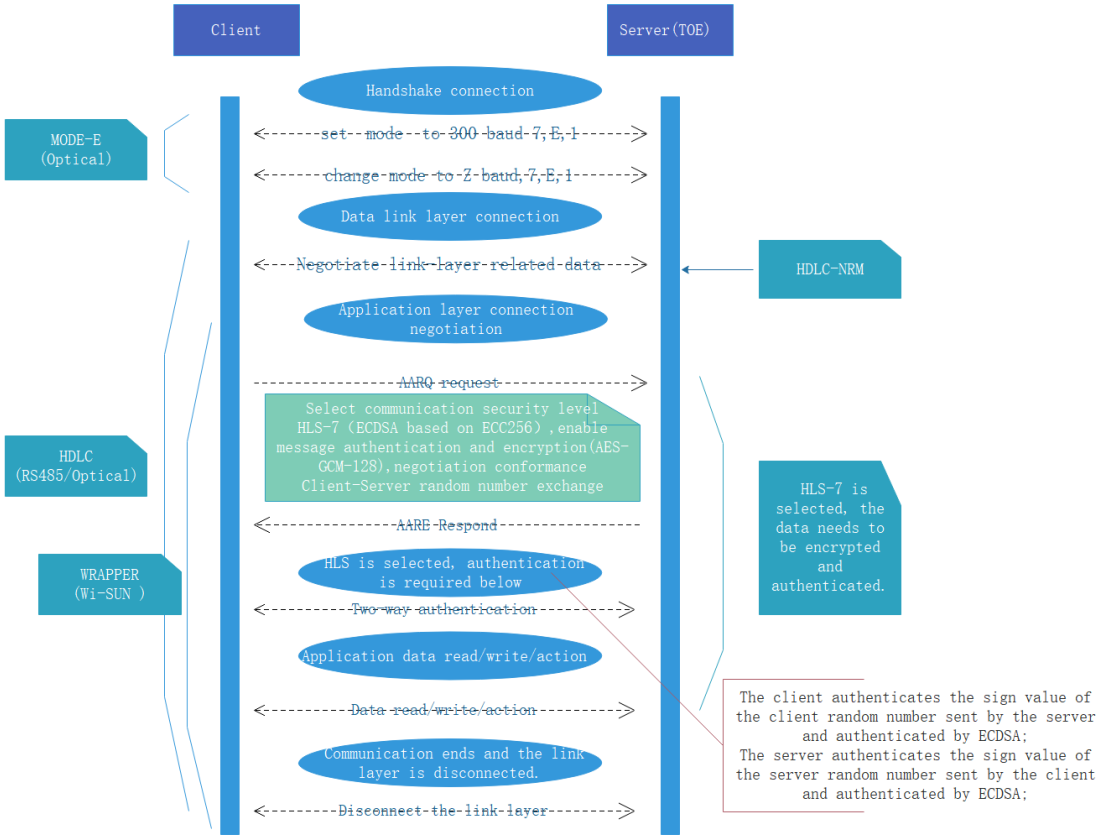


Figure 5：Identity authentication flow chart

The Client and the Server (TOE) conduct handshake negotiation. The negotiation process clarifies that the two parties use HLS-7 (ECDSA based on ECC256) for authentication, and exchange 32 to 64 bytes of random numbers with each other. Then, the two parties use each other's random numbers to calculate the digital signature of the ECC Key Pair Generation, and send it to each other for digital signature. If the authentication of each other is passed, the authentication is successful.

Client initiates handshake negotiation request

Client informs Server that it is ready to start authentication using HLS-7(ECDSA based on ECC256).

Send the random number of 32-64 bytes generated by Client to Server.

Server response to client request

Server informs Client that it agrees to use HLS-7(ECDSA based on ECC256) for authentication.

Send the 32-64 byte random number generated by Server to Client.

Client initiates identity authentication request

Client uses sha256 to compute a digest of Server's random number and to compute a digital signature using Client's own signature private key.

Client sends the digital signature value to Server for signature verification.

Server verifies Client signature

Server uses sha256 to digest the 32-64 bit random numbers it generates and sends to Client.

Server uses the signature public key of Client to verify the digest calculated by Server and the signature value received from Client.

Signature verification succeeds and Client identity is recognized by server.

Server initiates identity authentication request

Server uses sha256 to compute a digest of Client's random number and calculates a digital signature using Server's own signature private key.

Server sends that digital signature value to Client for signature verification.

Client verifies Server signature

Client uses sha256 to digest the 32-64 bit random numbers it generates and sends to Server.

Client uses the signature public key of Server to verify the digest calculated by Client and the signature value received from Server.

Signature verification succeeds and Server identity is recognized by Client.

Level description

No security (Lowest Level Security**, NLS**) authentication, the lowest level without security authentication.

High Level Security (HLS) authentication, high level of security authentication.

Public	Administrator	Operator	Technician
NLS	HLS	HLS	HLS

Table 19：Client authentication description

6.2.3.2 Failure with preservation of secure state (FIA_AFL.1)

FIA_AFL.1 Authentication failure handling

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when an administrator configurable positive integer within *the range in the Authentication Failure Handling Table* **of** unsuccessful authentication attempts occur related to *consecutive failed authentication attempts for access to protected data objects*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been surpassed, the TSF shall *block access for that entity via the relevant interface to data requiring prior authentication until the time period shown in the Authentication Failure Handling Table has elapsed*.

ID	Type of authentication	Allowed range of authentication failures	Blocked time period
(i)	*ECDSA signature verification based on random number*	*1 to 10 times, with the default parameter set to 10 times.*	*3 to 10 minutes, with the default parameter set to 10 minutes.*

Table 20：Authentication Failure Handling Table

Note:
If the configured value for "authentication failures" exceeds the range specified in the table above, it shall be reset to the default of 10 attempts. Similarly, if the configured value for "blocked time" exceeds the specified range, it shall be reset to the default of 10 minutes.
Application Note 22

The authentication covered by FIA_AFL.1 is the authentication required for access to data requiring prior authentication as defined in FIA_UAU.6. The types of authentication are therefore required to cover all types of data included in the Re-authentication Table.

Setting the allowed number of unsuccessful attempts and the time period during which access is blocked is specified in FMT_MOF.1.

6.2.4 Protection of the TSF

6.2.4.1 Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1 Failure with preservation of secure state

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

(1) Watchdog trigger results in meter reset

(2) Failure of the random bit generator

(3) Module network interrupted.

Note：

After the watchdog is triggered, Holley's Single Phase and Three Phase Smart Meters will be reset for initialization. In this process, each module of Holley's Single Phase and Three Phase Smart Meters will be initialized, a self-test will be performed, and the pre-reset data will be read from the memory chip. After reset, Holley's Single Phase and Three Phase Smart Meters data such as power consumption, demand, and configuration parameters will be read from the non-volatile memory and the data will be saved to ensure the accuracy of Holley's Single Phase and Three Phase Smart Meters data.

If the chip random number fails, the software enables code generation random numbers instead of chip random number detection.

Module network interruption—which may occur during active communication—can be categorized into: (1) physical link disconnection between the module and the meter, and (2) communication-protocol failure between the module and the meter. For physical link disconnection, Holley's Single Phase and Three Phase Smart Meters generate an event log for subsequent maintenance review. For communication-protocol failure, an automatic recovery mechanism is employed: the meter and module attempt handshake every 3 minutes; once network connectivity is restored for more than 3 minutes, communication resumes (remote-communication interruption reset time = 3 minutes). If no data exchange is detected between the meter and module for 25 consecutive hours (per company standard), the meters reset the communication block and re-initialize the module link to restore connectivity. Consequently, if a meter remains offline for over 25 hours, on-site inspection by maintenance personnel is required.

6.2.4.2 Tamper notification (FPT_TNN.1)

FPT_TNN.1 Tamper notification

Dependencies: None

FPT_TNN.1.1 The TSF shall monitor *list of TSF devices/elements for which active detection is required stated in Table 21：Tamper notification* and notify *designated user(s), role(s), or interface(s) stated in Table 21：Tamper notification* when physical tampering of the following types has occurred:

(1) Magnetic interference

(2) *list of additional physical tampering scenarios stated in Table 21：Tamper notification*.

list of TSF devices/elements for which active detection is required	designated user(s), role(s), or interface(s)	physical tampering scenarios	Note
meter cover	MCU Hardware interface: IO/EXIT interrupt When the meter cover is open, the third lower triangle symbol from left to right is always bright. 	meter cover detect	Two buttons are installed under the main meter cover and the terminal cover, respectively. When a cover is removed, the corresponding button state changes. Upon meter power-up, the system monitors the button status every second for 3 seconds to detect cover-open conditions. If a cover-open event is detected, the meter records the event in the security log and sends an alert. During a power outage, a cover-open state transition (from closed to open) triggers an interrupt that wakes the meter from sleep mode and switches the MCU to low-power operation; the meter then writes the cover-open status to EEPROM. Following power restoration, the meter checks the stored cover-open status in the MCU. If the status is TRUE, the meter records the event in the security log and sends an alert.
terminal cover	MCU Hardware interface: IO/EXIT When the terminal cover is open, the second lower triangle symbol from left to right is always bright. 	terminal detect	
Magnetic induction detection chip	MCU Hardware interface: IO When magnetic influence occurs, the fourth lower triangle symbol from left to right is always bright.	magnetic field detect	There is a magnetic sensor installed within the meter for Magnetic field detection.

			
modem cover	MCU Hardware interface: IO When the modem cover is open, the first lower triangle symbol of the LCD from left to right is always bright. 	modem cover detect	A hardware-based Modem cover-open detection circuit is implemented. The cover status is polled every second, and three consecutive stable readings are used to determine whether the Modem cover has been removed. This check is performed only while the meter is powered on. Upon detection of cover removal, the meter records the event in the event log and triggers an alert.
battery interface	The MCU provides hardware interfaces via ch0&ch1 for battery voltage monitoring. When the voltage is between 3.0V and 3.3V, a steady "battery undervoltage" symbol is displayed. If the voltage drops below 3.0 V, the symbol flashes to prompt battery replacement.	battery level detect	The main chip ADC module calculates the voltage value of the connected battery, and compares it with the standard voltage to determine whether it is undervoltage or the battery needs to be replaced. When the voltage is 3.0v-3.3v, the battery is undervoltage. The battery needs to be replaced when it is below 3.0V.

Table 21： Tamper notification

Application Note 23

The second assignment ('designated user, role, or interface'), describes the way in which notification is conveyed via communication with a specific subject or else by using a particular interface (or both). The use of an interface could include, for example, a light on a device panel, or the sending of a particular alarm message, or the recording of a particular log entry. The content of the alarm message and/or log entry should be described using FAU_ARP.2, and the protection of the log against modification (cf. FAU_STG.2) associated with the tamper event should be described in the TOE Summary Specification.

Where an alarm is raised, this shall be sent at or before the meter's next default communication opportunity.

The final assignment for additional tampering scenarios may be left blank if no additional scenarios are supported.

The requirement to monitor and notify the presence of magnetic interference relates to the electromagnetic disturbances requirements of the EU Measuring Instruments Directive 014/32/EU.

6.2.4.3 Basic TSF Self Testing (FPT_BST.1)

FPT_BST.1 Basic TSF Self Testing

Dependencies: No dependencies.

FPT_BST.1.1 The TSF shall run a suite of the following self-tests during Initial start-up (on power on), on reset to demonstrate the correct operation of the TSF:
(1) Firmware integrity test
(2) Random bit generator test
(3) Correct TSF start-up
(4) None.

Application Note 24

The ST author defines in the TOE Summary Specification the specific tests carried out.

6.2.4.4 Replay detection (FPT_RPL.1)

FPT_RPL.1 Replay detection

Dependencies: No dependencies

FPT_RPL.1.1 The TSF shall detect replay for the following **message types**: (1) *all communication data, and* (2) *all meter-communication data. After the first successful operation, any subsequent communication containing identical data shall be rejected.*

FPT_RPL.1.2 The TSF shall ~~**perform**~~ discard the message and *reply to the user with a failed message* when replay is detected.

6.2.4.5 Reliable time stamps (FPT_STM.1)

FPT_STM.1 Reliable time stamps

Dependencies: No dependencies

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application Note 25

The TOE must provide time stamps suitable for supporting the time in an audit record for FAU_GEN.1.

6.2.4.6 Trusted update (FPT_TSU.1)

FPT_TSU.1 Trusted Software/Firmware Update

Dependencies: FCS_COP.1

FPT_TSU.1.1 The TSF shall provide *all roles* the ability to query the currently executing version of the TOE **firmware**.

FPT_TSU.1.2 The TSF shall provide means to authenticate and verify the integrity of ***firmware*** updates to the TOE prior to installing those updates, using a digital signature mechanism that meets the following: *The client uses sha256 to compute a digest of the firmware to be updated. And the client uses ECDSA's signature algorithm to compute a digital signature of this digest with its own signature private key;*

After TOE receives the complete firmware upgrade package, it needs to use sha256 to calculate the summary of the firmware to be updated. TOE uses the client signature public key and ECDSA signature algorithm to verify the firmware signature information sent by the client. After successful signature verification, firmware update can be triggered.

FPT_TSU.1.3 The TSF shall provide means to verify the following additional properties of software/firmware updates to the TOE prior to installing those updates: *None*.

FPT_TSU.1.4 The TSF shall provide *Administrator, Operator* the ability to activate updates to TOE ***firmware***.

Application Note 26

In FPT_TSU.1.1 the version currently executing may not be the same as the version most recently downloaded, since a downloaded version may not yet have been activated.

In some cases the 'version' of the TOE firmware may be made up of a number of versions for

individually identified components of that firmware.

The cryptographic operations used to implement the digital signature mechanism in FPT_TSU.1.2 must be specified in iterations of FCS_COP.1.

Examples of the properties specified in FPT_TSU.1.3 might be ensuring that the update is intended for the TOE type or instance, or ensuring that the update is a later version than the currently executing version.

Activation in FPT_TSU.1.4 results in the updated firmware being executed.

If the TOE does not support the querying of the currently executing version then it is legitimate to complete the assignment of the list of roles in FPT_TSU.1.1 with 'None', and in this case the SFR element is treated as trivially satisfied.

As noted for O.SecureUpdate, FPT_TSU.1 applies to all firmware in the TOE that can be updated.

6.2.5 Security Management

6.2.5.1 Security roles (FMT_SMR.1)

FMT_SMR.1 Security roles

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1 The TSF shall maintain the roles *Public, Administrator, Operator, Technician*.

FMT_SMR.1.2 The TSF shall be able to associate **received messages and keys** with roles.

Application Note 27

Role-based access controls are defined in FDP_ACF.1, FDP_IFF.1/Msgs, FDP_IFF.1/Keys, FPT_TSU.1, FMT_MOF.1, FMT_MTD.1/Audit and FMT_MTD.1/Time.

The roles described here include all the roles necessary to use any type of access on any of the available interfaces in FDP_IFF.1/Int, which include all operational interfaces to the device. The list of roles thus includes any roles that have special access not available to other roles, such as administrative or maintenance roles.

If the permissions allocated to roles are configurable then this is described by the ST author in FMT_MOF.1

6.2.5.2 Management of Security Functions Behaviour (FMT_MOF.1)

FMT_MOF.1 Management of Security Functions Behaviour

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to determine the behaviour of the functions *listed in the TSF Configuration Table* to *the authorised identified roles in the TSF Configuration Table*.

Application Note 28

For each row in the TSF Configuration Table, if configuration of the identified item in the Function column is possible then the ST author selects 'Configurable' in the Configurable Status column for that row, and adds the list of roles that can configure it in the final column of the row. If it is not possible to configure this TSF data then the ST author selects 'Not configurable' in the Configurable Status column and completes the assignment in the final column of that row ('the authorised identified roles') as 'None'. The ST author may add other rows to the table below the rows specified in the PP, if applicable.

ID	**function**	**Configurable status**	**Authorised configured roles**
(i)	Allowed number of consecutive failed authentication attempts (FIA_AFL.1)	Configurable	*Administrator, Operator*
(ii)	The time to block access when the number of consecutive failed authentication attempts exceeds the permitted limit(FIA_AFL.1).	Configurable	*Administrator, Operator*
(iii)	The protection level applicable to the data exchange for all types of applications (FDP_IFF.1/Msgs)	Not configurable	*None*
(iv)	Trigger an alarm when an event occurs (FAU_ARP.2)	Not configurable	*None*
(v)	The alarm destination when	Not configurable	*None*

	the event occurred (FAU_ARP.2)		
(vi)	Permissions assigned to a role (FDP_ACF.1, FDP_IFF.1/Msgs, FDP_IFF.1/Keys, FPT_TSU.1, FMT_MOF.1, FMT_MTD.1/Audit FMT_MTD.1/Time)	Not configurable	*None*

Table 22：TSF Configuration Table

Application Note 29

For row (iii), the ST author identifies any configuration that the TSF permits of the protection levels in terms of the message types and attributes identified in FDP_IFF.1/Msgs. This can be done by identifying each of the different available types of configuration when completing the assignment of 'authorised identified roles' (e.g. "...protection level for 'meter update' message type by Meter Owner role only; protection level for 'Energy Supplier update' messages by Supplier role only; ..."). If permissions allocated to roles are configurable in row (vi) then the impact of this configurability must be noted by the ST author for any other SFRs that require identification of permitted roles (e.g. FMT_MOF.1, all FMT_MTD.1 iterations, and FAU_SAR.1). In other words: if permissions allocated to roles can change according to configuration settings, s, then the other SFRs that depend on permissions allocated to roles must be stated in a way that takes account of possible changes to the role-permissions configuration.

6.2.5.3 Management of TSF data (FMT_MTD.1) - Audit

FMT_MTD.1/Audit Management of TSF data

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/Audit The TSF shall restrict the ability to delete the *audit log records* to *Administrator, Operator*.

Application Note 30

When audit log records are overwritten because space for new records is exhausted (cf. FAU_STG.4 in section 6.2.6.6) then there may be no role involved and this situation does not need to be covered in this SFR. This SFR describes the roles that can delete (or clear) the audit log records for all other cases in which audit records are deleted. Any roles are taken from the list of defined roles in FMT_SMR.1 (section 6.2.5.1).

If an alarm message is sent before old records are overwritten then this is included under FAU_ARP.2 (Section 6.2.6.1).

6.2.5.4 Management of TSF data (FMT_MTD.1) - Time

FMT_MTD.1/Time Management of TSF data

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/Time The TSF shall restrict the ability to modify the *meter time* to *Administrator, Operator*.

6.2.6 Security Audit

6.2.6.1 Security Event Alarm (FAU_ARP.2)

FAU_ARP.2 Security Event Alarm

Dependencies: No dependencies

FAU_ARP.2.1 The TSF shall send an alarm message to the indicated destination for the following events:

• Critical events: *defined in the Critical Events Table*

Event ID	Items	Destination
2105	Watchdog trigger results in meter reset	Local storage and AMI System
2104	Random number error	Local storage and AMI System
5023	Change in network status	Local storage and AMI System

Table 23：Critical Events

•Physical tampering events: *defined in the Physical Tampering Events Table*

Event ID	Items	Destination
495	Open modem cover start	Local storage and AMI System
203	Open terminal cover start	Local storage and AMI System
201	Open meter cover start	Local storage and AMI System
204	Magnetic influence start	Local storage and AMI System
1603	Battery undervoltage	Local storage and AMI System

Table 24：Physical Tampering Events

•Other events: *defined in the Other Events Table*.

Event ID	Items	Destination

1502	Change of stored external party key	Local storage and AMI System
1504	HLS_Unsuccess	Local storage and AMI System

Table 25：Other Events

FAU_ARP.2.2 The TSF shall include within each alarm message at least the following information:

a) Date and time of the event;

b) Type of event.

FAU_ARP.2.3 The TSF shall include the following additional alarm information: *Sequence Number, Event Id.*

FAU_ARP.2.4 The TSF shall send alarms according to the following timing rules:

• *Alarms shall be sent at or before the meter's next default communication opportunity.*

Application Note 31

If the criteria for sending alarms are configurable in the TOE then this is specified in FAU_ARP.2.1 and the constraints on the roles that can perform configuration are specified in FMT_MOF.1. The physical tampering scenarios as specified in FPT_TNN.1 are included in the physical tampering events in FAU_ARP.2.1 – other events included in FPT_TNN.1 that result in sending of alarm messages should also be included in this SFR.

Note:

1) Sequence Number is a unique number used to identify the order of log entries, ensuring that each log record is uniquely identified and arranged in the order in which it was generated for subsequent trail, auditing, and analysis.

2) Event ID is a unique identifier used to represent a specific event type. By assigning a unique number to each specific event, the system can accurately identify and classify various events. It is a key element in event management and log analysis.

3) Alarm events can be viewed under different event types defined in the TOE based on their Event IDs. For details, refer to the appendix.

6.2.6.2 Audit data generation (FAU_GEN.1)

FAU_GEN.1 Audit data generation

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate audit data of the following auditable events:

~~a) **Start-up and shutdown of the audit functions;**~~

b) ~~**All auditable events for the not specified level of audit;**~~

c) Power-up/resume of the TOE

d) Power-down of the TOE

e) Reset or reboot of the TOE

f) Reset triggered by watchdog timer (FPT_FLS.1)

g) Change in network status

h) Energy supply connect/disconnect

i) Load limitation configuration/activation

j) Authentication failure (FIA_UAU.6, FIA_AFL.1)

k) Successful firmware update (FPT_TSU.1)

l) Firmware update attempt failure due to invalid digital signature (FPT_TSU.1)

m) Setting/updating meter time (FMT_MTD.1/Time)

n) Tamper detection events (FPT_TNN.1)

o) Detected replay events (FPT_RPL.1)

p) Change of stored external party key (FDP_IFF.1/Keys)

q) Key generation (FCS_CKM.1)

r) Message received from an unauthorised source (FDP_IFF.1/Msgs)

s) Key received from an unauthorised source (FDP_IFF.1/Keys)

t) Change of stored meter key (FDP_IFF.1/Keys)

u) Change of access rights (FAU_SAR.2, FMT_MOF.1)

v) Device error events as follows: Network interruption, etc. (FPT_BST.T.1, FPT_FLS.1)

w) Failure of the random bit generator ((FPT_BST.T.1, FCS_RNG.1)

x) Clearing the audit log (FAU_STG.2)

y) Security anomaly events as follows: None.

z) Modification of defined in the Modification of data Type Table

Data Type
Meter Configuration Parameters

Table 26：Modification of Data Type

aa) Self-test completed FPT_BST.1

bb) See appendix.

Note:
Audit events can be viewed under different event types defined in the TOE based on their Event IDs. For details, refer to the appendix.

FAU_GEN.1.2 The TSF shall record within the audit data at least the following information:

a) Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;

b) For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST:

- *Each audit record shall include a sequence number*;
- *None*.

Application Note 32

If a listed event can never arise on a meter then the audit requirement for that event is considered to be trivially satisfied. For example, if the meter does not generate its own keys (cf.Application Note 10) then the requirement in item p) is considered to be trivially satisfied, although any change of the stored meter key (e.g. due to receiving an updated key from an authorised source) must be audited for items).

The events 'message received from an unauthorised source' and 'key received from an unauthorised source' in FAU_GEN.1.1 items r) and s) are interpreted by the ST author according to the specific mechanisms used to receive messages and keys, as described for FDP_IFF.1/Msgs and FDP_IFF.1/Keys(e.g. this may be message-based or channel-based).

In some TOEs, FAU_GEN.1.1 item q) (meter key generation) and item t) (change of stored meter key)may be the same event, provided that the log record makes it unambiguous which key has been generated.

'Security anomaly events' in FAU_GEN.1.1 item y) are events that are logged in order to assist in detection or investigation of security incidents involving the TOE. The 'auditable data categories' in FAU_GEN.1.1 item z) are related to the objects defined in the access control rules in FDP_ACF.1.

6.2.6.3 Audit review (FAU_SAR.1 – refined)

FAU_SAR.1 Audit review

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide *Public, Administrator, Operator, Technician* with the capability to *read the contents* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in **the format specific in the following reference:** ***defined in the following Log Format***.

Application Note 33

The method of authorisation for reading audit records is described in FAU_SAR.2 (section 6.2.6.4).

Log Format:

Structure of audit records

Time + Sequence Number + Event Id + EventType OBIS

Analysis of audit record structure

<Structure Qty="04" >

<!-- 2023/9/15 17:07:00-08:00 -->

< Time ="07E7090F051107000001E080" />

< Sequence Number ="00000032" />

< Event Id ="012C" />

< Event OBIS ="0000636200FF" />

</Structure>

1) Analysis of time structure

The time structure is as follows, where "07E7090F051107000001E080" is the concatenation of the hexadecimal strings of the fields below.

OCTET STRING (SIZE(12))

{

year highbyte,

year lowbyte,

month,

day of month,

day of week,

hour,

minute,

second,

hundredths of second,

deviation highbyte,

deviation lowbyte,

clock status

}

2) Sequence Number *is the serial number of the audit record,*

represented as a hexadecimal number, which accumulates as audit events are continuously recorded.

3) ***Event Id*** *refers to a specific event, with the detailed content found in Appendix Table 35-Table 39, where "012C" is the hexadecimal representation of the Event Id.*

4) ***Event OBIS*** *refers to a specific event type, with the detailed content found in Appendix Table 34, where "0000636200FF" is its hexadecimal representation.*

6.2.6.4 Restricted audit review (FAU_SAR.2 – refined)

FAU_SAR.2 Restricted audit review

Dependencies: FAU_SAR.1 Audit data generation

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted ~~**explicit**~~ read-access **by** *defining the read permissions for the audit records in the dlms_obis.h file, as shown in the Items and Access Authorization Table, which is not modified.*

.

Items	**Access Authorization**
Standard Event	Public /Administrator/ Operator / Technician can read events. Administrator/ Operator can clear events.
Power Grid Event	Public /Administrator/ Operator / Technician can read events. Administrator/ Operator can clear events.
Disconnector Event	Public /Administrator/ Operator / Technician can read events. Administrator/ Operator can clear events.
Current Event	Public /Administrator/ Operator / Technician can read events. Administrator/ Operator can clear events.
Security Event	Public /Administrator/ Operator / Technician can read events. Administrator/ Operator can clear events.
Other Event	Public /Administrator/ Operator / Technician can read events. Administrator/ Operator can clear events.

Table 27：Items and Access Authorization

6.2.6.5 Protected audit data storage (FAU_STG.2)

FAU_STG.2 Protected audit data storage

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to prevent ~~**unauthorised**~~ modifications to the stored audit records in the audit trail.

Application Note 34

Authorised deletion of audit log records is as specified in FMT_MTD.1/Audit (section 0) and is not considered to be a 'modification' of the log records. It is not expected that the TOE will allow any form of modification to stored audit records.

6.2.6.6 Action in case of possible audit data loss (FAU_STG.4)

FAU_STG.4 Action in case of possible audit data loss

Dependencies: FAU_STG.2 Protected audit data storage

FAU_STG.4.1 The TSF shall *overwrite the oldest record* if the audit trail exceeds *pre-defined limit* ***in terms of number of records supported*** *defined in the Pre-defined Limit for Different Event Type Table*.

Event Type	Limit in terms of number of records
Standard Event	250
Power Grid Event	250
Disconnector Event	100
Current Event	250
Security Event	100
Other Event	100

Table 28：Pre-defined Limit for Different Event Type

Application Note 35

If the TOE overwrites audit records when space for new records is exhausted then this SFR applies to the action taken before overwriting audit records that have not yet been read from the TOE.

6.2.7 Inter-TSF trusted channel

6.2.7.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1 Inter-TSF trusted channel

Dependencies: No dependencies

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit *AMI Key Management System* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *key import*.

Note: The imported keys include: Mater key, Global Authentication key, Global Encryption key, Global Broadcast key, and Client Public Key. The trusted channel used is a specialized VPN network, and the port used by Holley's Single Phase and Three Phase Smart Meters is a Wi-SUN network port.

6.3 Security Assurance Requirements

The evaluation assurance level for this ST is EAL4 augmented with ALC_FLR.3. The assurance components are identified in the table below (with augmentations in bold).

Assurance Class	Assurance Components
Security Target (ASE)	ST introduction (ASE_INT.1)
	Conformance claims (ASE_CCL.1)
	Security problem definition (ASE_SPD.1)
	Security objectives (ASE_OBJ.2)
	Extended components definition (ASE_ECD.1)
	Derived security requirements (ASE_REQ.2)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Security architecture description (ADV_ARC.1)

	Complete functional specification (ADV_FSP.4)
	Basic modular design (ADV_TDS.3)
	Implementation representation of the TSF (ADV_IMP.1)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life cycle support (ALC)	Production support, acceptance procedures and automation (ALC_CMC.4)
	Problem tracking CM coverage (ALC_CMS.4)
	Delivery procedures (ALC_DEL.1)
	Identification of security controls (ALC_DVS.1)
	Developer defined life-cycle processes (ALC_LCD.1)
	Systematic flaw remediation (ALC_FLR.3)
	Well-defined development tools (ALC_TAT.1)
Tests (ATE)	Functional testing (ATE_FUN.1)
	Analysis of coverage (ATE_COV.2)
	Testing: basic design (ATE_DPT.1)
	Independent testing – sample (ATE_IND.2)
Vulnerability assessment (AVA)	Focused vulnerability analysis (AVA_VAN.3)

Table 29：Security Assurance Requirements

6.3.1 Refinements of Security Assurance Requirements

The following refinements are made to selected assurance requirements in Table 29：Security Assurance Requirements. The following refinements are based on Smart Meter Minimum Security requirements [1].

6.3.1.1 Derived Security Requirements (ASE_REQ.2)

ASE_REQ.2 Derived security requirements

Refinement:

When interpreting the generic work unit requirements for ASE_REQ.2 to apply to the meter, the evaluator shall check that the SFRs in the ST are consistent in their descriptions as described in the PP Application Notes (e.g. the action in the case of a meter that does not generate keys as described in Application Note 10, and the complete coverage of interfaces, operations and data between SFRs as described in Application Note 17).

6.3.1.2 Security Architecture Description (ADV_ARC.1)

ADV_ARC.1 Security architecture description

Refinement:

When interpreting the generic work unit requirements for ADV_ARC.1 to apply to the meter, the following specific topics must be addressed for this Protection Profile. It is acceptable for references to deliverables supplied for other assurance families, such as ADV_FSP, to be used to meet these requirements, provided that the relationship of the relevant interface specifications to the concepts in the Protection Profile is clear.

1. The Security Architecture Description shall include:

    a) A description of the parts of the TOE firmware that can be updated and the mechanisms used to perform the updates. The evaluator shall confirm that all parts of the TOE firmware that can be updated are updated according to FPT_TSU.1

    b) A description of the way in which the TOE erases keys (for FCS_CKM.6) and deallocates objects identified in FDP_RIP.1. This shall include source code excerpts and corresponding compiler output showing that the deletion process is effective, that it is retained during compilation (e.g. that it is not removed by compiler optimisation rules) and is applied at all necessary points in the TSF (i.e. in all situations where the keys and objects are deleted). The evaluator shall confirm that the code meets the requirements of the SFRs, and that it is applied in all relevant deletion situations.

2. The evaluator assessment of ADV_ARC.1.4C and ADV_ARC.1.5C shall include:

    a) Confirmation that the developer's lifecycle includes effective techniques to prevent and minimise the likely effects of failures, flaws or effects of malicious payloads sent to the meter. Examples of such techniques could be static analysis using MISRA rules, and use of compiler-supported stack protection. Note that use of these techniques is closely related to the requirement (in the refinement of ADV_TDS.3) for a rationale relating to the use of firmware protection measures.

    b) Confirmation that the access controls over types of data defined in FDP_ACF.1.1 are given equivalent protection when the data is accessed via messages, according to the rules in FDP_IFF.1/Msgs (possibly in combination with the rules in FDP_IFF.1/Keys)

    c) Confirmation that data exchanges between the meter and message originator/recipient are protected over the entire communication path between the endpoints.

6.3.1.3 Complete functional specification (ADV_FSP.4)

ADV_FSP.4 Complete functional specification

Refinement:

When interpreting the generic work unit requirements for ADV_FSP.4 to apply to the meter,

the following specific topics must be addressed for this Protection Profile. It is acceptable for references to deliverables supplied for other assurance families to be used to meet these requirements, provided that the relationship of the relevant interface specifications to the concepts in the Protection Profile is clear.

1. The Functional Specification shall describe, for each interface to the meter that is available and that is enabled, how the security requirements supporting the SFRs are implemented for messages at different levels of protocol (e.g. application and communications levels). T The evaluator shall confirm that the application layer implements at least the following security properties for defined groups of messages:

    - Authentication of message origin
    - Protection against replay of messages
    - Encryption of sensitive data
    - Integrity protection of message content
    - Authorisation rules to recognise sources that are permitted to send the message type.

    This may be demonstrated by reference to external reference documents (e.g. message specifications for a national smart meter infrastructure). Different groups of message types may be allocated different levels of protection, but the level of protection for each message type must be specified (such that the expected protection for any given message can be unambiguously determined from the specification). The description shall include the protocols used and the ways that the relevant security properties (authentication, encryption, etc.) are provided by cryptographic mechanisms.

    The Functional Specification shall identify any secure channels (or other secure communication mechanism) used for the import of secret or private keys or random bits (cf. Application Note 10, Application Note 17). The evaluator shall check that these secure channels are described in SFRs, and that they are included in the testing for ATE_IND.

2. The evaluator shall confirm that all message types, operations and data types available over all interfaces are covered unambiguously by the defined protection and authorisation rules in the Meter Data SFP (FDP_ACF.1), Messages SFP (FDP_IFF.1/Msgs), and the Keys SFP (FDP_IFF.1/Keys).

3. Description of the cryptographic mechanisms shall include:

    - Cryptographic algorithms
    - Key and signature length
    - Client/server authentication
    - Specification of entropy
    - Cryptographic Random Bit Generation
    - Storage of keys.

    The evaluator shall confirm that all cryptographic mechanisms and key management mechanisms used are defined in terms of open standards. The developer shall identify the source used for definition of approval of the mechanisms used by the meter, and the

evaluator shall check that this information is included in the ST.

4. All keys required for the enforcement of the SFRs shall be listed in the design documentation, and for each key the following details shall be described:

    - purpose of the key
    - source (e.g. import or specific method of internal generation in the meter)
    - storage location (e.g. non-volatile memory within the meter, or a separate tamper-resistant secure module within the meter case)
    - storage format (e.g. wrapped according to a specified standard)
    - the method of replacement (if applicable) (e.g. in terms of a specific message type from a specific role)
    - the method of destruction of the key (cf. FCS_CKM.6).

    The evaluator shall check this list against the rules in FDP_IFF.1/Keys to ensure that all keys are covered by the defined rules.

5. The Functional Specification shall identify all interfaces to the meter that are available, and shall distinguish any of these interfaces that are disabled as required by FDP_IFC.1.5/Int from those interfaces that are enabled. The Functional Specification shall describe which functional interfaces are accessible over each of the communications interfaces (WAN, Neighbourhood Network, Local Network or direct connection). (Note that the refinement of ADV_TDS.3 requires additional information about these disabled interfaces.) The evaluator shall check that only operational interfaces are enabled in the operational configuration, and that these are all subject to the SFRs.

6. The Functional Specification shall specify any roles and associated interfaces that are supported in any stage of the device lifecycle (e.g. menus or command sets that are available before installation or after decommissioning). The device design information shall include a complete definition of the logical and physical interfaces that are available (such that the information could be used to create a test tool that will exercise all parts of the interface, with an ability to define expected results for any communication). The evaluator shall check that any such interfaces from lifecycle stages other than the normal operational stage (i.e. as used to monitor the supply to a consumer) that are not fully governed by the SFRs are not accessible in the normal operational stage.

7. The evaluator shall confirm, by examining the relevant channel, protocol and message definitions, that entities with which the meter communicates by messaging are uniquely identifiable.

8. The Functional Specification shall describe the types of failure identified by the TSF and the recovery actions taken by the TOE for FPT_FLS.1 (this information is used by the evaluator to support testing of failures as part of ATE_IND).

9. The Functional Specification shall describe the boundary over which FPT_TNN.1 applies in terms of the meter architecture (this information is used by the evaluator to support testing of physical protection in FPT_TNN.1 and FDP_IFF.1/Int as part of ATE_IND and AVA_VAN).

10. Description of the digital signature mechanism used for firmware updates (FPT_TSU.1), including the format of the updates. (This supports evaluator testing of specific types of unsuccessful update attempts as part of ATE_IND).

6.3.1.4 Basic modular design (ADV_TDS.3)

ADV_TDS.3 Basic modular design

Refinement:

When interpreting the generic work unit requirements for ADV_TDS.3 to apply to the meter, the following specific topics must be addressed for this Protection Profile as part of the TOE Design Specification:

1. The TOE Design shall describe the mechanisms that protect data at rest in the meter. The evaluator shall confirm that these are sufficient to enforce the data protection SFRs in FDP_ACF.1 and FDP_IFF.1/Keys.

2. The TOE Design shall describe, in terms of the firmware design, why all operational interfaces are subject to the requirements of FDP_ACF.1, FDP_IFF.1/Msgs and FDP_IFF.1/Keys (e.g. in terms of the paths through which received messages are routed in the firmware and the order of processing fields in inputs).

3. The TOE Design shall justify that all instances of cryptographic mechanisms used at meter interfaces (e.g. for message protection, authentication, and random seed creation) and to protect data at rest (e.g. encryption of confidential information stored inside the meter) use approved mechanisms, and shall identify the nature of the approval and any relevant evidence (e.g. NIST CAVP certificates). The evaluator shall confirm the correctness of any identified evidence (i.e. that they relate to the relevant TOE components and that the components are used in accordance with any conditions of the certification)

4. The TOE Design shall describe the keys held in the meter, their source (e.g. imported, or generated in the meter using FCS_RNG.1), their storage location in the meter, and their storage format (e.g. wrapped or encrypted by a key encryption key). The evaluator shall confirm that this information is consistent with the requirements of FCS_CKM.1, FCS_CKM.6, and FDP_IFF.1/Keys

5. The TOE Design shall identify and describe the purpose of all data generated by the random bit generator in the TOE. (This information supports the evaluator analysis of key generation and support for any randomness properties relied upon in other SFRs.)

6. The TOE Design shall describe the way in which the boundary over which FPT_TNN.1 is enforced, at a level of detail that enables evaluators to construct and carry out tests to investigate the generation of the relevant notifications when the tamper events occur (FPT_TNN.1). (This information supports evaluator testing under ATE_IND and AVA_VAN.)

7. The TOE Design shall describe the purpose and use of any interface that is presented but

disabled as required by FDP_IFF.1.5/Int (i.e. what is intended to be achieved by using the interface and the protocols/commands that it uses). In particular this description shall describe:

- what elements of the TOE (e.g. configuration data, other stored data, firmware) are accessible over the interface before it is disabled
- how the interface is disabled
- whether the disabled state of the interface is reversible, and how any such re-enablement is achieved.

The evaluator shall confirm that the methods of disablement are of at least equivalent strength to the methods of authorisation for access to data and functions in the TOE, and that any reenablement attack can only be carried out in physical proximity to the device and above the attack potential required under AVA_VAN.

8. The TOE Design shall include a rationale for how specific firmware protection measures are included in order to prevent or mitigate the potential effects of failures, flaws or malicious payloads sent to the meter. Examples of such techniques could be static analysis against MISRA rules, stack and heap protection measures to respond to corruption of these structures, and making it impossible to execute code from certain areas of memory. This rationale supports the evaluator analysis (in the refinement of ADV_ARC.1) to confirm the use of effective techniques to prevent and minimise the likely effects of failures, flaws or effects of malicious payloads.

6.3.1.5 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1 Operational user guidance

Refinement:

When interpreting the generic work unit requirements for AGD_OPE.1 to apply to the meter, the following specific topics must be addressed for this Protection Profile as part of the Operational Guidance for the TOE:

1. Resources available for the audit log shall be described, including their limitations, such that users (i.e. the AMI system entities concerned with collecting and analysing the audit log) are made aware of any situations in which audit information might be lost (FAU_STG.4)

2. Resources available for firmware updates and any operational limitations imposed during the update process (FPT_TSU.1)

3. Description of the access control policies and identification of the implementation-specific objects that they refer to, including those objects referred to as ‘metrologically certified data’, ‘credentials’, ‘meter configuration’ and ‘controlled meter data items’ in FDP_ACC.2 and FDP_ACF.1.

4. Description of any user actions required in order to put the meter into its operational

configuration (e.g. any configuration steps, key generation, or trust anchor key installation). The evaluator shall confirm that this is consistent with the description of keys in the TOE Design, and with the requirements of the SFRs.

5. Description of the results of self-tests carried out by the meter or secure failure recovery actions, and the expected actions from the user in response to each of these results (cf. FPT_BST.1, FPT_FLS.1)

6. Description of configurable parameters and their allowed values (cf. FMT_MOF.1). If the allowed actions for roles are configurable then this must also be described in the operational guidance.

6.3.1.6 Identification of Security Measures (ALC_DVS.1)

ALC_DVS.1 Identification of Security Measures

Refinement:

When interpreting the generic work unit requirements for ALC_DVS.1 to apply to the meter, the following specific topics must be addressed for this Protection Profile as part of the Development Security for the TOE:

1. The development security documentation shall include a description of the security-related activities carried out in the manufacturing environment of the meter and the security measures implemented to protect those activities. Examples of such activities would be disabling of test interfaces, installation of public key certificates to act as trust anchors, generation and injection of keys or random number seeds, and setting default security configuration parameters.

2. In addition to visiting the development environment, the evaluator shall also visit the manufacturing environment to examine the implementation of the security measures, to determine that the security measures are being applied, and to determine the sufficiency of the security measures employed.

3. The evaluator shall confirm that manufacturing leaves the meter in a secure state in which unauthorised users cannot change the security configuration (e.g. by changing access controls or changing installed keys), or else that the delivery procedures sufficiently protect the physical instances of the TOE against tampering between manufacturing and delivery to the customer.

6.3.1.7 Independent Testing – Sample (ATE_IND.2)

ATE_IND.2 Independent testing – sample

Refinement:

When interpreting the generic work unit requirements for ATE_IND.2 to apply to the meter, for the purposes of this Protection Profile the evaluator’s test sample shall include at least:

1. Testing the correct response to consecutive authentication failures that exceed the threshold in FIA_AFL.1 as configured according to FMT_MOF.1 (in terms of the failures threshold and the time for which access is blocked)
2. Testing that re-authentication behaviour is as specified (FIA_UAU.6).
3. Testing each of the rules for message protection in FDP_IFF.1/Msgs. As part of the tests the evaluator shall check that the cryptographic formatting specified in design deliverables is applied to messages sent to the TOE (e.g. by constructing messages in accordance with the design deliverables) and responses received from the TOE (e.g. by decoding responses, including decrypting and checking MACs and signatures as specified in the design deliverables).
4. Testing each of the rules for export of meter keys in FDP_IFF.1/Keys
5. Testing each of the rules for import of other entity keys in FDP_IFF.1/Keys
6. Testing communications failures of the following types:
    - message floods
    - out-of-sequence messages
    - malformed messages
    - lack of expected response
    - lack of expected regular input.
7. Testing for correct rejection of a sample of replayed messages (FPT_RPL.1).
8. Testing a sample of the failure types identified in FPT_FLS.1.
9. Testing a sample of the failure types identified in FPT_BST.1.
10. Testing a sample of the tampering events identified in FPT_TNN.1 and.
11. Testing successful firmware update and unsuccessful update due to invalid digital signature conditions as in FPT_TSU.1 (depending on the signature mechanism this may require several tests to cover different reasons for failure, such as failure of a certification path validation, incorrect digital signature value, and incorrect image hash value (if the image hash is separate from the digital signature).
12. Confirming by examination of configuration interfaces that all the restriction of configuration operations is as specified in FMT_MOF.1, FMT_MTD.1/Audit and FMT_MTD.1/Time. This shall include a check that the relevant parameters either are not configurable or else can only be modified by the identified roles
13. If the TOE supports configuration of permissions allocated to roles (see row (vi) in the TSF Configuration Table and FMT_MOF.1) then this configuration shall also be tested in terms of both positive and negative effects (i.e. tests of changes to both actions allowed and actions not allowed).
14. The evaluator shall test the deletion of keys (as in FCS_CKM.6) and the objects identified in FDP_RIP.1, to demonstrate that after deletion then the key/object cannot be accessed

via at least one of the functions that would previously have been used to access it.

15. The evaluator shall test at least one instance of each type of audit message in FAU_GEN.1.

16. The evaluator shall confirm by testing that unauthorised attempts to access the audit log are rejected (FAU_STG.2, FMT_MTD.1/Audit).

Note that testing of rules (such as in item 3 above) generally requires tests to demonstrate both positive (acceptance) and negative (rejection) cases.

6.3.1.8 Focused vulnerability analysis (AVA_VAN.3)

AVA_VAN.3 Focused vulnerability analysis

When interpreting the generic work unit requirements for AVA_VAN.3 to apply to the meter, the evaluator shall address the following specific topics for this Protection Profile.

1. Confirming (including testing) that, after installation, the power-up process does not allow the device to be launched into any mode other than the normal operating mode (e.g. no access is granted to diagnostic or recovery functions, including engineering menus, other than those permitted via the enabled interfaces according to FDP_IFF.1/Int)

2. Confirming (including testing) that, cycling power preserves the blocking time in FIA_AFL.1.2 (i.e. cycling power does not provide a method to remove the block on access)

3. Confirming (including testing) that disabled interfaces as in FDP_IFF.1/Int are not usable in practice (using the information on the disabled interfaces provided in ADV_FSP.4 and ADV_TDS.3)

7. Rationales

7.1 Security Objectives Rationale

7.1.1 Security Objectives Coverage

The table below shows the mapping of Threats, Organisational Security Policies and Assumptions to Security Objectives for the TOE and for the TOE Environment.

	O.Authorisation	O.Messages	O.DataAtRest	O.Crypto	O.Interfaces	O.Resilience	O.SecureUpdate	O.Logging	O.Alarms		OE.ExternalData	OE.AuditSupport	OE.InspectionSupport	OE.UniqueSubjectIDs
T.NetworkDisclosure	X	X	X	X	X									
T. DirectDisclosure	X	X	X	X	X								X	
T.NetworkDataMod	X	X	X	X	X									
T. DirectDataMod	X	X	X	X	X								X	
T.Malfunction					X	X	X							
P.Logging								X						
P.Alarms									X					
A.ExternalData											X			
A.AuditSupport												X		
A.InspectionSupport													X	
A.UniqueSubjectIDs														X

Table 30：Security Problem Definition mapping to Security Objectives

7.1.2 Security Objectives Sufficiency

The following paragraphs describe the rationale for the sufficiency of the Security Objectives relative to the Threats, OSPs and Assumptions.

7.1.2.1 Threats

T.NetworkDisclosure is addressed by TOE objectives as follows:

• O.Authorisation requires that successful authorisation has been checked by the TOE before an action (such as reading) is carried out on data at the request of any direct or network entity

• O.Messages requires that messages are protected against various forms of attack that might otherwise enable unauthorised messages to be used to read data remotely

• O.DataAtRest requires that data stored in the TOE is protected against unauthorised access

• O.Crypto requires the use of approved cryptographic techniques which therefore provide suitable cryptographic strength to resist attackers

• O.Interfaces ensures that there are no interfaces available that would circumvent the protections above.

T.DirectDisclosure is addressed by TOE objectives as described for T.NetworkDisclosure above, noting that the relevant TOE Objectives apply to both direct and network entities. In addition, OE.InspectionSupport supports detection of attacks that rely on physical modification of direct interfaces.

T.NetworkDataMod is addressed by TOE objectives as described for T.NetworkDisclosure above, noting that the relevant TOE Objectives apply to data modification as well as to reading data.

T.DirectDataMod is addressed by TOE objectives as described for T. NetworkDisclosure above, noting that the relevant TOE Objectives apply to both direct and network entities and to data modification as well as to reading data. In addition, OE.InspectionSupport supports detection of attacks that rely on physical modification of direct interfaces.

T.Malfunction is addressed by TOE objectives as follows:

• O.Interfaces ensures that there are no interfaces available that might enable unauthorised access to induce faults or that might assist in exploiting security vulnerabilities arising from a

malfunction.

• O.Resilience requires that the TOE checks its start-up process, and detects and recovers from identified failures in a secure way.

• O.SecureUpdate ensures that the TOE provides a secure way to update its firmware, so that malfunctions can potentially be addressed by new firmware, but that the ability to load new firmware does not provide an opportunity for unauthorised modifications of the firmware.

7.1.2.2 Organisational Security Policies

P.Logging is addressed by O.Logging, which directly translates the policy into an objective for the TOE.

P.Alarms is addressed by O.Alarms, which directly translates the policy into an objective for the TOE.

7.1.2.3 Assumptions

Each of the Assumptions in section 3.5 is directly matched by a security objective for the operational environment in section 4.2. The wording of each objective for the operational environment includes the wording of each assumption, and no further rationale is therefore given here.

7.2 Security Requirements Rationale

7.2.1 Security Objectives Coverage

The table below summarises the mapping of Security Objectives for the TOE to SFRs.

	O.Authorisation	O.Messages	O.DataAtRest	O.Crypto	O.Interfaces	O.Resilience	O.SecureUpdate	O.Logging	O.Alarms
FCS_CKM.1		X		X					
FCS_CKM.6		X	X						
FCS_COP.1/firmware signature verification		X		X			X		
FCS_COP.1/message		X		X			X		

encryption and decryption									
FCS_COP.1/key wrap		X		X			X		
FCS_RNG.1				X					
FDP_ACC.2	X		X						
FDP_ACF.1	X		X						
FDP_IFC.1/Msgs	X	X							
FDP_IFF.1/Msgs	X	X							
FDP_IFC.2/Int					X				
FDP_IFF.1/Int					X				
FDP_IFC.1/Keys	X			X					
FDP_IFF.1/Keys	X			X					
FDP_RIP.1			X						
FIA_UAU.6	X								
FIA_AFL.1	X								
FPT_BST.1						X			
FPT_FLS.1						X			
FPT_TNN.1								X	X
FPT_RPL.1		X							
FPT_STM.1								X	X
FPT_TSU.1							X		
FMT_SMR.1	X							X	X
FMT_MOF.1	X								X
FMT_MTD.1/Audit								X	
FMT_MTD.1/Time	X							X	X
FAU_ARP.2									X
FAU_GEN.1								X	
FAU_SAR.1								X	
FAU_SAR.2								X	
FAU_STG.2								X	
FAU_STG.4								X	
FTP_ITC.1		X		X					

Table 31：TOE Security Objectives mapping to SFRs

O.Authorisation is addressed by the TOE security requirements as follows:

• FDP_ACC.2 and FDP_ACF.1 state rules for authorisation of access to TOE object data

• FDP_IFC.1/Msgs and FDP_IFF.1/Msgs state rules for authorisation of messages received by the TOE

• FDP_IFC.1/Keys and FDP_IFF.1/Keys state rules for authorisation specifically related to operations on keys (noting that keys will generally form the basis for the TOE to determine the authorisation of other messages)

• FIA_UAU.6 states requirements for authentication which forms the basis for authorisation (including both initial authentication and subsequent re-authentication after a defined expiry time for the initial authentication), with FIA_AFL.1 stating the requirements for acting on repeated authentication failures, and FMT_MOF.1 stating the requirements for defined authorisation parameters (including protection levels for categories of application data) and the roles that are permitted to set them

• FMT_MTD.1/Time ensures that only authorised roles can modify the TSF time (on which authorisation decisions and expiry of authentication) may be based

• FMT_SMR.1 supports the configuration permissions in FMT_MOF.1 and FMT_MTD.1/Time by defining the relevant roles.

O.Messages is addressed by the TOE security requirements as follows:

• FCS_CKM.1 and FCS_COP.1 describe the key generation and cryptographic operations that are used to support message protection; FCS_CKM.6 ensures the protection of the cryptographic keys from unauthorised access after of deletion

• FDP_IFC.1/Msgs and FDP_IFF.1/Msgs state rules for authorisation of messages received by the TOE, with respect to roles defined in FMT_SMR.1 (thus supporting protection against unauthorised disclosure/modification and against forgery) and ensure that the TOE will not respond to unauthorised messages

• FPT_RPL.1 requires specific protection against replay of identified message types (which may include all messages)

• FTP_ITC.1 requires the provision of a secure communication channel to guarantee the security of key import to the TOE

• Implementation of the protection at the application layer (therefore providing independence from the underlying communication protocol) is confirmed as part of the refinement of ADV_FSP.4 in section 6.4.1.3.

O.DataAtRest is addressed by the TOE security requirements as follows:

• FDP_ACC.2 and FDP_ACF.1 state the rules for authorised access to various types of data object

• FCS_CKM.6 and FDP_RIP.1 ensure that when keys and other data objects are deleted then they do not present opportunities for unauthorised access.

O.Crypto is addressed by the TOE security requirements as follows:

• FCS_CKM.1 and FCS_COP.1 describe the key generation and cryptographic operations used by the TSF protection mechanisms, and the standards that these are based on

• FCS_RNG.1 states the requirements on the random bit generator

• FDP_IFC.1/Keys and FDP_IFF.1/Keys state rules to control access to keys, thus supporting the security of the cryptographic mechanisms.

• FTP_ITC.1 uses cryptographic protection mechanisms within the secure channel to protect the keys transmitted within the channel

O.Interfaces is addressed by the TOE security requirements as follows:

• FDP_IFC.2/Int and FDP_IFF.1/Int state rules to control the availability of interfaces, identifying the interfaces required for normal operation and requiring all other interfaces to be disabled. The use of FDP_IFC.2 in this case emphasises the need for an ST to account for all the interfaces present in the TOE, regardless of their intended use

• Refinements of ADV_FSP.4 and ADV_TDS.3 support the identification with more detail that enables the evaluators to confirm the completeness of the interfaces identified, and require the strength of the disabling method to be consistent with the strength of protection provided for authentication and authorisation for other operations using message-based interfaces.

O.Resilience is addressed by the TOE security requirements as follows:

• FPT_BST.1 states requirements for self-test to ensure a secure start-up of the TOE

• FPT_FLS.1 states requirements for recovery to a secure state after defined failure conditions occur.

O.SecureUpdate is addressed by the TOE security requirements as follows:

• FPT_TSU.1 requires that the TSF provides a secure update mechanism based on digital signatures

• Refinement of ADV_ARC.1 includes a requirement for the evaluator to confirm that the secure mechanism applies to all TSF firmware that can be updated

• FCS_COP.1 specifies the cryptographic operation(s) used to protect authenticity and integrity of updates.

O.Logging is addressed by the TOE security requirements as follows:

• FPT_TNN.1 identifies requirements for physical tampering attempts to be logged

• FAU_GEN.1 states requirements for other events to be logged and the basic content of the log

records

• FPT_STM.1 requires the TOE to provide accurate time for use in the log records, and FMT_MTD.1/Time ensures that this can only be modified by authorised roles

• FMT_MTD.1/Audit and FAU_STG.2 ensure that audit records can only be deleted by authorised roles and that they cannot be modified (by any role)

• FAU_SAR.1 requires that only authorised entities can read the audit log; this is reinforced by FAU_SAR.2 which requires the description of the specific method by which access is granted to the audit log

• FAU_STG.4 states the action to be taken if the log is in danger of filling up

• FMT_SMR.1 defines the roles on which audit activity and constraints are based.

O.Alarms is addressed by the TOE security requirements as follows:

• FAU_ARP.2 identifies the events that give rise to alarms (including the physical tamper and any other events required to raise alarms in FPT_TNN.1), and the basic content of an alarm

• FPT_STM.1 requires the TOE to provide accurate time for use in the log records, and FMT_MTD.1/Time ensures that this can only be modified by authorised roles

• FMT_MOF.1 defines the authorised roles that can configure alarm behaviour

• FMT_SMR.1 defines the roles on which alarm activity and constraints are based.

7.2.2 SFR Dependencies

The dependencies between SFRs are addressed as shown in Table 34. Where a dependency is not met in the manner defined in [3] then a rationale is provided for why the dependency is unnecessary or else met in some other way.

Requirement	Dependencies	Fulfilled by
FCS_CKM.1	[FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1] FCS_CKM.3 [FCS_RBG.1 or FCS_RNG.1] FCS_CKM.6	FCS_COP.1/firmware signature verification FCS_COP.1/message encryption and decryption FCS_COP.1/key wrap FCS_RNG.1 FCS_CKM.6 Because specific attributes for the SFP are not defined in the PP, the dependency on

		FCS_CKM.3 is not required.
FCS_CKM.6	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1/firmware signature verification	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.3	FCS_CKM.1 Because specific attributes for the SFP are not defined in the PP, the dependency on FCS_CKM.3 is not required.
FCS_COP.1/message encryption and decryption	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.3	FCS_CKM.1 Because specific attributes for the SFP are not defined in the PP, the dependency on FCS_CKM.3 is not required.
FCS_COP.1/key wrap	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.3	FCS_CKM.1 Because specific attributes for the SFP are not defined in the PP, the dependency on FCS_CKM.3 is not required.
FCS_RNG.1	No dependencies	
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 Because the attributes used for the access control rules are simply identity and/or role, no additional statement of management of these attributes in FMT_MSA.3 is considered necessary.
FDP_IFC.1/Msgs	FDP_IFF.1	FDP_IFF.1/Msgs
FDP_IFF.1/Msgs	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/Msgs Because specific attributes for the SFP are not defined in the PP, the dependency on FMT_MSA.3 is not required.
FDP_IFC.2/Int	FDP_IFF.1	FDP_IFF.1/Int
FDP_IFF.1/Int	FDP_IFC.1 FMT_MSA.3	FDP_IFC.2/Int Because specific attributes for the SFP are not defined in the PP, the dependency on FMT_MSA.3 is not required.
FDP_IFC.1/Keys	FDP_IFF.1	FDP_IFF.1/Keys
FDP_IFF.1/Keys	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/Keys Because specific attributes are not defined in the PP, the dependency on FMT_MSA.3 is not required.
FDP_RIP.1	No dependencies	

FIA_UAU.6	No dependencies	
FIA_AFL.1	FIA_UAU.1	For this TOE the authentication conditions (and timing of authentication) for access to private data via the user interface are defined in FIA_UAU.6 (and the transitive dependency from FIA_UAU.1 to FIA_UID.1 is not applicable because users at the user interface are not individually identified).
FPT_BST.1	No dependencies	
FPT_FLS.1	No dependencies	
FPT_TNN.1	No dependencies	
FPT_RPL.1	No dependencies	
FPT_STM.1	No dependencies	
FPT_TSU.1	FCS_COP.1	FCS_COP.1/firmware signature verification FCS_COP.1/message encryption and decryption FCS_COP.1/key wrap
FMT_SMR.1	FIA_UID.1	This dependency is not required because the TOE associates messages with roles, rather than users with roles. This approach reflects the organisational infrastructure used in smart metering.
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1
FMT_MTD.1/Audit	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1
FMT_MTD.1/Time	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1
FAU_ARP.2	No dependencies	
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_STG.2	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.2	FAU_STG.2
FTP_ITC.1	No dependencies	

Table 32：SFR Dependencies Rationale

7.2.3 Rationale for SARs

The assurance level for this security target is EAL4 augmented with ALC_FLR.3.

EAL4 represents an assurance level based on the use of positive security engineering based on good commercial development practices, and it is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. As such, EAL4 is appropriate to a metering environment that requires intermediate to advanced security features, where the design of cryptographic architectures and other AMI components contributes to security. This is consistent with the description of EAL4 in [6] as "a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs". Augmentation with ALC_FLR.3 is included as a recognition of the importance of timely remediation of any flaws discovered in meters after delivery and deployment.

Component	Depends On:	Which is:
ADV_ARC.1	ADV_FSP.1	hierarchically higher component ADV_FSP.4 is included.
	ADV_TDS.3	included
ADV_FSP.4	ADV_TDS.1	hierarchically higher component ADV_TDS.3 is included.
ADV_IMP.1	ADV_TDS.3	included
	ALC_TAT.1	included
ADV_TDS.3	ADV_FSP.4	included
AGD_OPE.1	ADV_FSP.1	hierarchically higher component ADV_FSP.4 is included.
AGD_PRE.1	no dependencies	not applicable
ALC_CMC.4	ALC_CMS.1	hierarchically higher component ALC_CMS.4 is included.
	ALC_DVS.1	included
	ALC_LCD.1	included
ALC_CMS.4	no dependencies	not applicable
ALC_DEL.1	no dependencies	not applicable
ALC_DVS.1	no dependencies	not applicable
ALC_LCD.1	no dependencies	not applicable
ALC_TAT.1	ADV_IMP.1	included
ALC_FLR.3	no dependencies	not applicable
ASE_INT.1	no dependencies	not applicable
ASE_CCL.1	ASE_INT.1	included
	ASE_ECD.1	included
	ASE_REQ.1	hierarchically higher component ASE_REQ.2 is included
ASE_SPD.1	no dependencies	not applicable
ASE_OBJ.2	ASE_SPD.1	included

ASE_ECD.1	no dependencies	not applicable
ASE_REQ.2	ASE_OBJ.2	included
	ASE_ECD.1	included
ASE_TSS.1	ASE_INT.1	included
	ASE_REQ.1	hierarchically higher component ASE_REQ.2 is included
	ADV_FSP.1	hierarchically higher component ADV_FSP.4 is included
ATE_COV.2	ADV_FSP.2	hierarchically higher component ADV_FSP.4 is included
	ATE_FUN.1	included
ATE_FUN.1	ATE_COV.1	hierarchically higher component ATE_COV.2 is included
ATE_IND.2	ADV_FSP.2	hierarchically higher component ADV_FSP.4 is included
	AGD_OPE.1	included
	AGD_PRE.1	included
	ATE_COV.1	hierarchically higher component ATE_COV.2 is included
	ATE_FUN.1	included
ATE_DPT.1	ADV_ARC.1	included
	ADV_TDS.2	hierarchically higher component ADV_TDS.3 is included
	ATE_FUN.1	included
AVA_VAN.3	ADV_ARC.1	included
	ADV_FSP.4	included
	ADV_IMP.1	included
	ADV_TDS.3	included
	AGD_OPE.1	included
	AGD_PRE.1	included
	ATE_DPT.1	included

Table 33：SAR Dependencies Rationale

8. TOE Summary Specification

8.1 Message Security

The interaction between Holley's Single Phase and Three Phase Smart Meters and the subject includes different message types. And as the specific message types described in FDP_IFC.1.1/Msgs, subject can send and receive these messages. Holley's Single Phase and

Three Phase Smart Meters have four roles: Public, Administrator, Operator, and Technician (FMT_SMR. 1).

Subjects and messages have different security attributes, specifically identity authentication, message encryption, access permissions, and TOE interfaces (RS485, Optical, and Wi-SUN)(FDP_IFF.1.1/Msgs). In addition, the TSF shall allow controlled subjects and controlled information to flow through controlled operations when the following rules hold. (FDP_IFF.1.2/Msgs)

1. Except for public (public can only read messages), the remaining entities will perform authentication (ECDSA) and message encryption (AES-GCM-128) when sending or receiving the above message types.
2. Except for public (public can only read messages), the other subjects can send or receive the object data in FDP_ACF.1 through RS485, Optical, and Wi-SUN. And message encryption measures will be carried out during the transmission of the data.

TSF can explicitly reject information flows (FDP_IFF.1.5/Msgs) when it receives messages from sources that are not authorized to send messages of this type according to the rules.

TSF detects replays of all communication data (FPT_RPL.1.1). Upon detecting a potential replay, the TSF executes the following operation: after receiving a new data item, it determines whether the item duplicates previously received data. If a duplicate is identified, the TSF returns a failure response to the user, as specified in FPT_RPL.1.2.

TSF allows the AMI Key Management System to import keys into the TOE through a trusted channel (FTP_ITC.1).

8.2 TSF Protection

After the watchdog is triggered, Holley's Single Phase and Three Phase Smart Meters will be reset for initialization. In this process, each module of Holley's Single Phase and Three Phase Smart Meters will be initialized, a self-test will be performed, and the pre-reset data will be read from the memory chip. After reset, data such as power consumption, demand, and configuration parameters will be read from the non-volatile memory and the data will be saved to ensure the accuracy of Holley's Single Phase and Three Phase Smart Meters data. （FPT_FLS.1）

If the chip random number fails, the software enables code generation random numbers to replace chip random number detection.（FPT_FLS.1）

Upon interruption of the module network, ongoing communication sessions are terminated. If network connectivity is restored within 3 minutes, Holley's Single Phase and Three Phase Smart Meters will automatically re-establish communication (3-minute reset period for remote-communication interruption). If the interruption persists for 25 hours, the module performs a hardware reset to restore communication capability, in accordance with the company standard (FPT_FLS.1).

Firmware Integrity Test（FPT_BST.1, FPT_TSU.1）:

Executable Firmware saves the internal flash of the MCU, and the external flash saves the OTA firmware image.

- Bootloader:

Bootloader is responsible for verifying the integrity of non-metrology firmware, validating firmware images, loading firmware from backup memory when necessary, and initiating firmware execution.

- Firmware OTA process

The bootloader may only be programmed during the manufacturing process. Prior to leaving the factory, the programming interface will be permanently disabled. The MCU memory regions containing the bootloader are hardware-protected, and write access to these regions is likewise permanently disabled, securing the bootloader against post-manufacture modification. During power-on and during restart from failure, Holley's Single Phase and Three Phase Smart Meters will perform Bootloader CRC validation. If it fails, Holley's Single Phase and Three Phase Smart Meters will not be able to execute any functionality and has to return to the manufacture. During power-on and during restart from failure, when the validation firmware integrity fails 3 times in a row, Holley's Single Phase and Three Phase Smart Meters records the failure to MCU Flash, and reload the firmware again from the external Flash if there is a valid copy of firmware (supply signature ECDSA is correct).

The entire upgrade process is designed in full compliance with the requirements of the DLMS protocol blue book(Blue-Book-Ed14--V1.0)

The Image transfer usually takes place in several steps:

- Step 1: (Optional): Get ImageBlockSize;
- Step 2: Client initiates Image transfer;
- Step 3: Client transfers ImageBlocks;
- Step 4: Client checks completeness of the Image; each packet of data contains 262 bytes.

After saving the received data, Holley's Single Phase and Three Phase Smart Meters calculate the check code through an algorithm and compare it with the last two bytes in the received data to ensure that the data is correct.

- Step 5: Server verifies the Image (Initiated by the client or on its own);
- Step 6: (Optional): Client checks the information on the images to activate;

- Step 7: Server activates the Image(s) (Initiated by the client or on its own).

Trusted update(FPT_TSU.1) :

All roles can query the currently executing version of Holley's Single Phase and Three Phase Smart Meters' firmware.

Holley's Single Phase and Three Phase Smart Meters provide mechanisms for authenticating and verifying the integrity of firmware updates to the TOE prior to installing those updates.

- The client computes a sha256 digest of the firmware to be updated, and then generates a digital signature of this digest using the ECDSA signature algorithm with its own private signature key.
- After Holley's Single Phase and Three Phase Smart Meters receive the complete firmware upgrade package, it needs to use sha256 to calculate the summary of the firmware to be updated.
- Holley's Single Phase and Three Phase Smart Meters use the client signature public key and ECDSA signature algorithm to verify the firmware signature information sent by the client.
- After successful signature verification, the firmware update can be triggered.

Holley's Single Phase and Three Phase Smart Meters provide Administrator and Operator the ability to activate updates to TOE firmware.

Random bit generator test(FPT_BST.1) :

Upon power-up and initialization, Holley's Single Phase and Three Phase Smart Meters generate multiple distinct random numbers. The meter then verifies that each generated value differs from the others. If all values are unique, the test passes; if any duplicate is detected, the test fails, indicating a fault in the random-number generation mechanism.

Correct TSF startup(FPT_BST.1) :

Holley's Single Phase and Three Phase Smart Meters perform a self-test within 5 seconds after power-up. The test verifies all functional modules and continuously monitors the fault-reset status word at 1-second intervals. If a fault is cleared, monitoring for that specific fault ceases. If a fault persists after 100 consecutive detection cycles, monitoring for that fault is also terminated.

During normal operation, Holley's Single Phase and Three Phase Smart Meters perform a memory integrity check once per day, while simultaneously monitoring the fault-reset status word at 1-second intervals. If a detected failure is resolved, monitoring for that specific failure ceases. If a failure persists after 100 consecutive detection cycles, monitoring for that failure is also terminated.

The system defines and logs fault-type events, including Watchdog error, Measurement system error, Program memory error, RAM error, NV memory error, and Flash memory error. An event

is recorded if the same fault condition is detected consecutively 100 times. Subsequent records are generated only if the fault persists without recovery; once the fault is cleared, repeated logging ceases.

The data in the primary and backup areas can be corrected to each other as follows:

- When an error occurs in the primary area, the data in the primary area will be overwritten with the backup area.
- When an error occurs in the backup area, the data in the backup area will be overwritten with the primary area.

Provide reliable time stamp for audit generation. When an event occurs, Holley's Single Phase and Three Phase Smart Meters obtain the chip RTC time and saves it to the memory chip as the occurrence time of the event (FPT_STM.1).

Replay detection (FPT_RPL.1):

When a client repeatedly transmits encrypted data packets (frames) with content identical to previously sent packets, Holley's Single Phase and Three Phase Smart Meters employ a frame-sequence-number validation mechanism. Packets carrying duplicate sequence numbers are rejected, an appropriate security response is triggered, and a replay event is logged for audit purposes.

Tamper notification (FPT_TNN.1):

When the following physical tampering events occur, Holley's Single Phase and Three Phase Smart Meters generate local alarms and logs, and the remote AMI System also receives alarms.

- meter cover detect
- terminal detect
- magnetic field detect/ magnetic interference
- modem cover detect
- battery level detect

8.3 Audit

Holley's Single Phase and Three Phase Smart Meters can automatically record all important events in the meter system, such as access control, larceny, grid monitoring, parameter configuration and other security events, and generate a complete log. The classification of these events is described in FAU_ARP.2.

Each generated record contains the event time stamp, type, and unique identifier (FAU_GEN.1). All records are stored in a uniform format to ensure events are archived and traceable by

category. In accordance with regulatory requirements, the records are transmitted on or before the next default communication opportunity of Holley's Single Phase and Three Phase Smart Meters.

TSF provides the ability for authorized users (Public, Administrator, Operator, Technician) to read audit records (FAU_SAR.1), facilitating their review of relevant audit information. Correspondingly, the TSF prohibits all users not explicitly granted access from reading audit records. It further specifies the access-permission model for different event categories—standard events, grid events, disconnector events, current events, security events, and other events—defining which user roles are permitted to read and which are permitted to clear each event type (FAU_SAR.2).

TSF shall protect audit records stored in the audit trail from unauthorized deletion and prevent unauthorized modification of these records (FAU_STG.2). Simultaneously, it shall define the authorized conditions and procedures for the deletion of audit-log records.
If the audit trail exceeds a predefined record limit—where different limits apply per event category (e.g., 250 records for standard, grid, and current events; 100 records for disconnector, safety, and other events)—the TSF shall overwrite the oldest stored record and shall provide applicable instructions governing the overwrite operation (FAU_STG.4).

8.4 Authentication & Authorisation

Authentication is employed to verify the legitimacy of a user's or system's claimed identity, thereby ensuring that each communicating party is genuine. The TOE utilizes mutual authentication to enhance system security. During the authentication exchange, the Client and Server transmit authentication messages secured by the ECDSA signature algorithm, with authentication tags ensuring message integrity against tampering.

The re-authentication function (FIA_UAU.6) ensures that re-authentication is triggered according to the data type in the authentication mode and meets the specified time requirements (local: 1 min, remote: 3 min). It covers the full authentication process, from Client-Server handshake negotiation to mutual authentication-request exchange and signature verification. Only the maximum number of consecutive failed attempts and the lockout duration after exceeding that limit are configurable; all other parameters are factory-set and non-configurable. Configuration authority for these two features is restricted to the Administrator, Operator, and Technician roles (FMT_MOF.1).
Following an authentication failure (FIA_AFL.1), the TSF shall monitor the count of consecutive unsuccessful authentication attempts. When the predefined failure threshold is

exceeded, the TSF shall prevent the corresponding entity from accessing any data requiring prior authentication via the associated interface, until the lockout period specified in the authentication-failure handling table has elapsed. Both the allowable number of unsuccessful attempts and the lockout duration are defined in FMT_MOF.1.

8.5 Data Protection

TSF will perform data SFP operation on subjects (Public, Administrator, Operator, Technician) and objects (metrologically certified data, credentials, energy meter configuration, ...), and the operation between subject and object to ensure the security of Holley's Single Phase and Three Phase Smart Meters data (FDP_ACC. 2).

Subjects and objects contain different security attributes, such as authentication, access permissions, data encryption, and TOE interfaces (RS485, Optical, and Wi-SUN)(FDP_ACF.1.1). The TSF enforces the following four rules to allow manipulation between controlled subjects and controlled objects (FDP_ACF.1.2). When critical data changes, corresponding log records are produced (FAU_GEN.1).

1. Public can only read the above data other than credentials but can not modify any of the data.
2. Administrator can read the above data other than credentials, clear Load Profile Data/Freeze Data/Event Log data, modify configuration parameters, modify credentials, but cannot clear metering authentication data.
3. Operator can read the above data other than credentials, clear the Load Profile Data/Freeze Data/Event Log data, modify the configuration parameters, but cannot clear the metrologically certified data(except security key data) or modify the credentials.
4. Technician can read the above data other than credentials, configure network-related operation data, but cannot clear any data or modify credentials.

TSF also denies subjects access to objects according to the following rules (FDP_ACF.1.4)

1. All other subjects except the Administrator cannot modify the credentials.
2. Administrator and Operator cannot clear metrologically certified data.
3. Technician cannot clear any data.

TSF implements interface SFP to secure all communications generated by that subject using the interface (FDP_IFC. 2). Holley's Single Phase and Three Phase Smart Meters provides six interfaces: Display, Keypad, Optical, RS485, P1, and Wi-SUN (FDP_IFF.1.1/Int), and provides the operation usage mode of each enabled interface (FDP_IFF.1.2/Int). TSF shall explicitly deny information flows in accordance with the rule that any interface not listed in FDP_IFF.1.2/Int is disabled, as specified in FDP_IFF.1.5/Int.

TSF ensures that when releasing metrologically certified data, credentials, Freeze Data, Event Log and energy meter configuration from storage, any previous information of the resource is not available (FDP_RIP.1、FCS_CKM.6).

Administrator and Operator have permission to delete audit logging (FMT_MTD.1 /Audit).

Administrator and Operator have permission to modify the time of Holley's Single Phase and Three Phase Smart Meters (FMT_MTD.1/Time).

8.6 Underlying Cryptography

The keys used by Holley's Single Phase and Three Phase Smart Meters are generated by the KMS (Key System) of the external AMI and are transmitted via a private VPN network. The smart meter internally generates a 256-bit signature private key by utilizing the ECC256-based ECDSA algorithm in conjunction with a hybrid physical random number generator. (FCS_CKM.1).

Holley's Single Phase and Three Phase Smart Meters internally use the AES-CGM-128 algorithm to encrypt the information during the entire communication process (FCS_COP. 1/Message encryption and decryption). Holley's Single Phase and Three Phase Smart Meters sign random numbers through the ECDSA algorithm based on ECC256 before the internal communication is established, and exchange and upgrade the firmware signature (FCS_COP. 1/Firmware Signature Verification). Holley's Single Phase and Three Phase Smart Meters internally encrypt the replaced key through the AES key wrap algorithm so that the replaced key is the cipher text (FCS_COP. 1/Key wrap).

The encryption key is destroyed by writing new key data to the key-storage location, thereby overwriting and irreversibly erasing the existing key, as required by FCS_CKM.6.

Hybrid physical RNG generates entropy that meets or exceeds the entropy capacity of its output. It produces 32-bit random numbers in compliance with the requirements of NIST Special Publication 800-90A Revision 1 (FCS_RNG.1).

Random number generation and function

Random number generation:

The hybrid physical RNG produces the amount of entropy that the RNG output may contain by mixing physical random numbers and pseudorandom numbers to generate the random numbers required by Holley's Single Phase and Three Phase Smart Meters.

Random number function:

Random numbers generated by the RNG are incorporated into the handshake frame exchanged between Holley's Single Phase and Three Phase Smart Meters and the PC/Internet. This ensures communication-session uniqueness, enhances information security, and provides the necessary randomness for generating the digital-signature private key of the meter itself.

The key types include Master Key, Global Authentication Key, Global Encryption Key, Global Broadcast Key, Client Public Key, Server Private Key, and Server Public Key. When the entity (only the Administrator) sends or imports keys, authentication of the entity is performed (based on ECC256 ECDSA). At the same time, the interfaces for key sending and importing are restricted to interfaces Optical, RS485, and Wi-SUN. During the process of sending or importing keys, the keys are encrypted (AES Key Wrap) (FDP_IFC.1/ Keys).

Holley's Single Phase and Three Phase Smart Meters explicitly deny an information flow based on the following rules:
(1) A key received from a source that is not authorised to provide keys of that type shall be rejected;
(2) No read access shall be provided to plaintext private or secret keys stored in the meter; (FDP_IFF.1/ Keys)

9. Appendix

All alarm and audit events in the TOE are defined in the appendix, categorized into six types: Standard Event, Power Grid Event, Disconnector Event, Current Event, Security Event, and Other Event. Different event types have specific identifiers, and specific events are represented by different Event IDs.

Identification of event types

Items	Identification of event types
Standard Event	**0.0.99.98.0.255**
Power Grid Event	**0.0.99.98.1.255**
Disconnector Event	**0.0.99.98.4.255**
Current Event	**0.0.99.98.2.255**
Security Event	**0.0.99.98.5.255**
Other Event	**0.0.99.98.9.255**

Table 34：Identification of event types

Standard Event

Event ID	Event Name	Description	Destination
300	Power down	It indicates a complete power down of the device.	Local storage
301	Power up	It indicates that the device is powered again after a complete power down.	Local storage
1204	Clock adjusted (old date/time)	It indicates that the clock has been adjusted. The date/time that is stored in the event log is the old date/time before adjusting the clock.	Local storage
1202	Clock adjusted (new date/time)	It indicates that the clock has been adjusted. The date/time that is stored in the event log is the new date/time after adjusting the clock.	Local storage
1203	Clock invalid	It indicates a potential clock invalidity condition, such as depletion of the clock's backup power reserve. The detection logic is activated at system powerup.	Local storage
1603	Battery	It indicates that the current battery	Local storage and

	undervoltage	voltage is low.	AMI System
1605	Battery replacement	It indicates that the battery must be exchanged due to the expected end of life time.	Local storage
332	Power up\down reset	It indicates that the reset when the device is powered again after a complete power down.	Local storage
2105	Watchdog error	It indicates a watch dog reset or a hardware reset of the microcontroller.	Local storage and AMI System
2106	Measurement system error	It indicates a logical or physical error in the measurement system.	Local storage
2102	Program memory error	It indicates a physical or a logical error in the program memory.	Local storage
2103	RAM error	It indicates a physical or a logical error in the RAM.	Local storage
2100	NV memory error	It indicates a physical or a logical error in the non-volatile memory.	Local storage
2101	Flash memory error	It indicates a physical or a logical error in the Data Flash memory.	Local storage
1503	Association authentication failure	It indicates attempted unauthorized access at the LLS interface using an incorrect password (intrusion detection) or repeated authentication failures (n-time) at the HLS challenge-response interface.	Local storage
1302	One or more parameters changed	It indicates that one or more parameters is changed.	Local storage
1303	Global key(s) changed	It indicates that one or more global keys is changed.	Local storage
1503	Decryption or authentication failure (n time failure)	It indicates that decryption with currently valid key (global or dedicated) failed to generate a valid APDU or authentication tag.	Local storage
2121	Replay attack	It indicates that the frame counter value is less or equal to the last	Local storage

		successfully received frame counter in the received APDU.	
3002	Firmware ready for activation	It indicates that the new firmware has been successfully downloaded and verified, and is now pending activation.	Local storage
3003	Firmware activated	It indicates that a new firmware has been activated.	Local storage
2120	Diagnostic failure	It indicates that the device detected error in Self-Diagnostic process.	Local storage
3001	Firmware verification failed	It indicates that the transferred firmware verification failed and cannot be activated.	Local storage
3004	Firmware upgrade failed	It indicates the firmware upgrade failed i.e., cannot be activated.	Local storage
101	Clear all	It indicates that all registers and data records were cleared.	Local storage
100	Load profile cleared	It indicates that the load profile was cleared.	Local storage
10	Event log cleared	It indicates that the event log was cleared.	Local storage
20	Error register cleared	It indicates that the error register was cleared.	Local storage
21	Alarm register cleared	It indicates that the alarm register was cleared.	Local storage
2104	Random number error	It indicates the random number error in AARQ process.	Local storage and AMI System
333	Reset triggered by watchdog timer	It indicates that a watchdog reset occurs.	Local storage
12	Self-test completed	It indicates that the smart meter self-test is completed.	Local storage

Table 35：Standard Event

Power Grid Event

Event ID	Event Name	Description	Destination
300	Power off start	It indicates a complete power off of the device.	Local storage
301	Power off end	It indicates that the device is	Local storage

		powered again after a power off.	
204	Magnetic influence start	It indicates that a strong magnetic field has been detected.	Local storage and AMI System
205	Magnetic influence end	It indicates that a strong magnetic field has been disappeared.	Local storage
203	Open terminal cover start	It indicates that the terminal cover has been removed.	Local storage and AMI System
202	Open terminal cover end	It indicates that the terminal cover has been closed.	Local storage
495	Open modem cover start	It indicates that the modem cover has been removed.	Local storage and AMI System
494	Open modem cover end	It indicates that the modem cover has been closed.	Local storage
201	Open meter cover start	It indicates that the meter cover has been removed.	Local storage and AMI System
200	Open meter cover end	It indicates that the meter cover has been closed.	Local storage
1902	Limiter threshold changed	It indicates that the limiter threshold has been changed.	Local storage

Table 36：Power Grid Event

Disconnector Event

Event ID	Event Name	Description	Destination
1006	Remote disconnection	It indicates that the disconnector has been remotely disconnected.	Local storage
1005	Remote connection	It indicates that the disconnector has been remotely connected.	Local storage

Table 37：Disconnector Event

Current Event

This type of event is not related to TSF.

Security Event

Event ID	Items	Description	Destination
1502	Change of stored external party key	It indicates that one or more HLS Key(s) changed.	Local storage and AMI System
1504	HLS_Unsuccess	It indicates that HLS Communication failed.	Local storage and AMI System

1506	Detected replay events	It indicates that multiple authentication errors occurred.	Local storage
1507	Key generation	It indicates that the smart meter changes its signature public-private key pair.	Local storage
1508	Message received from an unauthorised source	It indicates that an unrecognized client(such as an unknown client) initiates communication.	Local storage
1509	Change of access rights	It indicates that the client's authorization to modify other clients' access configurations or retrieve system logs is being managed.	Local storage
1510	Key received from an unauthorised source	It indicates that a client that cannot change its key requests a key change.	Local storage

Table 38：Security Event

Other Event

Event ID	Items	Description	Destination
5009	Signal quality low	It indicates that signal strength is too low, not known, or not detectable.	Local storage
5010	Local communication attempt	It indicates that a successful communication on any local port has been initiated.	Local storage
5011	External pin reset	It indicates that record reset event is caused by MCU external pin abnormalities.	Local storage
5013	Unexpected ADPU	It indicates that an APDU containing an incorrect tag was received.	Local storage
5014	Unauthorized access	It indicates that an access ADPU was received when AARQ is not established.	Local storage
5021	Modem SW reset	It indicates that Modem is restarted by SW reset.	Local storage
5022	Modem HW reset	It indicates that the Modem is	Local storage

		restarted via a HW reset event (distinct from a restart following a general power restoration).	
5023	Change in network status	It indicates that the module network status changes.	Local storage and AMI System

Table 39：Other Event

10. References

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

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

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

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

[5] 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

Note that references [2], [3], [4] and [5] above are also published as ISO/IEC 15408.

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

Note that reference [6] above is also published as ISO/IEC 18045.

[7] Smart Meter Co-ordination Group Privacy and Security Approach – Part IV: Minimum security requirements for AMI components – European level requirements for Smart Metering, v1.1, 17 July 2016

[8] Functional reference architecture for communications in smart metering systems, CEN/CLC/ETSI TR 50571, December 2011

[9] IEEE Standard for Low-Rate Wireless Personal Area Networks (WPANs), IEEE 802.15.4, 2011

[10] Recommended Standard 485, EIA-485-B, 2003

[11] Electricity metering - Data exchange for meter reading, tariff, and load control - Part 21: Local data exchange, NEN-EN-IEC 62056-21, 2020

[12] Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA), FIPS PUB 186-5, July 2023

[13] Recommendations for Pair-Wise Key Establishment Schemes Using Elliptic Curve Cryptography, NIST SP 800-56A Rev. 3, May 2023

[14] IPsec and IKEv2, IETF RFC 8247, November 2022

[15] Device Language Message Specification (DLMS) / Companion Specification for Energy Metering (COSEM), DLMS/COSEM 2.0, 2021

[16] D_HW240F_Guidance Documents_V1.6, V1.6, 2026-1-21

