COMMON CRITERIA PROTECTION PROFILE

for

SMART METER OF TURKISH ELECTRICITY ADVANCED METERING INFRASTRUCTURE

(SMTEAMI PP)

TSE-CCCS-PP-004

Revision No	1.1
Revision Date	29.08.2014
Document Code	TSE-CCCS-PP-004
File Name	SMTEAMI PROTECTION PROFILE
Prepared by	Muhammet Öztemur, Neslihan Güler
Approved by	Turkish Standards Institution (TSE)

This page left blank intentionally

Revision History

Revision No	Revision Reason	Date of Revision
1.0	First Release	20.06.2014
1.1	Expression Update	28.08.2014

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 PP INTRODUCTION

This Protection Profile (PP) describes the following items:

- The Target of Evaluation (TOE) as a product and its position in production life cycle,
- The security environment of the TOE includes: the assets to be protected, the threats to be encountered by the TOE , the development environment and production utilization phases,
- The security objectives of the TOE and its supporting environment in terms of integrity and confidentiality of User Data and TSF Data,
- Protection of the TOE and associated documentation during the development and production phases,
- The Information Technology (IT) security requirements which include the TOE functional requirements and the TOE assurance requirements.

1.1 PP Reference

Title	**:** Common Criteria Protection Profile for Smart Meter of Turkish Electricity Advanced Metering Infrastructure (SMTEAMI PP)
Sponsor	**:** Turkish Standards Institution (TSE)
Editor(s)	**:** Prepared by Muhammet ÖZTEMÜR and Neslihan GÜLER Approved by Turkish Standards Institution (TSE)
CC Version	**:** 3.1 (Revision 4)
Assurance Level	**:** The assurance level for this PP is EAL 2+ (AVA_VAN.3).
General Status	**:** Final
Version Number	**:** 1.1 as of 29th August 2014
Registration	**:** TSE-CCCS-PP-004
Key words	: Smart Meter, OSOS, Protection Profile, Meter, PP.
Note	**:** A glossary of terms used in the Protection Profile is given in ACRONYMS section of the document (Section 7).

1.2 TOE Overview

1.2.1 Introduction

The TOE, as defined in this Protection Profile, is the Smart Meter of Turkish Electricity Advanced Metering Infrastructure. In the following subsections the overall Advanced Metering Infrastructure will be described first and the Smart Meter itself will be described afterwards.

1.2.2 General Overview of Turkish Electricity Advanced Metering Infrastructure

Figure 1 represents the general overview of the Turkish Electricity Advanced Metering Infrastructure where TOE is located. As seen in the figure, the system is comprised of three main components.

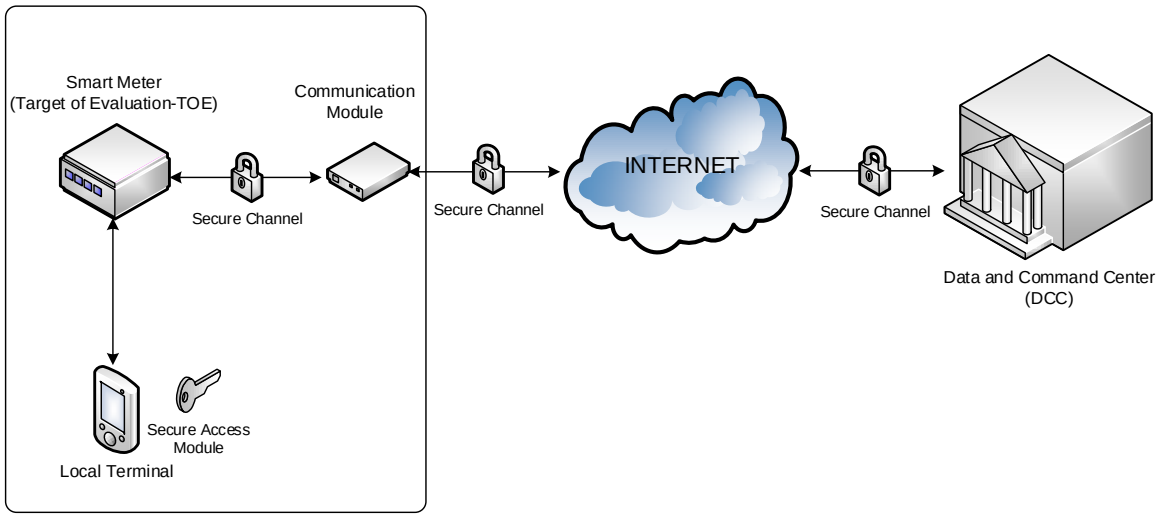


Figure 1 TOE and Its Operational Environment

Smart Meter is the main component of the system. It is responsible for measuring the electricity consumption, storing and transferring the data related to consumption in a secure way.

Communication Module differs according to communication technology it uses: GPRS/3G, PLC, Ethernet, DSL etc. It takes encrypted and authenticated data from Smart Meter, formats it suitably to transmit over the communication line and transfers data to the DCC over a secure channel established by TLS (as defined in [6]). Communication Module behaves similarly in the opposite direction where data is transmitted from DCC to Smart Meter.

Communication Module has TCP/IP communication capability to perform TLS connection by itself or by using any other module.

Data and Control Center (DCC) is the remote management center at Electricity Distribution Company premises which receives User Data, loads configuration parameters, updates firmware and controls the Smart Meter.

Smart Meter and the Metering Infrastructure are managed by the operators in DCC. There are also some applications that can be performed by using Local Interface of Smart Meter. There might be other centers and applications working behind DCC. The system can run different processes after receiving the Smart Meter data. But these processes are not in the scope of this Protection Profile.

1.2.3 TOE Description

The Smart Meter (as defined in this PP) may serve various functionalities like metering, communication, security and storage. The Smart Meter measures the electricity consumption, stores data related to the consumption, and generates audit data about TOE's operational processes. It also provides the security of consumption related data by anti-tamper mechanisms, cryptographic operations and access control functions.

The major functional features of the TOE are described below:

- TOE measures electricity consumption as detailed in document [5]
- TOE stores consumption related data as detailed in document [5]
- TOE provides a Local Interface for reading and configuration operations
- TOE provides a Remote Interface for reading and configuration operations
- TOE supports firmware update operation only via its Remote Interface
- TOE generates audit data about Smart Meter configuration and update operations and regular operations.

The major security features of the TOE are described below.

- TOE implements tamper resistant, tamper evident and tamper respondent mechanisms for physical protection.
- TOE implements access control mechanisms for access from both Remote and Local Interfaces.
- TOE provides symmetric encryption/decryption and integrity protection.
- TOE provides data origin authentication and data integrity verification mechanisms.
- TOE provides storage integrity for integrity critical data.
- TOE provides self-test functionality to test its security functions.

- TOE generates an audit data and informs users, when any of the security anomalies detailed in section 6 is detected.

1.2.4 TOE Type

The TOE comprises of hardware and firmware parts that provide metering, communication, storage and security functionalities for TAMIS (Turkish Advanced Metering Infrastructure).

1.2.5 Logical and Physical Interfaces of TOE

TOE has two logical interfaces:

- **Remote Interface** for DCC operations
- **Local Interface** for local operations

TOE has the physical interfaces listed below:

- **Remote Interface Port** is used to connect to Communication Module. Port types are RS-485 and RS-232.
- **Optical Port** is used for operations performed by Local Administrator.
- **Visual Display and Button** to read regular information like Consumption Index and Smart Meter's date and time information.

1.2.6 TOE Life Cycle

The life-cycle of the Smart Meter can be separated into the following phases.

- Development
- Manufacturing
- Initialization
- Operation

This Protection Profile focuses on Initialization and Operation phases. It has to be ensured that previous phases are performed by trusted personnel in secure environments. The TOE manufacturer loads necessary cryptographic parameters and terminates the manufacturing phase before TOE is delivered to DCC as detailed in [6].

2 CONFORMANCE CLAIMS

2.1 CC Conformance Claim

This protection profile claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012 [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012 [3]

As follows

- Part 2 extended due to the use of FCS_RNG.1, FMT_LIM.1, FMT_LIM.2 and FPR_CON.1.
- Part 3 conformant.

2.2 PP Claim

This PP does not claim conformance to any protection profile.

2.3 Package Claim

This PP claims an assurance package EAL2 augmented by AVA_VAN.3 as defined in Part 3[3] for product certification.

2.4 Conformance Claim Rationale

Since this PP does not claim conformance to any protection profile, this section is not applicable.

2.5 Conformance Statement

This PP requires demonstrable conformance of any ST or PP claiming conformance to this PP.

3 SECURITY PROBLEM DEFINITION

3.1 Introduction

3.1.1 External Entities and Roles

The following external entities interact with Smart Meter. Those roles have been defined for the use in this Protection Profile. It is possible that a party implements more than one role in practice.

Table 1 Entities and Roles

External Entity	Role	Description
DCC	Authenticated DCC	Authenticated DCC is the remote center at Electricity Distribution Company premises which takes User Data, loads configuration parameters, updates firmware and controls TOE via Remote Interface.
Local Administrator	Authenticated Local Administrator	Authenticated Local Administrator is the user who takes User Data, loads configuration parameters and controls TOE via its Local Interface.
DCC Initialization Agent	Authenticated DCC Initialization Agent	Authenticated DCC Initialization Agent is the user who works for Electricity Distribution Company and loads initialization parameters to TOE
DCC Controller	-	DCC Controllers work for Electricity Distribution Company. They perform random and periodic control on TOE and check TOE's functional and physical reliability.
Smart Meter Developer	-	Smart Meter Developer is the entity who develops Smart Meter hardware and firmware.
Smart Meter Manufacturer	-	Smart Meter Manufacturer is the entity who manufactures smart meter. Usually, Smart Meter Manufacturer might be the same entity as Smart Meter developer.
Consumer	-	Consumer is the entity who consumes electricity and pays the bills. Consumer sometimes can act as an attacker.
Attacker	-	Attacker tries to manipulate the TOE in order to change its expected behavior and functionality. Attacker tries to breach confidentiality, integrity and availability of the Smart Meter.

3.1.2 Modes of TOE

3.1.2.1 Initialization Mode

Initialization mode is the mode which is used to load initialization parameters, especially TSF Data. The process is managed by authorized DCC Initialization Agent.

3.1.2.2 Operational Mode

Operational mode is the normal-expected mode of TOE. TOE measures electricity consumption and performs its normal functions. An indicator is shown on Meter display that TOE works in normal operational condition without any problem.

3.1.2.3 Break State Mode

TOE enters this mode when one of the following conditions occurs;

- Opening and enforcement of anti-tamper mechanism,
- Low battery detection below %10,
- Detection of the fullness of System and High Critical log memory,

When TOE enters Break State Mode because of one of the conditions above,

- HMAC Key and Encryption Key are deleted,
- Measurement operation is stopped,
- A High Critical Security Log is generated,
- A warning on Smart Meter display is shown,

After the TOE enters break state mode, there is no way to go back to operational mode. Data and the services are insecure for Controllers anymore. Assets

In the following tables, The User Data and the TSF Data on TOE are described. Additionally, their protection needs in terms of confidentiality, integrity and authenticity are marked.

3.1.2.4 Primary Assets

The primary assets to be protected by the TOE as long as they are in scope of the TOE are given in Table 2. All these primary assets represent User Data in the sense of the CC.

Table 2 TOE User Data and Protection Need

Asset	Description	Need for Protection		
		Conf.	Int.	Auth.

Asset		Description	Need for Protection		
			Conf.	Int.	Auth.
Consumption Data	Consumption Index Data	Consumption Index Data is the amount of electricity consumed over a period.	-	X	X
	Detailed Consumption Data	Detailed Consumption Data is the detailed and statistical amount of electricity consumed over a specific period. It includes; consumption profile calculated using the past consumption data, inductive and capacitive consumptions and demand value. It might be used as commercial data by EDC. It might also be used by consumers to get more information about their consumption.	X	X	X
Event Data	Security Log	Security Logs are produced when security problems are detected. High critical security logs show that Smart Mater has been attacked or there is a serious security problem. Low critical security logs show that there might be an attack or there can be a serious security problem.	-	X	X
	System Log	System Logs are kinds of Event Data which give information about Smart Meter configuration and update operations. They are produced during any update and load operation.	X	X	X
	Regular Log	Regular Logs are kinds of Event Data which give information about Smart Meter's regular operations like metering.		X	X
DCC Parameters	Price Plan Parameters (T1, T2, T3.)	Electric Distribution Company may vary the price depending on the time-of-day. These parameters show the time of day price schedules.	-	X	X
	DCC Configuration Parameters	Any parameters loaded into Meter by DCC.	-	X	X
Fabrication Parameters	Calibration Parameter	Calibration Parameter is used as a factor when Smart Meter calculates the electricity consumption. The correctness of the measurement depends on the correctness of this parameter.	-	X	-

Asset		Description	Need for Protection		
			Conf.	Int.	Auth.
	Smart Meter Manufacture Date	Date on which the Smart Meter became a product.	-	X	-
	Smart Meter Start-up Date	Date on which Smart Meter started to be used.		X	-
	Manufacturer Code	It is the unique code of Smart Meter's manufacturer.	-	X	-
	Serial Number	Serial Number is a unique ID of Smart Meter that is given by Manufacturer. Different Manufacturers can give the same serial number to their product. So, Serial Number and Manufacturer Code are combined to form a unique Smart Meter ID.	-	X	-

Application Note 1: Confidentiality of Consumption Data is important in terms of consumer privacy and commercial secrecy of EDC. Attacker needs to analyze these data in time intervals to exploit security (not just in a moment). So, Confidentiality of Consumption Data is meaningful in operational mode. There is no need for confidentiality in break state mode.

Application Note 2: System Log might be used by attacker to get information about Smart Meter to perform more specific attacks. So, confidentiality of System Log is meaningful in operational mode. There is no need for confidentiality after TOE enters break state mode.

3.1.2.5 Secondary Assets

The secondary assets also have to be protected by the TOE in order to achieve a sufficient protection of the primary assets. The secondary assets represent TSF-data and TSF in the sense of the CC.

Table 3 TOE TSF Data and Protection Need

Asset	Description	Need for Protection		
		Conf.	Int.	Auth.
Initialization Key	It is used to initialize TOE in a secure way. It is loaded during manufacturing phase.	X	X	
Firmware Update Public Key	It is used to update Smart Meter's Firmware in a secure way. It is loaded during manufacturing phase.	-	X	X

Asset	Description	Need for Protection		
		Conf.	Int.	Auth.
Local Access Control Root Public Key	It is used to control access to TOE via its Local Interface. It is loaded during initialization phase.	-	X	X
Smart Meter Time	It is time of Smart Meter. It is loaded during manufacturing phase and shall be updated during operational phase.	-	X	-
Smart Meter Firmware	It is the firmware of Smart Meter. It is loaded during manufacturing phase and shall be updated during operational phase.	-	X	-
Encryption Key	Encryption Key is used to encrypt and decrypt User Data that is transmitted from Meter to DCC or from DCC to Meter. It is loaded during initialization phase and can't be updated.	X	X	X
HMAC Key	HMAC Key is used to calculate and verify the MAC value for User Data that is transmitted from Meter to DCC or from DCC to Meter. HMAC Key is used to calculate the hash of stored integrity critical data. It is loaded during initialization phase and can't be updated.	X	X	X

Application Note 3: An additional term "Device Information Data" will be used throughout the document especially when describing Threats and SFRs. It includes any data sent from TOE and gives information about TOE and its configuration like Fabrication Parameters, DCC Parameters and Configurations and Smart Meter Time.

Table 4 TSF and Protection Need

Asset	Description	Need for Protection
Genuineness of the TOE	It guaranties for TOE to be authentic in order to provide the claimed security functionality in a proper way.	Availability
Security Services provided by the TOE.	They provide for TOE to apply security functions.	Availability

3.2 Threats

Two kinds of attackers should be considered when the threats are being identified.

- **Local Attacker:** Attackers who have physical access to TOE via its physical interfaces. They might try to attack TOE by physical and environmental tampering. They can also abuse TOE's Local Interface.

- **Remote Attacker:** Attackers who are away from TOE and have a remote access to TOE non-physically. Remote Attackers try to conquer TOE by cyber-attacks and try to compromise the confidentiality, integrity and authenticity of data when it is transmitted between TOE and DCC. They also try any type of attack which doesn't need physical access to TOE:

T.Transfer_Modification:

A remote attacker may try to modify (i.e. alter, delete, insert, replay); Consumption Data, Event Data, DCC Parameters, Smart Meter Time, Smart Meter Firmware and Device Information Data when transmitted between the TOE and DCC.

Attacker may try to mislead DCC by modification of Device Information Data during transmission. Attacker may try to alter Consumption Data to gain economic benefit.

Attacker may also lead to malfunctions on TOE by modifying Smart Meter Update Firmware, DCC Parameters and Smart Meter Time.

Attacker may exploit misleading of DCC and malfunction of TOE to get advantages for more specific attacks.

T.Local_Modification:

A local attacker may try to modify Consumption Data, Event Data, DCC Parameters, Fabrication Parameters and TSF Data stored in TOE by using Local Interface of TOE.

Attacker may try to mislead DCC and Local Administrator by modification of any data stored. Attacker may try to alter Consumption Data to gain economic benefit.

Attacker may also lead to malfunctions on TOE by modifying Smart Meter Firmware, DCC Parameters, Fabrication Parameters and Smart Meter Time. Particularly, he/she may by-pass cryptographic mechanisms of TOE. These malfunctions may be used to get advantages for more specific attacks.

T.Transfer_Disclosure:

A remote attacker may try to intercept and analyze Detailed Consumption Data and System Log when transmitted between the TOE and DCC.

When Detailed Consumption Data is disclosed, attacker may try to violate the privacy of the consumer. Attacker may also use System Log to get information to perform more specific attacks.

In addition, the security level of Detailed Consumption Data may be commercially restricted. Attackers may violate EDC economically by disclosing this information.

T.Local_Disclosure:

A Local Attacker may try to get and analyze Detailed Consumption Data, System Log and TSF Data[1] by using TOE Local Interface.

When Detailed Consumption Data is disclosed, attacker may try to violate the privacy of the consumer. Attacker may also use System Log and TSF Data (i.e. cryptographic parameters) to get information about system and by-pass TOE security mechanism for more specific attacks.

In addition, the security level of Detailed Consumption Data may be commercially restricted. Attackers may violate EDC economically by disclosing this information.

T.Counterfeit:

A remote or local attacker may imitate TOE to respond DCC. Attacker may gain economic benefit by sending fake Consumption Data. Attacker may try to mislead DCC and cause malfunctions by sending fake Event Data and Device Information Data to DCC.

T.Skimming:

A remote attacker may imitate DCC to get Detailed Consumption Data and Event Data from TOE.

When Detailed Consumption Data is disclosed, attacker may try to violate the privacy of the consumer.

Attacker may also use System Log to get information for more specific attacks.

In addition, Detailed Consumption Data may be commercially restricted. Attackers may violate EDC economically by disclosing this information.

T.Update:

A remote or local attacker may try to update Smart Meter Firmware by using a malicious or older version of code to get advantages for more specific attacks. By updating the meter's firmware, attacker may modify and disclose all User/TSF Data.

T.Fake_Ini:

A local attacker may try to initialize TOE by using his/her own fake keys (HMAC and encryption key that will be used in operational mode). When the attacker initializes TOE by this way, he/she may modify and disclose all User/TSF Data later during TOE operation.

T.Physcal_Tamper:

[1] It is for TSF data which is critical in terms of confidentiality (Initialization Key, HMAC Key and Encryption Key.)

A local attacker may try to access TOE's internal processor and storage memory by physical tampering and manipulation. By succeeding to access these components, attacker may modify and disclose all User/TSF Data.

T.Env_Malfunction:

A local attacker may manipulate TOE by environmental stress (i.e. electromagnetic field, high temperature). When these manipulations are applied to TOE, TOE may not measure the amount of consumption correctly. Attacker may gain economic benefit by this way.

T.Battery_Disable:

A remote or local attacker may use up internal battery by sending continuous operation requests or applying environmental stress. If TOE's internal battery has not got enough capacity, tamper detection mechanisms becomes out of service without line voltage. So, it can't detect physical tampers.

T.Sec_Function:

TOE security functions may fail because of unintentional malfunctions (not because of an attack). A remote or local attacker may exploit these failures to modify and disclose all User/TSF Data.

T.Abuse_Function:

An attacker may try to use some functions of TOE which are not needed by TOE during operational phase in order to disclose or manipulate sensitive User Data or TSF Data, manipulate the TOE's firmware or manipulate (explore, bypass, deactivate or change) security features or functions of the TOE.

T.Cyber_Attack:

A remote attacker may try to manage TOE via its remote interface by cyber-attacks. Attackers may try to modify and disclose all User/TSF Data by this way.

T.Availability:

A remote or local attacker may send continuous operation requests to busy TOE with processing these requests. TOE can't perform measurement activity because of processing these requests. Consumption Data may be modified by this way.

T.Flow_Analyze

A remote attacker may analyze the data traffic (i.e. frequency of data sent, absence of external communication) between TOE and DCC (without knowing the data content). Attacker may

disclose some information about Consumption Data and violates the privacy of consumers by this way.

3.3 Organizational Security Policies

OSP.Functional_Test:

TOE shall be tested and certified by the related authority for all of its functionality except security specifications.

OSP.Comm_Mod:

Communication Module shall perform TLS operation as detailed in document [6]

OSP.Crypto_Man:

Generation of cryptographic parameters and loading process shall be performed according to document [6].

OSP.Update:

Smart Meter Update Firmware shall be controlled and certified by an authorized Authority. Firmware package shall be prepared as defined in document [6]

3.4 Assumptions

This section describes assumptions that shall be satisfied by the TOE's operational environment.

A.Trusted_Entities:

It is assumed that authorized and authenticated external entities are trustworthy. They don’t let any damage to data they receive because of carelessness and abusement.

A.Trusted_Admins:

It is assumed that the DCC Administrator and the Local Administrator are trustworthy and well-trained.

During any operation via Local Interface, Local Administrator doesn’t let eavesdropping and modification between terminal and TOE local port.

A. Network:

It is assumed that network connection between TOE and DCC is sufficiently reliable and bandwidth for the individual situation is available

A.Trusted_Manufacturer:

It is assumed that manufacturing is done by trusted manufacturers. They process manufacturing step in a manner which maintains IT security.

A.Trusted_Designer:

It is assumed that TOE is designed and implemented by trusted designers. They design and implement it in a manner which maintains IT security.

A. Control:

It is assumed that DCC controllers perform periodic and random physical controls on TOE. They check TOE's functional and physical reliability during these controls. If any problems are detected, TOE shall be out of order and unique TOE ID must be excluded from DCC list of available meters.

4 OBJECTIVES

4.1 Security Objectives for the TOE

O.Access_Control:

The TOE shall control the access of external entities to functions and any information that is sent to, or from TOE via its external interfaces.

O.Event:

TOE shall record some regular operations, security and device configuration relevant events as detailed in Table 7.

O.Storage_Integrity:

TOE shall provide integrity check of integrity critical data which is stored on internal memory.

O.Authentication:

TOE shall run authentication mechanism for users and systems. It shall provide authentication verification and MAC addition.

O.Transfer:

TOE shall provide encryption and integrity protection for the communication with the DCC[2].

O.Protect:

TOE shall have self-test mechanisms to control security functions and detect the cases of malfunction.

O.Physcal_Tamper:

TOE shall have mechanisms to resist and respond physical attacks. TOE shall force attacker to leave evidence after any physical attack attempt.

O.Env_Tamper:

TOE shall detect and respond environmental stress.

O.Battery_Control:

TOE shall control battery level and give reaction (generate and send an audit) when it drops under a certain level. If the battery level drops to a critical low level TOE shall interpret this as an attack and enter to break state mode.

[2] The implementation of a secure channel between the Smart Meter and DCC is a security function of both parties. So DCC shall also has a capability to perform secure communication.

O.Abuse_Function:

The TOE shall prevent the usage of functions which are not used by TOE during initialization and operational phases (i.e: test functions).

O.Update:

TOE shall provide firmware update functionality only via its Remote Interface. TOE shall accept only the firmware updates controlled, authenticated and signed by an authority. TOE shall control firmware version number and accept only the versions higher than the version of installed firmware.

O.Multi_Process:

TOE shall have a multi-process capability to perform measurement function and other functions (i.e: communication) at the same time.

O.Separate_IF:

TOE shall have different and independent physical interfaces for local and remote operations.

O.Conceal:

TOE shall prevent violation of consumer privacy achieved by analyzing network traffic.

4.2 Security Objectives for the Operational Environment

OE.Functional_Test:

Manufacturer shall ensure that TOE is tested and certified by the Authority according to the related standard [5].

OE.Crypto_Man:

Cryptographic parameters shall be generated and loaded according to document [6].

OE.Upgrade_Software:

TOE Update Firmware shall be controlled and certified by an authorized entity. Firmware package shall be prepared as defined in [6].

OE.Comm_Mod:

Communication Module shall support TCP/IP communication to perform TLS connections initiated by itself or any other module.

OE.Trusted_Entities:

Authorized and authenticated external entities shall be trustworthy. They don't let any damage to data that they receive because of carelessness and abusement.

OE.Trusted_Admin:

DCC Administrator and the Local Administrator shall be trustworthy and well-trained. Local Administrator shall not let eavesdropping and modification action between terminal and TOE local port during operation by using Local Interface,

OE.Network:

A network connection with a sufficient reliability and bandwidth shall be available between TOE and DCC.

OE.Manufacturing:

Manufacturer shall ensure that TOE is manufactured in a manner which maintains IT security. They also don't put any security hole on TOE intentionally.

OE.Development:

Developers shall ensure that they design and implement TOE in a manner which maintains IT security during development. They also don't put any security hole on TOE intentionally.

OE.Control:

DCC controllers shall perform periodic and random physical controls on TOE. They check TOE's functional and physical reliability during controls. If any problems are detected, TOE shall be out of order and unique TOE ID excluded from DCC list of available meters.

4.3 Security Objective Rationale

The table given below provides security problem definition covered by security objectives. Threats and OSPs are addressed by security objectives for the TOE and its operational environment. Assumptions are addressed by only security objectives for the operational environment.

Table 5 Security Objectives Rationale

	O.Access_Control	O.Event	O.Storage_Integrity	O.Authentication	O.Transfer	O.Protect	O.Physcal_Tamper	O.Env_Tamper	O.Battery_Control	O.Abuse_Function	O.Update	O.Multi_Process	O.Separate_IF	O.Conceal	OE.Functional_Test	OE.Crypto_Man	OE.Upgrade_Software	OE.Comm_Mod	OE.Trusted_Entities	OE.Trusted_Admin	OE.Network	OE.Manufacturing	OE.Development	OE.Control
T.Transfer_Modification					X																			
T.Local_Modification	X	X	X	X		X																		
T. Transfer_Disclosure					X																			
T.Local_Disclosure	X	X		X																				
T.Counterfeit				X																				
T.Skimming	X			X																				
T.Update	X	X		X							X						X							
T.Fake_Ini	X			X												X								
T.Physcal_Tamper		X					X																	
T.Env_Malfunction		X						X																
T.Battery_Disable		X							X															
T.Sec_Function						X																		
T.Abuse_Function										X														
T.Cyber_Attack	X	X		X									X											
T. Availability												X												
T.Flow_Analyze														X										
OSP.Functional_Test															X									
OSP.Crypto_Man																X								
OSP.Update																	X							
OSP.Comm_Mod																		X						
A.Trusted_Entities																			X					
A.Trusted_Admins																				X				
A.Network																					X			
A.Trusted_Manufacturer																						X		
A.Trusted_Designer																							X	
A. Control																								X

Justification about Table 5 is given below;

T.Transfer_Modification is addressed by O.Transfer to ensure integrity of communication channel.

T.Local_Modification is addressed by O.Access_Control, O.Event, O.Storage_Integrity, O.Authentication and O.Protect.

O.Access_Control ensures that only permitted systems has access to the functions and data.

O.Event provides audit record for unsuccessful authentication attempt.

O.Authentication ensures the authenticity of users.

O.Storage_Integrity provides control operation for integrity of critical data.

O.Protect defines that the TOE provides self-test mechanism to ensure the correct operation of critical function.

T.Transfer_Disclosure is addressed by O.Transfer to ensure the confidentiality of communication channel.

T.Local_Disclosure is addressed by O.Access_Control, O.Event, O.Storage_Integrity and O.Authentication.

O.Access_Control ensures that only permitted users have access to the functions and data.

O.Event provides audit record for unsuccessful authentication attempt.

O.Authentication ensures the authenticity of users.

T.Counterfeit is addressed by O.Authentication to ensure the identity of TOE.

T.Skimming is addressed by O.Access_Control and O.Authentication.

O.Access_Control ensures that only permitted systems have access to the functions and data. O.Authentication ensures the origin of external entity.

T.Update is addressed by O.Access_Control, O.Authentication, O.Update and OE.Upgrade_Software.

O.Access_Control ensures that only permitted user may perform Smart Meter Firmware update. O.Authentication and O.Update ensure the origin and integrity of firmware which will be loaded as a new version.

OE.Upgrade_Software supports these objectives by the approval of updated firmware by a trusted authority.

T.Fake_Ini is addressed by O.Access_Control O.Authentication and OE.Crypto_Man. O.Access_Control ensures that only permitted user may perform TOE Initialization, O.Authentication to ensure the origin of external entity.

OE.Crypto_Man supports these objectives by the management of cryptographic parameters responsively outside of TOE.

T.Physcal_Tamper is addressed by O.Physcal_Tamper to ensure that the TOE will provide mechanisms against an attacker to resist manipulation and modifications of the TOE by physical probing.

O.Event contributes to this aspect as it provides the audit generation during a physical tampering.

T.Env_Malfunction is addressed by O.Env_Malfunction to ensure that the TOE will provide environmental protection mechanism.

O.Event contributes to this aspect as it provides the audit generation during an environmental malfunction.

T.Battery_Disable is addressed by O.Battery_Control to ensure that the TOE will provide battery control mechanism.

O.Event contributes to this aspect as it provides the audit generation about battery level.

T.Sec_Function is addressed by O.Protect. It defines that the TOE provides self-test mechanism to ensure the correct operation of critical function.

T.Abuse_Function is addressed by O.Abuse_Function to ensure not using test features of TOE during Initialization and Operational Phase.

T.Cyber_Attack is addressed by O.Access_Control, O.Authentication, O.Event and O.Separate_IF.

O.Access_Control ensures only permitted systems has access to the functions and data. O.Authentication ensures the origin of external entity.

O.Event contributes to this aspect as it provides the audit generation for unsuccessful authentication attempt.

O.Separate_IF provides different interfaces for local and remote connection and ensures the separation of critical data for different interface.

T. Availability is addressed by O.Multi_Process to prevent the interaction for communication process and other functions of TOE.

T.Flow_Analyze is addressed by O.Conceal to prevent flow analysis between TOE and external entity.

OSP.Functional_Test is directly and completely covered by the security objective OE.Functional_Test.

OSP.Crypto_Man is directly and completely covered by the security objective OE.Crypto_Man.

OSP.Update is directly and completely covered by the security objective OE.Upgrade_Software.

OSP.Comm_Mod is directly and completely covered by the security objective OE.Comm_Mod.

A.Trusted_Entities is directly and completely covered by the security objective OE.Trusted_Entities.

A.Trusted_Admins is directly and completely covered by the security objective OE.Trusted_Admin.

A.Network is directly and completely covered by the security objective OE.Network.

A. Control is directly and completely covered by the security objective OE.Control.

A.Trusted_Manufacturer is directly and completely covered by the security objective OE.Manufacturing

A.Trusted_Designer is directly and completely covered by the security objective OE.Development.

5 EXTENDED COMPONENTS DEFINITION

This Protection Profile uses components defined as extensions to CC Part 2 [CC2]. The components FCS_RNG, FMT_LIM and FPR_CON are common in Protection Profiles for similar devices.

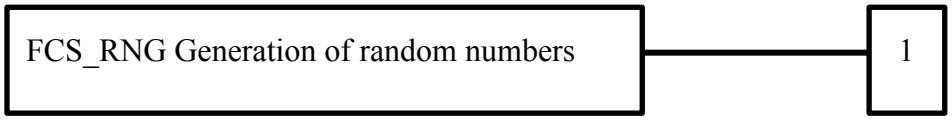
5.1 Definition of the Family FCS_RNG

To define the IT security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (Cryptographic Support) is defined here. This extended family FCS_RNG describes an SFR for random number generation used for cryptographic purposes.

Family Behavior:

This family defines quality requirements for the generation of random numbers, which are intended to be used for cryptographic purposes.

Component Leveling:



FCS_RNG.1 Generation of random numbers requires that the random number generator implements defined security capabilities and the random numbers meet a defined quality metric.

Management

FCS_RNG.1 There is no management activities foreseen.

Audit

FCS_RNG.1 There are no actions defined to be auditable.

FCS_RNG.1 Random number generation

Hierarchical to: -

Dependencies: -

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid*] random number generator, which implements: [assignment: *list of security capabilities*].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment*: a defined quality metric*].

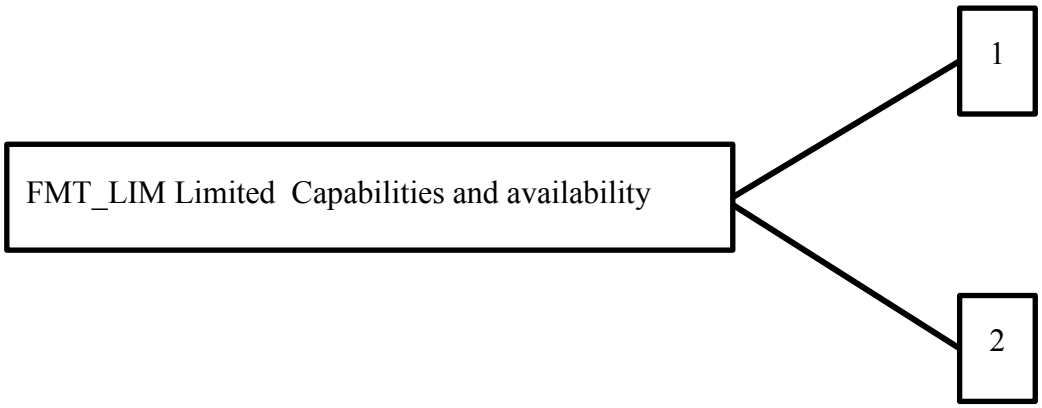
5.2 Definition of the Family FMT_LIM

To define the IT security functional requirements of the TOE an additional family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

Family Behavior:

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component Leveling:



FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life cycle.

Management

FMT_LIM.1, FMT_LIM.2 There are no management activities foreseen.

Audit

FMT_LIM.1, FMT_LIM.2 There are no actions defined to be auditable.

FMT_LIM.1 Limited capabilities

Hierarchical to: -

Dependencies: FMT_LIM.2 Limited availability

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced [assignment: *Limited capability and availability policy*].

FMT_LIM.2 Limited availability

Hierarchical to: -

Dependencies: FMT_LIM.2 Limited capability

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: *Limited capability and availability policy*].

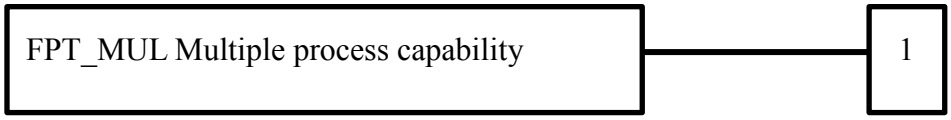
5.3 Definition of the Family FPT_MUL

To define the IT security functional requirements of the TOE an additional family (FMT_MUL) of the Class FPT (Protection of TSF) is defined here. This extended family FMT_MUL describes an SFR for availability.

Family Behavior:

This family defines availability requirements for TOE operation, which are intended to be used against specific attacks.

Component Leveling:



This family consists of only one component, FPT_MUL.1 multi process capability, which requires that the TSF provide process capability for TSF functions.

Management

FPT_MUL.1 There is no management activities foreseen.

Audit

FPT_MUL.1 There are no actions defined to be auditable.

FPT_MUL.1 Multiple Process Capability

Hierarchical to: -

Dependencies: -

FPT_MUL.1.1 The TSF shall be able to provide multiple process capability.

5.4 Definition of the Family FPR_CON

The additional family Communication concealing (FPR_CON) of the Class FPR (Privacy) is defined here to describe the specific IT security functional requirements of the TOE. The TOE shall protect privacy of the consumer that may be obtained by an attacker by observing the encrypted communication of the TOE with remote entities.

Family Behavior

This family defines requirements to mitigate attacks against communication channels in which an attacker tries to obtain privacy relevant information based on characteristics of an encrypted communication channel. Examples include but are not limited to an analysis of the frequency of communication or the transmitted workload.

Component Leveling:

Management

The following actions could be considered for the management functions in FMT:

a) Definition of the interval in FPR_CON.1.2 if definable within the operational phase of the TOE.

Audit

There are no auditable events foreseen.

FPR_CON.1 Communication concealing

Hierarchical to: -

Dependencies: -

FPR_CON.1.1 The TSF shall enforce the [assignment: *information flow policy*] in order to ensure that no personally identifiable information (PII) can be obtained by an analysis of [assignment: *characteristics of the information flow that need to be concealed*].

FPR_CON.1.2 The TSF shall connect to [assignment: *list of external entities*] in intervals as follows [selection: *weekly, daily, hourly, [assignment: other interval]*] to conceal the data flow.

6 SECURITY REQUIREMENTS

6.1 Overview

This chapter describes the security functional and the assurance requirements which have to be fulfilled by the TOE. Those requirements comprise functional components from part 2 of [CC] and the assurance components as defined for the Evaluation Assurance Level 4 from part 3 of [CC].

The following notations are used:

Refinement operation (denoted in such a way that added words are in **bold text** and changed words are ~~**crossed out**~~): is used to add details to a requirement, and thus further restricts a requirement.

Selection operation (denoted by ***italicized bold text*** and placed in square bracket): is used to select one or more options provided by the [CC] in stating a requirement.

Assignment operation (denoted by underlined text and placed in square bracket): is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.

Iteration operation are identified with a slash (e.g. "(/)")

It should be noted that the requirements in the following chapters are not necessarily be or dared alphabetically. Where useful the requirements have been grouped.

The following table summarizes all TOE security functional requirements of this PP:

Table 6 List of SFRs

FAU: Security Audit	
FAU_ARP.1	Security alarms for log
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAA.1:	Potential violation analysis
FAU_SAR.1	Audit review
FAU_STG.1	Protected audit trail storage

FAU_STG.4/SEC_HIGH	Prevention of audit data loss - high critical security log
FAU_STG.4/ SEC_LOW	Prevention of audit data loss - low critical security log
FAU_STG.4/REGULAR	Prevention of audit data loss - regular log
FAU_STG.4/SYS	Prevention of audit data loss - system log
FCS: Cryptographic Support	
FCO_NRO.2	Enforced proof of origin
FCS_COP.1/ENC-DEC	Cryptographic operation - Smart Meter encryption/decryption operation
FCS_COP.1/INT-AUTH	Cryptographic operation - Smart Meter integrity/authenticity operation
FCS_COP.1/SIGN-VER	Cryptographic operation - signature verification
FCS_RNG.1	Random number generation
FDP: User Data Protection	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.2	Complete information flow control
FDP_IFF.1	Simple security attributes
FDP_ITC.1	Import of User Data without security attributes
FDP_ITC.2	Import of User Data with security attributes
FDP_ETC.1	Export of User Data without security attributes
FDP_ETC.2	Export of User Data with security attributes
FDP_SDI.2	Stored data integrity monitoring and action
FDP_UIT.1	Data exchange integrity
FDP_UCT.1	Basic data exchange confidentiality
FIA: Identification and Authentication	
FIA_ATD.1	User attribute definition

FIA_AFL.1	Authentication failure handling
FIA_UAU.2	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.6	Re-authenticating
FIA_UID.2	User identification before any action
FIA_USB.1	User-subject binding
FMT: Security Management	
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FMT_LIM.1	Limited Capabilities
FMT_LIM.2	Limited availability
FMT_MTD.1/INI	Management of TSF Data - Initialization Data
FMT_MTD.1/TIME	Management of TSF Data - Date and Time
FMT_MTD.1/SECRET_READ	Management of TSF Data - Secret Read
FMT_MTD.1/FIRMWARE	Management of TSF Data - Smart Meter Firmware
FMT_MSA.3	Static attribute initialization for Smart Meter Access SFP
FPR: PRIVACY	
FPR_CON.1	Communication Concealing
FPT: Protection of TSF	
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.2	Notification of physical attack
FPT_PHP.3	Resistance to physical attack
FPT_TST.1	TSF testing
FPT_RPL.1	Replay detection

FPT_STM.1	Reliable time stamps
FPT_MUL.1	Multiple process capability
FTP: Trusted Path/Channel	
FTP_ITC.1	Inter-TSF trusted channel

6.1.1 Class FAU Security Audit

Table 7 List of Logs

Security Log		Regular Log	System Log
High Critical	**Low Critical**		
• Electromechanic seal is opened or forced • Battery level detected less than %10 • Environmental stress detected • Integrity check failures of User Data and TSF Data detected • Insufficient entropy during random number generation detected • Failure detected by periodic self-test function as detailed in FPT_TST.1 • Errors detected during processing cryptographic operations, • Unsuccessful software update detected • Unsuccessful authentication attempt detected from local	• Low battery level under %30 detected • DCC connection problem detected • Absent of line voltage is detected • Low critical log memory fullness detected more than %60 • Low critical log memory fullness detected more than %80 • System log memory	• Connection established via DCC • Connection established via Local Administrator • Consumption Data has been read • Event Data has been read	• Date and Time adjusted • Price Plan updated • DCC Configuration done • Smart Meter Firmware updated successfully

Security Log		Regular Log	System Log
High Critical	**Low Critical**		
interface • System log memory fullness detected • Unsuccessful authentication attempt detected from remote interface	fullness detected more than %60 • System log memory fullness detected more than %80		

6.1.1.1 FAU_ARP Security Alarms

FAU_ARP.1: Security Alarms for Log

Hierarchical to: -

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall ~~**take**~~ [generate a high critical log and inform authenticated DCC as soon as possible] upon detection of a potential security violation.

6.1.1.2 FAU_GEN Security audit data generation

FAU_GEN.1 Audit data generation

Hierarchical to: -

Dependencies: FPT_STM.1 Reliable time stamps.

FAU_GEN.1.1 The TSF shall be able to generate an audit record 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; and

c) [the auditable events specified in Table 7].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [none].

FAU_GEN.2: User identity association

Hierarchical to: -

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_SAA Security audit analysis

FAU_SAA.1: Potential violation analysis

Hierarchical to: -

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [High Critical Security Log listed in Table 7] known to indicate a potential security violation;

b) [assignment: any other rules].

6.1.1.4 FAU_SAR Security audit review

FAU_SAR.1 Audit review

Hierarchical to: -

Dependencies: FAU_GEN.1 Audit data generation.

FAU_SAR.1.1 The TSF shall provide [only Local Administrator] with the capability to read [all Event Data] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.5 FAU_STG Security audit event storage

FAU_STG.1 Protected audit trail storage

Hierarchical to: -

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthenticated deletion.

FAU_STG.1.2 The TSF shall be able to [***prevent***] unauthenticated modifications to the stored audit records in the audit trail.

FAU_STG.4/SEC_HIGH Prevention of audit data loss-High Critical Security Log

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1/SEC_HIGH

The TSF shall [***ignore audited events***] and [enter TOE break state mode (as detailed in 3.1.2.3)] if the **high critical security** audit trail is full.

FAU_STG.4/ SEC_LOW Prevention of audit data loss - Low Critical Security Log

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1/ SEC_LOW

The TSF shall [***overwrite the oldest stored audit records***] and [none] if the **low critical security** audit trail is full.

Application Note 4: TOE shall keep at least 50 Low Critical Security Logs.

FAU_STG.4/ REGULAR Prevention of audit data loss - Regular Log

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1/ REGULAR

The TSF shall [***overwrite the oldest stored audit records***] and [none] if the **regular** audit trail is full.

Application Note 5: TOE shall keep at least 50 Regular Logs.

FAU_STG.4/SYS Prevention of audit data loss - System Log

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1/SYS The TSF shall [***ignore audited events***] and [enter TOE break state mode (as detailed in 3.1.2.3)] if the **system** audit trail is full.

6.1.2 Class FCO Communication

6.1.2.1 FCO_NRO Non-repudiation of origin

FCO_NRO.2 Enforced proof of origin

Hierarchical to: FCO_NRO.1 Selective proof of origin

Dependencies: FIA_UID.1 Timing of identification

FCO_NRO.2.1 The TSF shall enforce the generation of evidence of origin for transmitted [any data sent from TOE to DCC (Consumption Data, Event Data and Device Information Data)] at all times.

FCO_NRO.2.2 The TSF shall be able to relate the [originator identity, time of origin] of the originator of the information, and the [body of the message] of the information to which the evidence applies.

FCO_NRO.2.3 The TSF shall provide a capability to verify the evidence of origin of information to [***recipient***] given [immediately]

6.1.3 Class FCS Cryptographic Support

6.1.3.1 FCS_COP Cryptographic operation

FCS_COP.1/ENC-DEC Cryptographic Operation-Smart Meter Encryption/Decryption Operation

Hierarchical to: -

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.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [encryption, decryption] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [256 bit] that meet the following: [FIPS 197].

Application Note 6: Decryption is also used during Smart Meter initialization.

FCS_COP.1/INT-AUTH Cryptographic Operation-Smart Meter Integrity/Authenticity Operation

Hierarchical to: -

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.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [authentication, integrity protection] in accordance with a specified cryptographic algorithm [HMAC] and cryptographic key sizes [256 bit] that meet the following: [FIPS 198-1].

FCS_COP.1/SIGN-VER Cryptographic Operation-Signature Verification

Hierarchical to: -

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.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [signature verification] in accordance with a specified cryptographic algorithm [RSA] and cryptographic key sizes [2048] that meet the following: [PKCS#1 v2.1].

Application Note 7: This operation necessary for Smart Meter Firmware Update and Local Administrator Authentication.

FCS_RNG.1 Random Number Generation

Hierarchical to: -

Dependencies: -

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid*] random number generator, which implements: [assignment: *list of security capabilities*].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment*: a defined quality metric*].

6.1.4 Class FDP User Data Protection

6.1.4.1 FDP_ACC Access control policy

FDP_ACC.1 Subset access control

Hierarchical to: -

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [Smart Meter Access Control SFP] on [

Subjects:

- Authenticated DCC Initialization Agent
- Authenticated DCC
- Authenticated Local Administrator

Objects:

- User data stored in Smart Meter
    - Consumption data
    - Event data
    - DCC Parameters
    - Fabrication Parameters
- TSF Data
    - Initialization Key
    - Local Access Control Root Public Key
    - Smart Meter Time
    - Smart Meter Firmware
    - Encryption Key
    - HMAC Key
- Operations: write, read, modify

]

6.1.4.2 FDP_ACF Access control functions

FDP_ACF.1 Security attribute based access control

Hierarchical to: -

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce [Smart Meter Access Control SFP] to objects based on following: [

Subjects:

- Authenticated DCC Initialization Agent
- Authenticated DCC
- Authenticated Local Administrator

Subject Attributes:

- User Identity,
- Authentication Status,
- TOE Interface,

Objects:

- User data stored Smart Meter
    - Consumption Data
    - Event Data
    - DCC Parameters
    - Fabrication Parameters
- TSF Data (as detailed in FDP_ACC.1.1)

Object Attributes:

- Access Control List,
- Object ID,
- Command freshness,
- Firmware signature (for Smart Meter Firmware update),
- Firmware version (for Smart Meter Firmware update),

- Message Authentication Code

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- an Authenticated DCC Initialization Agent is only allowed to write initialization parameters (Local Access Control Root Public Key, Encryption Key, HMAC Key) via Local Interface.
- an Authenticated DCC is only allowed to have read access User Data (Consumption Data, Event Data, Fabrication and DCC Parameters) and Smart Meter Time via Remote Interface.
- an Authenticated Local Administrator is only allowed to have read access Detailed Consumption Data, Event Data, Fabrication and DCC Parameters via Local Interface.
- any User is allowed to have read access Consumption Index Data and Smart meter Time via Local Interface (Visual Display).
- TOE accepts write and modification operation for DCC Parameters and Smart Meter Time via Remote Interface only if {
    - sender: an Authenticated DCC
    - Command freshness=successful (not replayed)
    - MAC control: successful

    }
- TOE accepts Smart Meter Firmware update operation for via Remote Interface only if {
    - Sender: an Authenticated DCC
    - Command freshness=successful (not replayed)
    - MAC control: successful
    - Firmware signature control: successful
    - Firmware version: recent

    }

- an Authenticated Local Administrator is only allowed to have write and modify access for DCC Parameters and Smart Meter Time via Local Interface.

].

FDP_ACF.1.3 The TSF shall explicitly authorize 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: [

- nobody shall be allowed to modify or delete
  - Consumption Data
  - Event Data
  - Fabrication Parameters
  - TSF Data excluding Smart Meter Time and Smart Meter Firmware.
- nobody shall be allowed to have read access TSF Data except Smart Meter Time].

6.1.4.3 FDP_IFC Information flow control policy

FDP_IFC.2 Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the [Smart Meter Information Flow Control SFP] on [TOE, DCC, Local Administrator and all information flowing between them] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 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.

6.1.4.4 FDP_IFF Information flow control functions

FDP_IFF.1 Simple security attributes

Hierarchical to: -

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [Smart Meter Information Flow Control SFP] based on the following types of subject and information security attributes: [

subjects: The TOE and external entities on DCC or local side

information: any information that is sent to, from or via the TOE

security attributes: destination interface, source interface, destination authentication status, command freshness, connection interval (against data traffic analysis)].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- Information flow with DCC is allowed, if
  - source interface=TOE/DCC and destination interface=DCC/TOE
  - secure communication with MAC Authentication=true,
  - command freshness=successful,
  - connection interval=acceptable
- Local port connection establishment is allowed, if
  - source interface=TOE/local port and destination interface=local port/TOE
  - local authentication=true

].

FDP_IFF .1.3 The TSF shall enforce the [none].

FDP_IFF .1.4 The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF .1.5	The TSF shall explicitly deny an information flow based on the following rules: [The TOE shall deny any acceptance of information by external entities in the unless the authenticity, integrity, confidentiality and freshness of the Data could be verified].

Application Note 8: FDD_IFF.1.5 is applicable for Remote Interface only

6.1.4.5 FDP_ITC Import from the outside of the TOE

FDP_ITC.1 Import of User Data without security attributes

Hierarchical to:	-
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialization
FDP_ITC.1.1	The TSF shall enforce the [Smart Meter Access Control SFP and Smart Meter Information Flow Control SFP] when importing User Data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing User Data controlled under the SFP from outside the TOE: [none].

Application Note 9: FDP_ITC.1 is applicable for import of: Local Access Control Root Public Key, Encryption Key, HMAC Key, DCC Parameters and Smart Meter Time via Local Interface

FDP_ITC.2: Import of User Data with security attributes

Hierarchical to:	-
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF Data consistency

FDP_ITC.2.1 The TSF shall enforce the [Smart Meter Access Control SFP and Smart Meter Information Flow Control SFP] when importing User Data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported User Data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the User Data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported User Data is as intended by the source of the User Data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing User Data controlled under the SFP from outside the TOE: [

- upgrade of Smart Meter Firmware components only if the integrity and the authenticity of the upgrade firmware package is confirmed, signature of authority verified and version approved by TOE
- upgrade of the DCC Parameters only if the integrity and the authenticity of the upgrade package is confirmed by virtue of the upgrade credentials
- upgrade of the Smart Meter Time only if the integrity and the authenticity of the upgrade package is confirmed by TOE

].

6.1.4.6 FDP_ETC Export from the TOE

FDP_ETC.1 Export of User Data without security attributes

Hierarchical to: -

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FDP_ETC.1.1 The TSF shall enforce the [Smart Meter Access Control SFP and Smart Meter Information Flow Control SFP] when exporting User Data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the User Data without the User Data's associated security attributes

Application Note 10: FDP_ETC.1 is applicable for export of data from via Local Interface

FDP_ETC.2 Export of User Data with security attributes

Hierarchical to:	-
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ETC.2.1	The TSF shall enforce the [Smart Meter Access Control SFP and Smart Meter Information Flow Control SFP] when exporting User Data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2	The TSF shall export the User Data with the User Data's associated security attributes.
FDP_ETC.2.3	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported User Data.
FDP_ETC.2.4	The TSF shall enforce the following rules when User Data is exported from the TOE: [• TOE adds Message Authentication Code and command time for any data before sending DCC.]

Application Note 11: FDP_ETC.2 is applicable for export of data from Remote Interface

6.1.4.7 FDP_SDI Stored data integrity

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	-
FDP_SDI.2.1	The TSF shall monitor User Data stored in containers controlled by the TSF for [integrity errors] ~~on all objects, based on the following attributes: [assignment: User Data attributes].~~
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall [generate a high critical log and inform authenticated DCC as soon as possible].

6.1.4.8 FDP_UIT Inter-TSF User Data Integrity Transfer Protection

FDP_UIT.1 Data exchange integrity

Hierarchical to: -

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

FDP_UIT.1.1 The TSF shall enforce [Smart Meter Access Control SFP] to [***transmit, receive***] ~~**User Data**~~ **any transmitted and received data between TOE and DCC** in a manner protected from [***modification, deletion, insertion, replay errors***].

FDP_UIT.1.2 The TSF shall be able to determine on receipt of ~~**User Data**~~ any **received data from DCC**, whether [***modification, deletion, insertion, replay***] has occurred.

6.1.4.9 FDP_UCT Inter-TSF User Data Confidentiality Transfer Protection

FDP_UCT.1: Basic data exchange confidentiality

Hierarchical to: -

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

[FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1 The TSF shall enforce the [Smart Meter Access Control SFP] to [***transmit, receive***] ~~**User Data**~~ any **transmitted and received data between TOE and DCC** in a manner protected from unauthenticated disclosure.

6.1.5 Class FIA: Identification and Authentication

6.1.5.1 FIA_ATD User Attribute Definition

FIA_ATD.1: User attribute definition

Hierarchical to: -

Dependencies: -

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

- User Identity
- Status of Identity (Authenticated or not)
- Role Membership
- [assignment: *list of security attributes*].

6.1.5.2 FIA_AFL Authentication failures

FIA_AFL.1 Authentication failure handling

Hierarchical to: -

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [five (5)] unsuccessful authentication attempts occur related to [authentication attempts at Local Interface].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [enter TOE break state mode, generate an audit, inform Authenticated DCC (as detailed in 3.1.2.3) and show a warning indicator on display].

Application Note 12: Only applicable for Local Interface Authentication

6.1.5.3 FIA_UAU User authentication

FIA_UAU.2: User authentication before any action

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note 13: Consumption Index Data and Smart Meter Time can be read with no authentication via Local Interface

FIA_UAU.5: Multiple authentication mechanisms

Hierarchical to: -

Dependencies: -

FIA_UAU.5.1 The TSF shall provide [

- HMAC authentication via Symmetric keys at the Remote Interface
- Password-Token authentication at the Local Interface
- Decryption authentication at the Local Interface for Initialization

] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [

- DCC shall be authenticated via MAC Authentication at the Remote Interface
- Local Administrator shall be authenticated via token-password at the Local Interface
- DCC Initialization Agent shall be authenticated via decryption authentication at the Local Interface also

].

Application Note 14: Authentication Methods are detailed in document **Hata! Başvuru kaynağı bulunamadı.**

FIA_UAU.6: Re-authenticating

Hierarchical to: -

Dependencies: -

FIA_UAU.6.1 The TSF shall re-authenticate an external entity under the conditions [

- Password-token authentication shall be re-authenticated after 10 minutes of inactivity for local users
- HMAC and decryption authentication shall be repeated for any command

].

6.1.5.4 FIA_UID User Identification

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: -

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.5.5 User-subject binding (FIA_USB)

FIA_USB.1: User-subject binding

Hierarchical to: -

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [attributes as defined in FIA_ATD.1].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [none].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [none].

6.1.6 Class FMT: Security Management

6.1.6.1 FMT_SMF Specification of Management Functions

FMT_SMF.1: Specification of Management Functions

Hierarchical to: -

Dependencies: -

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- Initialization
- Date Time Configuration
- Smart Meter Firmware Update
- DCC Parameters Configuration

].

6.1.6.2 FMT_SMR Security management roles

FMT_SMR.1: Security roles

Hierarchical to: -

Dependencies: -

FMT_SMR.1.1 The TSF shall maintain the roles [

- Authenticated DCC Initialization Agent
- Authenticated DCC
- Authenticated Local Administrator

].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.6.3 FMT_LIM Limited Capabilities and Availability

FMT_LIM.1 Limited Capabilities

Hierarchical to: -.

Dependencies: FMT_LIM.2 Limited availability

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: [

Deploying Test Features after TOE Delivery do not allow:

- User Data to be manipulated and disclosed,
- TSF Data to be manipulated or disclosed,
- Embedded software to be reconstructed,
- substantial information about construction of TSF to be gathered which may enable other attacks

].

FMT_LIM.2 Limited availability

Hierarchical to: -

Dependencies: FMT_LIM.1 Limited capabilities

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced:[

Deploying Test Features after TOE Delivery do not allow,

- User Data to be manipulated and disclosed,
- TSF Data to be manipulated or disclosed,
- Embedded software to be reconstructed,
- substantial information about construction of TSF to be gathered which may enable other attacks

]

6.1.6.4 FMT_MTD Management of TSF Data

FMT_MTD.1/INI Management of TSF Data - Initialization Data

Hierarchical to: -

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/INI The TSF shall restrict the ability to ***[write]*** the [Initialization Data] to [Authenticated DCC Initialization Agent].

Application Note 15: Initialization Data includes; Initialization Key, Local Access Control Root Public Key, Encryption Key, HMAC Key

FMT_MTD.1/TIME Management of TSF Data - Date and Time

Hierarchical to: -

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 [Smart Meter Time] to [Authenticated DCC and Authenticated Local Administrator].

FMT_MTD.1/SECRET_READ Management of TSF Data - Secret Read

Hierarchical to: -

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/SECRET_READ

The TSF shall restrict the ability to ***[read]*** the [TSF Data except Smart meter time] to [none].

FMT_MTD.1/FIRMWARE Management of TSF Data - Smart Meter Firmware

Hierarchical to: -

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/FIRMWARE

The TSF shall restrict the ability to ***[modify]*** the [Smart Meter Firmware] to [Authenticated DCC].

6.1.7 Class FPR: Privacy

6.1.7.1 FPR_CON Communication Concealing

FPR_CON.1: Communication Concealing

Hierarchical to: -

Dependencies: -

FPR_CON.1.1 The TSF shall enforce the [Smart Meter Information Flow Control SFP] in order to ensure that no personally identifiable information (**PII**) can be obtained by an analysis of [assignment: *characteristics of the information flow that need to be concealed*].

FPR_CON.1.2 The TSF shall connect to [Authenticated DCC] in intervals as follows [selection: *weekly, daily, hourly, [assignment: other interval*] to conceal the data flow.

Application Note 16: Only applicable for Remote Interface

6.1.8 Class FPT: Protection of the TSF

6.1.8.1 FPT_FLS Fail Secure

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: -

Dependencies: -

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

- detection of physical manipulation to electromechanic seal
- detection of low battery level under %10,
- detection of the fullness of System and High Critical log memory [assignment *: list of other types of failures in the TSF, or none*].

6.1.8.2 FPT_PHP TSF Physical Protection

FPT_PHP.2 Notification of physical attack

Hierarchical to: FPT_PHP.1 Passive detection of physical attack

Dependencies: FMT_MOF.1 Management of security functions behavior

FPT_PHP.2.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.2.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.2.3 For [Smart Meter Module], the TSF shall monitor the devices and elements and notify [any user by generating audit and showing a warning on display] when physical tampering with the TSF's devices or TSF's elements has occurred.

Application Note 17: Physical tampering includes environmental stress in this case.

FPT_PHP.3 Resistance to physical attack

Hierarchical to: -

Dependencies: -

FPT_PHP.3.1 The TSF shall resist [physical tampering] to the [Smart Meter] by responding automatically such that the SFRs are always enforced.

FPT_TST TSF Self-Test

FPT_TST.1 TSF testing

Hierarchical to: -

Dependencies: -

FPT_TST.1.1 The TSF shall run a suite of self-tests ***[periodically, during normal operation]*** to demonstrate the **integrity of TSF Data including stored executable code** and correct operation of ***[the TSF]***.

FPT_TST.1.2 The TSF shall ~~provide authenticated users with the capability to~~ verify the integrity of ***[TSF Data]***.

FPT_TST.1.3 The TSF shall ~~provide authenticated users with the capability to~~ verify the integrity of ***[TSF]***.

6.1.8.3 FPT_RPL Replay Detection

FPT_RPL.1: Replay detection

Hierarchical to: -

Dependencies: -

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [Authenticated DCC].

FPT_RPL.1.2 The TSF shall perform [ignore replayed data] when replay is detected.

Application Note 18: Replay attack protection is provided by time control as defined in document Hata! Başvuru kaynağı bulunamadı.

6.1.8.4 FPT_STM Time Stamps

FPT_STM.1: Reliable time stamps

Hierarchical to: -

Dependencies: -

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

6.1.8.5 FPT_MUL Process Capability

FPT_MUL.1 Multiple Process Capability

Hierarchical to: -

Dependencies: -

FPT_MUL.1.1 The TSF shall be able to provide multiple process capability.

6.1.9 Class FTP: Trusted path/channels

6.1.9.1 FTP_ITC Inter -TSF trusted channel

FTP_ITC.1: Inter -TSF trusted channel for DCC

Hierarchical to: -

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 [***the TSF***] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [Authenticated DCC].

6.2 Security Assurance Requirements for the TOE

The assurance requirements for the evaluation of the TOE and for its development and operating environment are chosen as the predefined assurance package EAL2 augmented by AVA_VAN.3.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

Table 8 provides an overview for security functional requirements coverage and also giving an evidence for sufficiency and necessity of the SFRs chosen.

Table 8 Coverage of Security Objectives by SFRs for TOE

	O.Access_Control	O.Event	O.Storage_Integrity	O.Authentication	O.Transfer	O.Protect	O.Physcal_Tamper	O.Env_Tamper	O.Battery_Control	O.Abuse_Function	O.Update	O.Multi_Process	O.Separate_IF	O.Conceal
FAU_ARP.1		X												
FAU_GEN.1		X							X					

	O.Access_Control	O.Event	O.Storage_Integrity	O.Authentication	O.Transfer	O.Protect	O.Physcal_Tamper	O.Env_Tamper	O.Battery_Control	O.Abuse_Function	O.Update	O.Multi_Process	O.Separate_IF	O.Conceal
FAU_GEN.2		X												
FAU_SAA.1:		X												
FAU_SAR.1		X												
FAU_STG.1		X	X											
FAU_STG.4/SEC_HIGH		X	X											
FAU_STG.4/ SEC_LOW		X	X											
FAU_STG.4/ REGULAR		X	X											
FAU_STG.4/SYS		X	X											
FCO_NRO.2				X										
FCS_COP.1/ENC-DEC				X	X						X			
FCS_COP.1/INT-AUTH			X	X	X						X			
FCS_COP.1/SIGN-VER											X			
FCS_RNG.1	X			X										
FDP_ACC.1	X													
FDP_ACF.1	X												X	
FDP_IFC.2	X													
FDP_IFF.1	X												X	
FDP_ITC.1	X													
FDP_ITC.2	X				X						X			
FDP_ETC.1	X													

	O.Access_Control	O.Event	O.Storage_Integrity	O.Authentication	O.Transfer	O.Protect	O.Physcal_Tamper	O.Env_Tamper	O.Battery_Control	O.Abuse_Function	O.Update	O.Multi_Process	O.Separate_IF	O.Conceal
FDP_ETC.2	X				X									
FDP_SDI.2			X											
FDP_UIT.1					X						X			
FDP_UCT.1					X						X			
FIA_ATD.1				X										
FIA_AFL.1	X													
FIA_UAU.2	X			X										
FIA_UAU.5	X			X										
FIA_UAU.6	X			X										
FIA_UID.2	X			X										
FIA_USB.1				X										
FMT_SMF.1											X			
FMT_SMR.1	X													
FMT_LIM.1	X									X				
FMT_LIM.2	X									X				
FMT_MTD.1/INI	X													
FMT_MTD.1/TIME	X													
FMT_MTD.1/SECRET_READ	X													
FMT_MTD.1/FIRMWARE	X										X			
FPR_CON.1														X
FPT_FLS.1			X				X	X	X					

	O.Access_Control	O.Event	O.Storage_Integrity	O.Authentication	O.Transfer	O.Protect	O.Physcal_Tamper	O.Env_Tamper	O.Battery_Control	O.Abuse_Function	O.Update	O.Multi_Process	O.Separate_IF	O.Conceal
FPT_PHP.2		X					X	X						
FPT_PHP.3							X							
FPT_TST.1			X			X								
FPT_RPL.1					X									
FPT_STM.1		X	X											
FPT_MUL.1												X		
FTP_ITC.1					X						X			

A detailed justification of required for suitability of the security functional requirements to achieve the security objectives is given in Table 9.

Table 9 Suitability of the SFRs

Security Objective	Security Functional Requirement	
O.Access_Control	FDP_ACC.1	Provides security functional policy for data access
	FDP_ACF.1	Defines security attributes and rules for access control policy
	FDP_IFC.2	Provides security functional policy for information flow
	FDP_IFF.1	Defines subjects, attributes and information within the scope of information flow control policy. Provides information flow control policy and deny access rules.
	FDP_ITC.1	Provides import of Local Access Control Root Public Key, Encryption Key, HMAC Key, DCC Parameters and Smart Meter Time from outside of

Security Objective	Security Functional Requirement	
		the TOE with the role of authenticated Local Administrator using Access Control SFP and Information Flow Control SFP.
	FDP_ITC.2	Provides import of DCC Parameters, Smart Meter Time and Smart Meter Firmware from outside of the TOE with the role of Authenticated DCC using Access Control SFP and Information Flow Control SFP.
	FDP_ETC.1	Provides export of Consumption Data, Event Data and Device Information to outside of the TOE with the role of authenticated Local Administrator using Access Control SFP and Information Flow Control SFP.
	FDP_ETC.2	Provides export of Consumption Data, Event Data and Device Information to outside of the TOE with the role of Authenticated DCC using Access Control SFP and Information Flow Control SFP.
	FIA_AFL.1	Detects and records authentication failure events for Authenticated DCC and authenticated Local Administrator
	FIA_UAU.2	No allowed actions before authentication
	FIA_UAU.5	Defines multiple authentication mechanisms for remote access and local access.
	FIA_UAU.6	Defines re-authentication mechanisms for remote access and local access.
	FIA_UID.2	No allowed actions before identification
	FMT_SMR.1	Defines roles used in Security functional policies
	FMT_LIM.1	Provide deploying test features for limiting

Security Objective	Security Functional Requirement	
		capabilities for disclosure and modification of User Data and TSF Data.
	FMT_LIM.2	Provide deploying test features for limiting availabilities for disclosure and modification of User Data and TSF Data.
	FMT_MTD.1/INI	Define initialization data management rule
	FMT_MTD.1/TIME	Define current date and time management rule
	FMT_MTD.1/SECRET_READ	Define reading TSF Data except Smart Meter Time management rule
	FMT_MTD.1/FIRMWARE	Define Smart Meter Firmware management rule
	FCS_RNG.1	Provides random number
O.Event	FAU_ARP.1	Define actions maintained during detection of a potential security violation.
	FAU_GEN.1	Generates correct audit events
	FAU_GEN.2	Generates audit events with the identity of the user that caused the event
	FAU_SAA.1	Defines violation analysis for logs
	FAU_SAR.1	Allows Local Administrator to read audit records
	FAU_STG.1	Protects stored audit data from unauthorized deletion
	FAU_STG.4/SEC_HIGH	Define actions carried out during audit trail is full
	FAU_STG.4/	Define actions carried out during audit trail is full

Security Objective	Security Functional Requirement	
	SEC_LOW	
	FAU_STG.4/ REGULAR	Define actions carried out during r audit trail is full
	FAU_STG.4/SY S	Define actions carried out during audit trail is full
	FPT_PHP.2	Generation of audit event detection of physical tampering
	FPT_STM.1	Provides accurate time for logging events
O.Storage_Integrity	FAU_STG.1	Protects stored audit data integrity from unauthorized modification
	FAU_STG.4/SE C_HIGH	Define actions carried out during audit trail is full
	FAU_STG.4/ SEC_LOW	Defines actions carried out during audit trail is full
	FAU_STG.4/ REGULAR	Define actions carried out during audit trail is full
	FAU_STG.4/SY S	Defines actions carried out during audit trail is full
	FCS_COP.1/ INT-AUTH	Controls integrity of stored integrity critical data
	FDP_SDI.2	Monitors User Data stored for integrity errors
	FPT_STM.1	Provides accurate time for integrity check
	FPT_TST.1	Detects integrity failures for TSF Data including stored executable code

Security Objective	Security Functional Requirement	
O.Authentication	FCO_NRO.2	Generates evidence of origin of the data to be transferred to the DCC
	FCS_COP.1/INT_AUTH	Provides origin authentication and verification for any data that is sent or taken by the TOE
	FCS_COP.1/ENC-DEC	Provides authentication mechanism by decryption operation during Smart Meter Initialization.
	FCS_RNG.1	Provides random number
	FIA_UAU.2	No allowed actions before authentication
	FIA_UAU.5	Defines multiple authentication mechanisms for remote access and local access.
	FIA_UAU.6	Defines re-authentication mechanisms for remote access and local access.
	FIA_UID.2	No allowed actions before identification
	FIA_USB.1	Defines user - subject binding mechanism for the TOE
	FIA_ATD.1	Defines subject attributes
	FPT_RPL.1	Protect received data from replay attack
O.Transfer	FCS_COP.1/ENC-DEC	Provides the encryption and decryption operations for secure communication between DCC and Smart Meter

Security Objective	Security Functional Requirement	
	FCS_COP.1/INT-AUTH	Provides the integrity protection operations for secure communication between DCC and Smart Meter
	FDP_ETC.2	Provides export of Detailed Consumption Data, Consumption Index data ,Event Data, device information, IP Access List, DCC Parameters and Smart Meter Time to outside of the TOE with the role of Authenticated DCC using Access Control SFP and Information Flow Control SFP
	FDP_ITC.2	Provides import of DCC Parameters, Smart Meter Time, Smart Meter Firmware from outside of the TOE with the role of Authenticated DCC using Access Control SFP and Information Flow Control SFP
	FTP_ITC.1	Provide a secure communication channel to the DCC
	FDP_UCT.1	Protect received and transmitted data from unauthenticated disclosure
	FDP_UIT.1	Protect received and transmitted data from unauthenticated modification
	FPT_RPL.1	Protect received data from replay attack
O.Protect	FPT_TST.1	Provide self-test mechanism to demonstrate TSF and TSF Data integrity
O.Physcal_Tamper	FPT_FLS.1	Defines failure conditions including physical tamper for preservation of secure state
	FPT_PHP.2	Provide notification of physical tampering
	FPT_PHP.3	Define resistive mechanism of the TOE to the

Security Objective	Security Functional Requirement	
		physical tampering
O.Env_Tamper	FPT_PHP.2	Provide notification of physical tampering including environmental stress.
O.Battery_Control	FAU_GEN.1	Generate audit event for low battery level under %10
	FPT_FLS.1	Defines failure conditions including detection of low battery level for preservation of secure state.
O.Abuse_Function	FMT_LIM.1	Provide deploying test features for limiting capabilities for disclosure and modification of User Data and TSF Data.
	FMT_LIM.2	Provide deploying test features for limiting availabilities for disclosure and modification of User Data and TSF Data.
O.Update	FCS_COP.1/ENC-DEC	Provides the encryption and decryption operations for secure communication between DCC and Smart Meter during Smart Meter Firmware update
	FCS_COP.1/INT-AUTH	Provides the integrity protection operations for secure communication between DCC and Smart Meter during Smart Meter Firmware update
	FDP_ITC.2	Provides import of Smart Meter Firmware from outside of the TOE.
	FCS_COP.1/SIGN-VER	Provides verification of Smart Meter Firmware signature before upgrade the working one.
	FDP_UCT.1	Protect received and transmitted data from unauthenticated disclosure

Security Objective	Security Functional Requirement	
	FDP_UIT.1	Protect received and transmitted data from unauthenticated modification
	FMT_MTD.1/FIRMWARE	Define Smart Meter Firmware management rule
	FMT_SMF.1	Provide management functions including firmware update
	FTP_ITC.1	Provides a secure communication channel to the DCC
O.Multi_Process	FPT_MUL.1	Provides multiple process capability for TOE.
O.Separate_IF	FDP_ACF.1	Provides security functional policy for data access
	FDP_IFF.1	Defines subjects, attributes and information within the scope of information flow control policy. Provides information flow control policy and deny access rules.
O.Conceal	FPR_CON.1	Prevent disclosure of personally identifiable information (PII) by concealing the data flow.

6.3.2 Rationale for Security Functional Requirements dependencies

Selected security functional requirements include related dependencies. Table 10 below provides a summary of the security functional requirements dependency analysis.

Table 10 Security Functional Requirements Dependencies

Component	Dependencies	Included / not included
FAU_ARP.1	FAU_SAA.1	included
FAU_GEN.1	FPT_STM.1	included
FAU_GEN.2	FAU_GEN.1	included
FAU_SAR.1	FAU_GEN.1	included
FAU_STG.1	FAU_GEN.1	included
FAU_STG.4/SEC_HIGH	FAU_STG.1	included

Component	Dependencies	Included / not included
FAU_STG.4/ SEC_LOW	FAU_STG.1	included
FAU_STG.4/REGULAR	FAU_STG.1	included
FAU_STG.4/SYS	FAU_STG.1	included
FCO_NRO.2	FIA_UID.1	FIA.UID.2 is hierarchical to FIA.UID.1
FCS_COP.1/ENC-DEC	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 ; FCS_CKM.4	FDP_ITC.1 included. According to communication protocol encryption key should not be deleted. Tamper system of the TOE protects keys from misuse, disclosure or modification.
FCS_COP.1/INT-AUTH	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 ; FCS_CKM.4	FDP_ITC.1 included. According to communication protocol MAC key should not be deleted. Tamper system of the TOE protects keys from misuse, disclosure or modification.
FCS_COP.1/SIGN-VER	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 ; FCS_CKM.4	FDP_ITC.1 included. According to communication protocol Firmware Update Public Key should not be deleted. Tamper system of the TOE protects keys from misuse, disclosure or modification.
FDP_ACC.1	FDP_ACF.1	included
FDP_ACF.1	FDP_ACC.1; FMT_MSA.3	FDP_ACC.1included. The access control TSF according to FDP_ACF.1 uses security attributes having been defined during the manufacturing and fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1and FMT_MSA.3) is necessary here.
FDP_IFC.2	FDP_IFF.1	included
FDP_IFF.1	FDP_IFC.1; FMT_MSA.3	FDP_IFC.2 is hierarchical to

Component	Dependencies	Included / not included
		FDP_IFC.1; The access control TSF according to FDP_ACF.1 uses security attributes having been defined during the manufacturing and fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1and FMT_MSA.3) is necessary here.
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1 ; FMT_MSA.3	FDP_ACC.1 and FDP_IFC.1 Included. The access control TSF according to FDP_ACF.1 uses security attributes having been defined during the manufacturing and fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1and FMT_MSA.3) is necessary here.
FDP_ITC.2	FDP_ACC.1 or FDP_IFC.1 ; FMT_MSA.3	FDP_ACC.1 and FDP_IFC.1 included. The access control TSF according to FDP_ACF.1 uses security attributes having been defined during the manufacturing and fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1and FMT_MSA.3) is necessary here.
FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	included
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	included
FDP_SDI.2	-	-
FDP_UIT.1	FDP_ACC.1 or FDP_IFC.1; FTP_ITC.1 or FTP_TRP.1	FDP_ACC.1, FDP_IFC.1, FTP_ITC.1 included
FDP_UCT.1	FDP_ACC.1 or FDP_IFC.1;	FDP_ACC.1, FDP_IFC.1,

Component	Dependencies	Included / not included
	FTP_ITC.1 or FTP_TRP.1	FTP_ITC.1 included
FIA_ATD.1	-	-
FIA_AFL.1	FIA_UAU.1	FIA.UAU.2 is hierarchical to FIA.UAU.1
FIA_UAU.2	FIA_UID.1	FIA.UID.2 is hierarchical to FIA.UID.1
FIA_UAU.5	-	-
FIA_UAU.6	-	-
FIA.UID.2	-	-
FIA_USB.1	FIA_ATD.1	included
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1	included
FMT_LIM.1	FMT_LIM.2	included
FMT_LIM.2	FMT_LIM.1	included
FMT_MTD.1/INI	FMT_SMR.1; FMT_SMF.1	included
FMT_MTD.1/TIME	FMT_SMR.1; FMT_SMF.1	included
FMT_MTD.1/SECRET_READ	FMT_SMR.1; FMT_SMF.1	included
FMT_MTD.1/FIRMWARE	FMT_SMR.1; FMT_SMF.1	included
FPR_CON.1	-	-
FPT_FLS.1	-	-
FPT_PHP.2	FMT_MOF.1	Management functions having been defined during the manufacturing and fixed over the whole life time of the TOE. No management of these functions is necessary here.
FPT_PHP.3	-	-
FPT_TST.1	-	-
FPT_RPL.1	-	-
FPT_STM.1	-	-
FPT_TDC.1	-	-

Component	Dependencies	Included / not included
FTP_ITC.1	-	-

6.3.3 Security Assurance Requirements Rationale

In order to keep evaluations according to this Protection Profile commercially feasible EAL 2 has been chosen as assurance level as this is the lowest level that provides the prerequisites for the use of AVA_VAN.3. AVA_VAN.3 is chosen because the threats that were chosen are consistent with an attacker of Enhanced-Basic attack potential.

6.3.4 Security Requirements - Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together forms an internally consistent whole.

The dependency analysis in Table 10 shows that the basis for internal consistency between all defined functional requirements is satisfied.

The assurance package EAL2 is a pre-defined set of internally consistent assurance requirements. AVA_VAN.3 as augmented does not cause inconsistencies with EAL2 package. The assurance requirements are internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met. So, there are no inconsistencies between the goals of these two groups of security requirements.

7 ACRONYMS

AES	: Advanced Encryption Standard
CC	: Common Criteria
CCMB	: Common Criteria Management Board
DCC	: Data and Control Center
DSL	: Digital Subscriber Line
EAL	: Evaluation Assurance Level (defined in CC)
EDC	: Electricity Distribution Company
GPRS	: General Packet Radio Service
OSP	: Organizational Security Policy
PP	: Protection Profile
PKI	: Public Key Infrastructure
PLC	: Power Line Communication
SFR	: Security Functional Requirements
SHA	: Secure Hash Algorithm
TAMIS	: Turkish Advanced Metering Infrastructure System
TOE	: Target of Evaluation
TSF	: TOE Security Functionality (defined in CC)
TSE	: Turkish Standards Institute

8 BIBLIOGRAPHY

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1:Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012

Turkish Electricity Advanced Metering Infrastructure

[5] Technical Requirements For Smart Meter Of Turkish Electricity Advanced Metering Infrastructure (Document will be prepared)

[6] Türkiye Gelişmiş Ölçüm Altyapısında Kullanılacak Akıllı Sayaçlar Güvenlik Mimarisi, Sürüm 1.0, 07.02.2014.