Certification Report

EAL 2+(AVA_VAN.3)

Evaluation of

Turkish Standards Institution Common Criteria Protection Profile for Smart Meter of Turkish Electricity Advanced Metering Infrastructure

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

TABLE OF CONTENTS

Document Information

Date of Issue	03.09.2014
Version of Report	1
Author	Zümrüt MÜFTÜOĞLU
Technical Responsible	Mustafa YILMAZ
Approved	Mariye Umay AKKAYA
Date Approved	03.09.2014
Certification Report Number	21.0.01/14-025
Sponsor and Developer	Turkish Standards Institution/Türk Standardları Enstitüsü
Evaluation Lab	TUBİTAK BİLGEM OKTEM
PP Name	Common Criteria Protection Profile for Smart Meter of Turkish Electricity Advanced Metering Infrastructure(SMTEAMI PP)
Pages	19

Document Change Log

Release	***Date***	***Pages Affected***	***Remarks/Change Reference***
v1	02.09.2013	All	Final Released

DISCLAIMER

This certification report and the PP defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 4, using Common Methodology for IT Products Evaluation, version 3.1, revision 4. This certification report and the associated Common Criteria document apply only to the identified version and release of the PP in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the PP by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the PP by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the STCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCEF) under CCCS' supervision. CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned /PP have been performed by TUBİTAK BİLGEM OKTEM, which is a public CCTL.

A Common Criteria Certificate given to a PP means that such PP meets the security requirements defined in its PP document that has been approved by the CCCS. The PP document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the PP should also review the PP document in order to understand any assumptions made in the course of evaluations, the environment where the PP will run, security requirements of the PP and the level of assurance provided by the PP.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for Common Criteria Protection Profile for Smart Meter of Turkish Electricity Advanced Metering Infrastructure (PP version: 1.1) whose evaluation was completed on 30.06.2014 and whose evaluation technical report was drawn up by OKTEM (as CCTL), and with the PP document with version no 1.1.

The certification report, certificate of PP evaluation and PP document are posted on the STCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org.

1 - EXECUTIVE SUMMARY

This report describes the certification results by the certification body on the evaluation results applied with requirements of APE(Protection Profile Evaluation) assurance class of the Common Criteria for Information Security Evaluation in relation to Common Criteria Protection Profile for Smart Meter of Turkish Electricity Advanced Metering Infrastructure (SMTEAMI PP).This report describes the evaluation results and its soundness and conformity.

The evaluation on was conducted Common Criteria Protection Profile for Smart Meter of Turkish Electricity Advanced Metering Infrastructure (SMTEAMI PP) v1.1 by TÜBİTAK-BİLGEM-OKTEM and completed on 30.06.2014.Contents of this report have been prepared on the basis of the contents of the ETR submitted by OKTEM. The evaluation was conducted by applying CEM. This PP satisfies all APE requirements of the CC, therefore the evaluation results were decided to be “suitable”.

The TOE (TOE is the product described in the PP) is the Smart Meter of Turkish Electricity Advanced Metering Infrastructure. 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 system is comprised of three main components : Smart meter, Communication Module, Data and Control Center(DCC)

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.

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 is detected.

2 CERTIFICATION RESULTS

2.1 PP Identification

Project Identifier	TSE-CCCS/PP-004
PP Name and Version	Common Criteria Protection Profile for Smart Meter of Turkish Electricity Advanced Metering Infrastructure (SMTEAMI PP) v1.1
PP Document Title	Common Criteria Protection Profile for Smart Meter of Turkish Electricity Advanced Metering Infrastructure (SMTEAMI PP)
PP Document Version	v1.1
PP Document Date	29.08.2014
Assurance Level	EAL 2+(AVA_VAN.3)
Criteria	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model,CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components,CCMB-2012-09-002, Version 3.1, Revision 4, September 2012 Common Criteria for Information Technology Security Evaluation,Part 3: Security Assurance Requirements,CCMB-2012-09-003,Version 3.1, Revision 4, September 2012
Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology;CCMB-2012-09-004, v3.1 rev4, September 2012
Protection Profile Conformance	None
Common Criteria Conformance	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components,CCMB-2012-09-002, Version 3.1, Revision 4, September 2012,extended Common Criteria for Information Technology Security Evaluation,Part 3: Security Assurance Requirements,CCMB-2012-09-003,Version 3.1, Revision 4, September 2012,Conformant Package Conformant to EAL2 augmented by AVA_VAN.3 as defined in Part 3[3]
Sponsor and Developer	Turkish Standards Institution/Türk Standardları enstitüsü
Evaluation Facility	TÜBİTAK-BİLGEM-OKTEM
Certification Scheme	Turkish Standards Institution Common Criteria Certification Scheme

2.2 Security Policy

The PP includes Organizational Security Policies, Threats and Assumptions. Some notions are explained in the PP document to make more understandable document. These notions are categorized External Entities, Roles, Authorized Manufacturer User, Modes of Smart-Meter and Assets. These notions are described in Table 1.

Table 1:

External Entities	1. **Data and Control Center(DCC):** Smart Meter and the Metering Infrastructure are managed by the operators in DCC.It is the remote management center at Electricity Distribution Company premises which receives User Data, loads configuration parameters, updates firmware and controls the Smart Meter. 2. **Local administrator:** Local Administrator is the user who takes User Data, loads configuration parameters and controls TOE via its Local Interface. 3. **DCC Initialization Agent:** DCC Initialization Agent is the user who works for Electricity Distribution Company and loads initialization parameters to TOE 4. **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. 5. **Smart Meter Developer:** Smart Meter Developer is the entity who develops Smart Meter hardware and firmware. 6. **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. 7. **Consumer:** Consumer is the entity who consumes electricity and pays the bills. Consumer sometimes can act as an attacker. 8. **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.
Roles	1. **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. 2. **Authenticated Local Administrator:**

	Authenticated Local Administrator is the user who takes User Data, loads configuration parameters and controls TOE via its Local Interface. **3. Authenticated DCC Initialization Agent:** Authenticated DCC Initialization Agent is the user who works for Electricity Distribution Company and loads initialization parameters to TOE
Modes of TOE	**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. **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. 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 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	**1. <u>Primary Assets</u>:** **Consumption Index Data:** Consumption Index Data is the amount of electricity consumed over a period. **Detailed Consumption Index 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. **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. **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. **Regular Log:** Regular Logs are kinds of Event Data which give information about Smart

	Meter’s regular operations like metering. **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. **DCC Configuration Parameters:** Any parameters loaded into Meter by DCC. **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. **Smart Meter Manufacture Date:** Date on which the Smart Meter became a product. **Smart Meter Start-up Date:** Date on which Smart Meter started to be used **Manufacturer Code:** It is the unique code of Smart Meter’s manufacturer **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. **2. <u>Secondary Assets:</u>** **Initialization Key:** It is used to initialize TOE in a secure way. It is loaded during manufacturing phase. **Firmware Update Public Key:** It is used to update Smart Meter’s Firmware in a secure way. It is loaded during manufacturing phase. **Local Access Control Root Public Key:** It is used to control access to TOE via its Local Interface. It is loaded during initialization phase. **Smart Meter Time:** It is time of Smart Meter. It is loaded during manufacturing phase and shall be updated during operational phase. **Smart Meter Firmware:** It is the firmware of Smart Meter. It is loaded during manufacturing phase and shall be updated during operational phase. **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. **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.

The PP includes 4 OSPs. These are:

- **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 **Hata! Başvuru kaynağı bulunamadı.**
- **OSP.Crypto_Man:**Generation of cryptographic parameters and loading process shall be performed according to document **Hata! Başvuru kaynağı bulunamadı.**.
- **OSP.Update:** Smart Meter Update Firmware shall be controlled and certified by an authorized Authority. Firmware package shall be prepared as defined in document **Hata! Başvuru kaynağı bulunamadı.**

2.3 Assumptions and Clarification of Scope

This section describes the assumptions must be satisfied by the TOE operational environment, threats satisfied by the TOE and/or operational environment. The PP includes following 6 assumptions:

- **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.

The PP includes following 16 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.

- **Remote Attacker:** Attackers who are away from TOE and have a remote access to TOE non-physically.

- **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 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:**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.

2.4 Architectural Information

Figure 1 represents the general overview of the Turkish Electricity Advanced Metering Infrastructure where TOE is located. The detailed information about TOE environment can be found in the TOE Overview Section of the PP document.

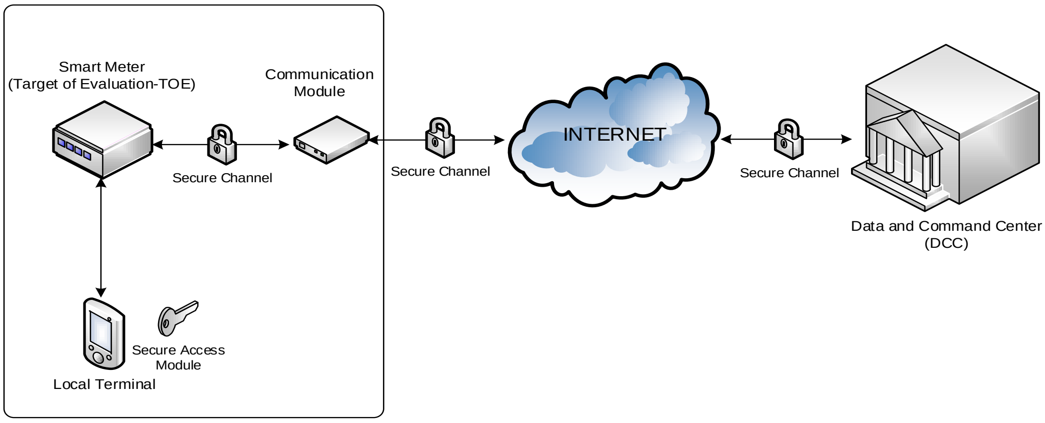

Figure 1 TOE and Its Operational Environment

2.5 Security Functional Requirements

Table 2 describes Security Functional Requirements.

Table 2

Security Functional Class	Security Functional Component
Security Audit (FAU)	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
Communication (FCO)	FCO_NRO.2-Enforced Proof of Origin
Cryptographic Support (FCS)	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
User Data Protection (FDP)	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
Identification and Authentication (FIA)	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
Security Management (FMT)	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
Privacy(FPR)	FPR_CON.1-Communication Concealing
Protection of The TSF (FPT)	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
Trusted Path/Channels (FTP)	FTP_ITC.1-Inter-TSF Trusted Channel

2.6 Security Assurance Requirements

Assurance requirements of Common Criteria Protection Profile for Smart Meter of Turkish Electricity Advanced Metering Infrastructure (SMTEAMI PP) are consistent with assurance components in CC Part 3 and evaluation assurance level is “EAL 2 augmented with AVA_VAN.3”.

2.7 Results of the Evaluation

The evaluation is performed with reference to the CC v3.1 and CEM v3.1.The verdict of Common Criteria Protection Profile for Smart Meter of Turkish Electricity Advanced Metering Infrastructure (SMTEAMI PP) is the pass as it satisfies all requirements of APE (Protection Profile, Evaluation) class of CC. Therefore, the evaluation results were decided to be suitable.

2.8 Evaluator Comments / Recommendations

There are no recommendations concerning the Common Criteria Protection Profile for Smart Meter of Turkish Electricity Advanced Metering Infrastructure (SMTEAMI PP) v1.1.

3 PP DOCUMENT

Information about the Protection Profile document associated with this certification report is as follows:
Name of Document: Common Criteria Protection Profile for Smart Meter of Turkish Electricity Advanced Metering Infrastructure (SMTEAMI PP)
Version No.:1.1
Date of Document:29.08.2013

4 GLOSSARY

CC: Common Criteria
CCMB: Common Criteria Management Board
EAL: Evaluation Assurance Level
Recording Unit
OSP: Organisational Security Policy
PP: Protection Profile
SFR: Security Functional Requirements
TOE: Target of Evaluation
TSF: TOE Security Functionality
TSE: Turkish Standards Institute
DCC: Data and Control Center
DSL: Digital Subscriber Line
EDC: Electricity Distribution Company
GPRS: General Packet Radio Service
TAMIS: Turkish Advanced Infrastructure System

5 BIBLIOGRAPHY

[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, v3.1 rev4, September 2012

[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.

[7] Evaluation Technical Report , DTR 31 TR01– 29.08.2014

[8] YTBD-01-01-TL-01 Certification Report Writing Instructions

6 ANNEXES

There is no additional information which is inappropriate for reference in other sections.