# Certification Report

## EAL 2 Evaluation of

## Ministry of Health

## Common Criteria Protection Profile for Secure Communication Module for Water Tracking System V1.5 (SCM_WTS PP V1.5)

issued by

**Turkish Standards Institution**
**Common Criteria Certification Scheme**

*Certificate Number: TSE-CCCS/PP-009*

## TABLE OF CONTENTS

## *Document Information*

| | |
|---|---|
| ***Date of Issue*** | ***14.10.2015*** |
| ***Version of Report*** | ***1*** |
| ***Author*** | ***İbrahim Halil Kırmızı / Halime Eda Bitlisli*** |
| ***Technical Responsible*** | ***Zümrüt Müftüoğlu*** |
| ***Approved*** | ***Mariye Umay Akkaya*** |
| ***Date Approved*** | ***15.10.2015*** |
| ***Certification Report Number*** | ***21.0.01/15-068*** |
| ***Sponsor and Developer*** | ***Ministry of Health*** |
| ***Evaluation Lab*** | ***TÜBİTAK BİLGEM OKTEM*** |
| ***PP Name*** | ***Common Criteria Protection Profile for Secure Communication Module for Water Tracking System V1.5*** |
| ***Pages*** | ***18*** |

## *Document Change Log*

| ***Release*** | ***Date*** | ***Pages Affected*** | ***Remarks/Change Reference*** |
|---|---|---|---|
| ***V1*** | ***15.10.2015*** | ***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 ITCD 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 (CCTL) 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 TÜBİTAK BİLGEM OKTEM, which is a public/commercial 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. 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 Secure Communication Module for Water Tracking System(PP version: 1.5) whose evaluation was completed on 12.10.2015 and whose evaluation technical report was drawn up by OKTEM (as CCTL), and with the PP document with version no1.5*

*The certification report, certificate of PP evaluation and PP document are posted on the ITCD 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 states the outcome of Common Criteria APE Assurance Class evaluation of Common Criteria Protection Profile for Secure Communication Module for Water Tracking System (SCM_WTS PP).

The evaluation was performed by TÜBİTAK-BİLGEM-OKTEM that is approved Common Criteria Testing Laboratory and was completed in October 2015. OKTEM used Common Criteria for IT Security Evaluation Version 3.1 Revision 4 for evaluation.

The information that provided in this report mainly derived from Evaluation Technical Report (ETR) prepared by OKTEM and Certification Body founded that SCM_WTS PP meets the requirements of all APE work units.

## TOE Description

The Secure Communication Module (TOE) of the Water Tracking System may serve various functionalities like collecting, communication, security and storage. The TOE collects the data of the quality of water in different metrics, such as conductivity of water, pH degree, temperature of water used in carboy cleaning, flow speed of water source, and carboy identification. It stores measurement related data, and provides the security of this data against physical attacks (such as tampering), cryptographic operations and access control functions and generates audit data about TOE’s operational processes.

- Sensing Modules are responsible for measuring water in terms of different metrics and transferring the data to the TOE. These functionalities include conductivity of water, pH degree, carboy cleaning water temperature, water source flow speed.
- TOE is responsible for most of the functionalities excluding the Sensing Module functions defined above. It receives data from different number of Sensing Modules, formats it into in a suitable form of data and stores the data for a while and then transmits the data to the DMC over a secure channel established by TLS. TOE also may receive data from an external ID-reader that reads RFID tags and 2D barcodes to identify the carboy. TOE outputs data in TCP/IP form. TOE is also responsible for generation of audit records of any received and sent data. It has data store capability and real time clock.

Following figure depicts the general overview of the Water Tracking System Infrastructure where TOE is placed.

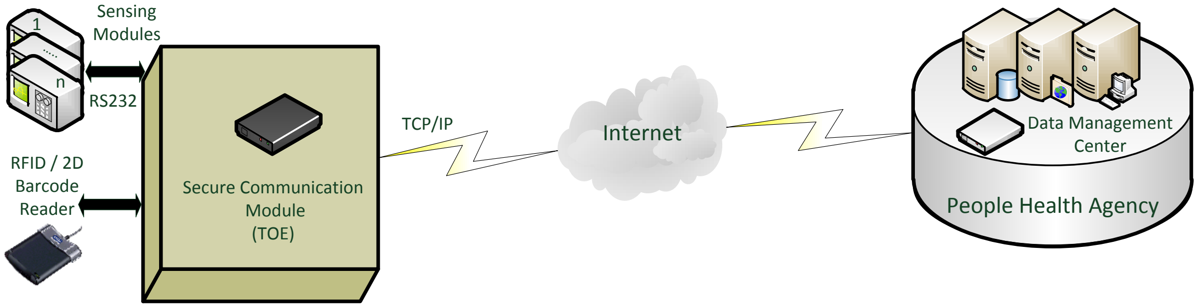

Figure 1 TOE and Its Operational Environment

The major functional features of the TOE are described below:

- TOE receives input data from sensing modules and stores measurement related data.
- TOE provides a Local Interface for reading and configuration operations.
- TOE provides a Remote Interface for communication and configuration operations.
- TOE supports firmware update operation via its Remote and Local Interface.
- The remote interface of TOE sends or receives packets in the form of TCP/IP packet.

The major security features of the TOE are described below:

- TOE implements tamper resistant, tamper evident and tamper respondent mechanisms (Electro-mechanic Seal).
- Sub-modules of TOE which store integrity have mesh cover mechanism to detect any physical attack.
- TOE implements access control mechanisms for both Remote and Local Interfaces.
- TOE supports TLS connections between DMC and TOE.
- TOE provides storage integrity.
- TOE provides self-test functionality for security functions.
- TOE generates audit data and informs users, when any of the security anomalies are detected.

# 2 CERTIFICATION RESULTS

## 2.1 PP Identification

| | |
|---|---|
| *Certificate Number* | TSE-CCCS/PP-009 |
| *PP Name and Version* | Common Criteria Protection Profile for Secure Communication Module for Water Tracking System V1.5 (SCM_WTS PP V1.5) |
| *PP Document Title* | Common Criteria Protection Profile for Secure Communication Module for Water Tracking System |
| *PP Document Version* | V1.5 |
| *PP Document Date* | 12.10.2015 |
| *Assurance Level* | EAL 2 |
| *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<br>Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components,CCMB-2012-09-002, Version 3.1, Revision 4, September 2012<br>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* | CC Part 2 Extended<br>CC Part 3 Conformant |
| *Sponsor and Developer* | Ministry of Health |
| *Evaluation Facility* | TÜBİTAK-BİLGEM-OKTEM |
| *Certification Scheme* | Turkish Standards Institution<br>Common Criteria Certification Scheme |

Table 1 Information for the PP identification

## 2.2 Security Policy

TOE shall comply with the following Organizational Security Policies.

**OSP.PKI:**

The Public Key Infrastructure (PKI) that supply certificate and private key shall be trusted and operate properly.

**OSP.Sym_Key:**

It is ensured that the cryptographic keys are generated securely and the security of the keys is guaranteed in the life cycle.

## *2.3 Assumptions and Clarification of Scope*

This part describes assumptions that must be satisfied by TOE.

**A.Trusted_Entities:**

It is assumed that authorized and authenticated external entities are trustworthy. They do not allow any damage to received data because of carelessness and abuse.

**A.Trusted_Admins:**

It is assumed that the DMC Administrator, the Local Administrator and the Maintenance Agent are trustworthy and well-trained.

During operation by using Local Interface, Local Administrator does not allow eavesdropping and modification between terminal and TOE local port.

**A. Authorized_Firmware:**

It is assumed that TOE firmware is controlled and certified by an authorized authority.

**A. Network:**

It is assumed that network connection with a sufficient reliability and bandwidth for the individual situation is available between TOE-and-DMC or TOE-and-remote Maintenance Agent.

**A. Control:**

It is assumed that DMC controllers perform periodic and random controls on TOE. They check TOE's functional and physical reliability during controls.

**A.Trusted_Manufacturer:**

It is assumed that manufacturing is done by trusted manufacturers.

**A.Trusted_Designer:**

It is assumed that TOE is designed and implemented by trusted designers. They design and implement it maintaining IT security.

**A.Protected_Input_Device:**

It is assumed that TOE receives input data from input devices located in a physically protected environment which is defined in [1].

The PP includes following threats averted by TOE and its environment.

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

- **Local Attacker:** Attackers who have physical access to TOE. They might try to attack TOE by physical tampering. They can also abuse TOE's Local Interface.
- **Remote Attacker:** Attackers who are away from TOE. Remote Attackers try to conquer TOE by cyber-attacks and try to compromise the confidentiality, integrity and authenticity of data when transmitted between TOE-to-DMC or TOE-to-Maintenance Agent that are connected to TOE via remote interface. They also try any attack concepts which does not need physical access to TOE:

**T.Transfer_Modification:**

A remote attacker may try to modify (i.e. alter, delete, insert, replay); Output Data, Event Log Data, TOE IP Access List, and TOE Firmware when transmitted between TOE-to-DMC or TOE-to-remote Maintenance Agent.

Attacker may mislead DMC or Maintenance Agent by any modification. When trying to modify Output Data, attacker may compromise the genuine data to a fake data which creates false information. Attacker may also lead to malfunctions on TOE by modifying; firmware, IP Access List and Clock information during data transfer from DMC to TOE. Attacker may exploit misleading of DMC/remote Maintenance Agent and malfunction of TOE to get advantages for more specific attacks.

**T.Local_Modification:**

A local attacker may try to modify Data Information, Event Information, Fabrication Parameters and TSF Data via local interface of TOE.

Attacker may mislead DMC and Local Administrator by any modification. When trying to modify any data mentioned above, attacker may compromise the genuine data to a fake data which creates false information. Attacker may also lead to malfunctions on TOE by modifying; TOE Firmware, DMC Parameters, Fabrication Parameters, IP Access List and Time. These malfunctions may be used to get advantages for more specific attacks.

**T.Transfer_Disclosure:**

A remote attacker may try to intercept the data transmitted between TOE-to-DMC or TOE-to-remote Maintenance Agent.

When disclosing Output Data between TOE-to-DMC, attacker may try to violate the data privacy of the company. When disclosing the data between TOE-to-remote Maintenance Agent attacker can get some specific information about device functionality.

**T.Local_Disclosure:**

A Local Attacker may try to obtain:

- Output Data
- TOE Private Key, and TLS session Keys.

When Output Data is disclosed, the attacker may try to violate the data privacy of the company.

When TOE Private Key, and TLS session Keys are disclosed, the attacker can by-pass TOE security mechanism for more specific attacks. Also attacker can compromise the genuine data to a fake data which creates false information.

**T.Initialization:**

A local attacker may try to initialize TOE by using his/her own fake keys. When the attacker initializes TOE, he/she may modify and disclose all user/TSF Data during TOE operation.

**T.Physical_Tamper:**

A local attacker may try to reach TOE internal processor and storage memory by physical tampering and manipulation. When these components are reached, attacker may modify and disclose all user/TSF Data.

**T.Counterfeit_Data:**

A remote or local attacker may imitate TOE to respond DMC. Attacker may mislead DMC by sending fake Output Data.

**T.Skimming:**

A remote attacker may imitate DMC to get the Output Data from the TOE. When Output Data is disclosed, attacker may try to violate the privacy of the company. Attacker may modify Access IP List for more specific attacks.

**T.Update:**

A remote or local attacker may try to update TOE Firmware by using a malicious or old version to get advantages for more specific attacks. When the attacker updates TOE, he/she may modify and disclose all user/TSF Data.

**T.Non-Repudiation**

A remote or local authenticated user may try to deny his/her access and the operations performed on the TOE.

**T.Battery_Disable:**

A remote or local attacker may use up internal battery by sending operation requests continuously. If TOE does not have internal battery, tamper detection mechanisms become out of order without line voltage. So, it cannot detect physical tampers. Attackers may chance to modify and disclosure all user/TSF Data by this way.

**T.Abuse_Function:**

An attacker may try to use functions of the TOE which shall not be used in TOE operational phase in order to disclose or manipulate sensitive User Data or TSF Data, manipulate the TOE's software or manipulate (explore, bypass, deactivate or change) security features or functions of the TOE.

**T.Cyber_Attack:**

A remote attacker may try to modify Access Control and Authentication so it's possible that the attacker increase his/her privileges. Event logs are also can be modified. Firewall settings could be changed as well. Attackers may try to modify, disclose and unavailable all assets by this way.

**T.Residual_Data:**

There might be critical parameters in terms of confidentiality on TOE which became out of order. Attackers may perform attacks on User/TSF Data by using this information.

**Security Objectives for the TOE**

**O.Access_Control:**

The TOE shall control restriction of access to functions and data.

**O.Event:**

TOE shall record important events about security problem and device configuration as listed in **Hata! Başvuru kaynağı bulunamadı.**.

**O.Storage_Integrity:**

TOE shall provide integrity check of the data which is stored in the internal memory.

**O.Authentication:**

TOE shall authenticate connected entities (users and systems). It shall provide authentication verification and MAC addition.

**O.Transfer:**

TOE shall provide encryption and integrity protection for transfer operation between TOE-to-DMC or TOE-to-remote Maintenance Agent.

**O.Protect:**

TOE shall have self-test mechanism to control security functions in case of malfunction. TOE shall also delete information which is not necessary for future operations.

**O.Physical_Tamper**

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

**O.Battery_Control**

TOE shall control battery level and respond under a definite level. TOE shall interpret as an attack and enter Maintenance mode under a more critical level.

**O.Abuse_Function:**

The TOE shall prevent the functions of the TOE which shall not be used in TOE operational phase.

**O.Update:**

TOE shall only accept controlled, authenticated and signed firmware by the authority. TOE shall control firmware version and accept only more recent version.

**O.Separate_IF:**

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

**O.Firewall:**

TOE accepts interaction only definite IP numbers which are appointed before.

**Security Objectives for the Operational Environment**

**OE.Trusted_Entities:**

Authorized and authenticated external entities should be trustworthy. They do not let any damage to data that they receive because of carelessness and abuse.

**OE.Trusted_Admin:**

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

**OE.Upgrade_Software:**

TOE firmware shall be controlled and certified by an authorized entity.

**OE.Network:**

A network connection with a sufficient reliability and bandwidth shall be available between TOE-and-DMC or TOE-and-remote Maintenance Agent.

**OE.Keyman:**

Generation and transportation of cryptographic parameters shall be secure.

**OE.Development:**

Developers shall ensure that they design and implement TOE, maintain IT security during development. They also do not introduce any security hole intentionally.

**OE.Manufacturing:**

Manufacturer should ensure that TOE is manufactured maintaining IT security. They also do not introduce any security hole intentionally.

**OE.Control:**

DMC controllers should perform periodic and random controls on TOE. They check TOE's functional and physical reliability during controls.

**OE.Physical_Security:**

The physical security of sensing modules and TOE shall be satisfied by the structure defined in [1].

## *2.4 Architectural Information*

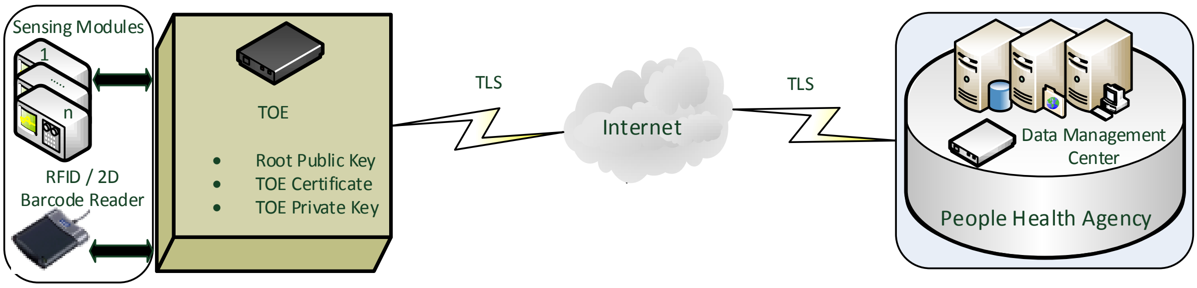

Figure 2 Sensing Module - TOE - DMC Communication Scenario

### 2.5 Security Functional Requirements

Following table describes the Security Functional Requirements of the TOE

| 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 - Encryption/Decryption |
| FCS_COP.1/INT-AUTH | Cryptographic operation - Integrity/Authenticity |
| FCS_COP.1/SIGN-VER | Cryptographic operation - signature verification |
| FCS_COP.1/TLS | Cryptographic operation -TLS |
| FCS_CKM.1/TLS_AES | Cryptographic AES key generation for TLS |
| FCS_CKM.1/TLS_HMAC | Cryptographic HMAC key generation for TLS |
| FCS_CKM.4 | Cryptographic key destruction |
| 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_RIP.1 | Subset residual information protection |
| 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/IP_LIST | Management of TSF Data - IP Access List |
| FMT_MTD.1/SECRET_READ | Management of TSF Data - Secret Read |
| FMT_MTD.1/FIRMWARE | Management of TSF Data Secure Communication Module Firmware |
| FMT_MSA.1 | Management of security attributes for Secure Communication Module Access Control SFP |

| | |
|---|---|
| FMT_MSA.3 | Static attribute initialization for Secure Communication Module access SFP |
| 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_TDC.1 | Inter-TSF basic TSF Data consistency |
| FTP: Trusted Path/Channel | |
| FTP_ITC.1 | Inter-TSF trusted channel for DMC |

Table 2 List of SFRs

### *2.6 Security Assurance Requirements*

Assurance requirements of Common Criteria Protection Profile for Secure Communication Module for Water Tracking Systemv1.5 (SCM_WTS v1.5) are consistent with assurance components in CC Part 3 and evaluation assurance level is “EAL 2”.

### *2.7 Results of the Evaluation*

The evaluation was conducted based upon the assurance activities specified in Common Criteria Protection Profile for Secure Communication Module for Water Tracking System v1.5, in conjunction with version 3.1, revision 4 of CC and CEM. The evaluation team’s assessment of evidence provided by OKTEM is that it satisfies all requirements of APE class of CC. Therefore, final verdict on APE is pass.

### *2.8 Evaluator Comments / Recommendations*

There are no recommendations concerning the Common Criteria Protection Profile for Secure Communication Module for Water Tracking Systemv1.5 (SCM_WTS v1.5).

## 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 Secure Communication Module for Water Tracking System (SCM_WTS)

**Version:** v1.5

**Date of Document:** 12.10.2015

## 4 GLOSSARY

| | |
|---|---|
| AES | : Advanced Encryption Standard |
| CC | : Common Criteria |
| CCMB | : Common Criteria Management Board |
| DMC | : Data Management Center |
| EAL | : Evaluation Assurance Level (defined in CC) |
| OSP | : Organizational Security Policy |
| PP | : Protection Profile |
| PKI | : Public Key Infrastructure |
| SFR | : Security Functional Requirements |
| TLS - CA | : Transport Layer Security - Client Authentication |
| TOE | : Target of Evaluation |
| TSF | : TOE Security Functionality (defined in CC) |
| TSE | : Turkish Standards Institute |
| WTS | : Water Tracking System |

## 5 BIBLIOGRAPHY

[1]Damacana Takip Sistemi Projesi Korumalı Sensör Birimi Sistem Gerekleri Dokümanı, Version 1.0.

## 6 ANNEXES

Not applicable.