COMMON CRITERIA PROTECTION PROFILE

for

SECURE COMMUNICATION MODULE FOR

WATER TRACKING SYSTEM

(SCM-WTS PP)

Revision No	1.5
Revision Date	12.10.2015
Document Code	
File Name	SCM-WTS PROTECTION PROFILE
Prepared by	Muhammed Ali BİNGÖL, Süleyman KARDAŞ and Ünal KOCABAŞ
Approved by	

Revision History

Revision No	Revision Reason	Date of Revision
1.0	First Version	05.03.2014
1.1	Threat Update	11.07.2014
1.2	"SCM_WTS_GözlemRaporu_1" "SCM_WTS_GözlemRaporu_2" update	09.06.2015
1.3	"SCM-WTS_GK_01" update	28.08.2015
1.4	"SCM_WTS_PP_GözlemKararı_2" update	08.09.2015
1.5	"SCM_WTS GK3" update	12.10.2015

İçindekiler

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 Secure Communication Module for Water Tracking System
Sponsor	: Ministry of Health – People Health Agency of Turkey
Editor(s)	: Prepared by Muhammed Ali BİNGÖL, Süleyman KARDAŞ and Ünal KOCABAŞ
CC Version	: 3.1 (Revision 4)
Publication Date	**:**12.10.2015
Assurance Level	: The assurance level for this PP is EAL 2.
General Status	: Draft
Version Number	: 1.5
Key words	:Water Tracking System, Secure Communication Module, Protection Profile, 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 Secure Communication Module for Water Tracking System (WTS). The TOE collects information from input devices such as pH sensor, conductivity sensor, temperature sensor, flow meter, RFID / 2D barcode reader, etc., and then it sends these collected data to the Data Management Center (DMC).

In this section, first the overall Water Tracking System is introduced. Then, details of Secure Communication Module (TOE) are given. Afterwards the components of TOE, the cryptographic operations performed by TOE and the capabilities of TOE are introduced.

1.2.2 General Overview of Water Tracking System Infrastructure

Figure 1 depicts the general overview of the Water Tracking System Infrastructure where TOE is placed. As seen in the figure, the system is simply composed of two main components.

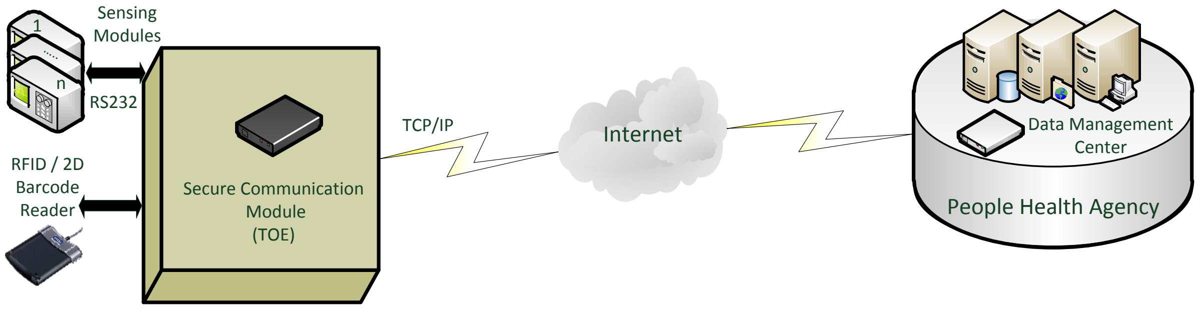


Figure 1 TOE and Its Operational Environment

Secure Communication Module is a component of the Water Tracking System (WTS). It is responsible for collecting some measurement values of water with different metrics (pH, conductivity, temperature, flow speed, RFID / 2D barcode reader). First of all, it collects and stores these values in TOE. Then, it transfers the data related to these measurements via TCP/IP.

Data Management Center (DMC) is the remote management center which receives water quality measurements, saves quantity of the production, loads configuration parameters, updates firmware and controls the SCM.

Secure communication Module is managed by the operators in DMC. In addition to this, there are also some operations, which are performed by using Local Interface of the TOE.

The system can perform different processes after receiving the quality/quantity data. But they are not in the scope of this Protection Profile.

1.2.3 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 (as defined in Section 1.2.7.2). 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.

<u>The major functional features of the TOE are described below:</u>

- 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.

<u>The major security features of the TOE are described below.</u>

- 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 detailed in Section 6.1.1 are detected.

1.2.4 TOE Type

The TOE comprises of hardware and firmware parts that provide collecting, communication, storage and security functionalities.

1.2.5 Logical and Physical Interfaces of TOE

TOE has two logical interfaces:

- **Remote Interface** for DMC or remote maintenance operations
- **Local Interface** for local operations

TOE has the physical interfaces below:

- **Remote Interface port** is used to connect to DMC or remote Maintenance Agent. A TOE can send or receive data over TCP/IP.
- **Possible TOE Design**

This Protection Profile does not imply a concrete physical architecture. However the expected configuration is that external Sensing Modules and external ID-readers are connected to the TOE.

Within this configuration;

- Sensing Modules are measuring the parameters about water quality and identity.
- TOE shall provide security and functional requirements listed in Section 1.2.3 and TLS related requirements as given in 1.2.7.2.

1.2.6 TOE Life Cycle

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

- Development
- Manufacturing
- Initialization
- Operation
- Maintenance

This Protection Profile focuses on Initialization, Operation and Maintenance phases. It has to be ensured that previous phases are performed by trusted personnel in secure environments. For the maintenance phase, manufacturer shall develop the TOE and maintenance tools so that TOE can be repaired properly within the guarantee period which is not in the scope of this protection profile. In this protection profile only the access control mechanism for local and remote maintenance agent is defined. The TOE manufacturer loads necessary cryptographic parameters and terminates the manufacturing phase before TOE is delivered to DMC as detailed in 1.2.7.

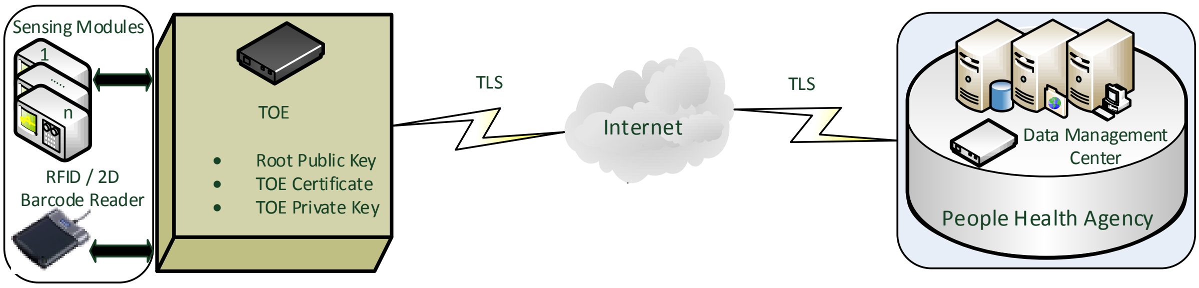


Figure 2 Sensing Module - TOE - DMC Communication Scenario

1.2.7 Major Cryptographic Functionalities of TOE

1.2.7.1 Authentication Mechanism for Local Interface

TOE should provide an access control mechanism for accesses from its Local Interface depending on the Role Attribute which is specified within the certificate of the entity.

<u>Preconditions for local access control are as follows:</u>

- Local user has a terminal which is compatible with TOE's Local interface (i.e., Serial Bus).
- Local user has a hardware token which includes local authentication private key and public key pair (certificate). The public key is issued by Root Public Key (see Table 3).
- Local user knows the PIN used to protect the Token.

Role Attribute: Role Attribute is an attribute field on certificate indicates the role of accessing the Local Interface. There are three types of roles and these are "Initialization Agent", "Maintenance Agent" and "Local Administrator".

<u>**Initialization Agent** Authentication Process is specified as follows:</u>

- The terminal is connected to TOE (via local interface).

- Token is plugged to the terminal.
- User enters token PIN via terminal.
- Token verifies the PIN.
- If verification is successful, Token sends its certificate to TOE via terminal.
- TOE verifies the Token's certificate using the Root Public Key.
- If verification is successful, TOE sends a random number to the Token.
- Token signs the random number and sends it to TOE.
- TOE verifies the signature. If the signature is verified then it reads the "Role Attribute" on the Token's certificate. If TOE reads **"Initialization Agent"** then authentication process is completed and Initialization Mode is available.

Maintenance Agent Authentication Process is specified as follows:

- The terminal is connected to TOE (via local or remote interface).
- Token is plugged to the terminal.
- Agent enters token PIN via terminal.
- Token verifies the PIN.
- If verification is successful, Token sends its certificate to TOE via terminal.
- TOE verifies the Token's certificate using the Root Public Key.
- If verification is successful, TOE sends a random number to the Token.
- Token signs the random number and sends it to TOE.
- TOE verifies the signature. If the signature is verified then it reads the "Role Attribute" on the Token's certificate. If TOE reads **"Maintenance Agent"** then authentication process is completed and Maintenance Mode is available.
- If the maintenance agent is connected via remote interface than a TLS connection shall be established as defined in 1.2.7.2. Messages exchanged via TLS tunnel.

Local Administrator Authentication Process is specified as follows:

- The terminal is connected to the Serial Port.
- Token is plugged to the terminal.
- User enters token PIN via terminal.
- Token verifies the PIN.
- If verification is successful, Token sends its certificate to TOE via terminal.

- TOE verifies the Token's certificate using the Root Public Key.
- If verification is successful, TOE sends a random number to the Token.
- Token signs the random number and sends it to TOE.
- TOE verifies the signature. If the signature is verified then it reads the "Role Attribute" on the Token's certificate. If TOE reads **"Local Administrator"** then authentication process is completed and Local Administrator access is available.

1.2.7.2 TLS Mechanism for Remote Interface

This mechanism provides a secure channel between TOE and DMC or between TOE and remote Maintenance Agent.

<u>Preconditions in manufacturing phase are as follows:</u>

- TOE Certificate which includes TLS Authentication Public Key and TOE Private Key, shall be loaded in manufacturing phase.
- Root Public Key which verifies the certificates of DMC shall be loaded in manufacturing phase.

<u>TLS features are specified as follows:</u>

- Only TLS version 1.2 (or latest upgraded version)shall be supported explained in RFC 5246 [5]
- Supported algorithm suite shall be ***TLS_DHE_RSA_WITH_AES256_CBC_SHA256*** or ***TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA***.
- Server certificates format shall be X.509.
- Session Resumption shall not be supported.
- Session Renegotiation shall not be supported.
- Both client and server authentication shall be used.
- Maximum session timeout value shall be 24 hours. TLS session shall be reestablished after lifetime is up.

<u>TLS mechanism is implemented as follows:</u>

- Handshake protocol is depicted in Figure 3.
- In Figure 3, both client and server use 12 handshake messages to establish the encrypted channel prior to message exchanging.
- *Client* sends **ClientHello** message proposing TLS options.
- *Server* responds with **ServerHello** message selecting the TLS options.

- *Server* sends **Certificate** message, which contains the server's certificate.
- *Server* requests client's certificate in **CertificateRequest** message, so that the connection can be mutually authenticated.
- *Server* concludes its part of the negotiation with **ServerHelloDone** message.
- *Client* responds with **Certificate** message, which contains the client's certificate.
- *Client* sends session key information (encrypted with server's public key) in **ClientKeyExchange** message.
- *Client* sends a **CertificateVerify** message to let the server know it owns the sent certificate.
- *Client* sends **ChangeCipherSpec** message to activate the negotiated options for all future messages it will send.
- *Client* sends **Finished** message to let the server check the newly activated options.
- *Server* sends **ChangeCipherSpec** message to activate the negotiated options for all future messages it will send.
- *Server* sends **Finished** message to let the client check the newly activated options.
- After handshake operation two party share any data over TLS secure channel. (Two party starts to communicate over secure TLS channels after handshaking.)

Application Note 1: Here TOE plays as client and DMC or remote Maintenance Agent as server.

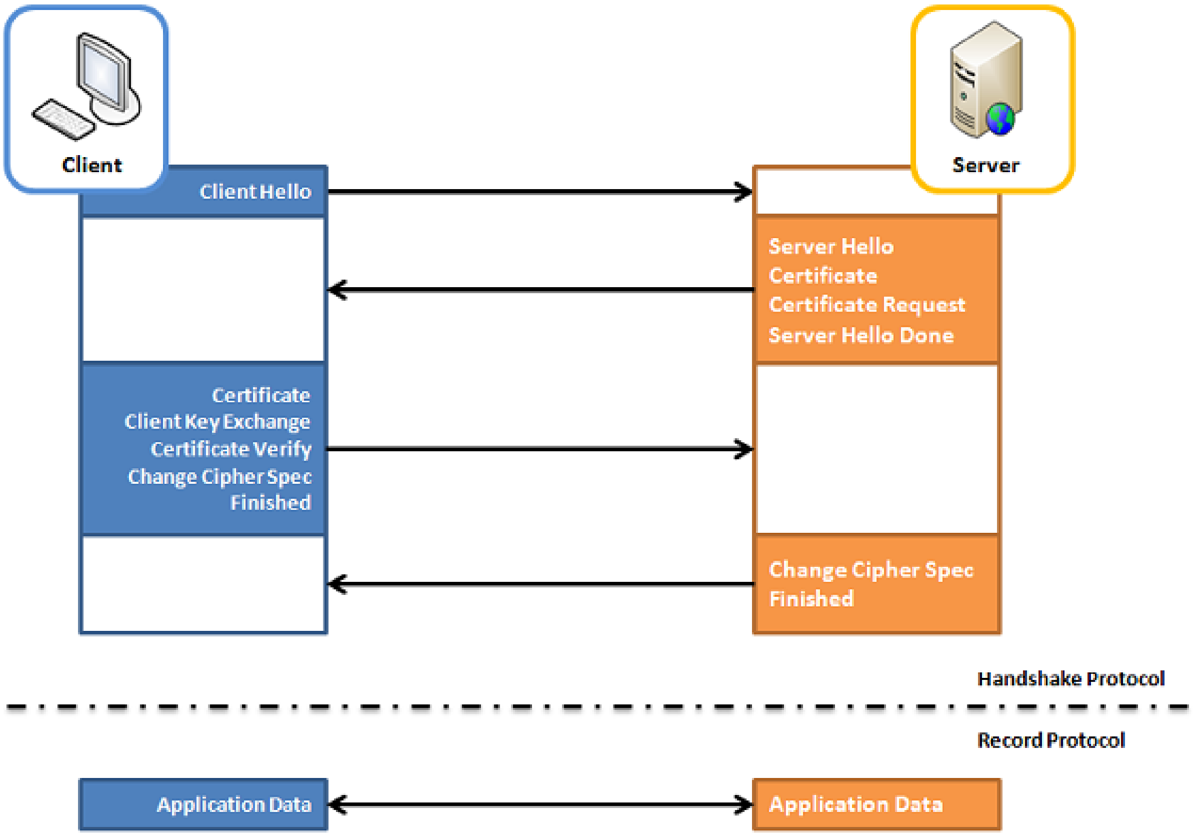


Figure 3 Mutual TLS Authentication Handshake Protocol

1.2.7.3 *Sensors and RFID/ 2D Barcode devices to TOE Communication*

TOE gets input data from Input Devices (Sensors and RFID/ 2D Barcode) devices without any cryptographic operation.

1.2.7.4 *TOE Firmware Update*

Firmware update of the TOE shall be performed via Remote and Local Interface by Authenticated DMC or Authenticated Local Administrator or Authenticated Maintenance Agent. Firmware Update Public Key shall be loaded into TOE during manufacturing process. Firmware update control mechanisms are applied as follows:

- Firmware Update Authority controls (tests) and signs the firmware with his Private Key. Firmware Update Authority ensures that the firmware version is upgraded.
- TOE verifies the signature by using the Firmware Update Public Key. TOE updates the firmware if the signature verification holds and the version of the new firmware is greater than the current version.

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.
- Part 3 conformant.

The

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

has to be taken into account.

2.2 PP Claim

This PP does not claim conformance to any protection profile.

2.3 Package Claim

The current PP is conformant to the following security requirements package:

- Assurance package EAL2 conformant to CC, part 3.

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 TOE. 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
DMC	Authenticated DMC	Authenticated DMC is the remote center which takes water quality data, loads configuration parameters, updates firmware and controls Water Tracking System via Remote Interface.
Local Administrator	Authenticated Local Administrator	Authenticated local administrator who can access User Data (see Table 2), configure parameters via its Local Interface.
Initialization Agent	Authenticated Initialization Agent	Initialization Agent is the authority who authorized by People Health Agency and loads initialization/configuration parameters and keys to the TOE.
Maintenance Agent	Authenticated Maintenance Agent	Maintenance Agent is the authority who authorized by People Health Agency and performs maintenance processes. Maintenance Agent can either connected to TOE via local interface (local Maintenance Agent) or via remote interface (remote Maintenance Agent).
Firmware Update Authority	-	Firmware Update Authority is the agent who authorized by People Health Agency. This authority is responsible for testing the firmware and signing the verified firmware.
DMC Controller	-	DMC Controller works for People Health Agency and performs random and periodic control on Water Tracking System and checks TOE's functional and physical reliability.
TOE Developer	-	TOE Developer is the entity who develops TOE

		hardware and software.
TOE Manufacturer	-	TOE Manufacturer is the entity who manufactures TOE. Usually, TOE Manufacturer might be the same as TOE developer.
Water Producer Company	-	Water Producer Company (or Company) is the entity that produces water with carboy.
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 Water Tracking System.

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 Initialization Agent.

3.1.2.2 Operational Mode

Operational mode is the normal-expected mode of TOE. TOE collects input data and sends output data. Input Data is the data collected from different Input Devices (such as Sensors and RFID/ 2D Barcode devices) over a period of time. Input Device ID is a unique number identifying the input device connected to the TOE. It includes the location information, type of process binding the source information to a specific address.

TOE receives input data either from sensing modules and/or RFID/2D Barcode Reader. TOE verifies the received Input Data and prepares an Output Data such that

Output = Input Data || time.

TOE performs cryptographic operations on Output Data using TLS (or latest upgraded version) session keys and sends it either to DMC.

An indicator is shown on TOE stating that TOE works in normal operational mode without any problems (e.g., green light etc.).

3.2 *Maintenance Mode*

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

1. Opening and enforcement of electromechanical seal,

2. Mesh cover monitoring check failures (Mesh cover is an electromechanical structure that covers and protects User Data and TSF Data),
3. Low battery detection below %10,
4. Detection of environmental stress for five (5) times,
5. Integrity check failures of User Data and TSF Data for ten (10) successive times,
6. Insufficient entropy during random number generation for ten (10) times,
7. Failure detection by periodic self-test functions for five (5) times,
8. Error detection during processing cryptographic operations for five (5) times,
9. Unsuccessful software update detection for five (5) times,
10. Detection of unsuccessful authentication attempt via local interface for five (5) times,
11. Detection of the fullness of system log memory.

If TOE enters Maintenance Mode because of one of the first three conditions above, the following operations are done:

- Cryptographic Keys (TLS session Keys) are deleted,
- Input Data collection is stopped,
- A High Critical Security Log is generated,
- An indicator is shown on TOE stating that TOE entered a high critical state (eg. A red lamb etc.).

If TOE enters Maintenance Mode because of the other reasons, the following operations are done:

- Operational Mode activities go on if possible,
- A High Critical Security Log is generated and sent to DMC automatically
- An indicator is shown on TOE stating that TOE entered a medium critical state.

3.2.1 Assets

In the following tables, The User Data and the TSF Data on TOE are described. Additionally, their protection needs in terms of confidentially, integrity and authenticity are marked. Mark “X” and color “red” show that the asset needs protection. Color “orange” shows that, the protection need is less critical.

Table 2 TOE User Data and Protection Need

Asset		Description	Need for Protection		
			Conf.	Int.	Auth.
Data Information	Input Data Collection Time	It represents the exact date and time that an Input Data is received from an Input Device. This time is generated by TOE Clock.	-	X	-
	Output Data	Output data is the collection of Input Data that is packaged by TOE over a specific period of time. Output data includes Input Data received by input devices Input Data Collection Time and Input Device ID.	X	X	X
Event Information	Security Log	Security Logs are produced when security problems are detected. These logs are sent to DMC as soon as they are appeared and are available to local and remote users. • High critical security logs show that TOE 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 security problem. These logs are kept with the log generation time.	-	X	-
	System Log	System Logs are kinds of Event Information which show TOE configuration and update operations. They are produced during any update and load operation. These logs are kept with the log generation time.	-	X	-

	Regular Log	Regular logs are kinds of Event Information which show connection establish, event data read and output data generated. These logs are kept with the log generation time.			
Fabrication Parameters	Serial Number	Serial Number is a unique ID of TOE that is given by Manufacturer. Different Manufacturers may give the same serial number to their product. Therefore, Serial Number and Manufacturer Code are combined to form a unique Communication Module ID.	-	X	-
	Manufacturer Code	It is the unique code of TOE manufacturer.	-	X	-

Table 3 TOE TSF Data and Protection Need

Asset	Description	Need for Protection		
		Conf.	Int.	Auth.
Root Public Key	Root Public Key is used to verify the certificates of DMC. It is loaded during manufacturing phase and cannot be updated.	-	X	-
TOE Certificate	This certificate is owned by TOE that is used to establish a TLS channel between TOE and DMC. It is loaded during manufacturing phase.	-	X	X
TOE Private Key	This private key is owned by TOE that is used to establish a TLS channel between TOE and DMC. It is loaded during manufacturing phase. This key should be confidential and cannot be changed.	X	X	-

TLS session Keys	They are generated during the establishment of TLS sessions and deleted when the session terminates. They are used for TLS encryption/ decryption and MAC computations.	X	X	X
TOE Access IP List	It is a list of IP addresses which includes the DMC’s IP and/or other communication module(s) that the TOE can be communicate. An entity can communicate with TOE, if and only if it is configured according to those IP parameters. IP Access List is loaded in maintenance phase and can be updated via access control.	-	X	X
Firmware Update Public Key	It is used to update TOE’s Firmware in a secure way. This key is loaded during manufacturing phase. New Firmware is signed using corresponding private key of Firmware Update Authority.	-	X	X
Firmware Version	It is used during Firmware update procedure. An update is allowed if the new Firmware Version is greater than the current Firmware Version.	-	X	-
TOE Clock	It is clock of TOE. It is set during manufacturing phase and shall be updated during operational phase.	-	X	X
TOE Firmware	It is firmware of TOE. It is loaded during manufacturing phase and shall be updated during Operational or Maintenance Phase via Remote or Local Access.	-	X	X

Application Note 2: The expression "Device Information Data" might also be used when Threats and SFRs are being described. It includes any data that give information about TOE and its configuration like Fabrication Parameters, DMC Parameters and Configurations, TOE Time and IP Access List.

3.3 Threats

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.

3.4 OSPs

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.

3.5 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 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 [6].

4 OBJECTIVES

4.1 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 Table 6.

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.

4.2 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 [6].

4.3 Security Objective Rationale

Table 4 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 4 Security Objective Rationale

	O.Access_Control	O.Event	O.Storage_Integrity	O.Authentication	O.Transfer	O.Protect	O.Physcal_Tamper	O.Battery_Control	O.Abuse_Function	O.Update	O.Separate_IF	O.Firewall	OE.Trusted_Entities	OE Trusted_Admin	OE.Upgrade_Software	OE.Network	OE.Keyman	OE.Development	OE.Manufacturing	OE.Control	OE.Physical_Security
T.Transfer_Modification					X																
T.Local_Modification	X	X	X	X		X															
T. Transfer_Disclosure					X																
T.Local_Disclosure	X	X		X																	
T.Initialization	X			X													X				
T.Physical_Tamper		X					X														
T.Counterfeit_Data				X																	
T.Skimming	X			X																	
T.Update	X	X		X						X					X						
T.Battery_Disable		X						X													
T.Abuse_Function									X												
T.Cyber_Attack	X	X		X							X	X									
T.Residual_Data						X															
T.Non Repudation		X																			
OSP.PKI																	X				
OSP.Sym_Key																	X				
A.Trusted_Entities													X								X
A.Trusted_Admins														X							
A.Authorized_Firmware															X						
A.Network																X					
A. Control																				X	
A.Trusted_Manufacturer																			X		
A.Trusted_Designer																		X			
A.Protected_Input_Device																					X

Justification about Table 4 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 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. Initialization is addressed by O.Access_Control O.Authentication and OE.KeyMan.

O.Access_Control ensures that only permitted user may perform TOE Initialization,

O.Authentication to ensure the origin of external entity.

OE.KeyMan 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.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.Event, O.Authentication, O.Update and OE.Upgrade_Software.

O.Access_Control ensures that only permitted user may perform firmware update.

O.Event provides audit record for 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.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.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, O.Firewall 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.

O.Firewall provides protect against cyber attack.

T.Residual_Data is addressed by O.Protect.

It defines that the TOE provides self-test mechanism to ensure the correct operation of critical parameters.

T.Non Repudation is adressed by O.Event.

OSP.PKI and OSP.Sym_Key is directly and completely covered by the security objective OE.Keyman

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.Authorized_Firmware is directly and completely covered by the security objective OE. OE.Development.Update

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

A.Protected_Input_Device is directly and completely covered by the security objective OE.Physical Security.

5 EXTENDED COMPONENTS DEFINITION

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

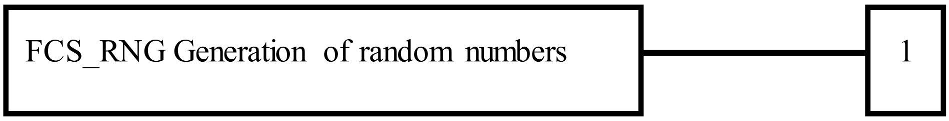
5.1 Definition of the Family FCS_RNG

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*].

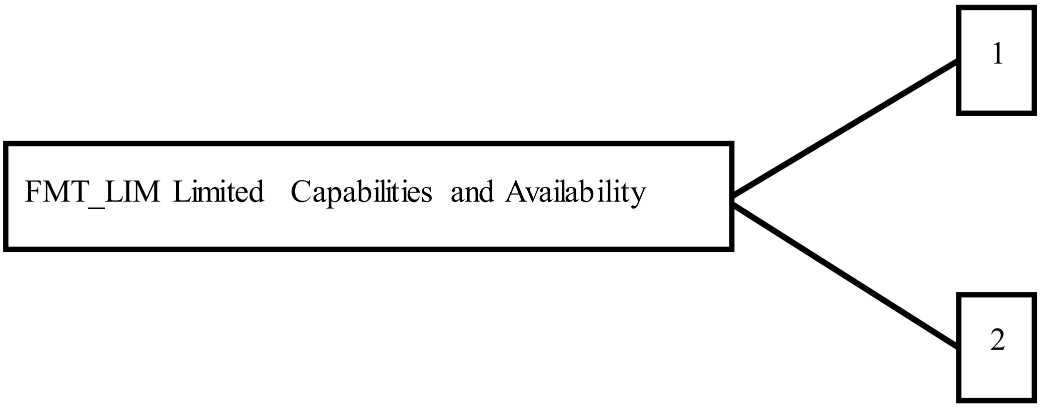
5.2 Definition of the Family FMT_LIM

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 require 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*].

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 2 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 (SFR) of this PP:

Table 5 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 - 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

6.1.1 Class FAU Security Audit

Table 6 List of Logs

Security Log		**Regular Log**	**System Log**
High Critical	**Low Critical**		
• Electro-mechanic seal is opened or forced • Mesh cover monitoring check failed • 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	• Low battery level under %30 detected • DMC connection problem is detected • Absent of line voltage is detected • Low critical log memory fullness detected more than %60	• Connection established via DMC • Connection established via Local Administrator (logs with ID of Local Administrator) • Connection established via Maintenance Agent (logs with ID of	• Date/Time adjusted • DMC Configuration done • TOE Firmware updated successfully • IP Access List changed

Security Log		Regular Log	System Log
High Critical	Low Critical		
self-test function. - Errors detected during processing cryptographic operations, - Unsuccessful software update detected - Unsuccessful authentication attempt detected from local interface - System log memory fullness detected	- Low critical log memory fullness detected more than %80 - System log memory fullness detected more than %60 - System log memory fullness detected more than %80	Maintenance Agent) - Connection established via Initialization Agent (logs with ID of Initialization Agent) - Output Data has been generated - Event Data has been read	
- Save at least 100 logs. When the memory is full, Enter maintenance mode	- Save at least 50 logs - When the memory is full, override oldest data		- Guarantee memory for all TOE life - When the memory is full enter Maintenance mode

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~~ [enter TOE Maintenance mode (as detailed in 3.2)] 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 6].

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 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 6] known to indicate a potential security violation;

b) [Low Critical Security Log listed in Table 6 shows that there might be a security violation].

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 Authenticated DMC operators and local administrator] with the capability to read [all Event Log 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 Maintenance mode (as detailed in 3.2)] 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 3: 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 4: 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 Maintenance mode (as detailed in 3.2)] 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 DMC] 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 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 in CBC mode] and cryptographic key sizes [256 bit] that meet the following: [FIPS 197, NIST SP 800-38A].

Application Note 5: This operation is used for TLS Enc/Dec.

FCS_COP.1/INT-AUTH Cryptographic 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].

Application Note 6: This operation is used for HMAC generation/verification operations in TLS and Local Storage Integrity.

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 generation/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 only for TLS, Local Interface Access control and Firmware Update verification.

FCS_COP.1/TLS Cryptographic operation for TLS

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 [TLS authentication, encryption, decryption] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application Note 8: The TOE shall only use cryptographic specifications and algorithms (CipherSuite *TLS_DHE_RSA_WITH_AES_256_CBC_SHA256* or *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA*) as described in Section 1.2.7.2 (see [5]).

6.1.3.2 FCS_CKM Cryptographic Key Management

FCS_CKM.1/TLS_AES Cryptographic AES key generation for TLS

Hierarchical to: -

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [TLS v1.2 DHE_RSA or ECDHE_ECDSA] and specified cryptographic key sizes [256 bit] that meet the following: [RFC 5246, RFC 4492].

FCS_CKM.1/TLS_HMAC Cryptographic HMAC key generation for TLS

Hierarchical to: -

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [TLS v1.2 DHE_RSA or ECDHE_ECDSA] and specified cryptographic key sizes [256 bit] that meet the following: [RFC 5246, RFC 4492].

FCS_CKM .4 Cryptographic Key Destruction

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.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [none].

Application Note 9: Key destruction process is applied for TLS Enc/Dec and HMAC session keys.

6.1.3.3 FCS_RNG Generation of random numbers

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 [Secure Communication Module Access Control SFP] on [

Subjects:

- Authenticated DMC
- Authenticated Local Administrator
- Authenticated Initialization Agent
- Authenticated Maintenance Agent

Objects:

- User data stored in Secure Communication Module
    - Data Information

    - Output Data
        - Event Information
        - Fabrication Parameters
- TSF Data
    - Root Public Key
    - TOE Certificate
    - TOE Private Key
    - TLS session Keys
    - TOE Access IP List
    - Firmware Update Public Key
    - Firmware Version
    - TOE Clock
    - TOE Firmware
- 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 [Secure Communication Module Access Control SFP] to objects based on following :[

Subjects:

- Authenticated Initialization Agent
- Authenticated DMC
- Authenticated Local Administrator
- Authenticated Maintenance Agent

- Subject Attributes:

- User Identity,
- Authentication Status,

- TOE Interface,
- IP Access List,

Objects:

- User data stored in Secure Communication Module
    - Data Information
        - Output Data
    - Event Information
    - Fabrication Parameters
- TSF Data (as detailed in FDP_ACC.1.1)

Object Attributes:

- Access Control List,
- Object ID,
- Input Data Collection Time,
- Command freshness,
- Firmware signature (for Secure Communication Module Firmware update),
- Firmware version (for Secure Communication Module 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 Initialization Agent is only allowed to write initialization/configuration parameters via Local Interface.
- an Authenticated DMC is allowed to read access User Data (Output Data, Event Information, Fabrication Parameters), to read/write IP Access List, to set TOE Clock via Remote Interface. Also TOE Firmware can be updated via Remote Interface. DMC's IP is specifically defined in TOE Access IP List.

- an Authenticated Local Administrator is allowed read User Data (Data Information, Event Information and Fabrication Parameters), read/write/modify IP Access List, set TOE Clock and perform Firmware Update via Local Interface.
- Authenticated Maintenance Agent is allowed to read User Data (Data Information, Event Information and Fabrication Parameters), via Local Interface after TOE enters into Maintenance Mode. Also Authenticated Maintenance Agent is allowed to read/write/modify Input Device ID, IP Access List, set TOE Clock and performs Firmware Update via Local or Remote Interfaces.
- TOE accepts write and modification operation for TOE Clock and IP Access List via Remote Interface only if {
  - sender: an Authenticated DMC or Maintenance Agent and has an IP from IP Access List
  - Command freshness=successful (not replayed)
  - MAC control: successful

  }
- TOE accepts Secure Communication Module Firmware update operation via Remote Interface only if {
  - Sender: an Authenticated DMC or Maintenance Agent has an IP from IP Access List
  - Command freshness=successful (not replayed)
  - MAC control: successful
  - Firmware signature control: successful
  - Firmware version: recent}

  ].

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
  - Output Data
  - Event Information
  - Fabrication Parameters
  - TSF Data excluding TOE Clock, IP Access List and TOE Firmware.
- nobody shall be allowed to have read access TSF Data except TOE Clock and IP Access List, Firmware Version].

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 [Secure Communication Module Information Flow Control SFP] on [TOE, Sensing Modules, RFID/ 2D Barcode Readers, DMC, Local User 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 [Secure Communication Module Information Flow Control SFP] based on the following types of subject and information security attributes: [

subjects: The TOE and external entities on DMC or local side information: any information that is sent to, from or via the TOE

security attributes: destination interface, source interface, destination authentication status (Initialization Agent authentication status, Maintenance Agent 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: [

- DMC connection establishment is allowed, if
  - source interface=TOE/DMC and destination interface=DMC/TOE
  - secure communication with TLS-CA and MAC Authentication=true,
  - command freshness=successful,
  - connection interval=acceptable
- Local Interface connection establishment is allowed, if source interface=TOE/local port and destination interface=local port/TOE and local authentication=true
- Initialization Agent connection establishment is allowed, if
  - Initialization Agent authentication status=OK
- Local Administrator connection establishment is allowed, if
  - Local Administrator authentication status=OK
- Maintenance Agent (local) connection establishment is allowed, if
  - Maintenance Agent authentication status=OK
- Maintenance Agent (remote) connection establishment is allowed, if
  - source interface = TOE/Maintenance_Agent and destination interface= Maintenance_Agent /TOE
  - secure communication with TLS-CA and MAC Authentication=true,

    - command freshness=successful,
    - connection interval=acceptable
    - Maintenance Agent authentication status=OK
  - The data received from Sensing Modules, RFID/ 2D Barcode Readers is excepted

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: [none].

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 [Secure Communication Module Access Control SFP and Secure Communication Module 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 10: FDP_ITC.1 is applicable for import of: TOE Access IP List, Secure Communication Module 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 [Secure Communication Module Access Control SFP and Secure Communication Module 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 TOE 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 DMC Parameters only if the integrity and the authenticity of the upgrade package is confirmed by virtue of the upgrade credentials
- upgrade of the Secure Communication Module Time and IP Access List 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 [Secure Communication Module Access Control SFP and Secure Communication Module 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 11: FDP_ETC.1 is applicable for export of data via Local Interface after authentication is successful.

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 [Secure Communication Module Access Control SFP and Secure Communication Module 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 (HMAC) and command time for any data before sending to DMC or remote Maintenance Agent.]

Application Note 12: FDP_ETC.2 is applicable for export of data from Remote Interface. While communicating with DMC or remote Maintenance Agent, TLS connection is established that includes HMAC and encryption.

6.1.4.7 FDP_RIP Residual information protection

FDP_RIP.1 Subset residual information protection

Hierarchical to: -

Dependencies: -

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***deallocation of the resource from***] the following objects: [session keys generated during TLS Server Authentication].

6.1.4.8 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 an audit event. If this occurs ten times successively, enter TOE Maintenance mode, generate an audit, inform Authenticated DMC (as detailed in 3.2) and show a warning indicator on display].

6.1.4.9 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 [Secure Communication Module Control SFP] to [***transmit, receive***] ~~User Data~~ **any transmitted and received data between TOE and DMC** 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 DMC**, whether [***modification, deletion, insertion, replay***] has occurred.

6.1.4.10FDP_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 [Secure Communication Module Access Control SFP] to [***transmit, receive***] ~~User Data~~ **any transmitted and received data between TOE and DMC** 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 Attributes
    - Initialization Agent
    - Maintenance Agent
- [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 have been [***met***], the TSF shall [enter TOE Maintenance mode, generate an audit, inform Authenticated DMC (as detailed in 3.2) and show a warning indicator on the display].

Application Note 13: 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 Timing of authentication

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.

FIA_UAU.5: Multiple authentication mechanisms

Hierarchical to: -

Dependencies: -

FIA_UAU.5.1 The TSF shall provide [

- TLS authentication via certificates at the Remote Interface
- HMAC authentication via Symmetric keys at the Remote Interface
- Password-Token authentication at the Local Interface

] to support user authentication.

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

- DMC shall be authenticated via TLS-certificates and MAC Authentication at the Remote Interface. Remote Maintenance Agent shall be authenticated via token-password and shall be authenticated via TLS-certificates and MAC Authentication.
- Local Administrator, Initialization Agent and local Maintenance Agent shall be authenticated via token-password at the Local Interface.

].

FIA_UAU.6: Re-authenticating

Hierarchical to: -

Dependencies: -

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

- TLS channel to the WAN shall be disconnected after 24 hours,
- 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
- Secure Communication Module Firmware Update
- IP List Update

].

6.1.6.2 FMT_SMR Security management roles

FMT_SMR.1: Security roles

Hierarchical to: -

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [

- Authenticated Initialization Agent
- Authenticated Local Administrator
- Authenticated Maintenance Agent
- Authenticated DMC

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 Initialization Agent, Authenticated Maintenance Agent].

Application Note 14: Initialization data includes: TOE configuration parameters, TOE clock, ToE IP list.

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 [TOE Clock] to [Authenticated DMC, Authenticated Local Administrator, Authenticated Maintenance Agent and Authenticated Initialization Agent].

FMT_MTD.1/IP_LIST Management of TSF Data - IP Access List

Hierarchical to: -

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/IP_LIST

The TSF shall restrict the ability to ***[modify]*** the [IP Access List] to [Authenticated DMC and Authenticated Initialization Agent].

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 Secure Communication Module time and IP Access List] to [none].

FMT_MTD.1/FIRMWARE Management of TSF Data – Secure Communication Module 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 [Secure Communication Module Firmware] to [Authenticated remote Maintenance Agent and Authenticated DMC].

6.1.6.5 FMT_MSA Management of security attributes

FMT_MSA.1: Management of security attributes for Secure Communication Module Access Control SFP

Hierarchical to: -

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [Secure Communication Module Access Control SFP] to restrict the ability to [***modify***] the security attributes [IP Access List] to [Authenticated DMC and Authenticated Initialization Agent and Authenticated Maintenance Agent].

FMT_MSA.3: Static attribute initialization for Secure Communication Module access SFP

Hierarchical to: -

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [Secure Communication Module Access Control SFP] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [none] to specify alternative initial values to override the default values when an object or information is created.

6.1.7 Class FPT: Protection of the TSF

6.1.7.1 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 electro-mechanic seal
- detection of physical attack to mesh covers
- detection of environmental stress five (5) times
- detection of integrity check failures of User Data and TSF Data five (5) times
- detection of integrity check failures of User Data and TSF Data for ten (10) successive times,
- detection of insufficient entropy during random number generation ten (10) times
- detection of failures of periodic self-test functions for five (5) times,
- detection of low battery level under %10,
- detection of unsuccessful software update five (5) times,
- detection of unsuccessful authentication attempt from local interface five (5) times,
- detection of lack of system log memory,
- [assignment *: list of other types of failures in the TSF, or none*] .

Application Note 15: The above defined secure state is the Maintenance Mode (See Section 3.2).

6.1.7.2 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 [

- the Secure Communication Module,
- User Data and TSF Data storage memory in Secure Communication 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.

FPT_PHP.3 Resistance to physical attack

Hierarchical to: -

Dependencies: -

FPT_PHP.3.1 The TSF shall resist [

- physical attack to electro-mechanic seal
- physical attack to mesh covers
- environmental stress

] to the [

- Secure Communication Module,
- User Data and TSF Data storage memory in Secure Communication Module

] by responding automatically such that the SFRs are always enforced.

6.1.7.3 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 [selection: *during initial start-up,periodically during normal operation, at the request of the authorised user, at the conditions[assignment: conditions under which self-test should occur]*] 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]***.

6.1.7.4 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 DMC, Sensors and RFID/ 2D Barcode devices].

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

Application Note 16: Replay attack protection is provided by TLS and time control as defined in Section 1.2.7.2.

6.1.7.5 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.

Application Note 17: Reliable time stamp provide by authenticated users and authenticated DMC.

6.1.7.6 FPT_TDC Inter-TSF TSF Data consistency

FPT_TDC.1 Inter-TSF basic TSF Data consistency

Hierarchical to: -

Dependencies: -

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [TLS client / server authentication parameters] when shared between the TSF and ~~another trusted IT product~~ authenticated DMC.

FPT_TDC.1.2 The TSF shall use [TLS client / server authentication] when interpreting the TSF Data from ~~another trusted IT product~~ authenticated DMC.

6.1.8 Class FTP: Trusted path/channels

6.1.8.1 FTP_ITC Inter -TSF trusted channel

FTP_ITC.1: Inter -TSF trusted channel for DMC

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 DMC].

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.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

Table 7 provides an overview for security functional requirements coverage and also giving an evidence for sufficiency and necessity of the SFRs chosen.

Table 7 Coverage of Security Objectives by SFRs for TOE

	O.Access_Control	O.Event	O.Storage_Integrit	O.Authentication	O.Transfer	O.Protect	O.Physical_Tampe	O.Battery_Control	O.Abuse_Function	O.Update	O.Separate_IF	O.Firewall

	O.Access_Control	O.Event	O.Storage_Integrit	O.Authentication	O.Transfer	O.Protect	O.Physical_Tampe	O.Battery_Control	O.Abuse_Function	O.Update	O.Separate_IF	O.Firewall
FAU_ARP.1		X										
FAU_GEN.1		X						X				
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		
FCS_COP.1/SIGN-VER										X		
FCS_COP.1/TLS				X	X					X		
FCS_CKM.1/TLS_AES					X							

	O.Access_Control	O.Event	O.Storage_Integrit	O.Authentication	O.Transfer	O.Protect	O.Physical_Tampe	O.Battery_Control	O.Abuse_Function	O.Update	O.Separate_IF	O.Firewall
FCS_CKM.1/TLS_HMAC					X							
FCS_CKM.4					X							
FCS_RNG.1	X			X	X							
FDP_ACC.1	X											
FDP_ACF.1	X										X	X
FDP_IFC.2	X											X
FDP_IFF.1	X										X	X
FDP_ITC.1	X				X							X
FDP_ITC.2	X				X					X		
FDP_ETC.1	X											X
FDP_ETC.2	X				X							
FDP_RIP.1						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								

	O.Access_Control	O.Event	O.Storage_Integrit	O.Authentication	O.Transfer	O.Protect	O.Physical_Tampe	O.Battery_Control	O.Abuse_Function	O.Update	O.Separate_IF	O.Firewall
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/IP_LIST	X											
FMT_MTD.1/SECRET_READ	X											
FMT_MTD.1/FIRMWARE	X									X		
FMT_MSA.1	X											
FMT_MSA.3	X											
FPT_FLS.1			X				X	X				
FPT_PHP.2		X					X					
FPT_PHP.3							X					
FPT_TST.1			X			X						
FPT_RPL.1					X							
FPT_STM.1		X	X									
FPT_TDC.1				X	X					X		

	O.Access_Control	O.Event	O.Storage_Integrit	O.Authentication	O.Transfer	O.Protect	O.Physical_Tampe	O.Battery_Control	O.Abuse_Function	O.Update	O.Separate_IF	O.Firewall
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 8.

Table 8 Suitability of the SFRs

Security Objective	Security Functional Requirement	
O.Access_Control	FCS_RNG.1	Provides random number for Local Access control mechanism
	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 Firmware Update Public Key, Local Access Control Public Key, Encryption Key, HMAC Key, DMC Parameters, Secure

		Communication Module Time and IP Access List from outside of the TOE with the role of authenticated Local Administrator using Access Control SFP and Information Flow Control SFP.
	FDP_ITC.2	Provides import of DMC Parameters, IP Access List, Secure Communication Module Time, Secure Communication Module Firmware from outside of the TOE with the role of Authenticated DMC using Access Control SFP and Information Flow Control SFP.
	FDP_ETC.1	Provides export of Data Information, Event Information and Device Information to outside of the TOE with the role of authenticated Maintenance Agent using Access Control SFP and Information Flow Control SFP.
	FDP_ETC.2	Provides export of Data Information, Event Information and Device Information to outside of the TOE with the role of Authenticated DMC using Access Control SFP and Information Flow Control SFP.
	FIA_AFL.1	Detects and records authentication failure events for Authenticated DMC 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 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/IP_LIST	Define IP Access List management rule
	FMT_MTD.1/SEDRET_READ	Define reading TSF Data except Secure Communication Module time and IP Access List

		management rule
	FMT_MTD.1/FIRMWARE	Define Secure Communication Module Firmware management rule
	FMT_MSA.1	Provides the functions to restrict the ability to modify the security attributes to nobody
	FMT_MSA.3	Provides the functions to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
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 Authenticated DMC and 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/ SEC_LOW	Define actions carried out during audit trail is full
	FAU_STG.4/ REGULAR	Define actions carried out during r audit trail is full
	FAU_STG.4/SYS	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/SEC_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/SYS	Defines actions carried out during audit trail is full
	FDP_SDI.2	Monitors User Data stored for integrity errors
	FPT_FLS.1	Defines failure conditions including integrity failures for preservation of secure state
	FPT_TST.1	Detects integrity failures for TSF Data including stored executable code

	FPT_STM.1	Provides accurate time for integrity check
O.Authentication	FCO_NRO.2	Generates evidence of origin of the data to be transferred to the DMC
	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 Secure Communication Module Initialization.
	FCS_COP.1/TLS	Provides authentication mechanism between TOE-DMC and TOE-remote Maintenance Agent
	FCS_RNG.1	Provides random number for TLS mechanism
	FIA_ATD.1	Defines subject attributes
	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
	FPT_TDC.1	Provides the capability to consistently interpret TSF Data (Certificate and session key)
O.Transfer	FCS_COP.1/ENC-DEC	Provides the encryption and decryption operations for secure communication between DMC-TOE and TOE-remote Maintenance Agent
	FCS_COP.1/INT-AUTH	Provides the integrity protection operations for secure communication between DMC-TOE and TOE-remote Maintenance Agent
	FCS_COP.1/TLS	Provides the encryption and decryption operations for secure communication between DMC-TOE and DMC-TOE and TOE-remote Maintenance Agent
	FCS_CKM.1/TLS_AES	Generates session keys for communication between DMC-TOE and TOE-remote Maintenance Agent
	FCS_CKM.1/TLS_HMAC	Generates HMAC keys for communication between DMC-TOE and TOE-remote Maintenance Agent
	FCS_CKM.4	Destroys cryptographic keys in the TOE

	FCS_RNG.1	Provides random number for TLS mechanism
	FDP_ITC.1	Provides import of Firmware Update Public Key, Local Access Control Public Key, Encryption Key, HMAC Key, DMC Parameters, Secure Communication Module Time and IP Access List from outside of the TOE with the role of authenticated Local Administrator using Access Control SFP and Information Flow Control SFP.
	FDP_ITC.2	Provides import of DMC Parameters, IP Access List, Secure Communication Module Time, Secure Communication Module Firmware from outside of the TOE with the role of Authenticated DMC using Access Control SFP and Information Flow Control SFP
	FDP_ETC.2	Provides export of Data Information, Event Information, , IP Access List, DMC Parameters and Secure Communication Module time to outside of the TOE with the role of Authenticated DMC using Access Control SFP and Information Flow Control SFP
	FDP_UIT.1	Protect received and transmitted

		data from unauthenticated modification
	FDP_UCT.1	Protect received and transmitted data from unauthenticated disclosure
	FPT_RPL.1	Protect received data from replay attack
	FPT_TDC.1	Provides interpretation of private key and session key during communication with DMC
	FTP_ITC.1	Provide a secure communication channel to the DMC and remote Maintenance Agent
O.Protect	FDP_RIP.1	Defines protection of residual information
	FPT_TST.1	Provide self-test mechanism to demonstrate TSF Data integrity
O.Physical_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 physical tampering
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 DMC and Secure Communication Module during Secure Communication Module Firmware update
	FCS_COP.1/INT-AUTH	Provides the integrity protection operations for secure communication between DMC-TOE and TOE-remote Maintenance Agent during Secure Communication Module Firmware update
	FCS_COP.1/SIGN-VER	Provides verification of Secure Communication Module Firmware signature before upgrade the working one.
	FCS_COP.1/TLS	Provides the encryption and decryption operations for secure communication between DMC-TOE and TOE-remote Maintenance Agent

	FDP_ITC.2	Provides import of TOE Firmware from outside of the TOE.
	FDP_UIT.1	Protect received and transmitted data from unauthenticated modification
	FDP_UCT.1	Protect received and transmitted data from unauthenticated disclosure
	FMT_SMF.1	Provide management functions including firmware update
	FMT_MTD.1/FIRMWARE	Define Secure Communication Module Firmware management rule
	FPT_TDC.1	Provides interpretation session key during communication with DMC and remote Maintenance Agent
	FTP_ITC.1	Provides a secure communication channel to the DMC or remote Maintenance Agent
O.Separate_IF	FDP_ACF.1	Interfaces of the Secure Communication Module used in access control SPF are clear
	FDP_IFF.1	Interfaces of the TOE used in information flow control SPF are clear
O.Firewall	FDP_ACC.1	Define access conditions policy of the TOE
	FDP_ACF.1	Define access condition rules for the TOE

	FDP_IFC.2	Define information flow control policy of the TOE
	FDP_IFF.1	Define information flow control rules for the TOE
	FDP_ITC.2	Provides importation rules of DMC Parameters, IP Access List, Secure Communication Module Time, Secure Communication Module Firmware from outside of the TOE with security attribute
	FDP_ETC.2	Provides exportation rules of Data Information, Event Information and Device Information to outside of the TOE with security attribute

6.3.2 Rationale for Security Functional Requirements dependencies

Selected security functional requirements include related dependencies. Table 9 below provides a summary of the security functional requirements dependency analysis.

Table 9 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 FIA_UID.1	included
FAU_SAA.1	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
FAU_STG.4/ SEC_LOW	FAU_STG.1	included

Component	Dependencies	Included / not 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.
FCS_COP.1/TLS	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 ;	FCS_CKM.1 and FCS_CKM.4 included

Component	Dependencies	Included / not included
	FCS_CKM.4	
FCS_CKM.1/TLS_AES	FCS_CKM.2 or FCS_COP.1 ; FCS_CKM.4	FCS_COP.1 and FCS_CKM.4 included
FCS_CKM.1/TLS_HMAC	FCS_CKM.2 or FCS_COP.1 ; FCS_CKM.4	FCS_COP.1 and FCS_CKM.4 included
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FDP_ITC.1 and FCS_CKM.1 included
FCS_RNG.1	No dependencies	-
FDP_ACC.1	FDP_ACF.1	included
FDP_ACF.1	FDP_ACC.1; FMT_MSA.3	included
FDP_IFC.2	FDP_IFF.1	included
FDP_IFF.1	FDP_IFC.1; FMT_MSA.3	FDP_IFC.2 is hierarchical to FDP_IFC.1; FMT_MSA.3 included included
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1 ; FMT_MSA.3	included
FDP_ITC.2	FDP_ACC.1 or FDP_IFC.1 ; FTP_ITC.1 or FTP_TRP.1; FPT_TDC.1	included
FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	included
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	included
FDP_RIP.1	No dependencies	-
FDP_SDI.2	No dependencies	-
FDP_UIT.1	FDP_ACC.1 or FDP_IFC.1; FTP_ITC.1 or	FDP_ACC.1, FDP_IFC.1, FTP_ITC.1 included

Component	Dependencies	Included / not included
	FTP_TRP.1	
FDP_UCT.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
FIA_ATD.1	No dependencies	-
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	No dependencies	-
FIA_UAU.6	No dependencies	-
FIA.UID.2	No dependencies	-
FIA_USB.1	FIA_ATD.1	included
FMT_SMF.1	No dependencies	-
FMT_SMR.1	FIA_UID.1	FIA.UID.2 is hierarchical to FIA.UID.1
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/IP_LIST	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
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1; FMT_SMR.1; FMT_SMF.1	included

Component	Dependencies	Included / not included
FMT_MSA.3	FMT_MSA.1; FMT_SMR.1	included
FPT_FLS.1	No dependencies	-
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	No dependencies	-
FPT_TST.1	No dependencies	-
FPT_RPL.1	No dependencies	-
FPT_STM.1	No dependencies	-
FPT_TDC.1	No dependencies	-
FTP_ITC.1	No dependencies	-

6.3.3 Security Assurance Requirements Rationale

The current assurance package was chosen based on the pre-defined assurance packet EAL2. EAL2 is chosen because the threats that were chosen are consistent with an attacker of 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 9 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. 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
DMC	: Data Management Center
DSL	: Digital Subscriber Line
EAL	: Evaluation Assurance Level (defined in CC)
EDC	: Electricity Distribution Company
GPRS	: General Packet Radio Service
GPS	: Global Positioning System
OSP	: Organizational Security Policy
PP	: Protection Profile
PKI	: Public Key Infrastructure
PLC	: Power Line Communication
SFR	: Security Functional Requirements
SHA	: Secure Hash Algorithm
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

8 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, Version 3.1, Revision 4, September 2012

[5] The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246, August 2008.

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