Faculty of Fundamental Problems of Technology
Wrocław University of Science and Technology

Protection Profile

Team 3
Chmielowska Irmina
Czyszczonik Jakub
Drzazga Bartosz
Jachniak Mateusz
Kwiatkowski Kamil
Tański Gabriel

Politechnika
Wrocławska
Wrocław 2020

Contents

1 Introduction

1.1 PP reference

Title:	Protection Profile for Health Monitoring Station
Sponsor:	PWr
CC Version:	3.1 (Revision 2)
Version Number:	1.0
Registration:	BSI-CC-PP-XXXX
Keywords:	health, monitoring, medicine, identification, verification

1.2 Overview

The scope of this Protection Profile (PP) is to describe the security-related aspects of a medical device, the functionalities of which revolve around data collection, data sharing, and medication dosage. It is immediately apparent, that the security of said device and functionalities may have a significant impact on health, or even life, of its user. Therefore, it is vital to provide appropriate security that enables its safe utilization, especially given that the security of IoT devices has consistently been proven to be lackluster in recent years. It is difficult to overstate the importance of this matter in the aforementioned scenario, and therefore all possible steps need to be taken to ensure the confidentiality and integrity of the processed data, as well as availability and smooth operation of the device.

1.3 Terms

1.3.1 Common Criteria Terms

Common Criteria (CC) - Common Criteria for Information Technology Security Evaluation.

Protection Profile (PP) - An implementation independent set of security requirements for a category of products.

Target of Evaluation (TOE) - The product under evaluation.

Security Target (ST) - A set of implementation dependent security requirements for a specific product.

Security Functional Requirement (SFR) - A requirement for security enforcement by the TOE.

The TOE Security Function (TSF) - A set consisting of all hardware, software, and firmware of the product or system that must be relied upon for the correct enforcement of the TOE security policy.

1.3.2 Technology Terms

Administrator - An administrator is responsible for management of software and physical configuration of the TOE.

Credential - Data that establishes the identity of a user, e.g. a cryptographic key or password.

Operating System (OS) - Software that manages physical and logical resources and provides services for applications.

Personally Identifiable Information (PII) - Any information about an individual stored on TOE, including, but not limited to, medical history, and any information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Sensitive Data - Sensitive data may include all user or enterprise data or may be specific application data such as PII, configuration, and logs. Sensitive data must minimally include credentials and keys.
Access-control list (ACL) - An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

1.4 TOE Overview

The protection profile defines the security objectives and requirements for the Health Monitoring Station based on the requirements and recommendations of the World Health Organization (WHO), ISO/IEC GUIDE 63:2019, and ISO 13485:2016.

1.4.1 TOE Definition

The TOE addressed by PP is a health monitoring station. The TOE shall at least comprise of:

- the circuitry of the Health Monitoring Station (the integrated circuit, IC),
- the IC dedicated software, test software, and support software,
- the device embedded software (operating, system), including configuration data,
- the associated documentation.

The TOE includes all executable code (including related configuration data) running on the device. Since medical station supports contactless communication, the inlay with antenna should be part of the TOE covered by the evaluation.

The TOE is a wearable medical station in a form of a wristband which main feature is monitoring patient data and dosing medications.

1.4.2 The TOE Description

The physical scope of the TOE:
The TOE constitute the device of Health Monitoring Station as a hardware part, the device embedded software provided by its vendor as a software and firmware part.

The logical scope of the TOE:
The Health Monitoring Station is a smart device intended to be weared by a user on hand. It collects results of measurement of user parameters, stores the results and allows the authenticated member of healthcare staff to review them. It can dose medication according to configured treatments, proper to patient's needs. Thanks to this, the user does not have to worry about their medicaments.

1.4.3 TOE usage

TOE is a Health Monitoring Station able to connect to wearable or implanted sensors and medical equipment like drug delivery devices. The station collects and stores results of measurement of patient parameters and can send the results to an authenticated members of healthcare staff. The owner (patient) can manage the device and define a list of doctors allowed to review the patient's medical data. The authenticated medical staff is able to configure treatment procedures like medication dosages and review medical results from sensors. The device's firmware and software can be updated by an administrator. During the update procedure, the TOE also verifies integrity and authenticity of the new software. The TOE allows PKI-based authentication, protects against accidental data corruption, is able to distinguish roles of the entities with cryptographic means, and can enforce privileges or permissions using ACLs. For security and audit reasons the station logs every event. Its audit features are highly configurable, so as to allow detailed audit to be performed, while protecting the privacy and medical information of the owner. For that purpose, logs are divided into separate categories which are accessible for corresponding user groups. The administrator has access to updates and hardware performance logs. The owner has an insight into change history of admitted medical staff. The doctors can check logs of medication dosages and other actions performed by medical equipment.

In case of a medical emergency, if the unresponsive TOE owner is rushed to a medical facility, and medical staff there wants to access the TOE but has no access, the TOE administrator has the permission to grant temporary emergency access to the TOE owner's doctor. The TOE owner is immediately notified about such an action and can revert the decision at will.

1.4.4 TOE's security features for operational use

The device is protected by physical security measures, logical security measures and organizational security measures. The implemented features include:

- seals and anti-tamper circuitry,
- production control, quality control, screening of suppliers and subcontractors
- authentication keys,
- digital signatures and certificates,
- personalization procedures
- binding the device to the owner (e.g. embedding, cryptographic key(s) of the owner).

1.4.5 Required non-TOE hardware/software/firmware

The TOE is able to connect with sensors produced by 3rd parties. The communication between physical components is secured with symmetric cryptography for confidentiality and all data is signed in order to enforce integrity and authenticity. The pairing procedure between the TOE and a sensor is executed only by medical stuff allowed by the owner.

All entities use a client application to communicate with the TOE. All security requirements in that matter are assured by solutions based on PKI.

2 Conformance Claims

2.1 Conformance statement

To be conformant to this PP, a ST must demonstrate Exact Conformance, a subset of as defined in [3](ASE_CCL). The ST must include all components in this PP that are:

- unconditional (which are always required)
- selectionbased (which are required when certain selections are chosen in the unconditional requirements)

and may include components that are optional or objective.
Unconditional requirements are found in the main body of the document, while appendices contain the selectionbased, optional, and objective requirements. The ST may iterate any of these components, but it must not include any additional component (e.g. from CC Part 2 or 3 or a PP not conformant with this one, or extended by the ST) not defined in this PP or a PP conformant to this one.

2.2 CC Conformance Claims

- This PP has been developed using version 3.1 R2 of Common Criteria (CC) [3].
- This PP is compliant with Part 2 [4] and 3 [5] of the CC; no extended components have been defined.

2.3 PP Claim

- This PP does not claim conformance to any other Protection Profile.

2.4 Package Claim

- This PP does not claim conformance to any packages.

3 Security Problem Definition

3.1 External entities

The following external entities interact with the TOE:

- **TOE administrator** - The TOE administrator is authorised to perform the administrative TOE operations and able to use the administrative functions of the TOE. The administrator is also responsible for the installation and maintenance of the TOE. The actions that the TOE administrator is allowed to perform include updating the TOE software and access logs pertaining to TOE operations, exclusive of its primary functionality. In case of an emergency where the **user** is unresponsive, the TOE administrator can grant temporary emergency access (**Authorised healthcare staff** role) to the **user**'s doctor after being provided with convincing evidence.
- **User** - A person who is the sole user (and owner) of the TOE in question. A user can grant and revoke authorization for **healthcare staff**.
- **Authorised healthcare staff** - a person who is allowed by the **user** to interact with the TOE. This person is allowed to collect data pertaining to primary functionality of the TOE and modify its behavior in accordance with the current state of medical knowledge.
- **Sensor** - a device which collects data about the **User** and passes it to the TOE. Sensors are added by **healthcare staff**, along with cryptographic keys required for secure bilateral communication.
- **Attacker** - An attacker is any individual who is attempting to subvert the operation of the TOE. The intention may be to gain unauthorized access to the assets that otherwise require permissions. Another possible intention may be to modify the behavior of the TOE or cause the TOE to display false information to other entities.

3.2 Assets

The following assets are defined in the context of this Protection Profile:

- **Primary assets** - The most important asset that the TOE is designed to protect, is its user's health and life (Integrity & Availability). Another primary asset is the information about the health condition of the user (Confidentiality).
- **Supporting assets** - Assets which are generated by the TOE itself, its operational parametrs, and also cryptographic secrets used for interacting with the TOE by all of the authorised external entities.
  - Medical data - this is the data generated by the TOE or sensors paired with the TOE (Confidentiality, Integrity).
  - Medical parameters - this is the configuration of the device that can be changed by the authorized healthcare staff (Confidentiality, Integrity). This also includes the past values kept in the system logs.
  - The public key that enables the user to authenticate themselves with the TOE (Integrity).
  - The user-controlled list of cryptographic keys that enable the healthcare staff to authenticate themselves (Integrity).

- The list of shared secrets used for the communication with the sensors and for verifying the authenticity and integrity of incoming messages (Confidentiality, Integrity).
- The certificates that enable the TOE administrators to authenticate themselves (Integrity).
- The cryptographic secrets on the TOE that enable the TOE to authenticate itself when communicating with external entities (Confidentiality, Integrity).

3.3 Threats

- **T.ASSET_MODIFICATION** - An attacker may try to modify the secondary assets protected by the TOE, namely medical data or parameters. Such attacks could compromise the integrity of the user security attributes resulting in incorrect data or operational parameters that might cause unexpected behavior of the TOE. This threat covers a number of distinct types of attacks:
  - An attacker may attempt to modify the threshold levels used by the TOE to alert users and authorized healthcare staff. If the attacker is able to change the threshold this may adversely affect the health or, in extreme cases, the life of the user.
  - An attacker may attempt to modify the medical data. Modifying the medical data might result in ill-advised steps taken by the authorized healthcare staff, putting the primary assets at risk.
  - An attacker may try to modify the cryptographic secrets stored on the TOE to gain unauthorized access to the TOE and gain a foothold for further malicious actions.
  - An attacker may try to modify the logs. If the attacker is able to change the logs this may hide the malicious behavior.
- **T.DATA_EXTRACTION** - An attacker may try to access the TOE or eavesdrop on the communication between the TOE and external entities in order to gain access to the data stored thereon. This threat covers the case in which any medical information (sensor data, logs, or operational parameters) pertaining to the user is revealed to an unauthorized attacker.
- **T.SIGNAL_INTERFERENCE** - The physical conditions around the device, namely electromagnetic fields, can interfere with the proper operation of the device, preventing its primary or secondary functionality from being properly executed.
- **T.DENIAL_OF_SERVICE** - A malicious attacker can try to overload the TOE with wireless messages imitating the communication with external entities or the sensors, putting a strain on the processing power of the TOE and its ability to analyze sensor input and relay information to external entities.

3.4 Assumptions

- **A.ADMINISTRATION** - The TOE administrator is well trained and non hostile. He reads the guidance documentation carefully, completely understands and applies it. The TOE administrator is responsible to oversee the updates of the TOE software and ensure that any anomalies found in logs are immediately remediated. In case of an emergency whereby the TOE owner requires medical assistance but is unresponsive, the TOE administrator verifies the access request of the TOE owner's doctor and, based on the provided evidence, decides whether to grant access to the requestor. The TOE administrator does not abuse this privilege.
- **A.DOCTORS** - The authorized health staff is up to date with the current medical knowledge and is a non-malicious actor. An authorized person with this role has the user's best interests as their primary priority.
- **A.SENSOR** - The devices that relay their measurements to the TOE do so without measurement errors outside of their specification and without any corruption introduced in the process of sending. It is further assumed that the devices correctly reflect (with respect to the aforementioned measurement errors) the state of the user's vitals, and if they start malfunctioning, it becomes apparent for all parties involved. It is further assumed that the communication between the sensors and the TOE is not prone to eavesdropping or external interference.

- **A.ENVIRONMENT** - It is assumed that necessary TOE operating equipment and adequate infrastructure is available. This primarily includes the power supply and optimal operating temperature. This assumption is reasonable, given that the user provides the power supply for the TOE as a byproduct of their bodily processes. As for the environment temperature, the temperature tolerance of electrical devices dwarfs the sustainable temperature range of the human body (from which the operating temperature of the TOE will not differ by more than a negligible margin) on both ends of the spectrum. Any extreme environmental factor that is rare or lethal to humans (e.g. strong radiation) will not be taken into consideration for obvious reasons. This assumption does not cover common and relatively harmless environmental factors, the most important of which is electromagnetic field.
- **A.PHYSICAL** - It is assumed that the TOE and its components are physically protected against unauthorized access or destruction. Physical access to the hardware is impossible without detection and without performing a medical procedure on the user. Given the scope of the Protection Profile and the characteristics of the TOE, it is reasonable to assume that once the TOE is forcibly accessed, the interest of the user will shift far beyond the scope of this document.

3.5 Organizational Security Policies

- **OSP.CONNECTION_LIMIT** - Impostors must be prevented from gaining access to the device by making repeated connection attempts. This is solved by using secure cryptographic functions for communication, but it does not prevent the impostors from wasting the TOE's resources with brute-force attacks. Therefore the TOE shall be able to limit the maximum number of unsuccessful connection attempts.

4 Security Objectives

4.1 Security Objectives for the TOE

O.ALERT	It has to be ensured that the TOE is capable of detecting failures of critical components (i.e. when a critical sensor becomes unavailable) and, should such a situation arise, the TOE must also alert the user or any other authorized entity.
O.AUDIT	It has to be ensured that the TOE maintains audit records for use of the TOE functions, and must protect the stored audit records to prevent unauthorized modification or removal.
O.AUTHORIZATION	The TOE must provide a way to determine whether a user is authorized to perform a given action or access data stored on the TOE. This prevents unauthorized entities from activities beyond the scope of their roles.
O.BACKUP	The TOE must implement recovery and backup functionality which also restricts access to backed-up data only to authorized administrators.
O.INTEGRITY	The TOE must provide the capability to perform self tests to ensure that the integrity of critical functionality and data has been maintained. The TOE will also provide means to verify the integrity of downloaded updates. Furthermore, the communication between the TOE and external entities or the TOE components must utilize protocols allowing to verify that the messages were not doctored, and that any noise added during transmission can be at least identified.

4.2 Security Objectives for the Operational Environment

OE.ADMINISTRATION	It has to be ensured that the TOE administrator is well trained and non-hostile. He has to read the guidance documentation carefully, completely understand and apply it. The TOE administrator shall be responsible for ensuring that the updates of the TOE are performed as necessary and also making sure that any anomalies found in the logs are promptly addressed. The TOE administrator shall also be acquainted with the proper policies regarding storing cryptographic secrets used to authenticate themselves with the TOE. In addition, the TOE administrator has to be able to verify a doctor's license number and check whether an emergency access request is legitimate.
OE.DOCTORS	It has to be ensured that the authorized healthcare stuff is appropriately well trained on the usage of the TOE. Moreover, they need to be trained on how to store their cryptographic secrets used to authenticate themselves with the TOE.
OE.SENSOR	The sensors utilized as the external components of the TOE shall be tested prior to deployment. Moreover, they need to be used according to the manufacturer's documentation, including but not limited to regular maintenance and optimal operating conditions.
OE.ENVIRONMENT	The TOE basic conditions and infrastructure shall be available. Specifically, the following things have to be ensured: • The environment shall ensure a secure communication of security relevant data from and to the TOE. • The TOE environment has to be free of viruses, trojan horses, and other malicious software. • The TOE environment shall provide reliable time stamps
OE.PHYSICAL	The TOE with its components shall be introduced into the patient's body in a medical procedure further outlined in the appendix A, guaranteeing protection from unauthorized physical access to the TOE. In addition, they need to be properly configured before deployment to ensure secure communication with the TOE.

4.3 Security Objectives Rationale

4.3.1 Overview

The following table gives an overview, how the assumptions, threats, and organisational security policies are addressed by the security objectives. The text of the following subchapters justifies this in greater depth.

	O.ALERT	O.AUDIT	O.AUTHORISATION	O.BACKUP	O.INTEGRITY	OE.ADMINISTRATION	OE.DOCTORS	OE.SENSOR	OE.ENVIRONMENT	OE.PHYSICAL
T.ASSET_MODIFICATION		✓	✓	✓	✓					
T.DATA_EXTRACTION		✓	✓							
T.SIGNAL_INTERFERENCE	✓				✓					
T.DENIAL_OF_SERVICE		✓								
OSP.CONNECTION_LIMIT		✓								
A.ADMINISTRATION	▨	▨	▨	▨	▨	✓				
A.DOCTORS	▨	▨	▨	▨	▨		✓			
A.SENSOR	▨	▨	▨	▨	▨			✓		
A.ENVIRONMENT	▨	▨	▨	▨	▨				✓	
A.PHYSICAL	▨	▨	▨	▨	▨					✓

4.3.2 Coverage of the security objectives

The TOE security objective **O.ALERT** covers the severe cases outlined in T.SIGNAL_INTERFERENCE, where it is impossible to reach critical components for a prolonged period of time.

The TOE security objective **O.AUDIT** can be traced back to the threat T.ASSET_MODIFICATION (registering potentially unauthorized actions) and T.DATA_EXTRACTION (logging potential security breaches). In addition, this security objective fulfills OSP.CONNECTION_LIMIT and prevents T.DENIAL_OF_SERVICE (logging connection attempts in order to lock out malicious actors).

The TOE security objective **O.AUTHORISATION** can be traced back to the threats T.ASSET_MODIFICATION (to ensure that unauthorized users cannot modify the data, functionalities, or secrets on the TOE) and T.DATA_EXTRACTION (to ensure that only authorized personnel can read the data stored on the TOE).

The TOE security objective **O.BACKUP** serves as a fallback mechanism for when the two previous measures fail, allowing to restore the state from before the malicious actions covered by T.ASSET_MODIFICATION.

The TOE security objective **O.INTEGRITY** can be traced back to the threat T.ASSET_MODIFICATION (protection against simple modifications in the TOE internal assets) and T.SIGNAL_INTERFERENCE (identifying noise in the communication, error-correction or discarding affected messages).

4.3.3 Coverage of the assumptions, coverage of security objectives for the environment

The assumption **A.ADMINISTRATION** is covered by security objective **OE.ADMINISTRATION** as directly follows.

The assumption **A.DOCTORS** is covered by security objective **OE.DOCTORS** as directly follows.

The assumption **A.SENSOR** is covered by security objective **OE.SENSOR** as directly follows.

The assumption **A.ENVIRONMENT** is covered by security objective **OE.ENVIRONMENT** as directly follows, in addition to justified assumptions stemming from the purpose of the TOE.

The assumption **A.PHYSICAL** is covered by security objective **A.PHYSICAL** as directly follows, in addition to justified assumptions that are based on the purpose and the operating environment of the TOE.

For all assumptions, the corresponding objectives are stated in a way, which directly correspond to the description of the assumption. The only exceptions are in the case when the assumptions are logical given the nature of the TOE and its purpose. Everywhere else, it is clear from the description of each objective that the corresponding assumption is covered, if the objective is valid. In addition, some objectives exceed the statements of the assumptions they cover.

4.3.4 Countering the threats

The threat **T.ASSET_MODIFICATION** is fully countered by a security objective combination of O.AUTHORISATION, O.AUDIT, O.BACKUP, and O.INTEGRITY. O.AUTHORISATION ensures that only authorized personnel are allowed to modify the data stored on the TOE by limiting access to protected assets to corresponding roles. O.AUDIT logs every attempt to access said data. O.BACKUP ensures the ability to restore previous configuration in case any data is modified through means unknown. O.INTEGRITY ensures that any modifications will be swiftly detected.

The threat **T.DATA_EXTRACTION** is fully countered by a security objective combination of O.AUTHORISATION and O.AUDIT. O.AUTHORISATION ensures that no data can be downloaded from the TOE without proper privileges. O.AUDIT logs all such events in order to be able to monitor anomalous events and detect possible security flaws.

The threat **T.SIGNAL_INTERFERENCE** is countered by the combination of O.INTEGRITY and O.ALERT. The former ensures that all communications between the TOE and its components or external entities are validated. The effects of electromagnetic interference are easily noticeable, and in most cases, the error correction mechanisms allow for the correct reception of data. When, for any reason, the critical components are unreachable, the objective O.AUDIT provides a way to inform the proper entities about the issue (as such issues cannot be addressed by the TOE itself).

The threat **T.DENIAL_OF_SERVICE** is fully countered by O.AUDIT, which ensures that all unsuccessful authentication attempts are properly logged, and in case a malicious intent is apparent, the requests are no longer handled. In addition, the nature of the TOE and its environment renders it impossible to conduct a mass-scale DOS attack using multiple client devices, and therefore the O.AUDIT methods seem adequate.

4.3.5 Coverage of organisational security policies

The organisational security policy **OSP.CONNECTION_LIMIT** is met by **O.AUDIT** because this objective ensures that unsuccessful authentication attempts are logged, and the TOE takes appropriate action after a configurable number of those attempts occurred.

5 Security Requirements

5.1 Security Functional Requirements

The following table summarises all TOE functional requirements of this PP:

Class FAU: Security Audit	
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_STG.1	Protected audit trail storage, requirements are placed on the audit trail
FAU_STG.3	Action in case of possible audit data loss
FAU_SEL.1	Selective audit
Class FDP: User Data Protection	
FDP_RIP.2	Full residual information protection
FDP_SDI.2	Stored data integrity monitoring and action
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_DAU.1	Basic Data Authentication
FDP_ITT.1	Basic internal transfer protection
FDP_ITT.3	Integrity monitoring
FDP_ETC.2	Export of user data with security attributes
Class FIA: Identification and Authentication	
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UAU.3	Unforgeable authentication
FIA_UID.2	User identification before any action
Class FCO: Communication	
FCO_NRO.2	Enforced proof of origin
FCO_NRR.2	Enforced proof of receipt
Class FCS: Cryptographic support	
FCS_CKM.1/ECDSA	Cryptographic key generation (ECDSA)
FCS_CKM.1/AES	Cryptographic key generation (AES)
FCS_COP.1/ECDSA	Cryptographic operation (ECC signature generation/verification)
FCS_COP.1/AES	Cryptographic operation (AES symmetric encryption/decryption)
FCS_CKM.4	Cryptographic key destruction
Class FMT: Security Management	
FMT_MOF.1	Management of security function behaviour
FMT_MTD.1	Management of TSF data
FMT_MTD.2	Secure TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security management roles
Class FPT: Protection of the TSF	
FPT_RPL.1	Replay detection
FPT_STM.1	Reliable time stamps

5.1.1 Security audit (FAU)

5.1.1.1 FAU_GEN.1

FAU_GEN.1
Audit Data Generation

FAU_GEN.1.1
The TSF shall be able to generate an audit record of the following audit-able events:

- Start-up and shutdown of the audit functions
- All audit-able events for the basic level of audit
- Other specifically defined audit-able events

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST

Hierarchical to: No other components. **Dependencies:**

- FPT_STM.1

5.1.1.2 FAU_GEN.2

FAU_GEN.2
User identity association.

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.

Hierarchical to: No other components. **Dependencies:**

- FAU_GEN.1
- FIA_UID.1

5.1.1.3 FAU_STG.1

FAU_STG.1
Protected audit trail storage, requirements are placed on the audit trail.

FAU_STG.1.1
Protected audit trail storage, requirements are placed on the audit trail. It will be protected from unauthorised deletion and/or modification.

Hierarchical to: No other components.

Dependencies:

- FAU_GEN.1

5.1.1.4 FAU_STG.3

FAU_STG.3
Action in case of possible audit data loss.

FAU_STG.3.1
The following actions could be considered for the management functions in FMT:

- Maintenance of the threshold.
- Maintenance (deletion, modification, addition) of actions to be taken in case of imminent audit storage failure.

FAU_STG.3.2
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Actions taken due to exceeding of a threshold.

Hierarchical to:

- FAU_STG.3

Dependencies:

- FAU_GEN.1

5.1.1.5 FAU_SEL.1 Selective audit

FAU_SEL.1.1
The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

- object identity
- user identity
- subject identity
- event type

Hierarchical to: No other components
Dependencies:

- FAU_GEN.1 Audit data generation
- FMT_MTD.1 Management of TSF data

5.1.2 User Data Protection (FDP)

5.1.2.1 FDP_RIP.2

FDP_RIP.2
Full residual information protection.
FDP_RIP.2.1
The TSF shall ensure that any previous information content of a resource is made unavailable upon the all objects.
Hierarchical to:

- FDP_RIP.1

Dependencies: No dependencies.

5.1.2.2 FDP_SDI.2

FDP_SDI.2
Stored data integrity monitoring and action.
FDP_SDI.2.1
The TSF shall monitor the data stored in the TOE's data memory containers controlled by the TSF for integrity errors on all objects, based on user data.
FDP_SDI.2.2
Upon detection of a data integrity error, the TSF shall generate an audit record.
Hierarchical to: No other components. **Dependencies:** No dependencies.

5.1.2.3 FDP_ACC.1 Subset access control

FDP_ACC.1.1/Medical Data SFP
The TSF shall enforce the **Medical Data SFP** on the following list of subjects, objects and operations.
Subjects:

- S.DOCTOR
- S.SENSOR

Objects:

- O.MEDICAL_DATA
- O.TREATMENT_CONFIGURATION

Operations:

- Review results of measurement of patient parameters
- Check and change the treatment configuration and the medication dosages

Hierarchical to: No other components
Dependencies: FDP_ACF.1 Security attribute based access control.

5.1.2.4 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1/Medical Data SFP

The TSF shall enforce the **Medical Data SFP** to objects based on **following attributes**.

Subject/object	**Attribute**	**Values**
S.DOCTOR	Authentication	Yes, No
S.SENSOR	Data encryption	Yes, No
O.MEDICAL_DATA	Signed	Yes, No
O.TREATMENT_CONFIGURATION	Signed	Yes, No

FDP_ACF.1.2/Medical Data SFP

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

- Operations on **MEDICAL_DATA** are allowed only under the following circumstances:
  (a) if **Signed** [**MEDICAL_DATA**] is set to Yes and if Doctor has been correctly authenticated with **Authentication** [**Doctor**] set to Yes.
  (b) if **Signed** [**MEDICAL_DATA**] is set to Yes and if the **Data encryption** [**Sensor**] is set to Yes.
- Only Doctor correctly authenticated with **Authentication** [**Doctor**] set to Yes is allowed to review and update **TREATMENT_CONFIGURATION**

FDP_ACF.1.3/Medical Data SFP

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

FDP_ACF.1.4/Medical Data SFP

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **nobody** can modify **MEDICAL_DATA**.

Hierarchical to: No other components
Dependencies: FDP_ACC.1 Subset access control

5.1.2.5 FDP_DAU.1 Basic Data Authentication

FDP_DAU.1.1

The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of:

- Medical Data
- Treatment Configuration
- Logs

FDP_DAU.1.2

The TSF shall provide:

- Doctors
- User
- Administrator

with the ability to verify evidence of the validity of the indicated information.

Hierarchical to: No other components
Dependencies: No dependencies.

5.1.2.6 FDP_ITT.1 Basic internal transfer protection

FDP_ITT.1.1

The TSF shall enforce the **Medical Data SFP** to prevent the disclosure or modification of user data when it is transmitted between physically-separated parts of the TOE.

Hierarchical to: No other components
Dependencies: FDP_ACC.1 Subset access control

5.1.2.7 FDP_ITT.3 Integrity monitoring

FDP_ITT.3.1
The TSF shall enforce the **Medical Data SFP** to monitor user data transmitted between physically-separated parts of the TOE for integrity errors.

FDP_ITT.3.2
Upon detection of a data integrity error, the TSF shall issue a warning and offer an ability for retry.

Hierarchical to: No other components

Dependencies:

- FDP_ACC.1 Subset access control
- FDP_ITT.1 Basic internal transfer protection

5.1.2.8 FDP_ETC.2 Export of user data with security attributes

FDP_ETC.2.1
The TSF shall enforce the Medical Data 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 HMAC and command time for any data before sending.

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

5.1.3 Identification and Authentication (FIA)

5.1.3.1 FIA_AFL.1

FIA_AFL.1
Authentication failure handling.

FIA_AFL.1.1
The TSF shall detect and log unsuccessful authentication attempts of users and administrators.

FIA_AFL.1.2
When the defined number of unsuccessful authentication attempts has been exceeded, the TSF shall disable authentication functionalities for the corresponding user.

Hierarchical to: No other components.

Dependencies:

- FIA_UAU.1

5.1.3.2 FIA_ATD.1

FIA_ATD.1
User attribute definition.

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

- user ID and name
- role
- public key of the TOE owner
- public keys of doctors and administrators
- encryption keys utilized by the sensors

Hierarchical to: No other components.

Dependencies: No dependencies.

5.1.3.3 FIA_UAU.2

FIA_UAU.2
User authentication before any action.

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.

Hierarchical to:

- FIA_UAU.1

Dependencies:

- FIA_UID.1

5.1.3.4 FIA_UAU.3

FIA_UAU.3
Unforgeable authentication.

FIA_UAU.3.1
The TSF shall prevent use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2
The TSF shall prevent use of authentication data that has been copied from any other user of the TSF.

Hierarchical to: No other components.
Dependencies: No dependencies.

5.1.3.5 FIA_UID.2

FIA_UID.2
User identification before any action.

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.

Hierarchical to:

- FIA_UID.1

Dependencies: No dependencies.

5.1.4 Communication (FCO)

5.1.4.1 FCO_NRO.2

FCO_NRO.2
Enforced proof of origin.

FCO_NRO.2.1
The TSF shall enforce the generation of evidence of origin for transmitted changes of settings of medication dosages at all times.

FCO_NRO.2.2
The TSF shall be able to relate the user ID and name of the originator of the information, and the changes of settings of medication dosages to which the evidence applies.

FCO_NRO.2.3
The TSF shall provide a capability to verify the evidence of origin of information to administrator.

Hierarchical to:

- FCO_NRO.1

Dependencies:

- FIA_UID.1

5.1.4.2 FCO_NRR.2

FCO_NRR.2

Enforced proof of receipt.

FCO_NRR.2.1

The TSF shall enforce the generation of evidence of receipt for received changes of settings of medication dosages at all times.

FCO_NRR.2.2

The TSF shall be able to relate the user ID and name of the recipient of the information, and the changes of settings of medication dosages to which the evidence applies.

FCO_NRR.2.3

The TSF shall provide a capability to verify the evidence of receipt of information to administrator.

Hierarchical to:

- FCO_NRR.1

Dependencies:

- FIA_UID.1

5.1.5 Cryptographic support (FCS)

5.1.5.1 FCS_CKM.1/ECDSA

FCS_CKM.1/ECDSA

Cryptographic key generation (ECDSA)

FCS_CKM.1.1/ECDSA

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm (ECDSA key pair generation with given elliptic curve domain parameters) and specified cryptographic key sizes of minimum 256 bits that meet the following: ECDSA key pair generation for ECC domain parameters Curve P-256, Curve P-384 or Curve P-521 as specified in [FIPS 186-4][6]

Hierarchical to: No other components.

Dependencies:

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

5.1.5.2 FCS_CKM.1/AES

FCS_CKM.1/AES

Cryptographic key generation (AES)

FCS_CKM.1.1/AES

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm (AES key generation) and specified cryptographic key sizes of minimum 128 bits that meet the following: Advanced Encryption Standard (AES) as specified in [FIPS 197][1]

Hierarchical to: No other components.

Dependencies:

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

5.1.5.3 FCS_COP.1/ECDSA

FCS_COP.1/ECDSA

Cryptographic operation (ECC signature generation/verification)

FCS_COP.1.1/ECDSA

The TSF shall perform signature generation and verification in accordance with ECDSA algorithm with specified cryptographic key sizes of minimum 256 bits that meet the following: [FIPS 186-4][6]

Hierarchical to: No other components.

Dependencies:

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

5.1.5.4 FCS_COP.1/AES

FCS_COP.1/AES
Cryptographic operation (AES symmetric encryption/decryption)

FCS_COP.1.1/AES
The TSF shall perform symmetric encryption and decryption in accordance with a specified cryptographic algorithm AES in the mode CFB and cryptographic key sizes 128, 192 and 256 bits that meet the following: [FIPS 197][1]

Hierarchical to No other components.

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

5.1.5.5 FCS_COP.1/HMAC

FCS_COP.1/HMAC
Cryptographic operation (HMAC)

FCS_COP.1.1/HMAC
The TSF shall perform keyed-hash message authentication code calculation in accordance with a specified hash algorithm SHA-256, SHA-384 and SHA-512 and cryptographic key sizes that meet the following: [FIPS 198-1][2]

Hierarchical to: No other components.

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]

5.1.6 Security Management (FMT)

5.1.6.1 Management of functions in TSF (FMT_MOF)

FMT_MOF.1 Management of security function behaviour

FMT_MOF.1.1
The TSF shall restrict the ability to [determine the behaviour of, disable, enable, modify the behaviour of] the functions [

- Audit mechanism,

] to [TOE administrators].

FMT_MOF.1.2
The TSF shall restrict the ability to [determine the behaviour of, disable, enable, modify the behaviour of] the functions [

- Operating parameters,

] to [Authorized healthcare staff].

Hierarchical to: No other components

Dependencies:

- FMT_SMR.1
- FMT_SMF.1

5.1.6.2 Management of TSF data (FMT_MTD)

FMT_MTD.1 Management of TSF data
FMT_MTD.1.1

The TSF shall restrict the ability to [change_default, query, modify, delete, clear] the [

- user security attributes (authentication)

] to [TOE administrators].

FMT_MTD.1.2

The TSF shall restrict the ability to [query, modify, delete, clear] the [

- healthcare staff security attributes (authentication)

] to [Users].

FMT_MTD.1.3

The TSF shall restrict the ability to [query, modify, delete, clear] the [

- sensor encryption keys

] to [Healthcare staff].

FMT_MTD.1.4

The TSF shall restrict the ability to [append] the [

- healthcare staff security attributes (emergency access)

] to [TOE administrators].

Hierarchical to: No other components
Dependencies:

- FMT_SMR.1
- FMT_SMF.1

FMT_MTD.2 Secure TSF data
FMT_MTD.2.1

The TSF shall ensure that only secure values are accepted for [

- operating parameters of the TOE
- TSF security parameters

]

Hierarchical to: No other components
Dependencies:

- FMT_MTD.1

5.1.6.3 Specification of Management Functions (FMT_SMF)

FMT_SMF.1 Specification of Management Functions FMT_SMF.1.1

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

- grant and revoke access to a user
- grant and revoke access to health staff
- add and remove sensor encryption keys

]

Hierarchical to: No other components
Dependencies:

- FMT_SMR.1

5.1.6.4 Security management roles (FMT_SMR)

FMT_SMR.1 Security roles
FMT_SMR.1.1

The TSF shall maintain the roles [

- User
- TOE administrator
- Authorized health staff
- Sensor

]

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Hierarchical to: No other components
Dependencies: No dependencies

5.1.7 Protection of the TSF (FPT)

5.1.7.1 Replay detection

FPT_RPL.1 Exact match Replay detection
FPT_RPL.1.1 The TSF shall detect **exact match** replays for the following entities: [identification commitment].
FPT_RPL.1.2 The TSF shall ignore the replayed data when replay is detected.
Hierarchical to: No other components
Dependencies: No dependencies

5.1.7.2 Replay detection

FPT_STM.1 Reliable time stamps
FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.
Hierarchical to: No other components
Dependencies: No dependencies

5.2 Security Requirements rationale

	O.ALERT	O.AUDIT	O.AUTHORISATION	O.BACKUP	O.INTEGRITY
FAU_GEN.1		✓			
FAU_GEN.2		✓			
FAU_STG.1		✓			
FAU_STG.3		✓			
FAU_SEL.1		✓			
FDP_RIP.2					✓
FDP_SDI.2					✓
FDP_ACC.1			✓		
FDP_ACF.1			✓		
FDP_DAU.1			✓		
FDP_ITT.1					✓
FDP_ITT.3					✓
FDP_ETC.2				✓	
FIA_AFL.1			✓		
FIA_ATD.1			✓		
FIA_UAU.2			✓		
FIA_UAU.3			✓		
FIA_UID.2			✓		
FCO_NRO.2				✓	
FCO_NRR.2				✓	
FCO_CKM.1/ECDSA			✓		
FCO_CKM.1/AES			✓		
FCO_COP.1/ECDSA			✓		
FCO_COP.1/AES			✓		
FCS_COP.1/HMAC			✓		
FMT_MOF.1			✓		
FMT_MTD.1			✓		
FMT_MTD.2					✓
FMT_SMF.1			✓		
FMT_SMR.1			✓		
FPT_RPL.1			✓		
FPT_STM.1	✓				

The following paragraphs contain more details on this mapping.

O.ALERT

- **FPT_STM.1** provides reliable time stamps, allowing TOE to raise an alert if one or more sensors have stopped working

O.AUDIT

- **FAU_GEN.1** defines that the TOE has to capture all the events as required by O.AUDIT
- **FAU_GEN.2** ensures that events can be traced back to the identity of a user if the event was caused by a user.
- **FAU_STG.1** protects audit trail storage and places requirements on the audit trail
- **FAU_STG.3** performs actions in case of possible audit data loss, specifies actions to be taken if a threshold on the audit trail is exceeded.
- **FAU_SEL.1** ensures that TSF is able to select the set of events to be audited.

O.AUTHORISATION

- **FDP_ACC.1** enforces the Medical Data SFP on the mentioned subjects, objects and operations.
- **FDP_ACF.1** authorises access of subjects to objects.
- **FDP_DAU.1** provides a capability to generate evidence that can be used as a guarantee of the validity specified data.
- **FIA_AFL.1** handles accountability failures.
- **FIA_ATD.1** maintains the list of security attributes
- **FIA_UAU.2** prevents unauthenticated actions.
- **FIA_UAU.3** provides unforgeability.
- **FIA_UID.2** prevents unidentified actions.
- **FCO_CKM.1/ECDSA** provides ability to generate secure asymmetric keys
- **FCO_CKM.1/AES** provides ability to generate secure symmetric keys
- **FCO_COP.1/ECDSA** provides ability to perform secure handshakes
- **FCO_COP.1/AES** provides ability to securely transfer messages
- **FCS_COP.1/HMAC** provides ability to securely communicate with sensor
- **FMT_MOF.1** prevents unauthorized entities from performing changes reserved for specific roles.
- **FMT_MTD.1** prevents unauthorized entities from accessing or modifying data they should not have access to.
- **FMT_SMF.1** grants the TSF the ability to maintain its access list.
- **FMT_SMR.1** grants the TSF the ability to limit the access of authenticated entities.
- **FPT_RPL.1** prevents replay attacks and impersonation attempts.

O.BACKUP

- **FCO_NRO.2** provides history of applied changes with proof of origin on side of users device.
- **FCO_NRR.2** provides history of applied changes with proof of receipt on side of doctors or administrators device.
- **FDP_ETC.2** grants ability to export data with security attributes, allowing backups.

O.INTEGRITY

- **FDP_RIP2** previous information content from any source shall be destructed.
- **FDP_SDI2** requires the TOE to monitor stored data for integrity errors.
- **FDP_ITT.1** prevents the disclosure or modification of user data when it is transmitted between physically-separated parts of the TOE
- **FDP_ITT.3** monitors user data transmitted between physically-separated parts of the TOE
- **FMT_MTD.2** ensures that the data accepted by the TSF cannot cause security vulnerabilities.

Bibliography

[1] Advanced encryption standard (aes). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf, November 2001.

[2] The keyed-hash message authentication code (hmac). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf, July 2008.

[3] Common criteria for information technology security evaluation, part 1: Introduction and general model, ccmb-2012-09-001, version 3.1 revision 4. http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf, September 2012.

[4] Common criteria for information technology security evaluation, part 2: Security functional components, ccmb-2012-09-002, version 3.1 revision 4. http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf, September 2012.

[5] Common criteria for information technology security evaluation, part 3: Security assurance componentsl, ccmb-2012-09-003, version 3.1 revision 4. http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf, September 2012.

[6] Digital signature standard (dss). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf, July 2013.

A Medical procedure outline

The general outline of the medical procedure in which the TOE is to be installed by authorized and trained medical personnel. The details of the procedure are beyond the scope of this Protection Profile.