Page **1** of **35** Protection Profile for Connected Diabetes Devices (CDD)

Version 0.7 December 28, 2015

Acknowledgements

This protection profile was developed by members of the Diabetes Technology Society Standard for Wireless Device Security (DTSec) working group. The DTSec working group wishes to acknowledge and thank the members of this group, which includes representatives from independent technology suppliers and cybersecurity experts, diabetes device manufacturers, government regulatory bodies, caregivers, and academia, whose dedicated efforts contributed significantly to the publication.

0. Preface

0.1 Objectives of Document

This document presents the ISO/IEC 15408 Protection Profile (PP) to express the fundamental security and evaluation requirements for a connected diabetes devices (CDDs), including blood glucose monitors (BGMs), continuous glucose monitors (CGMs), insulin pumps (IPs), and handheld controllers (e.g. remote control used to manage insulin pump and AP closed loop systems).

0.2 Scope of Document

The scope of the Protection Profile within the development and evaluation process is described in ISO/IEC 15408. In particular, a PP defines the IT security requirements of a generic type of TOE and specifies the functional and assurance security measures to be offered by that TOE to meet stated requirements [CC1, Section 8.3].

0.3 Intended Readership

The target audiences of this PP are CDD developers, evaluators and government accrediting bodies.

0.4 Related Documents

The following referenced documents are indispensable for the application of ISO/IEC 15408. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

[CC1]	ISO/IEC 15408-1 – Information technology — Security techniques - Evaluation criteria for IT security - Part 1: Introduction and General Model
[CC2]	ISO/IEC 15408-2 – Information technology — Security techniques -— Evaluation criteria for IT security - Part 2: Security Functional Components
[CC3]	ISO/IEC 15408-3 – Information technology — Security techniques -— Evaluation criteria for IT security - Part 3: Security Assurance Components
[CEM]	ISO/IEC 18045 – Information technology — Security techniques -— Methodology for IT security evaluation
[MED]	IEC 62304 – Medical device software – Software life cycle processes – Second edition

0.5 Revision History

Table 1 - Revision history

Version	**Date**	**Description**
0.0	August 21, 2015	Initial Release
0.1	August 28, 2015	Remove EAL column from table 2 – some reviewers found it confusing and it was informative only. Add DTSec to glossary. Clarify definition of assurance package (DTSec Class C). Generalize secure channel requirement and move Bluetooth specifics to application note as an example of one possible method1
0.2	September 9, 2015	Based on feedback from developers, move physical security objectives and requirements to optional/environment instead of required for this version of the PP. as today's consumer diabetes devices are generally unsuitable for physical security technical protections today. Remove explicit JTAG as this PP prefers positive requirements; in other words, allowing JTAG access would violate the general physical security requirement so it need not be explicitly included. Remove FAU class requirements given feedback that BGs are highly unlikely to be actively monitored/managed by a security admin in the near future. Added user data protection to guard internal BG readings (FPT_TST protects only the TSF). Add assumption about the trustworthiness of peer devices.
0.3	September 21, 2015	Strengthen by removing the assumption of a trusted peer and instead add new requirements for information flow control to ensure the TOE can protect itself against untrusted peers (e.g. smartphones). Reduce clutter/duplicate content between main body and appendices. Other miscellaneous edits from feedback. Replace unnecessary extended comms SFR with standard FTP_ITC.
0.4	October 8, 2015	Add insulin pump and AP (controller) to the PP. Move optional functional requirements into separate section for clarity. Variety of minor improvements and clarifications resulting from numerous reviews across clinicians, regulators, evaluators, and others.
0.5	November 20, 2015	Add layman's description of requirements into the Introduction.
0.6	December 3, 2015	Add optional physical anti-tamper requirement
0.7	December 20, 2015	Minor revisions after final round of working group review prior to public review

Contents

1. PP Introduction

1.1 PP Reference Identification

PP Reference:	Protection Profile for Connected Diabetes Devices
PP Version:	0.7
PP Date:	December 20, 2015

1.2 Glossary

Term	Meaning
Administrator	The Administrator is responsible for management activities, including setting the policy that is applied by the service provider, on the device. If the security policy is defined during manufacturing and never changed, then the developer acts as administrator. If management activities can be performed by the user, then the user may also act as administrator.
Assurance	Grounds for confidence that a TOE meets the SFRs [CC1].
AP	Artificial pancreas
BG	Blood Glucose (e.g. BG reading)
BGM	Blood Glucose Monitor
Caregiver	Additional operator and authorized user of the TOE (in addition to the patient)
CGM	Continuous Glucose Monitor
CRC	Cyclic redundancy check
GM	Glucose Monitor
DTSec	Diabetes Technology Society cybersecurity standard for connected diabetes devices
Evaluator	Independent testing laboratory that evaluates the TOE against its ST by analyzing documentation and performing testing such as vulnerability assessment
PP	Protection Profile
RBG	Random Bit Generator
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
Target of Evaluation	A set of software, firmware and/or hardware possibly accompanied by guidance. [CC1]
TOE	Target of Evaluation

TOE Security Functionality (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs. [CC1]
TSS	TOE Summary Specification
User	Authorized operator of the CDD. The primary owner and patient is the most obvious example of authorized user; however, authorized family members or caregivers assisting the patient are other possible examples of authorized user. This PP does not distinguish between different user roles; an authorized user is assumed to be able to access any of the device's documented user interfaces.
CDD	Connected Diabetes Device

See [CC1] for other Common Criteria abbreviations and terminology.

1.3 TOE Overview

Medical devices used for monitoring and managing diabetes provide life-saving benefits to patients and effective treatment options for healthcare providers. These CDDs include blood glucose meters and continuous glucose monitors (Figure 1), insulin pumps, and closed loop artificial pancreas systems. The ever-increasing connectivity to other devices (such as smartphones, other CDDs, and cloud-based servers) allows patients, their families, and their healthcare providers to more closely monitor and manage their health and experience a concomitant increase in quality of life. At the same time, improperly secured CDDs present risks to the safety and privacy of the patient.

This assurance standard specifies information security requirements for CDDs. A CDD in the context of this assurance standard is a device composed of a hardware platform and its system software. For example, a blood glucose monitor may include software for functions like analyzing blood samples to compute a blood glucose (BG) reading, displaying the BG reading, storing BG readings in local non-volatile memory, transferring BG readings to a PC via USB cable, managing user input peripherals (e.g. buttons) that configure operation of the monitor, and transmitting BG readings wirelessly to a receiver, such as an insulin pump or a smartphone.

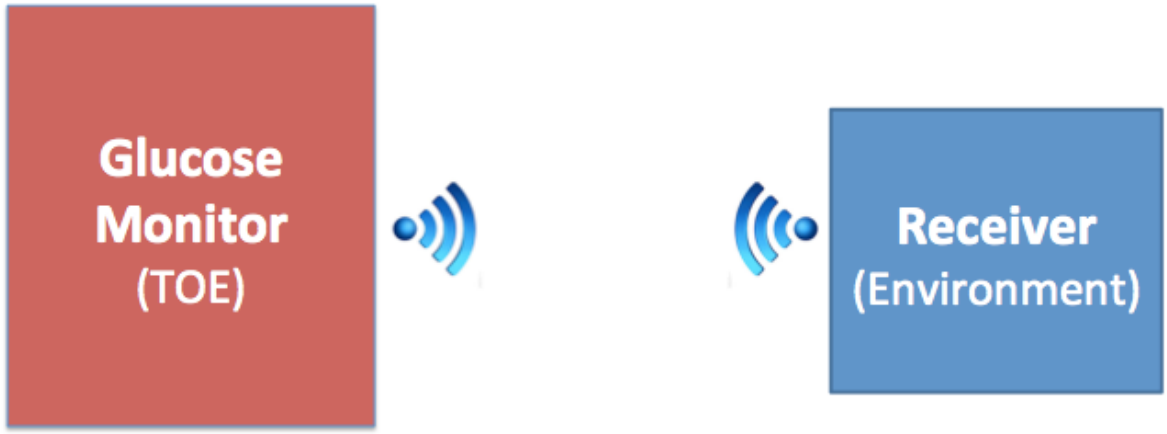

Figure 1 - Network operating environment for a glucose monitor TOE

Examples of a CDD that should claim conformance to this Protection Profile include simple blood glucose monitors (BGM), more sophisticated BGMs – e.g. with larger displays and audio functions, Continuous Glucose Monitors (CGMs), remote controllers of other CDDs, and insulin pumps. A closed loop artificial pancreas (AP) system may be a TOE itself or may be comprised by evaluated TOEs that make the overall system secure (Figure 2):

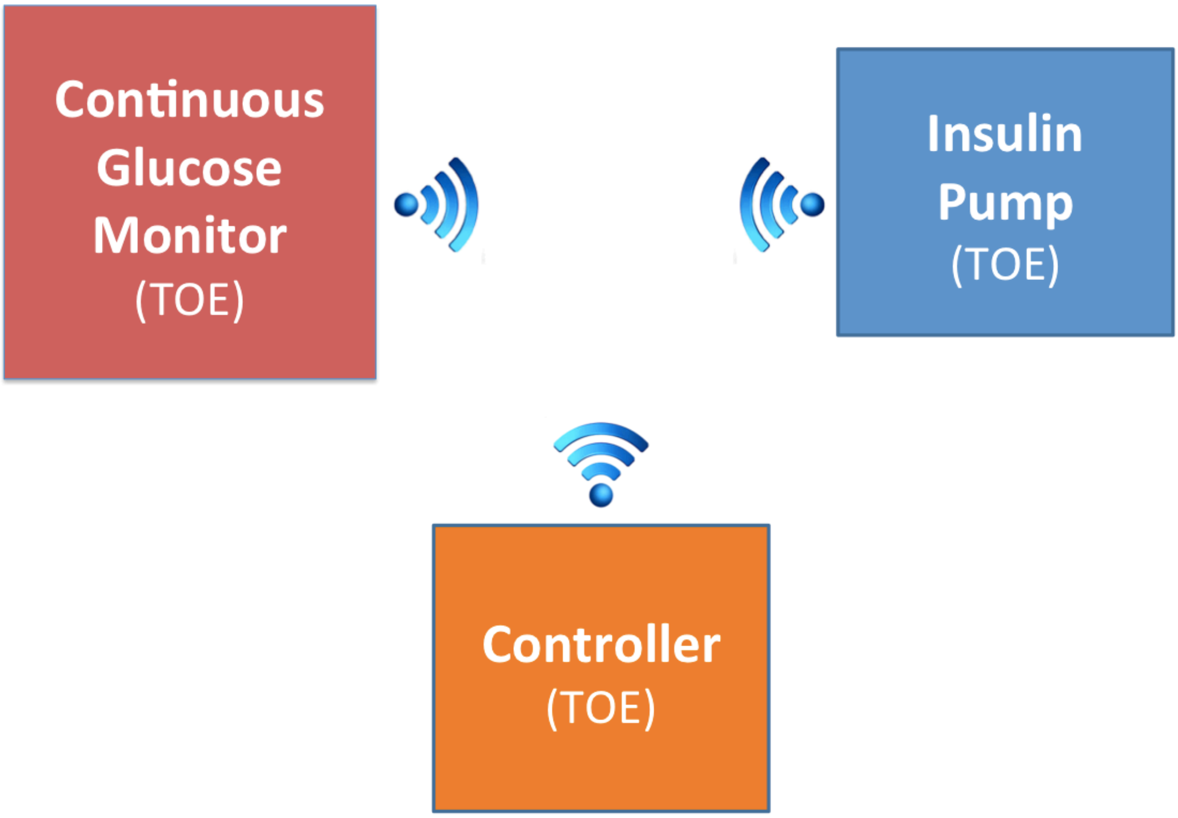

Figure 2 – One potential closed loop AP system consisting of 3 TOEs, each applicable to this PP

The CDD provides essential services, such as protected wireless communications to a companion device, to support the operation of the device. For example, an insulin pump TOE may receive BG readings from a BGM or operational commands from a handheld remote control, which may be a smart phone. A CGM TOE may wirelessly receive readings from an interstitial fluid analysis sensor attached to the body (and external to the TOE). The wireless communications is best thought of as a general information channel that must be adequately protected. Additional security features such as firmware and safety-critical user data integrity protection are implemented in order to address threats.

In order to make this PP practical for evaluation of modern medical devices, it is acknowledged that this PP and associated ST and evaluations must strive to balance the need for high assurance of protection via evaluation with the need to ensure safe clinical operation, market viability of devices, and timely availability to users and patients. It is unlikely that the use of this PP and derived STs for the evaluation of mass-market consumer medical devices will be mandated or even recommended without a proper balance. An example of proper balance is the relegation of user authentication requirements to OPTIONAL within this standard. While security experts agree that user authentication to the CDD is important to protect against unauthorized access to security-critical operations (such as user authorization of a remote endpoint pairing), user authentication must not get in the way of safe, simple clinical use. Furthermore, biometrics and other authentication mechanisms may be prohibitive for certain classes of CDDs. For this version of the PP for CDDs, the authors want to encourage developers to consider a safe and effective user authentication method but will not currently mandate it due to the aforementioned concerns that have yet to be robustly researched and implemented in practice.

While multiple TOEs may interact in a larger system – for example, a BGM communicating wirelessly with an insulin pump – each TOE must satisfy the requirements in this PP (and derived ST) and will be evaluated independently against its ST. Of note, this PP does not necessarily assume that devices authenticated and connected to the TOE are trustworthy. The ST developer must specify the *network information flow Security Function Policy (SFP)* (see requirements in the FDP_IFC and FDP_IFF families in this PP) appropriate for the TOE. For example, if a BGM TOE is permitted to connect to a commercial-off-the-shelf smartphone, the information flow control functions and policy for the BGM must ensure that a malicious smartphone (e.g. one that has been commandeered by malware from an open app store) cannot subvert the integrity of the BGM's safety and security functionality. The BGM ST developer may define the network information flow SFP to allow only status and BG readings to flow out of the BGM and disallow any security-relevant control and operation commands to flow in from the smartphone. If a commercial-off-the-shelf smartphone is used directly for safety-relevant control (for example, as the controller in a closed-loop AP), then the full device and its software would need to be evaluated against this PP/ST. At time of this writing, it is unlikely that a smartphone with arbitrary access to Internet and installed apps would be able to meet the assurance requirements of this PP due to frequent discovery of vulnerabilities and the lack of compliance of smartphone software to IEC 62304 safety lifecycle process. However, a customized firmware that limits the smartphone to clinical operation alone may be evaluable under this PP/ST.

This assurance standard describes these essential security services provided by the CDD and serves as a foundation for a secure CDD architecture. It is expected that some deployments would also include either third-party or bundled components. Whether these components are bundled as part of the CDD by the manufacturer or developed by a third-party, they must be separately validated against the related assurance standards (PPs and/or STs). It is the responsibility of the architect of the overall secure CDD architecture to ensure validation of these components. Additional applications that may come pre-installed on the CDD that are not validated are considered to be potentially flawed, but not malicious.

1.4 Requirements Summary for Non-technical Audiences

This section summarizes the security requirements of this Protection Profile in layman's terms, i.e. intended for a wide range of stakeholders in CDD safety and security, many of whom do not have a technical and/or cybersecurity background.

The Diabetes Technology Society has authored this Protection Profile (PP) specifically toward CDDs, which are currently used in healthcare facilities and in outpatient settings. With the diverse environments where such devices are used and the varied mechanisms employed to manage safe operation and protection of sensitive data, this PP aims to identify the potential security threats and risks faced by these devices and then present the functional and assurance requirements that counter these threats and thereby minimize risk.

1.4.1 Security Functional Requirements Summary

The Protection Profile has defined a set of ***mandatory*** security functional requirements that can be summarized as follows:

- *Integrity protection for CDD firmware/software*

This requirement answers the question: how can we know the CDD's software has not been tampered with? For example, a security vulnerability in the CDD may be exploited by attackers to modify the behavior of the CDD in such a manner as to make its continued use dangerous or otherwise unable to fulfill its original design intent.

- *Integrity protection for safety-critical stored data (e.g. BG readings)*

This requirement answers the question: how do we know any stored data, potentially used as input to diabetes clinical decisions, has not been tampered with? For example, a security vulnerability in the CDD may be exploited by attackers to modify stored BG readings within the CDD, leading a user, caregiver, or secondary device (e.g. insulin pump) to make poor clinical decisions that may adversely impact patient health.

- *Secure communications channel*

This requirement answers the question: how we can we ensure that only authorized devices can communicate with the CDD and only in authorized ways? For example, we want to prevent a remote device, controlled by an attacker, from connecting to the CDD and modifying its life-critical function and/or data. Even if the remote device is authorized to connect, this requirement further ensures that the remote device is only able to communicate to the CDD in prescribed ways. For example, an insulin pump CDD may receive BG readings from an authorized CGM; no other information flow to or from the CGM should be possible. If the secure communications channel fails to enforce this information flow constraint, then a commandeered CGM may be able to send additional commands that would adversely impact operation of the insulin pump.

- *Commercial best practice cryptography*

This requirement addresses a common design and implementation flaw in connected devices in which the developer may use cryptographic algorithms that are not widely accepted in the cryptographic community or not certified to well-established standards. Since cryptography forms the foundation of many higher-level security functions, it is critical that commercial best practices always be followed in this area.

The Protection Profile has also defined ***optional*** security functional requirements that can be summarized as follows:

- *User authentication to CDD*

Similar to consumer smartphones and other common computing devices, user authentication (login) ensures that only authorized individuals access the system. A CDD that lacks user authentication may be susceptible to unauthorized tampering by a malicious user who is able to obtain physical access to the CDD (e.g. if the CDD is lost or stole). CDDs must balance the desire for such physical protection with the challenge of implementing user authentication that does not impact clinical use. Since user authentication is nascent in the field of CDDs due to these concerns, the DTSec working group has decided to make this requirement optional; rationale is further described in this document.

- *Resistance to physical attack through open ports*

This requirement addresses a flaw in which physical input/output interfaces used during development – such as a USB port used to download test firmware from a PC into the CDD – are left open in the final production device rather than ensuring those ports are permanently disabled during the manufacturing process. While physical security is generally beyond the scope of requirements for products under this PP, this kind of physical security may be critical in ensuring that an attacker cannot use a device sample (e.g. purchased over the Internet) to reconnoiter the system to understand how it works, search for software flaws, and test attacks that could then be exploited over the device's wireless interfaces.

It should be noted that this PP does not include requirements associated with confidentiality protection of user data, such as BG readings, stored within CDDs. The consensus amongst the DTSec working group is that privacy concerns are better relegated to back-end systems (e.g. cloud) where this data is aggregated and processed rather than the CDDs themselves.

1.4.2 Security Assurance Requirements Summary

The Protection Profile has defined a set of assurance requirements that can be summarized as follows:

- Input that the product developer provides to evaluation labs, consisting of the product itself and a set of written artifacts such as design and specification documentation and testing results
- Actions that the evaluation lab must take, such as vulnerability assessment (including penetration testing) on the product, in order to ascertain that it actually satisfies the claimed security functional requirements

The assurance requirements are grouped into an assurance package - DTSec Class C – that can be reused (e.g. for future Protection Profiles). The evaluator actions are necessary for obtaining independent assurance of CDD security. If none of the penetration attacks are successful and all other evaluator actions pass, the evaluation is successful. If not, the product and/or the documentation will have to be modified and the evaluation has to be repeated. This PP requires vulnerability assessment that emulates a "moderate attack potential" attacker. The definition for moderate attack potential can be found in CEM, but roughly means more rigorous than the casual attacker and less rigorous than nation-state sophistication. It is also important to note that the authors of this PP expect medical device developers to already have the vast majority of the aforementioned artifacts at their disposal due to adherence to IEC 62304 and its constituent standards. Thus, vulnerability assessment is expected to be the dominant additional burden needed to pass an evaluation.

2. CC Conformance

As defined by the references [CC1], [CC2] and [CC3], this PP conforms to the requirements of ISO/IEC 15408, third edition. This PP is ISO/IEC 15408-2 extended and ISO/IEC 15408-3 extended. The methodology applied for the PP evaluation is defined in [CEM].

2.1 Assurance Package Claim

This PP conforms to assurance package *DTSec Class C*. The assurance package and its associated security assurance requirements are defined in section 6. The assurance package is a custom assurance package, tailored to meet the needs of connected, mass-market, life-critical medical devices.

3. Security Problem Definition

3.1 Threats

CDDs are subject to the threats of traditional computer systems along with those entailed by their mobile nature. The threats considered in this Protection Profile are those of network eavesdropping, network attacks, physical access, and malicious or flawed software, as detailed in the following sections. Of note, this PP primarily considers threats that would impact safe clinical function and does not consider confidentiality of locally stored user data (e.g. BG readings). Therefore, the firmware and execution of the TOE is an asset to be protected against the defined threats. In addition, while locally stored user data (e.g. BG readings) are an asset to protect, we aim to protect the integrity and not the confidentiality of these user data. Another way to look at this PP's scope is that every threat and countermeasure is considered from the perspective of safety. Therefore, any data or operation that is safety-critical is also, therefore, considered security-critical in that we must ensure threats cannot add undue risk to safety.

3.1.1 T.NETWORK Network Attack

An attacker (not an authenticated network peer) is positioned on a wireless communications channel or elsewhere on the network infrastructure. Attackers may initiate communications with the CDD or alter communications between the CDD and other endpoints in order to compromise the CDD.

3.1.2 T.PHYSICAL Physical Access

The loss or theft of the CDD may give rise to unauthorized modification of critical data and TOE software and firmware. These physical access threats may involve attacks that attempt to access the device through its normal user interfaces (especially if the device lacks user authentication to prevent unauthorized access), external hardware ports, and also through direct and possibly destructive access to its storage media. In the case of pairing the TOE to remote devices, unauthorized physical access to printed or displayed unique serial numbers could be used to establish malicious (yet device-authenticated) remote connections.

3.1.3 T.BAD_SOFTWARE Malicious Firmware or Application

Software loaded onto the CDD may include malicious or exploitable code or configuration data (e.g. certificates). This code could be included intentionally by its developer or unknowingly by the developer, perhaps as part of a software library, or via an over-the-air software update mechanism. Malicious software may attempt to exfiltrate data or corrupt the device's proper functioning. Malicious or faulty software or data configurations may also enable attacks against the platform's system software in order to provide attackers with additional privileges and the ability to conduct further malicious activities. Flawed software or configurations may give an attacker access to perform network-based or physical attacks that otherwise would have been prevented.

3.1.4 T.BAD_PEER Malicious Peer Device

A properly authenticated network peer may act maliciously and attempt to compromise the TOE using its network connection to the TOE.

3.1.5 T.WEAK_CRYPTO Weak Cryptography

Cryptography may be used for a variety of protection functions, such as data confidentiality and integrity protection, and weaknesses in the cryptographic implementation may enable compromise of those functions. Weaknesses may include insufficient entropy, faulty algorithm implementations, and insufficient strength key lengths or algorithms.

3.2 Assumptions

The specific conditions listed below are assumed to exist in the TOE’s Operational Environment. These include both the environment used in development of the TOE as well as the essential environmental conditions on the use of the TOE.

3.2.1 A.PHYSICAL Physical Security Precaution Assumption

It is assumed that the user exercises precautions to reduce the risk of unauthorized access, loss or theft of the CDD and any security-relevant data that is stored within or transferred beyond the TOE (e.g. BG readings).

3.3 Organizational Security Policy

There are no OSPs for the CDD.

4. Security Objectives

4.1 Mandatory Security Objectives for the TOE

The minimum security objectives for the CDD are defined as follows.

4.1.1 **O.COMMS** **Protected Communications**

To address the network eavesdropping and network attack threats described in Section 3.1, conformant TOEs will use a trusted communication path, which includes protection (via mutual device-level authentication) against unauthorized connections to the TOE and ensures the integrity and confidentiality of data transiting between the TOE and its network peers. High availability of network communication is not an explicit objective of this PP; the authors view current short-range wireless RF and associated protocols as susceptible to jamming, flooding, and other attacks against availability beyond the scope of a typical TOE developer to mitigate and relatively low risk due to the localized nature of CDD communications.

4.1.2 **O.INTEGRITY** **TOE Integrity**

Conformant TOEs shall ensure the integrity of critical operational functionality, software/firmware and safety-critical data (e.g. stored BG readings) has been maintained. The user shall be notified of any integrity violation that is not implicit or automatically prevented. (This will protect against the threat T.BAD_SOFTWARE and provide some protection against T.PHYSICAL.)

4.1.3 **O.STRONG_CRYPTO** **Strong Cryptography**

To guard against cryptographic weaknesses (T.CRYPTO), the TOE will provide cryptographic functions that follow commercial best practices, standards, and certifications.

4.2 Optional Security Objectives for the TOE

The optional security objectives for the CDD are defined as follows.

4.2.1 **OP.USER_AUTH** **User Authentication**

To address the issue of loss of confidentiality of user data and loss of safe function in the event of unauthorized physical access to the CDD (T.PHYSICAL), users are required to enter an authentication factor to the TOE prior to accessing protected functionality and data. Some safety-critical functionality may be accessed prior to entering the authentication factor but must be justified as appropriate relative to the risk of unauthorized access.

4.2.2 **OP.HW_PHYSICAL** **Hardware Physical Protection**

To address the issue of loss of confidentiality and/or integrity of the TSF and sensitive data (e.g. BG readings, private keys, device configuration policy files) in the event of a CDD being physically accessed by unauthorized agents (T.PHYSICAL), the device should protect itself against unauthorized access through external hardware ports and interfaces, such as serial flash programming interfaces and JTAG ports.

4.3 Security Objectives for the Operational Environment

4.3.1 OE.USER_PHYSICAL User Physical Protection

To address the issue of loss of confidentiality and/or integrity of the TSF and sensitive data (e.g. BG readings, private keys, device configuration policy files) in the event of a CDD being physically accessed by unauthorized agents (T.PHYSICAL), users must exercise precautions to eliminate the risk of corruption, loss or theft of the CDD or any security-relevant data (e.g. BG records and CDD calibration data) transferred beyond the TOE.

4.3.2 OE.USER_AUTH User Authentication

The user and/or caregiver must ensure that no one other than authorized individuals (e.g. owner of device, immediate family member, caregiver) are permitted to login or otherwise use the TOE’s defined user interfaces. This helps protect against unauthorized physical access (T.PHYSICAL).

5. Mandatory Security Functional Requirements

The individual security functional requirements are specified in the sections below.

5.1 Conventions

The following conventions are used for the completion of operations:

- [*Italicized text within square brackets*] indicates an operation to be completed by the ST author
- Underlined text indicates additional text provided as a refinement.
- [**Bold text within square brackets**] indicates the completion of an assignment.
- [***Bold-italicized text within square brackets***] indicates the completion of a selection.

5.2 Class: Cryptographic Support (FCS)

5.2.1 Cryptographic Operation (FCS_COP)

FCS_COP.1	**Cryptographic operation**

FCS_COP.1.1 The TSF shall perform [assignment: list of cryptographic operations] 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: Intent is to ensure compliance to widely used algorithm standards, such as NIST FIPS PUB 197, PKCS #1, PKCS #3, NIST FIPS PUB 186-3, ISO 19790, and NIST FIPS 140-2. Beyond algorithms, an ST should include key management guidance standards, such as NIST SP800-57 and NIST SP800-56 series, for example to ensure key strength is appropriate for intended TOE in-field service life. These requirements should be met where practically feasible, for example for any software cryptographic modules selected by the developer in implementing the TSF.

FCS_COP_EXT.1.2 (Extended) The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].

Application Note: At time of writing, current widely used algorithm validation schemes do not validate entropy source quality, hence the need for an extended requirement. At a minimum, RBGs require seeding with entropy at least equal to the greatest security strength of the keys and hashes that it will generate.

5.3 Class: Identification and Authentication (FIA)

5.3.1 Network Authorization and Authentication (FIA_NET)

FIA_NET_EXT.1	**Extended: Network Connection Authorization**

FIA_NET_EXT.1.1 The TSF shall require explicit user authorization of a permanent connection association with a remote device.

Application Note: This requirement is intended for wireless networks that offer user authorization for connection associations (e.g. some Bluetooth pairing modes such as *Numeric Comparison*, *Passkey Entry*, and some *Out of Band* mechanisms in the Bluetooth 4.2 standard). In such cases, explicit user interaction with the TOE must be required to permit the creation of the association; it must not be possible for software to programmatically create an authorized association. The ST developer must rationalize how the user authorization (possibly combined with trusted channel authentication mechanism from FTP_ITC) is of sufficient strength for the selected networking technology.

5.4 Class: User Data Protection (FDP)

5.4.1 Data Authentication (FDP_DAU)

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 [assignment: *list of objects or information types*].

FDP_DAU.1.2 The TSF shall provide [assignment: *list of subjects*] with the ability to verify evidence of the validity of the indicated information.

Application Note: The intent is that digital signatures or message authentication codes, in combination with immutable firmware that validates them, are used to cover the safety critical user data (e.g. BG readings). Signatures must leverage a manufacturer-trusted hardware-protected root of trust to guard against tampering of the data (e.g. through exploitable software vulnerabilities). In particular, a non-cryptographic mechanism such as a CRC does not meet the intent of this requirement.

5.4.2 Information Flow Control Policy (FDP_IFC)

FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [**network information flow control SFP**] on [**Subjects: TOE network interfaces, Information: User data transiting the TOE, Operations: Data flow between subjects**]

5.4.3 Information Flow Control Functions (FDP_IFF)

FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [**network information flow control SFP**] based on the following types of subject and information security attributes: [**Subjects: TOE network interfaces**, **Information: User data transiting the TOE,** assignment*: security attributes for subjects and information controlled under the SFP*].

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: [assignment*: for each operation, the attribute-based relationship that must hold between subject and information security attributes*].

FDP_IFF.1.3 The TSF shall enforce the [**no additional rules**].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [**no additional rules**].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**no additional rules**].

Application Note: The intent is that the TOE should protect itself against authenticated but malicious peers that may use the established channel to attack the TOE, by forcing unauthorized TSF configuration changes or behavior. For example, a CGM may implement an information policy that permits a 1-way incoming flow of sensor readings from an implantable sensor and a 1-way outgoing flow of BG readings to a separately paired and connected pump. In this example, the sensor connection protocol may not permit outgoing data, and the pump connection protocol may not accept incoming data. Both connections should protect against implementation flaws, such as buffer overflows, that could be exploited by malicious peers to impact the operation of the CGM. The ST must define the specific **network information flow control SFP**. A properly constrained and assured network information flow SFP may enable the pairing of TOEs to untrusted, off-the-shelf computing devices such as smartphones that would be used to monitor and display CDD-transmitted information (but not control the safe and secure operation of the TOE).

5.5 Class: Protection of the TSF (FPT)

5.5.1 TSF Integrity Checking (FPT_TST)

FPT_TST_EXT.1	**Extended: TSF Integrity Checking**

FPT_TST_EXT.1.1 The TSF shall verify its integrity prior to its execution.

Application Note: The intent is that digital signatures or message authentication codes, in combination with immutable firmware that validates them, are used to cover the full firmware and software implementation of the TOE. Signatures must leverage a manufacturer-trusted hardware-protected root of trust to guard against tampering of the TSF (e.g. through exploitable software vulnerabilities). In particular, a non-cryptographic mechanism such as a CRC does not meet the intent of this requirement. Also note that this requirement covers TSF updates as no post-market installed update can run if it too does not satisfy this requirement.

5.6 Class: Trusted path/channels (FTP)

5.6.1 Inter-TSF Trusted Channel (FTP_ITC)

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall provide communication channel between itself and another trusted IT product that is logically distinct from other communication channels are 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 [selection: *the TSF, another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].

Application Note: For example, for Bluetooth LE, the combination of security mode 1 and security level 3 may be used to meet these requirements, based on the Bluetooth standard's glucose profile as well as guidance from NIST SP800-121. The ST developer must specify the TOE communications mechanism and argue why the authentication and encryption mechanism is of sufficient strength to protect the communication channel against unauthorized access.

6. Optional Security Functional Requirements

The individual OPTIONAL security functional requirements are specified in the sections below.

6.1 Conventions

The following conventions are used for the completion of operations:

- [*Italicized text within square brackets*] indicates an operation to be completed by the ST author
- Underlined text indicates additional text provided as a refinement.
- [**Bold text within square brackets**] indicates the completion of an assignment.
- [***Bold-italicized text within square brackets***] indicates the completion of a selection.

Optional security functional requirements, corresponding to optional security objectives, are indicated with the **OPTIONAL** identifier within the component label.

6.2 Class: Identification and Authentication (FIA)

6.2.1 Authentication Failures (FIA_AFL)

FIA_AFL.1 OPTIONAL: Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [selection: *positive integer number*], *an administrator configurable positive integer within* [assignment: *range of acceptable values*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].

Application Note: The corrective action must carefully weigh the desire to protect against unauthorized access with the requirement to provide safety-critical functioning to the user. The ST developer must specify and rationalize the choice. The counter of unsuccessful attempts must not be reset when the device is powered off.

6.2.2 User Authentication (FIA_UAU)

FIA_UAU.1 OPTIONAL: Timing of authentication

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

Application Note: User authentication should not get in the way of life-critical operation. The ST must specify which operations are explicitly allowed without user authentication.

FIA_UAU.6 OPTIONAL: Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [assignment: *list of conditions under which re-authentication is required*].

Application Note: User authentication should not get in the way of life-critical operation. However, if the optional objectives of protecting against unauthorized physical access are included in the ST, then the TOE must implement some method for ensuring that a device no longer in the possession of an authorized user can be accessed through its normal interfaces.

6.3 Class: Protection of the TSF (FPT)

6.3.1 TSF Physical Protection (FPT_PHP)

FPT_PHP.3 OPTIONAL: Resistance to physical attack

FPT_PHP.3.1 [**Refinement**] The TSF shall resist [*unauthorized physical access to the TOE through* [assignment: *list of hardware interfaces*] ~~to the [assignment: *list of TSF devices/elements*] by responding automatically such that the SFRs are always enforced~~.]

Application Note: While physical security is an objective of the environment rather than the TOE in this PP, it is highly desirable that TOE developers prevent unauthorized use of external ports: open hardware interfaces can lower the cost of exploit, including non-physical exploitation of the TOE. For example, an attacker in possession of a TOE sample could use an active JTAG port to reconnoiter or download and test malicious software. Or an attacker could test malicious code modifications by reprogramming internal TOE flash memory over a USB serial interface. By raising the cost of an attack, this requirement may improve a TOE's chances of passing an evaluation since AVA_VAN related testing should reflect the increased required attack potential due to a lack of easily accessible physical access ports.

This requirement does not necessarily imply the need for any TOE automated response; if external ports are permanently disabled during the manufacturing process, then the TOE's resistance is implicit and automatic.

7. Security Assurance Requirements

The Security Objectives for the TOE in Section 4 were constructed to address threats identified in Section 3. The Security Functional Requirements (SFRs) in Section 5 are a formal instantiation of the Security Objectives. This section identifies the Security Assurance Requirements (SARs) to frame the extent to which the evaluator assesses the documentation applicable for the evaluation and performs independent testing.

This section lists the set of SARs that are required in evaluations against this PP. The general model for evaluation of TOEs against STs written to conform to this PP is as follows:

- After the ST has been approved for evaluation, the evaluator will obtain the ST, TOE, supporting environmental IT, the administrative/user guides for the TOE, and the artifacts that demonstrate compliance to IEC 62304 as applied to the TOE product development. These artifacts include architecture description, specification, design, testing, configuration management, and user documentation.
- The evaluator is expected to perform actions mandated by the Common Evaluation Methodology (CEM) for applicable SARs (e.g. AVA_VAN).
- The evaluator also performs the additional assurance activities contained within this section.

In order to make this PP/ST practical for evaluation of modern medical devices, it is acknowledged that evaluations must strive to balance the need for high assurance of protection via evaluation with the need to perform evaluations in a cost and time efficient manner to ensure market viability of devices and timely availability to users and patients. Indeed, application of the ISO 15408 standard in national security systems has been widely criticized of such an imbalance. It is unlikely that the use of this PP and derived STs for the evaluation of mass-market consumer medical devices will be mandated or even recommended if this balance is not properly struck.

In order to strike this balance, this PP leverages an assumed compliance of the medical device manufacturer of applicable TOEs to the IEC 62304 standard governing life cycle processes for medical device software ([MED]). As shown in Table 2, there is significant overlap between IEC 62304 and the life cycle related requirements defined by ISO/IEC 15408. The table also shows the target equivalent leveling for each corresponding SAR, although this PP does not claim compliance to any ISO/IEC 15408 EAL assurance package. Rather, this PP claims compliance to a custom assurance package, *DTSec Class C*. It should also be noted that ISO/IEC 15408 incorporates, by normative reference, ISO 14971, risk management process for medical devices. Since security threats pose a safety risk, manufacturers are already required to consider them in their risk management and SDLC processes.

***DTSec Class C* Assurance Package**

This assurance package is targeted at connected life-critical medical devices that utilize local/short-range wireless networks (e.g. Bluetooth) and must protect, at a minimum, against a moderate attack potential. The assurance package is defined by the assurance requirements listed in Table 3, including AVA_VAN.4 and requirements associated with ST evaluation (class ASE). The extended requirement, IEC_62304_EXT, reflects the package's prerequisite for TOE developer's IEC 62304 conformance and leverages the documentation artifacts from this standard as primary input for evaluation and vulnerability assessment. Table 2 (informative) illustrates the additional ISO 15408 assurance components that are targeted by IEC_62304_EXT and map to components of the IEC 62304 standard and its expected artifact outputs.

Table 2 - Mapping of target ISO 15408 assurance components to assurance package DTSec Class C (Informative)

Target ISO 15408 family and component	***IEC 62304 coverage ([MED])***
ADV_ARC.1	5.3
ADV_FSP.5	5.2
ADV_IMP.1	B.5.5
ADV_INT.2	5.5.3
ADV_TDS.4	5.4
AGD_OPE.1	5.2.2
AGD_PRE.1	5.2.2
ALC_CMC.5	8
ALC_CMS.5	8
ATE_COV.2	5.6.4 and 5.7
ATE_DPT.2	5.7
ATE_FUN.1	5.6.4 and 5.7
ATE_IND.2	5.7
AVA_VAN.4	not covered

As seen in the above table, this protection profile assurance package (*DTSec Class C*) explicitly includes AVA_VAN.4 as an assurance requirement. AVA_VAN.4 is arguably the most important component in the package because security vulnerability analysis is not addressed by medical software and quality standards (today) and makes an enormous contribution towards assurance by exposing the TOE and TSF to independent analysis and penetration testing that emulates a moderate level of attack potential (third highest of four attack potential classifications defined in the CEM). An evaluator will typically use thorough yet creative means to attempt to locate exploitable security vulnerabilities in the TOE. This assessment is made possible by analyzing the TOE and TSF-related documentation artifacts generated as part of the standard IEC 62304 lifecycle.

The TOE security assurance requirements are identified in Table 3. This set of requirements comprises the definition of *DTSec Class C* assurance package.

Table 3 - Security Assurance Requirements – DTSec Class C Assurance Package

Assurance Class	**Assurance Components**
Security Target (ASE)	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)
	Security objectives (ASE_OBJ.2)
	Derived security requirements (ASE_REQ.2)
	Security Problem Definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Vulnerability assessment (AVA)	Methodical vulnerability analysis (AVA_VAN.4)
IEC_62304_EXT	Extended: life-cycle related requirements adapted from IEC 62304

7.1 Class ASE: Security Target

The ST is evaluated as per ASE activities defined in [CEM].

7.2 Class AVA: Vulnerability Assessment

7.2.1 Vulnerability Survey (AVA_VAN)

Developer action elements:

AVA_VAN.4.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.4.1C The TOE shall be suitable for testing.

The TOE is evaluated as per AVA_VAN.4 activities defined in [CEM] and [CC3].

7.3 IEC_62304_EXT

The *DTSec Class C* assurance package, to which this PP claims compliance, targets the ISO 15408 components as described in Table 2. However, neither the assurance package nor this PP assert compliance to those components but rather aim to leverage the existing IEC 62304 life cycle compliance artifacts, augmented by inclusion of security-specific principles, and to use those artifacts as the primary input for vulnerability assessment (AVA_VAN.4).

For example, the objective of ATE_2 is to determine whether the developer has tested all the TSF subsystems and modules against the TOE design and security architecture description. The IEC 62304 testing artifacts should provide a mapping that demonstrates correspondence of tests that exercise the behavior of the TSF and TSFIs with the security design and architecture of the TOE. This mapping helps the evaluator perform AVA_VAN.4 by making it easier to identify gaps or design weaknesses or areas that have been tested less rigorously and hence potential candidates for exploitable implementation flaws. If the IEC 62304 testing artifacts do not provide this mapping, then the evaluator may reject the vendor submission as insufficient for testing in order to ensure evaluation remains efficient and economical. However, for some TOEs, the evaluator may feel AVA_VAN.4 can be performed without additional artifacts.

The remainder of this section is informative.

7.3.1 **ADV_ARC.1**

[MED section 5.3] requires an architecture description. Developers should ensure that this description covers the TSF.

The evaluator should use [CEM 11.3.1 – ADV_ARC.1] as a guideline for evaluation.

7.3.2 **ADV_FSP.5**

[MED section 5.2] requires a functional specification that includes the interfaces of software components. Developers should ensure that this specification and interfaces cover the TSFIs, including error messages that directly or indirectly result from execution of the TSFIs. In addition, the IEC 62304 and product documentation set should include a tracing of the specification to the SFRs.

The functional specification should use a standardized format with a well-defined syntax that reduces ambiguity that may occur in informal presentations.

The evaluator should use [CEM 11.4.5 – ADV_FSP.5] as a guideline for evaluation.

7.3.3 **ADV_IMP.1**

[MED section B.5.5] describes the translation of design to implementation.

The evaluator should use [CEM 11.5.1 – ADV_IMP.1] as a guideline for evaluation.

7.3.4 **ADV_INT.2**

[MED section 5.5.3] provides examples of acceptance criteria for software components. An explicit criterion for quality security design and ultimately a successful vulnerability assessment is that the TSF be well structured. While “well structured” is not rigorously defined by [CC3] or [CEM], the evaluator should use [CEM 11.6.2 – ADV_INT.2] as a guideline for evaluation.

7.3.5 **ADV_TDS.3**

[MED section 5.4] requires detailed design and refinement from design to implementation. The design should additionally make clear the boundary of the TSF and its distinction from the non-TSF subsystems of the TOE.

The evaluator should use [CEM 11.8.3 – ADV_TDS.3] as a guideline for evaluation.

7.3.6 AGD_OPE.1

[MED section 5.2.2] requires user documentation. Developers should ensure this documentation includes any security-relevant user guidance.

The evaluator should use [CEM 12.3.1 – AGD_OPE.1] as a guideline for evaluation.

7.3.7 AGD_PRE.1

[MED section 5.2.2] requires user documentation. Developers should ensure this documentation includes any security-relevant preparation procedures for the TOE.

The evaluator should use [CEM 12.4.1 – AGD_PRE.1] as a guideline for evaluation.

7.3.8 ALC_CMC.5

[MED section 8] requires a rigorous configuration management documentation and process.

The evaluator should use [CEM 13.2.5 – ALC_CMC.5] as a guideline for evaluation.

7.3.9 ALC_CMS.5

[MED section 8] requires a rigorous configuration management documentation and process. The CM system should include evaluation evidence (e.g. design documentation) per the SARs in this assurance package.

The evaluator should use [CEM 13.3.5 – ALC_CMS.5] as a guideline for evaluation.

7.3.10 ATE_COV.2

[MED sections 5.6.4 and 5.7] cover testing. The developer should ensure testing includes the full TSF, interfaces of TSF modules, and all TSFIs.

The evaluator should use [CEM 14.3.2 – ATE_COV.2] as a guideline for evaluation. However, the intent of this assurance package is not to duplicate testing performed during AVA_VAN.4; the evaluator is likely to execute test cases using documentation from the developer as part of vulnerability assessment, in which case additional independent testing may not be required.

7.3.11 ATE_DPT.2

[MED sections 5.6.4 and 5.7] cover testing. The developer should ensure testing includes the full TSF, interfaces of TSF modules, and all TSFIs.

The evaluator should use [CEM 14.4.2 – ATE_DPT.2] as a guideline for evaluation. However, the intent of this assurance package is not to duplicate testing performed during AVA_VAN.4; the evaluator is likely to execute test cases using documentation from the developer as part of vulnerability assessment, in which case additional independent testing may not be required.

7.3.12 **ATE_IND.2**

[MED section 5.6.4 and 5.7] cover testing. The developer should ensure testing includes the full TSF, interfaces of TSF modules, and all TSFIs.

The evaluator should use [CEM 14.6.2 – ATE_IND.2] as a guideline for evaluation.

A. Rationale

The following tables rationalize the selection of objectives and SFRs by showing the mapping between threats and assumptions to objectives and then objectives to SFRs.

A.1 Security Problem Definition Correspondence

The following table serves to map the threats and assumptions defined in this PP to the security objectives also defined or identified in this PP.

Table 4 - Security Problem Definition Correspondence

Threat or Assumption	**Security Objectives**
A.PHYSICAL	OE.USER_PHYSICAL, OP.HW_PHYSICAL
T.NETWORK	O.COMMS, OP.USER_AUTH,OE.USER_AUTH
T.PHYSICAL	OP.USER_AUTH, OP_HW_PHYSICAL, OE.USER_AUTH, O.INTEGRITY,OE.USER_PHYSICAL
T.BAD_SOFTWARE	O.COMMS,O.INTEGRITY
T.BAD_PEER	O.COMMS
T.WEAK_CRYPTO	O.STRONG_CRYPTO

A.2 Security Objective Correspondence

The following table shows the correspondence between TOE Security Functional Requirement (SFR) families and Security Objectives identified or defined in this PP. The first table includes mandatory objectives and requirements, while the second table includes optional objectives and requirements.

Table 5 - Mandatory security objective correspondence to mandatory SFR families

Mandatory Security Objective	**Mandatory SFRs**
O.COMMS	FIA_NET, FDP_IFC, FDP_IFF, FTP_ITC
O.INTEGRITY	FPT_TST, FDP_DAU
O.STRONG_CRYPTO	FCS_COP

Table 6 - Optional security objective correspondence to optional SFR families

Optional Security Objective	**Optional SFRs**
OP.USER_AUTH	FIA_UAU, FIA_AFL
OP.HW_PHYSICAL	FDP_PHP