
1 Page **1** of **29** Protection Profile for Connected
2 Diabetes Devices (CDD)
3
4
5

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 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, government regulatory bodies, 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
0.1	August 21, 2015	Initial Release
0.2	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
0.3	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.
0.4	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.
0.5	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.
0.6	November 20, 2015	Add layman's description of requirements into the Introduction.
0.7	December 3, 2015	Add optional physical anti-tamper requirement
0.8	December 20, 2015	Minor revisions after final round of working group review prior to public review
1.0	May 23, 2016	Revisions to incorporate public review
2.0	November 25, 2017	Move assurance requirements to Extended Package (EP)

Contents

46			
47	0. Preface	3	
48	0.1 Objectives of Document.....	3	
49	0.2 Scope of Document.....	3	
50	0.3 Intended Readership	3	
51	0.4 Related Documents	3	
52	0.5 Revision History.....	4	
53	1. PP Introduction	7	
54	1.1 PP Reference Identification.....	7	
55	1.2 Glossary.....	7	
56	1.3 TOE Overview	8	
57	1.4 Requirements Summary for Non-Technical Audiences	11	
58	1.4.1 Security Functional Requirements Summary	12	
59	1.4.2 Security Assurance Requirements Summary	13	
60	2. CC Conformance	14	
61	Security Problem Definition	15	
62	2.1 Threats.....	15	
63	2.1.1 T.NETWORK Network Attack	15	
64	2.1.2 T.PHYSICAL Physical Access	15	
65	2.1.3 T.BAD_SOFTWARE Malicious Firmware or Application	15	
66	2.1.4 T.BAD_PEER Malicious Peer Device	16	
67	2.1.5 T.WEAK_CRYPTO Weak Cryptography	16	
68	2.2 Assumptions.....	16	
69	2.2.1 A.PHYSICAL Physical Security Precaution Assumption	16	
70	2.3 Organizational Security Policy	16	
71	3. Security Objectives.....	17	
72	3.1 Mandatory Security Objectives for the TOE	17	
73	3.1.1 O.COMMS Protected Communications	17	
74	3.1.2 O.INTEGRITY TOE Integrity	17	
75	3.1.3 O.STRONG_CRYPTO Strong Cryptography	17	
76	3.2 Optional Security Objectives for the TOE	17	
77	3.2.1 OP.USER_AUTH User Authentication	17	
78	3.2.2 OP.HW_PHYSICAL Hardware Physical Protection	17	
79	3.3 Security Objectives for the Operational Environment	18	
80	3.3.1 OE.USER_PHYSICAL User Physical Protection	18	
81	3.3.2 OE.USER_AUTH User Authentication	18	
82	4. Mandatory Security Functional Requirements	19	
83	4.1 Conventions.....	19	
84	4.2 Class: Cryptographic Support (FCS)	20	
85	4.2.1 Cryptographic Operation (FCS_COP)	20	
86	4.3 Class: Identification and Authentication (FIA).....	21	
87	4.3.1 Network Authorization and Authentication (FIA_NET)	21	
88	4.4 Class: User Data Protection (FDP)	22	
89	4.4.1 Data Authentication (FDP_DAU)	22	
90	4.4.2 Information Flow Control Policy (FDP_IFC)	22	
91	4.4.3 Information Flow Control Functions (FDP_IFF)	22	
92	4.5 Class: Protection of the TSF (FPT).....	24	
93	4.5.1 TSF Integrity Checking (FPT_TST)	24	
94	4.6 Class: Trusted Path/Channels (FTP).....	25	
95	4.6.1 Inter-TSF Trusted Channel (FTP_ITC).....	25	
96	5. Optional Security Functional Requirements	26	
97	5.1 Conventions.....	26	

98	5.2	Class: Identification and Authentication (FIA).....	27
99	5.2.1	Authentication Failures (FIA_AFL).....	27
100	5.2.2	User Authentication (FIA_UAU).....	27
101	5.3	Class: Protection of the TSF (FPT).....	28
102	5.3.1	TSF Physical Protection (FPT_PHP)	28
103	A.	Rationale.....	29
104	A.1	Security Problem Definition Correspondence	29
105	A.2	Security Objective Correspondence.....	29
106			

107 1. PP Introduction

108 1.1 PP Reference Identification

PP Reference: Protection Profile for Connected Diabetes Devices

PP Version: 1.7

PP Date: December 20, 2015

109 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.
AP	Artificial pancreas
Assurance	Grounds for confidence that a TOE meets the SFRs [CC1].
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)
CDD, CMD	Connected Diabetes Device, Connected Medical Device
CGM	Continuous Glucose Monitor
CRC	Cyclic redundancy check
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 activities such as vulnerability assessment
GM	Glucose Monitor
Immutable Firmware	Firmware that cannot, by design, be modified through unauthorized means. Examples of immutable firmware include firmware written to read-only memory (ROM) or EEPROM whose re-programmability is protected against unauthorized use.
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.

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

111 1.3 TOE Overview

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

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



127

128

Figure 1 - Network operating environment for a glucose monitor TOE

129

130

131

132

133

134

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) TOE may be a single CDD from a single manufacturer or may be comprised of multiple evaluated CDDs from multiple manufacturers (example depicted in Figure 2):

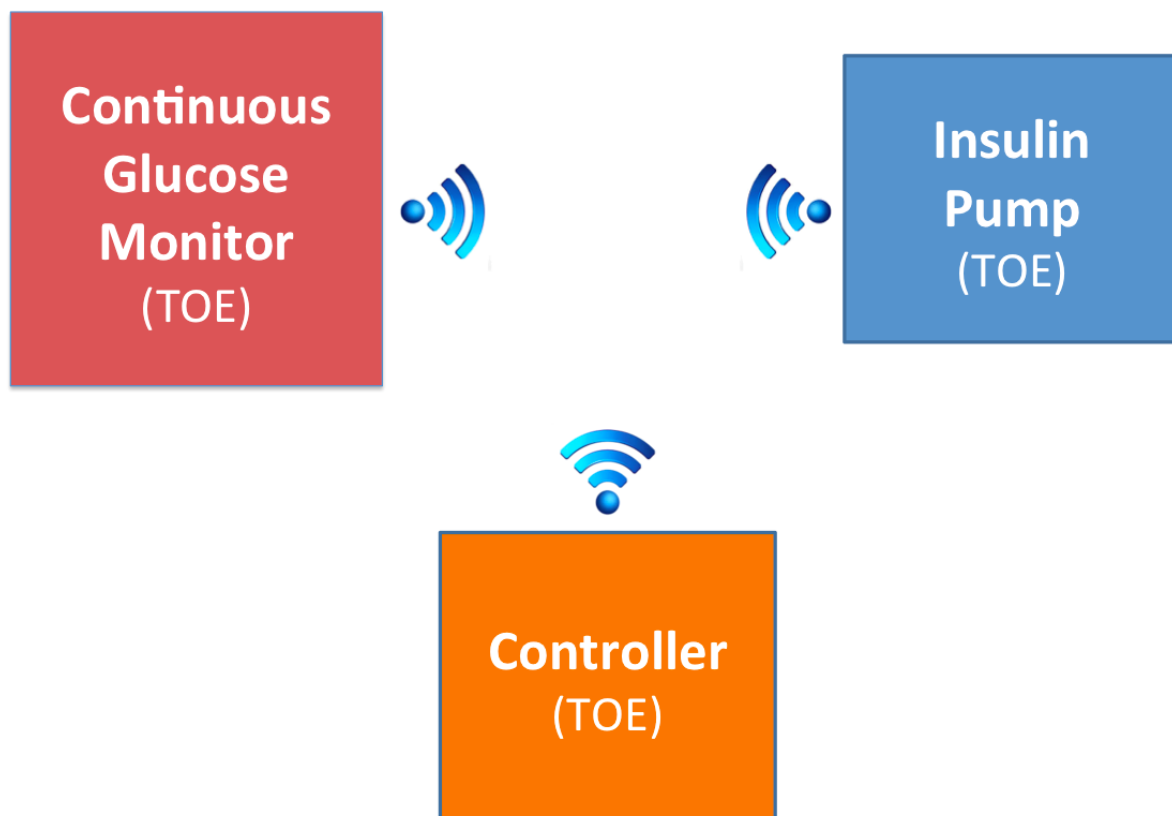


Figure 2 – One potential closed loop AP system consisting of 3 TOEs, each applicable to this PP

The CDD provides essential services, such as protected network 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. 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 are 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 safety-relevant portions of the smartphone (hardware, software) would be in scope for evaluation and need to be sufficiently protected from non-safety relevant portions of the smartphone. The precise specification of the scope, evaluation boundary, and security requirements would be codified in the 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, 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 security 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 for 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 stolen). 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 network 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 does not define security assurance requirements but rather is expected to be used in conjunction with Extended Packages (EPs) that define the assurance requirements suitable for use of the TOE in particular threat environments. It is expected that this conjunction of PP and EP is performed in the ST, which would then claim conformance to this PP as well as an applicable EP.

263 2. CC Conformance

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

Security Problem Definition

2.1 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 this 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.

2.1.1 T.NETWORK Network Attack

An attacker (not an authenticated network peer) is positioned on a network 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.

2.1.2 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.

2.1.3 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.

303 2.1.4 **T.BAD_PEER** **Malicious Peer Device**

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

306 2.1.5 **T.WEAK_CRYPTO** **Weak Cryptography**

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

311 2.2 **Assumptions**

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

315 2.2.1 **A.PHYSICAL** **Physical Security Precaution Assumption**

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

319 2.3 **Organizational Security Policy**

320 There are no OSPs for the CDD.

3. Security Objectives

3.1 Mandatory Security Objectives for the TOE

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

3.1.1 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.

3.1.2 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. (This will protect against the threat T.BAD_SOFTWARE and provide some protection against T.PHYSICAL.)

3.1.3 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.

3.2 Optional Security Objectives for the TOE

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

3.2.1 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.

3.2.2 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.

351 3.3 Security Objectives for the Operational Environment

352 3.3.1 OE.USER_PHYSICAL User Physical Protection

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

358 3.3.2 OE.USER_AUTH User Authentication

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

363

4. Mandatory Security Functional Requirements

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

4.1 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.

374 4.2 Class: Cryptographic Support (FCS)

375 4.2.1 Cryptographic Operation (FCS_COP)

376 FCS_COP.1 Cryptographic operation

377 **FCS_COP.1.1** The TSF shall perform [assignment: list of cryptographic operations] in
378 accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm]
379 and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following:
380 [assignment: list of standards].

381 **Application Note:** Intent is to ensure compliance to widely used algorithm standards, such as
382 NIST FIPS PUB 197, PKCS #1, PKCS #3, NIST FIPS PUB 186-3, ISO 19790, and NIST FIPS
383 140-2. Beyond algorithms, an ST should include key management guidance standards, such as
384 NIST SP800-57 and NIST SP800-56 series, for example to ensure key strength is appropriate
385 for intended TOE in-field service life. These requirements should be met where practically
386 feasible, for example for any software cryptographic modules selected by the developer in
387 implementing the TSF.

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

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

394

395 **4.3 Class: Identification and Authentication (FIA)**

396 **4.3.1 Network Authorization and Authentication (FIA_NET)**

397 FIA_NET_EXT.1	Extended: Network Connection Authorization
--------------------------	---

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

400 **Application Note:** This requirement is intended for networks that offer user authorization for
401 connection associations (e.g. some Bluetooth pairing modes such as *Numeric Comparison*,
402 *Passkey Entry*, and some *Out of Band* mechanisms in the Bluetooth 4.2 standard). In such cases,
403 explicit user interaction with the TOE may be required to permit the creation of the association
404 and prevent software from programmatically creating an authorized association. The ST
405 developer must rationalize how the user authorization (possibly combined with trusted channel
406 authentication mechanism from FTP_ITC) is of sufficient strength for the selected networking
407 technology.

408

409 4.4 Class: User Data Protection (FDP)

410 4.4.1 Data Authentication (FDP_DAU)

411 FDP_DAU.1 Basic Data Authentication

412 **FDP_DAU.1.1** The TSF shall provide a capability to generate evidence that can be used as a
413 guarantee of the validity of [assignment: *list of objects or information types*].

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

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

422 4.4.2 Information Flow Control Policy (FDP_IFC)

423 FDP_IFC.1 Subset Information Flow Control

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

427 4.4.3 Information Flow Control Functions (FDP_IFF)

428 FDP_IFF.1 Simple Security Attributes

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

433 **FDP_IFF.1.2** The TSF shall permit an information flow between a controlled subject and
434 controlled information via a controlled operation if the following rules hold: [assignment: *for*
435 *each operation, the attribute-based relationship that must hold between subject and*
436 *information security attributes*].

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

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

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

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

455

456 **4.5 Class: Protection of the TSF (FPT)**

457 **4.5.1 TSF Integrity Checking (FPT_TST)**

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

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

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

467

468 4.6 **Class: Trusted Path/Channels (FTP)**

469 4.6.1 **Inter-TSF Trusted Channel (FTP_ITC)**

470 **FTP_ITC.1 Inter-TSF Trusted Channel**

471 **FTP_ITC.1.1** The TSF shall provide a communication channel between itself and another
472 trusted IT product that is logically distinct from other communication channels and provides
473 assured identification of its end points and protection of the channel data from modification or
474 disclosure.

475 **FTP_ITC.1.2** The TSF shall permit [selection: *the TSF, another trusted IT product*] to initiate
476 communication via the trusted channel.

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

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

5. Optional Security Functional Requirements

The individual OPTIONAL 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.

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

497 5.2 Class: Identification and Authentication (FIA)

498 5.2.1 Authentication Failures (FIA_AFL)

499 FIA_AFL.1 OPTIONAL: Authentication failure handling

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

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

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

510 5.2.2 User Authentication (FIA_UAU)

511 FIA_UAU.1 OPTIONAL: Timing of authentication

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

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

516 FIA_UAU.6 OPTIONAL: Re-authenticating

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

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

523 5.3 **Class: Protection of the TSF (FPT)**

524 5.3.1 **TSF Physical Protection (FPT_PHP)**

525 **FPT_PHP.3 OPTIONAL: Resistance to physical attack**

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

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

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

541

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 2 - 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 3 - 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 4 - 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