Protection Profile for Connected Diabetes Devices (CDD PP) Extended Package: Moderate

Acknowledgements

This EP 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 Extended Package (EP) 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 EP within the development and evaluation process is described in ISO/IEC 15408. In particular, an EP 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 EP 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
1.0	November 25, 2017	Initial Release

Contents

0. Preface 3
  0.1 Objectives of Document 3
  0.2 Scope of Document 3
  0.3 Intended Readership 3
  0.4 Related Documents 3
  0.5 Revision History 4
1. EP Introduction 6
  1.1 EP Reference Identification 6
  1.2 Requirements Summary for Non-Technical Audiences 6
    1.2.1 Security Assurance Requirements Summary 6
2. CC Conformance 8
  2.1 Assurance Package Claim 8
  2.2 How to Use This Extended Package 8
3. Security Assurance Requirements 9
  3.1 Class ASE: Security Target 11
  3.2 Class AVA: Vulnerability Assessment 11
    3.2.1 Vulnerability Survey (AVA_VAN) 11
  3.3 IEC_62304_EXT 11
    3.3.1 ADV_ARC.1 12
    3.3.2 ADV_FSP.5 12
    3.3.3 ADV_IMP.1 12
    3.3.4 ADV_INT.2 12
    3.3.5 ADV_TDS.3 13
    3.3.6 AGD_OPE.1 13
    3.3.7 AGD_PRE.1 13
    3.3.8 ALC_CMC.5 13
    3.3.9 ALC_CMS.5 13
    3.3.10 ATE_COV.2 13
    3.3.11 ATE_DPT.2 14
    3.3.12 ATE_IND.2 14

1. EP Introduction

This Extended Package (EP) describes security assurance requirements for connected diabetes devices. However, this EP is not complete in itself, but rather extends the Protection Profile for Connected Diabetes Devices (CDD PP). Please refer to the CDD PP for description of relevant TOEs for this EP, glossary, and other important background information. This introduction will discuss how this EP is to be used in conjunction with the CDD PP.

1.1 EP Reference Identification

EP Reference: CDD PP Extended Package: Moderate

EP Version: 1.0

EP Date: November 25, 2017

1.2 Requirements Summary for Non-Technical Audiences

This section summarizes the security requirements of this EP 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 EP 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 EP aims to identify the potential security threats and risks faced by these devices and then present the assurance requirements that counter these threats and thereby minimize risk.

1.2.1 Security Assurance Requirements Summary

The EP 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 PPs and EPs). 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 EP requires vulnerability assessment that emulates an "moderate attack potential" attacker. The definition for moderate attack potential can be found in CEM. It is also important to note that the authors of this EP

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

The CDD PP defines the baseline Security Functional Requirements (SFRs) for connected diabetes devices. This EP serves to extend the CDD PP baseline with additional Security Assurance Requirements (SARs) specific to products whose anticipated threat profile is appropriate for the *DTSec Class C* assurance package.

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

2.1 Assurance Package Claim

This EP conforms to assurance package *DTSec Class C*. The assurance package and its associated security assurance requirements are defined in section 3. The assurance package is a custom assurance package, tailored to meet the needs of connected, mass-market, life-critical medical devices.

2.2 How to Use This Extended Package

As an EP of the CDD PP, it is expected that the content of both this EP and the CDD OO is appropriately combined in the context of each product-specific ST. This EP has been specifically defined such that there should be no difficulty or ambiguity in doing so. An ST must identify the applicable versions of the CDD PP and this EP in its conformance claims. This EP does not add any security functional requirements (SFRs) and therefore does not introduce any new product features or imply any new product types. This EP merely augments the CDD PP with assurance requirements that specify the level of attacker potential that compliant TOEs must be capable of defending against.

3. Security Assurance Requirements

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 of applicable TOEs. The general model for evaluation of TOEs against STs are written to conform to this EP 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 the CDD PP/EP/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 EP 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 EP 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 EP does not claim compliance to any ISO/IEC 15408 EAL assurance package. Rather, this EP 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 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.3	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 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

3.1 Class ASE: Security Target

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

3.2 Class AVA: Vulnerability Assessment

3.2.1 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].

3.3 IEC_62304_EXT

The *DTSec Class C* assurance package, to which this EP claims compliance, targets the ISO 15408 components as described in Table 2. However, neither the assurance package nor this EP 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.

3.3.1 **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.

3.3.2 **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.

3.3.3 **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.

3.3.4 **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.

3.3.5 **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.

3.3.6 **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.

3.3.7 **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.

3.3.8 **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.

3.3.9 **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.

3.3.10 **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.

3.3.11 **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.

3.3.12 **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.