

---

1 Protection Profile for Connected Diabetes  
2 Devices (CDD PP) Extended Package:  
3 Moderate  
4  
5  
6

---

7 **Acknowledgements**

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

14

15

16

17

18

19

20

21

22

DRAFT

---

## 23 0. Preface

### 24 0.1 Objectives of Document

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

### 30 0.2 Scope of Document

31 The scope of the EP within the development and evaluation process is described in ISO/IEC  
32 15408. In particular, an EP defines the IT security requirements of a generic type of TOE and  
33 specifies the security measures to be offered by that TOE to meet stated requirements [CC1,  
34 Section 8.3].

### 35 0.3 Intended Readership

36 The target audiences of this EP are CDD developers, evaluators, government regulatory bodies,  
37 and government accrediting bodies.

### 38 0.4 Related Documents

39 The following referenced documents are indispensable for the application of ISO/IEC 15408.  
40 For dated references, only the edition cited applies. For undated references, the latest edition  
41 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

42

43

---

44 **0.5 Revision History**

45 *Table 1 - Revision history*

<b>Version</b>	<b>Date</b>	<b>Description</b>
1.0	November 25, 2017	Initial Release

46

DRAFT

---

47 **Contents**

48	0. Preface.....	3
49	0.1 Objectives of Document.....	3
50	0.2 Scope of Document.....	3
51	0.3 Intended Readership.....	3
52	0.4 Related Documents.....	3
53	0.5 Revision History.....	4
54	1. EP Introduction.....	6
55	1.1 EP Reference Identification.....	6
56	1.2 Requirements Summary for Non-Technical Audiences.....	6
57	1.2.1 Security Assurance Requirements Summary.....	6
58	2. CC Conformance.....	8
59	2.1 Assurance Package Claim.....	8
60	2.2 How to Use This Extended Package.....	8
61	3. Security Assurance Requirements.....	9
62	3.1 Class ASE: Security Target.....	11
63	3.2 Class AVA: Vulnerability Assessment.....	11
64	3.2.1 Vulnerability Survey (AVA_VAN).....	11
65	3.3 IEC_62304_EXT.....	11
66	3.3.1 ADV_ARC.1.....	12
67	3.3.2 ADV_FSP.5.....	12
68	3.3.3 ADV_IMP.1.....	12
69	3.3.4 ADV_INT.2.....	12
70	3.3.5 ADV_TDS.3.....	13
71	3.3.6 AGD_OPE.1.....	13
72	3.3.7 AGD_PRE.1.....	13
73	3.3.8 ALC_CMC.5.....	13
74	3.3.9 ALC_CMS.5.....	13
75	3.3.10 ATE_COV.2.....	13
76	3.3.11 ATE_DPT.2.....	14
77	3.3.12 ATE_IND.2.....	14

78

---

## 79 1. EP Introduction

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

### 85 1.1 EP Reference Identification

EP Reference: CDD PP Extended Package: Moderate

EP Version: 1.0

EP Date: November 25, 2017

### 86 1.2 Requirements Summary for Non-Technical Audiences

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

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

#### 96 1.2.1 Security Assurance Requirements Summary

97 The EP has defined a set of assurance requirements that can be summarized as follows:

- 98 - Input that the product developer provides to evaluation labs, consisting of the  
99 product itself and a set of written artifacts such as design and specification  
100 documentation and testing results
- 101 - Actions that the evaluation lab must take, such as vulnerability assessment  
102 (including penetration testing) on the product, in order to ascertain that it actually  
103 satisfies the claimed security functional requirements  
104

105 The assurance PPs and EPs). The evaluator actions are necessary for obtaining independent  
106 assurance of CDD security. If none of the penetration attacks are successful and all other  
107 evaluator actions pass, the evaluation is successful. If not, the product and/or the documentation  
108 will have to be modified and the evaluation has to be repeated. This EP requires vulnerability  
109 assessment that emulates an “moderate attack potential” attacker. The definition for moderate  
110 attack potential can be found in CEM. It is also important to note that the authors of this EP

---

111 expect medical device developers to already have the vast majority of the aforementioned  
112 artifacts at their disposal due to adherence to IEC 62304 and its constituent standards. Thus,  
113 vulnerability assessment is expected to be the dominant additional burden needed to pass an  
114 evaluation.

DRAFT

---

## 115 2. CC Conformance

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

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

### 124 2.1 Assurance Package Claim

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

### 129 2.2 How to Use This Extended Package

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



---

### 138 3. Security Assurance Requirements

139 This section identifies the Security Assurance Requirements (SARs) to frame the extent to  
140 which the evaluator assesses the documentation applicable for the evaluation and performs  
141 independent testing.

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

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

154  
155 In order to make the CDD PP/EP/ST practical for evaluation of modern medical devices, it is  
156 acknowledged that evaluations must strive to balance the need for high assurance of protection  
157 via evaluation with the need to perform evaluations in a cost- and time-efficient manner to  
158 ensure market viability of devices and timely availability to users and patients. Indeed,  
159 application of the ISO 15408 standard in national security systems has been widely criticized  
160 of such an imbalance. It is unlikely that the use of this EP and derived STs for the evaluation  
161 of mass-market consumer medical devices will be mandated or even recommended if this  
162 balance is not properly struck.

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

#### 173 *DTSec Class C Assurance Package*

174 This assurance package is targeted at connected life-critical medical devices and must protect,  
175 at a minimum, against a moderate attack potential. The assurance package is defined by the  
176 assurance requirements listed in Table 3, including AVA\_VAN.4 and requirements associated  
177 with ST evaluation (class ASE). The extended requirement, IEC\_62304\_EXT, reflects the

178 package’s prerequisite for TOE developer’s IEC 62304 conformance and leverages the  
 179 documentation artifacts from this standard as primary input for evaluation and vulnerability  
 180 assessment. Table 2 (informative) illustrates the additional ISO 15408 assurance components  
 181 that are targeted by IEC\_62304\_EXT and map to components of the IEC 62304 standard and  
 182 its expected artifact outputs.

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

<i>Target ISO 15408 family and component</i>	<i>IEC 62304 coverage ([MED])</i>
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

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

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

208

209

210

*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

211

### 212 3.1 **Class ASE: Security Target**

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

### 214 3.2 **Class AVA: Vulnerability Assessment**

#### 215 3.2.1 **Vulnerability Survey (AVA\_VAN)**

##### 216 **Developer action elements:**

217 **AVA\_VAN.4.1D** The developer shall provide the TOE for testing.

##### 218 **Content and presentation elements:**

219 **AVA\_VAN.4.1C** The TOE shall be suitable for testing.

220 The TOE is evaluated as per AVA\_VAN.4 activities defined in [CEM] and [CC3].

### 221 3.3 **IEC\_62304\_EXT**

222 The *DTSec Class C* assurance package, to which this EP claims compliance, targets the ISO  
223 15408 components as described in Table 2. However, neither the assurance package nor this  
224 EP assert compliance to those components but rather aim to leverage the existing IEC 62304  
225 life cycle compliance artifacts, augmented by inclusion of security-specific principles, and to  
226 use those artifacts as the primary input for vulnerability assessment (AVA\_VAN.4).

227 For example, the objective of ATE\_2 is to determine whether the developer has tested all the  
228 TSF subsystems and modules against the TOE design and security architecture description.

---

229 The IEC 62304 testing artifacts should provide a mapping that demonstrates correspondence  
230 of tests that exercise the behavior of the TSF and TSFIs with the security design and  
231 architecture of the TOE. This mapping helps the evaluator perform AVA\_VAN.4 by making  
232 it easier to identify gaps or design weaknesses or areas that have been tested less rigorously  
233 and hence potential candidates for exploitable implementation flaws. If the IEC 62304 testing  
234 artifacts do not provide this mapping, then the evaluator may reject the vendor submission as  
235 insufficient for testing in order to ensure evaluation remains efficient and economical.  
236 However, for some TOEs, the evaluator may feel AVA\_VAN.4 can be performed without  
237 additional artifacts.

238 The remainder of this section is informative.

### 239 3.3.1 **ADV\_ARC.1**

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

242 The evaluator should use [CEM 11.3.1 – ADV\_ARC.1] as a guideline for evaluation.

### 243 3.3.2 **ADV\_FSP.5**

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

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

251

252 The evaluator should use [CEM 11.4.5 – ADV\_FSP.5] as a guideline for evaluation.

### 253 3.3.3 **ADV\_IMP.1**

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

255 The evaluator should use [CEM 11.5.1 – ADV\_IMP.1] as a guideline for evaluation.

### 256 3.3.4 **ADV\_INT.2**

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

---

262 **3.3.5 ADV\_TDS.3**

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

266 The evaluator should use [CEM 11.8.3 – ADV\_TDS.3] as a guideline for evaluation.

267 **3.3.6 AGD\_OPE.1**

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

270 The evaluator should use [CEM 12.3.1 – AGD\_OPE.1] as a guideline for evaluation.

271 **3.3.7 AGD\_PRE.1**

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

274 The evaluator should use [CEM 12.4.1 – AGD\_PRE.1] as a guideline for evaluation.

275 **3.3.8 ALC\_CMC.5**

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

277 The evaluator should use [CEM 13.2.5 – ALC\_CMC.5] as a guideline for evaluation.

278 **3.3.9 ALC\_CMS.5**

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

282 The evaluator should use [CEM 13.3.5 – ALC\_CMS.5] as a guideline for evaluation.

283 **3.3.10 ATE\_COV.2**

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

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

---

290 3.3.11 **ATE\_DPT.2**

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

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

297 3.3.12 **ATE\_IND.2**

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

300 The evaluator should use [CEM 14.6.2 – ATE\_IND.2] as a guideline for evaluation.