Global Platform®

The standard for secure digital services and devices

GlobalPlatform Technology

SESIP Profile for DTSec Connected Diabetes Device Platforms

Version 0.0.0.9

Public Review

October 2023

Document Reference: GPT_SPE_151

THIS SPECIFICATION OR OTHER WORK PRODUCT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE COMPANY, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER DIRECTLY OR INDIRECTLY ARISING FROM THE IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT.

Contents

Figures

Tables

1 INTRODUCTION

This SESIP profile describes the security requirements for the platform of a Connected Diabetes Device (CDD), so that the platform evaluation can be re-used in the evaluation of a CDD against the DTSec requirements as described in [DTSec PP].

Usage

Chapter 1 can be removed when this document is used as basis for a compliant Security Target (ST).

Informational notes may be copied from this profile into a compliant ST.

Application notes shall be copied from this profile into a compliant ST and shall be applied in the evaluation and certification of the ST and the platform.

Notes addressed to the ST writer are presented between angle brackets (i.e. “<>”) in roman letters (i.e. non-italic, so as not to mistake them with instantiations) and should be taken into account when writing an ST compliant to this profile, but not kept in the ST.

1.1 Audience

This document is intended primarily for the use of developers of CDDs and CDD platforms, evaluation laboratories, certification and approval bodies.

1.2 IPR Disclaimer

Attention is drawn to the possibility that some of the elements of this GlobalPlatform specification or other work product may be the subject of intellectual property rights (IPR) held by GlobalPlatform members or others. For additional information regarding any such IPR that have been brought to the attention of GlobalPlatform, please visit https://globalplatform.org/specifications/ip-disclaimers/. GlobalPlatform shall not be held responsible for identifying any or all such IPR, and takes no position concerning the possible existence or the evidence, validity, or scope of any such IPR.

1.3 References

The table below list references applicable to this profile. The latest version of each reference applies unless a publication date or version is explicitly stated.

Table 1-1: References

Standard / Specification	Description	Ref
Protection Profile for Connected Diabetes Devices	DTSec Protection Profile for Connected Diabetes Devices, v2.0, November 25, 2017	[DTSec PP]
GP_FST_070	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP)	[SESIP]
IEC 62304	IEC 62304 – Medical device software – Software lifecycle processes – Second edition	[IEC 62304]

1.4 Terminology and Definitions

Selected terms used in this document are included in Table 1-2.

Table 1-2: Terminology and Definitions

Term	Definition
Platform	In the context of this document, identical to Connected Platform, as defined in [SESIP].
SESIP Profile (SP)	A generic SESIP Security Target defining the SESIP requirements in terms of security features and evaluation activities to be addressed during the evaluation of a platform (part) of the type targeted by the profile.

1.5 Abbreviations

Table 1-3: Abbreviations

Abbreviation	Meaning
BG reading	Blood Glucose data acquired by the CDD device hardware
BGM	Blood Glucose Monitor
CDD	Connected Diabetes Device
CRC	Cyclic Redundancy Check
DTSec	Diabetes Technology Society cybersecurity standard for connected diabetes devices
SFR	Security Functional Requirement
ST	Security Target

1.6 Revision History

GlobalPlatform technical documents numbered *n*.0 are major releases. Those numbered *n*.1, *n*.2, etc., are minor releases where changes typically introduce supplementary items that do not impact backward compatibility or interoperability of the specifications. Those numbered *n.n*.1, *n.n*.2, etc., are maintenance releases that incorporate errata and clarifications; all non-trivial changes are indicated, often with revision marks.

Table 1-4: Revision History

Date	Version	Description
Feb 2021	1.0 draft	First official release by Silicon Labs / Brightsight BV
Nov 2022	0.0.0.3	Committee Review
Jun 2023	0.0.0.5	Member Review
Oct 2023	0.0.0.9	Public Review
month year	1.0	Initial Public Release

2 IDENTIFICATION

2.1 Identification of the Security Target

This section presents the identification information to be given in a Security Target that is compliant with GlobalPlatform *SESIP Profile for DTSec Connected Diabetes Device Platforms* ([Profile]).

<Provide here the title, version, and date of the Security Target.>

2.2 Identification of the Platform

The platform is uniquely identified by its chip (hardware) reference, its firmware and software as described below. The developer declares that only the successfully certified products identify in this way.

Table 2-1: Platform Identification

Reference	Value	Verification Method Described in:
Commercial name		
HW reference		
HW version		
FW name		
FW version		
SW name		
SW version		

2.3 Identification of the Guidance

<List here user and administrative manuals used for preparation and operation of the platform>

2.4 Documentation References

<List here all the documentation needed to comply with SESIP3 level>

Standard / Specification	Description	Ref
GPT_SPE_151	GlobalPlatform Technology SESIP Profile for DTSec Connected Diabetes Devices	[Profile]

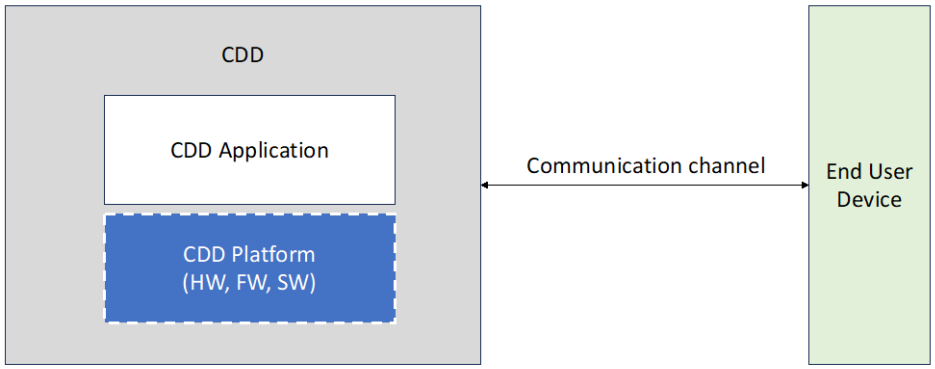
3 PLATFORM OVERVIEW

3.1 Platform Definition

The platform is the CDD platform depicted in Figure 3-1. It is composed of a combination of hardware, firmware and software that provides a runtime environment for the CDD application.

The platform implements all the security functionality defined in section 5.2 of this document. The platform is assumed to meet the applicable requirements of [IEC 62304] for this type of medical device.

Figure 3-1: CDD Platform and Environment



Non-platform components comprise:

- the CDD application which runs on top of the platform and processes BG readings, interacts with the user, etc. This is called the “application” in SESIP terms.
- and CDD non-platform hardware (cover, display, buttons, sensors, and other electronic components) required to provide the BG readings processing functions. This is thereafter called the local environment, or environment in short.

Application notes:

- The CDD developer may implement explicit user interaction which takes place (e.g. pressing a button) before the application calls a pairing function. This is optional in [DTSec PP].
- The CDD developer should make sure that the data coming out of the End User device (e.g. through a Bluetooth LE connection) that goes into the CDD application is sanitized before processing the data so that it cannot corrupt the application, e.g. by ensuring that:
  - The data is no longer than the application expects, possibly causing buffer overflows.
  - The data is no shorter than expected.
  - The data does not contain values the application does not understand (control characters, end-of-string markers in the middle of a string, etc.).
  - The data does not contain values that the application understands but may not be able to handle (e.g. choosing menu option #7 when there are only six menu options) for boundary conditions.

3.2 Use Case

<The Security Target must clearly identify the environmental conditions in which the TOE, due to its specific implementation, can be secured. In particular the Security Target must specify: 1) if the TOE can be accessed by untrusted users (in which case additional protection may be needed, e.g. physical protection), 2) if untrusted software can be installed and run on the TOE (in which case additional protection may be needed as well).>

3.3 Life Cycle

<The Security Target shall describe the life cycle of the CDD platform under evaluation.>

<The description must present an overview of the main phases from the hardware and software design to the product end-of-life; for each phase, all possible CDD platform state(s) must be identified. How transitions between those states are secured must also be explained.>

<The description must identify all Roots of Trust integrated into the CDD platform (e.g. for secure boot); for each RoT, it shall be specified in which phase and under which state the integration is performed, and how the integration is secured.>

<The description must include how the key provisioning is performed (directly in the ST or by referencing the appropriate guidance document).>

3.4 Threats

The following threats are extracted from [DTSec PP] and apply to the CDD and fully or partially to the platform. The platform security functionality is aimed to supporting the CDD to address them.

3.4.1 Network Attack (T.NETWORK)

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.

3.4.2 Physical Access (T.PHYSICAL)

The loss or theft of the CDD may give rise to unauthorized modification of critical data and CDD 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 CDD to remote devices, unauthorized physical access to printed or displayed unique serial numbers could be used to establish malicious (yet device-authenticated) remote connections.

3.4.3 Malicious Firmware or Application (T.BAD_SOFTWARE)

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.

3.4.4 Malicious Peer Device (T.BAD_PEER)

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

3.5 Platform Security Features

The main security features of the platform are:

- Secure boot, to control the platform's initialization sequence.
- Secure debugging in case of investigation need.
- Secure update for platform life cycle handling.
- Secure Communication.
- Secure Trusted Storage of sensitive data.
- Cryptographic support.

4 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

For the platform to fulfill its security requirements, the operational environment (technical or procedural) shall fulfill the following objectives:

- The CDD developer is expected to follow the platform's security guidance in <*Reference*>.
- The CDD developer is expected to make use of the <*Name of the secure boot*> feature as described in the <*Reference to documentation where this is described*>.
- The CDD developer is expected to configure the debug functionality as described in <*Reference to documentation where this is described*> to meet the extra physical attacker resistance if required.
- If no physical protection SFR is claimed, the user shall exercise precaution to protect physical access to the platform.
- The operational environment shall not allow the deployment of untrusted code. That means that all code running on the CDD is known to the CDD vendor and the CDD vendor can confirm that the code cannot harm the claimed security functionalities.
- The CDD developer shall disable debugging functionality using the <*required configuration*>.

More specifically, a CDD developer shall follow the security guidance in <*Reference*>:

- To ensure the integrity and authenticity of sensitive data (e.g. BGM readings).
- To extend the checking of the platform authenticity and integrity to the CDD Application.

5 SECURITY REQUIREMENTS

<The platform claiming conformance to this profile shall meet the assurance requirements identified in section 5.1 and the functional requirements described in section 5.2. This is the bare minimum intended to provide a base platform ready to implement the security requirements of DTSec in a CDD solution.>

<Optionally, the ST author can also select SFRs described in section 5.3 to be included in the platform scope to demonstrate readiness regarding a subset of the optional requirements of [DTSec PP].>

<The requirements defined in section 5.4 can be also included although they go beyond the requirements defined in [DTSec PP].>

5.1 Security Assurance Requirements

The security assurance requirements of **SESIP3** apply.

5.2 Mandatory Security Functional Requirements

5.2.1 Verification of Platform Identity

The platform provides a unique identification of the platform, including all its parts and their versions.

5.2.2 Secure Update of Platform

The platform can be updated to a newer version in the field such that the <*confidentiality,*> integrity and authenticity of the platform is maintained.

Application note: This requirement can only be removed (use strike-through) when in ALC_FLR.2 a strong argumentation is provided why updates are not necessary for this kind of device.

5.2.3 Secure Initialization of Platform

The platform ensures its integrity and authenticity during platform initialization. If the platform integrity or authenticity cannot be ensured, the platform will go to <*list of controlled states*>.

Extension: Note that for the purpose of meeting DTSec, this checking shall be extended to the BGM Application as well. The platform shall therefore also check the BGM application's integrity and authenticity.

5.2.4 Secure Debugging

The platform only provides <*list of endpoints*> authenticated as specified in <*specification*> with debug functionality.

The platform ensures that all user data stored, with the exception of <*list of exceptions*>, is made unavailable.

Application note: If debug features are available after the final product is delivered to the end-user, this SFR shall be used. If debug features are not available after the final product is delivered to the end-user, this SFR shall be struck through to indicate this (this fulfils the profile requirements). Any guidance instructing the user of the platform, i.e. the integrator, to disable debug functionality in the production steps, must be documented as a security objective for the operational environment with specific reference to where in the guidance this is described.

5.2.5 Secure Communication Support

The platform provides one or more secure communication channel(s).

The secure communication channel authenticates **End User Device** and protects against <*disclosure,*> **modification and replay** of messages between the endpoints, using <*list of protocols and measures*>.

5.2.6 Secure Communication Enforcement

The platform ensures that communication with the **End User Device** can only be done over the secure communication channel(s) supported by the platform using <*list of protocols and measures*>.

5.2.7 Secure Trusted Storage

The platform ensures that all user data stored, except for <*list of data stored in plaintext*>, is protected to ensure its integrity, authenticity, and binding to the platform instance.

Application note: The intent is that digital signatures or message authentication codes, in combination with immutable firmware that validates them, are used to protect the safety of critical user data (e.g. BG readings). Signatures should 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.

5.2.8 Cryptographic Operation

The platform provides <*encryption, decryption, signing, signature verification, MAC generation and verification*> functionalities with <*list of algorithms*> as specified in <*specification*> for key lengths <*list of key lengths*> and modes <*list of modes*>.

Application note: The key sizes shall be such that a security level of at least 128 bits is reached as per current state of the art.

Application note: *none* is an acceptable value of cryptographic functionality. This case cancels this SFR (assuming secure trusted storage and secure communication is enforced).

Note: Encryption/decryption goes beyond [DTSec PP], which does not require confidentiality protection of stored data.

5.2.9 Cryptographic Key Generation

The platform provides a way to generate cryptographic keys for use in <*list of cryptographic algorithms*> as specified in <*specification*> for key lengths <*list of key lengths*>.

Application note: *none* is an acceptable value of list of algorithms. This case cancels this SFR.

5.2.10 Cryptographic KeyStore

The platform provides a way to store <*list of assets, such as cryptographic keys and passwords*> such that not even the application can compromise the <*selection: confidentiality, integrity, authenticity*> of this data. This data can be used for the cryptographic operations <*list of operations*>.

Application note: *none* is an acceptable value of list of assets. This case cancels this SFR.

Application note: *none* is also an acceptable value of list of operations. This case does not cancel the SFR.

5.2.11 Cryptographic Random Number Generation

The platform provides a way based on <*list of entropy sources*> to generate random numbers to as specified in <*specification*>.

5.3 Optional SFRs from DTSec Protection Profile

<The following optional SFRs can be added to cover the optional SFR “TSF Physical Protection (FPT_PHP)” of [DTSec PP].>

5.3.1 Physical Attacker Resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises any of the other security functional requirements.

5.3.2 Limited Physical Attacker Resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises *<list of security functional requirements>*.

5.4 Other Optional SFRs Commonly Added

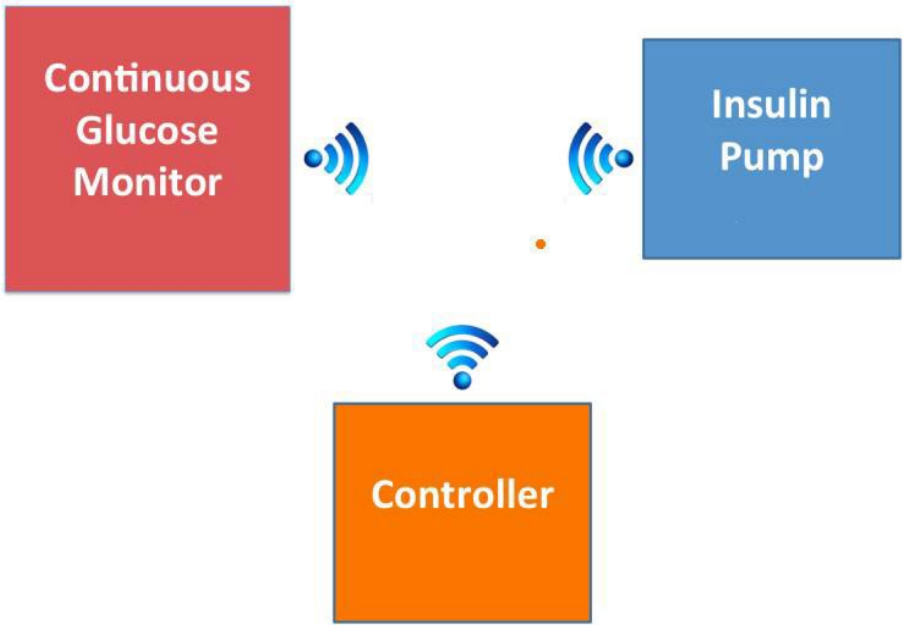
<Below is a list of additional SFRs that the platform developer can optionally include in the platform scope. These requirements do not model mandatory functionality described in [DTSec PP], but the optional requirements may be beneficial for the CDD platform and to the final product including the CDD Application. This chapter supplements these requirements by a number of optional requirements.>

5.4.1 Software Attacker Resistance: Isolation of Platform Parts

The platform provides isolation between platform parts, such that an attacker able to run code in **the networking part** cannot compromise <*confidentiality and*> integrity of **all other parts** nor the provision of any other Security Functional Requirements.

Informational note: This SFR should be claimed **only** when there are physically separated parts of the platform that are connected through a network protocol. The SFR would apply to a scenario equivalent to Figure 5-1.

Figure 5-1: One Potential Closed Loop AP System Consisting of Three Parts of the Platform



5.4.2 Secure Update of Application

The application can be updated to a newer version in the field such that the <*confidentiality,*> integrity and authenticity of the application is maintained.

5.4.3 Verification of Platform Instance Identity

The platform provides a unique identification of that specific instantiation of the platform, including all its parts.

5.4.4 Attestation of Platform Genuineness

The platform provides an attestation of the “Verification of Platform Identity” and “Verification of Platform Instance Identity”, in a way that ensures that the platform cannot be cloned or changed without detection.

5.4.5 Attestation of Application Genuineness

The platform provides an attestation of the application, in a way that ensures that the application has not been cloned or changed without detection.

5.4.6 Factory Reset of Platform

The platform can be reset to the state in which it exists when the product embedding the platform is delivered to the user, before any personal user data, user credentials, or user configuration is present on the platform.

5.4.7 Decommission of Platform

The platform can be decommissioned.

5.4.8 Residual Information Purging

The platform ensures that <*list of data*>, with the exception of <*list of data that is not erased automatically*>, is erased using the method specified in <*specification*> before the memory is used by the platform or application again and before an attacker can access it.

<This requirement goes beyond [DTSec PP], which does not require stored data confidentiality.>

6 MAPPING AND SUFFICIENCY RATIONALES

6.1 Security Assurance of SESIP3

Table 6-1: Assurance

Assurance Class	Assurance Families	Covered by	Rationale
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	Introduction	
	ASE_OBJ.1 Security requirements for the operational environment	Security objectives for the operational environment	The objectives for the operational environment refers to the guidance documents.
	ASE_REQ.3 Listed Security requirements	Security Requirements	All SFRs in the profile are taken from [SESIP].[1] "Verification of Platform Identity" is included. "Secure Update of Platform" is included.
	ASE_TSS.1 TOE Summary Specification	Security Requirements	
ADV: Development	ADV_FSP.4 Complete functional specification	Functional specification as specified in "Security Target defined"	
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs		
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	Guidance defined in "Identification of the guidance"	
	AGD_PRE.1 Preparative procedures	Guidance defined in "Identification of the guidance"	
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE	Configuration list as specified in "Security Target defined"	
	ALC_CMS.1 TOE CM Coverage	Configuration list as specified in "Security Target defined"	

[1] The developer must not remove or substantially change the SFRs listed in the profile, and must indicate any additional SFRs explicitly. The evaluator must check this in accordance to the assurance activity.

Assurance Class	Assurance Families	Covered by	Rationale
	ALC_FLR.2 Flaw reporting procedures	Flaw remediation procedures as specified in "Security Target defined"	
ATE: Tests	ATE_IND.1 Independent testing: conformance		
AVA: Vulnerability Assessment	AVA_VAN.3 Focused vulnerability analysis		

6.2 Functionality

Table 6-2: Functionality

[DTSec PP]	Covered by SESIP	Rationale
FTP_ITC.1	Secure Communication Support Secure Communication Enforcement	Full coverage by direct translation.
FIA_NET_EXT.1.1	None	This is a typical requirement for the CDD, rather than the CDD platform alone.
FDP_IFC.1		
FDP_IFF.1		
FDP_DAU.1	Secure Storage	The CDD will process BG readings and/or store them. This requirement ensures that these readings cannot be modified while stored without this being noticed.
FPT_TST_EXT.1	Secure Initialization of Platform	For the purpose of meeting DTSec, this checking shall be extended to the CDD Application as well. The platform shall therefore offer this functionality to the CDD Developer and describe how to do this in the developer's Guidance.
FCS_COP.1	Cryptographic Operation, iterated for: • Communication • Platform, Application, and BG Readings Integrity • Cryptographic Key Generation	Full coverage by direct translation.
FCS_COP_EXT.1	Cryptographic Random Number Generation	Full coverage by direct translation.

[DTSec PP]	Covered by SESIP	Rationale
FIA_AFL.1 (optional)		In this profile, the CDD Platform does not provide user authentication (which is associated with the CDD Application).
FIA_UAU.1 (optional)		
FIA_UAU.6 (optional)		
FPT_PHP.3 (optional)	Physical Attacker Resistance Limited Physical Attacker Resistance	Depending on the nature of the CDD Platform, the Platform may provide a different level of physical protection.