IEEE SA
STANDARDS ASSOCIATION

IEEE/UL Standard for Wireless Diabetes Device Security: Information Security Requirements for Connected Diabetes Solutions

STANDARDS

IEEE Engineering in Medicine and Biology Society

Developed by the
IEEE Engineering in Medicine and
Biology Standards Committee

IEEE Std 2621.2™-2022/UL 2621-2:2022

IEEE

IEEE/UL Standard for Wireless Diabetes Device Security: Information Security Requirements for Connected Diabetes Solutions

Developed by the

IEEE Engineering in Medicine and Biology Standards Committee
of the
IEEE Engineering in Medicine and Biology Society

Approved 25 March 2022

IEEE SA Standards Board

Recognized as an American National Standard

Abstract: A framework for a connected electronic product security evaluation program, with specific requirements and guidance relating to digital diabetes devices and solutions, such as insulin pumps is defined in this standard.

Keywords: assurance, diabetes, devices, evaluator, firmware, IEEE 2621.1™, protection profile, security, security target

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

ULSE Inc.
333 Pfingsten Road
Northbrook, IL 60062

PDF: ISBN 978-1-5044-8582-1 STD25339
Print: ISBN 978-1-5044-8583-8 STDPD25339

Commitments for amendments

This Standard is issued jointly by the Institute of Electrical and Electronics Engineers, Inc. (IEEE) and ULSE Inc. (ULSE) Comments or proposals for revisions or any part of the standard may be submitted to IEEE and/or ULSE at any time. Revisions to this Standard will be made only after processing according to the Standards development procedures of IEEE and ULSE.

Comments or proposals for revisions on any part of the Standard may be submitted to ULSE Inc. at any time. Proposals should be submitted via a Proposal Request in ULSE's On-Line Collaborative Standards Development System (CSDS) at https://csds.ul.com.

Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the IEEE SA myProject system.[1] An IEEE Account is needed to access the application.

Comments on IEEE standards should be submitted using the Contact Us form.[2]

Copyrights

Important Notices and Disclaimers Concerning IEEE Standards Documents

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

[1] Available at: https://development.standards.ieee.org/myproject-web/public/view.html#landing.
[2] Available at: https://standards.ieee.org/content/ieee-standards/en/about/contact/index.html.

are not necessarily members of IEEE or IEEE SA, and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents**.

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and Standards Coordinating Committees are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; https://www.copyright.com/. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore or contact IEEE.[3] For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website.[4] Search for standard number and year of approval to access the web page of the published standard. Errata links are located

[3] Available at: https://ieeexplore.ieee.org/browse/standards/collection/ieee.
[4] Available at: https://standards.ieee.org/standard/index.html.

under the Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata.

Patents

IEEE Standards are developed in compliance with the IEEE SA Patent Policy.[5]

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at https://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

[5] Available at: https://standards.ieee.org/about/sasb/patcom/materials.html.

Participants

At the time this IEEE standard was completed, the Healthcare Device Security Assurance Working Group had the following membership:

David Klonoff, *Chair*
David Kleidermacher, *Co-Chair*

Aiman Abdel-Malek
Carole C. Carey
Kong Chen
Sean Donahue
Anura Fernando
Brian Fitzgerald
Barry Ginsberg
Julia Han
Diana Pappas Jordan
Christopher Keegan
Kevin T Nguyen
Naomi Schwartz
Patricia Sena
Trisha Shang
Christine Sublett
Nicole Y Xu
Jennifer Y. Zhang
Margie Zuk

The following members of the individual Standards Association balloting group voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Pradeep Balachandran
Brian Blum
Carole C. Carey
Diego Chiozzi
Todd Cooper
Werner Hoelzl
Piotr Karocki
Edmund Kienast
David Kleidermacher
David Klonoff
Ting Li
Rajesh Murthy
Esteban Pino
Naomi Schwartz
Walter Struppler

When the IEEE SA Standards Board approved this standard on 25 March 2022, it had the following membership:

David J. Law, *Chair*
Ted Burse, *Vice Chair*
Gary Hoffman, *Past Chair*
Konstantinos Karachalios, *Secretary*

Edward A. Addy
Ramy Ahmed Fathy
J. Travis Griffith
Guido R. Hiertz
Yousef Kimiagar
Joseph L. Koepfinger*
Thomas Koshy
John D. Kulick
Johnny Daozhuang Lin
Kevin Lu
Daleep C. Mohla
Andrew Myles
Damir Novosel
Annette D. Reilly
Robby Robson
Jon Walter Rosdahl
Mark Siira
Dorothy V. Stanley
Lei Wang
F. Keith Waters
Karl Weber
Sha Wei
Philip B. Winston
Daidi Zhong

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 2621.2-2022/UL 2621-2:2022, IEEE/UL Standard for Wireless Diabetes Device Security: Information Security Requirements for Connected Diabetes Solutions.

Target of Evaluation (TOE) overview

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

Figure 1—Network operating environment for a glucose monitor the Target of Evaluation

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

Examples of a CDD that should conform to this standard include simple BGM, more sophisticated BGMs, e.g., with larger displays and audio functions, CGMs, remote controllers of other CDDs, and insulin pumps. An AID system Target of Evaluation (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):

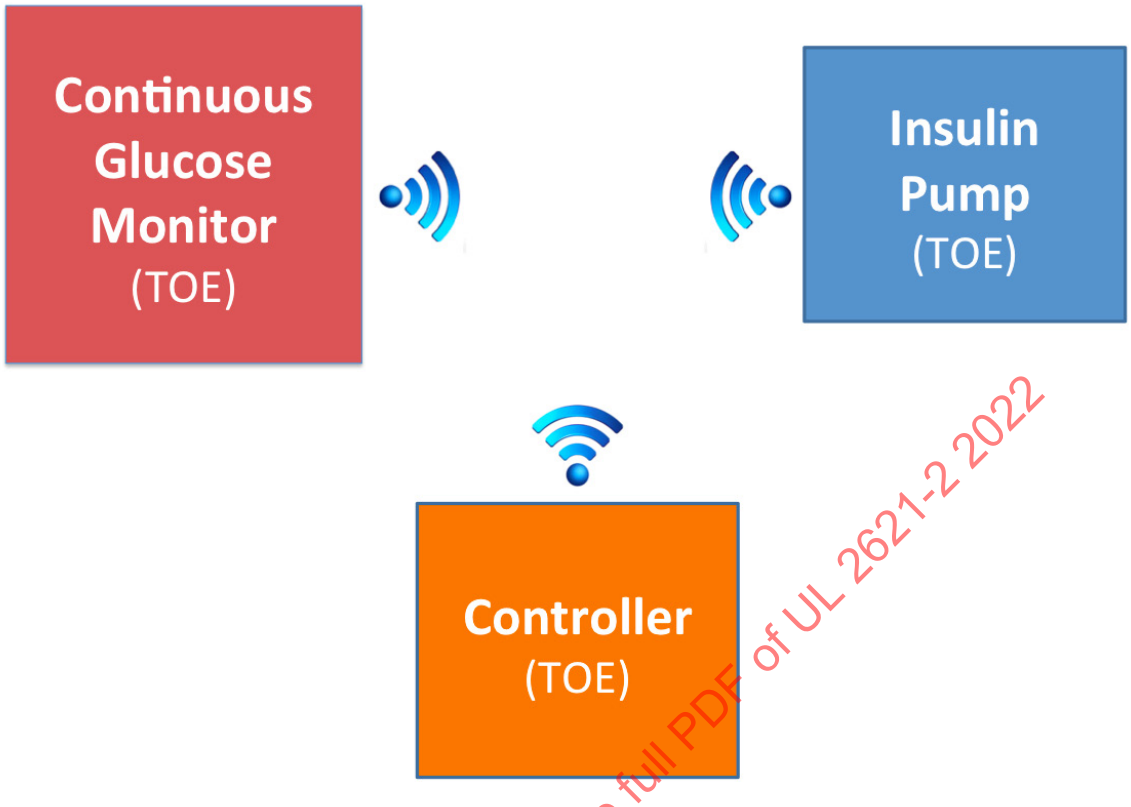

Figure 2—One potential AID system consisting of 3 TOEs, each applicable to this protection profile

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 should be adequately protected. Additional security features such as firmware and safety-critical user data integrity protection should be implemented in order to address threats.

In order to make this standard practical for evaluation of modern medical devices, this standard and associated security targets (STs) and evaluations strive to balance the need for high assurance of protection via evaluation with the need for safer clinical operation, market viability of devices, and timely availability to users and patients. Use of this standard and derived STs for the evaluation of mass-market consumer medical devices should not 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 should not interfere with safe clinical use. Furthermore, biometrics and other authentication mechanisms may be resource prohibitive for certain classes of CDDs. For this version of the standard for CDDs, developers are encouraged to consider safer and more effective user authentication methods, but this is not currently mandated 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 should satisfy the requirements in this standard (and derived ST) and should be evaluated independently against its ST. Note that this standard does not necessarily assume that devices authenticated and connected to the TOE are trustworthy. The ST developer should specify the

network information flow security function policy (SFP) [see requirements in the FDP_IFC and FDP_IFF families in this protection profile (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 should reduce the risk that a malicious smartphone (e.g., one that has been commandeered by malware from an open app store or downloaded from another source) can 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 an AID system), then the safety-relevant portions of the smartphone (hardware, software) would be in scope for evaluation and should be sufficiently protected from non-safety relevant portions of the smartphone. The precise specification of the scope, evaluation boundary, and security requirements should be codified in the ST.

This 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 establish 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.

Requirements summary for non-technical audiences

This section summarizes the security requirements of this standard 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.

With the diverse environments where CDDs are used and the varied mechanisms employed to manage safer operation and protection of sensitive data, this standard aims to identify the potential security threats and risks faced by these devices and then present the functional requirements that counter these threats and thereby help reduce or help minimize risk.

Security functional requirements summary

The standard has defined a set of mandatory security functional requirements (SFRs), grouped according to related function or purpose, that can be summarized as follows:

— *Integrity protection for CDD firmware/software*
This requirement answers the question: "How can one 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 does one 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 can one verify that only authorized devices can communicate with the CDD and only in authorized ways?" Examples may include: a remote device, controlled by an attacker, should be prevented 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 should provide that the remote device is only able to communicate to the CDD

in prescribed ways. Another example may include that 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 could 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 standard 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) can help to ensure 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 should 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, this requirement is 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 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 preventing an attacker from using 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 standard does not include requirements associated with confidentiality protection of user data, such as BG readings, stored within CDDs. One consensus is that privacy concerns may better be relegated to back-end systems (e.g., cloud) where this data is aggregated and processed rather than the CDDs themselves. This standard recognizes but does not intend to restate or replace applicable laws and regulations regarding data privacy and security. Users of this standard are responsible for referring to and observing all such laws and regulations. Compliance with the provisions of this standard does not imply compliance with any applicable legal or regulatory requirements.

Multi-part standard

This standard is a multi-part standard consisting of the following parts:

— IEEE Std 2621.1™/UL 2621-1:2022 (connected electronic product security evaluation programs)

— IEEE Std 2621.2™/UL 2621-2:2022 [information security requirements for connected diabetes solutions (this part)]

— IEEE Std 2621.3™/UL 2621-3:2022 (use of mobile devices in diabetes control contexts)

Contents

IEEE Standard for Wireless Diabetes Device Security: Information Security Requirements for Connected Diabetes Solutions

1. Overview

1.1 Scope

This standard describes the security functional requirements (SFRs), which compose a protection profile (PP), for connected diabetes devices (CDDs). The scope of the PP within the development and evaluation process is described in ISO/IEC 15408.[1] In particular, a PP defines the IT security requirements of a generic type of Target of Evaluation (TOE) and specifies the security measures to be offered by that TOE to meet stated requirements.

1.2 Purpose

The purpose of this standard is to define the SFRs for CDDs as deemed necessary and sufficient by an appropriate set of stakeholders. These requirements are intended to be used within a security evaluation program, as defined in other components of this multi-part standard.

1.3 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals is *required to*).[2,3]

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals is *recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals is *permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals is *able to*).

[1] Information on references can be found in Clause 2.
[2] The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations.
[3] The use of *will* is deprecated and cannot be used when stating mandatory requirements, *will* is only used in statements of fact.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

ISO/IEC 15408-1:2009—Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model.[4]

ISO/IEC 15408-2:2008—Information technology—Security techniques—Evaluation criteria for IT security—Part 2: Security functional components.

ISO/IEC 15408-3:2008—Information technology—Security techniques—Evaluation criteria for IT security—Part 3: Security assurance components.

ISO/IEC 18045, Information technology—Security techniques—Methodology for IT security evaluation.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.[5]

administrator: The administrator is responsible for management activities, including setting the policy that is applied by the service provider, on the device. If the security policy is defined during manufacturing and never changed, then the developer acts as administrator. If management activities can be performed by the user, then the user may also act as administrator.

assurance: Grounds for confidence that a Target of Evaluation (TOE) meets its security functional requirements (SFRs).

connected diabetes device (CDD): Any type of digital diabetes product whose security requirements are compatible with this standard [including but not limited to blood glucose meters (BGMs), continuous glucose monitors (CGMs), insulin pumps, and automated insulin dosing (AID) systems].

developer: The entity that brings to market a solution to which this standard applies; while the traditional developer in this sense is a medical device manufacturer, the entity may be some other systems integrator or service provider that is responsible for the safe and secure development and market deployment of the solution.

evaluator: Independent testing laboratory that evaluates the TOE against its security target (ST) by analyzing documentation and performing activities such as vulnerability assessment.

immutable firmware: Firmware that cannot, by design, be modified through unauthorized means. Examples of immutable firmware may include firmware written to read-only memory (ROM) or electrically erasable programmable read-only memory (EEPROM) whose re-programmability is protected against unauthorized use.

protection profile (PP): A set of standardized security requirements for a product class, such as connected diabetes devices.

[4] ISO/IEC publications are available from the ISO Central Secretariat (http://www.iso.org/). ISO/IEC publications are available in the United States from the American National Standards Institute (http://www.ansi.org/).
[5] *IEEE Standards Dictionary Online* is available at: http://dictionary.ieee.org. An IEEE Account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

security functional requirement (SFR): A translation of the security objectives for the Target of Evaluation (TOE) into a standardized language.

security Target (ST): The manifestation or mapping of protection profile (PP) requirements for a specific, individual electronic product, for example a specific version/SKU of a manufacturer's insulin pump. An ST may also cover multiple, similar instances (e.g., a product family with common security requirements).

security target assessment (ASE): Assurance requirements class defined by ISO/IEC 15408 standard—this class pertains to the security evaluation of security targets (STs).

Target of Evaluation (TOE): A set of software, firmware and/or hardware possibly accompanied by guidance.

Target of Evaluation (TOE) security functionality: A set consisting of all hardware, software, and firmware of the TOE that shall be relied upon for the correct enforcement of the security functional requirements (SFRs).

user: An authorized operator of the Target of Evaluation (TOE). For a diabetes device, 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 in this case. An authorized user is assumed to be able to access any of the device's documented user interfaces.

3.2 Acronyms and abbreviations

AID	automated insulin dosing
ASE	security target assessment
AVA	active vulnerability assessment
BG	blood glucose
BGM	blood glucose meter
CDD	connected diabetes device
CGM	continuous glucose monitor
PP	protection profile
SAR	security assurance requirement
SFP	security function policy
SFR	security functional requirement
ST	security target
TOE	Target of Evaluation
TSF	target of security functionality

4. Conformance

This clause specifies the mandatory and optional capabilities provided by conformant implementations of this standard.

4.1 Use of ISO/IEC 15408

This standard conforms to the requirements of ISO/IEC 15408, third edition. The requirements compose a PP that is ISO/IEC 15408-2:2008 extended and ISO/IEC 15408-3:2008 extended. The methodology applied for the PP evaluation is defined in ISO/IEC 18045.

STs applicable to this standard shall be evaluated and accepted by the scheme. STs may be published or kept confidential, depending on market demands.

This standard shall be applied by the scheme, leveraging scheme-accredited test labs to perform security evaluations for products or components of products against an appropriate ST. After a lab deems a product has passed its evaluation, the evaluation results shall be submitted to the scheme for certification. A certified product or component implies no further claims beyond this evaluation result. In particular, the accreditation of products by regulatory bodies or any decisions by consumers to use an evaluated product is beyond the scope of this standard.

4.2 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.
- ~~Strikethrough text~~ indicates text removed as a rrefinement.

Per ISO/IEC 15408 conventions, the protection profile security problem definition can be found in Annex A, security objectives in Annex B, and rationale in Annex C.

4.3 Mandatory security functional requirements (SFRs)

4.3.1 Cryptographic operation (FCS_COP)

FCS_COP.1	Cryptographic operation

FCS_COP.1.1 The TOE Security Functionality (TSF) shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

NOTE—Intent is for compliance to widely used algorithm standards, such as NIST FIPS PUB 197 [B4], PKCS #1 [B9], PKCS #3 [B8], NIST FIPS PUB 186-3 [B3], ISO/IECIS 19790 [B1], and NIST FIPS 140-2 [B2].[6] Beyond algorithms, an ST should include key management guidance standards, such as NIST SP800-57 [B6] and NIST SP800-56 [B5] series, for example so that key strength is appropriate for intended TOE in-field service life. These requirements should be met where practically feasible, for example for any software cryptographic modules selected by the developer in implementing the TSF.

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

NOTE—Current widely used algorithm validation schemes may not validate entropy source quality, hence the need for an extended requirement. At a minimum, random bit generators (RBGs) require seeding with entropy at least equal to the greatest security strength of the keys and hashes that it will generate.[7]

4.3.2 Network authorization and authentication (FIA_NET)

FIA_NET_EXT.1	Extended: Network connection authorization

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

NOTE—This requirement is intended for networks that offer user authorization for connection associations. In such cases, explicit user interaction with the TOE may be required to permit the creation of the association and prevent software from programmatically creating an authorized association. The ST developer rationalizes how the user authorization (possibly combined with trusted channel authentication mechanism from FTP_ITC) is of sufficient strength for the selected networking technology.

4.3.3 Data authentication (FDP_DAU)

FDP_DAU.1	Basic data authentication

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

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

NOTE—The intent is that digital signatures or message authentication codes, in combination with immutable firmware that validates them, are used to cover the safety critical user data (e.g., BG readings). Signatures 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.

4.3.4 Information flow control policy (FDP_IFC)

FDP_IFC.1	Subset information flow control

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

[6] The numbers in brackets correspond to those of the bibliography in Annex D.
[7] Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

4.3.5 Information flow control functions (FDP_IFF)

FDP_IFF.1	Simple security attributes

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

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

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

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

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

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

4.3.6 TSF integrity checking (FPT_TST)

FPT_TST_EXT.1	Extended: TSF integrity checking

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

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

4.3.7 Inter-TSF trusted channel (FTP_ITC)

FTP_ITC.1	Inter-TSF trusted channel

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

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

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

NOTE—For example, for IEEE 802.15.4™, the combination of security mode 1 and security level 3 may be used to meet these requirements, based on IEEE 802.15.4™'s glucose profile as well as guidance from NIST SP800-121 [B7]. The ST developer specifies the TOE communications mechanism and argues why the authentication and encryption mechanism is of sufficient strength to protect the communication channel against unauthorized access.

4.4 Optional security functional requirements (SFRs)

4.4.1 Authentication failures (FIA_AFL)

FIA_AFL.1	**OPTIONAL: Authentication failure handling**

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

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

NOTE—The corrective action should carefully weigh the desire to protect against unauthorized access with the requirement to provide safety-critical function to the user. The ST developer specifies and rationalizes the choice. The counter of unsuccessful attempts cannot be reset when the device is powered off.

4.4.2 User authentication (FIA_UAU)

FIA_UAU.1	**OPTIONAL: Timing of authentication**

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

NOTE—User authentication should not get in the way of life-critical operation. The ST specifies which operations are explicitly allowed without user authentication.

FIA_UAU.6	**OPTIONAL: Re-authenticating**

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

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

4.4.3 TSF Physical protection (FPT_PHP)

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

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

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

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

4.5 Security assurance requirements (SARs)

This standard defines three custom assurance packages (basic, enhanced-basic, and moderate), one of which shall be selected by the ST author in combination with the SFRs described in this standard. Each package composes security assurance requirements (SARs) to frame the extent to which the evaluator assesses the documentation applicable for the evaluation and performs independent testing.

The basic package is intended only as a developer (rather than lab) affirmation of conformance to the SFRs specified in the ST.

The general model for evaluation of TOEs against STs written to conform to either the enhanced-basic or moderate packages is as follows:

— After the ST has been approved for evaluation, the evaluator shall obtain the ST, TOE, supporting environmental IT, the administrative/user guides for the TOE, and any other artifacts that will assist the evaluator in determining conformance to this standard. These artifacts may include architecture description, specification, design, testing, configuration management, and user documentation.

— The evaluator shall perform actions mandated by the Common Evaluation Methodology (ISO/IEC 18045) for applicable SARs.

— The evaluator shall perform any other additional assurance activities that the evaluator deems necessary in order to achieve sufficient confidence in product conformance to this standard and the product's ST.

4.5.1 Basic package SARs

4.5.1.1 Security target (ST)

The ST should be evaluated as per security target assessment (ASE) activities defined in ISO/IEC 18045.

An evaluator should perform a minimal audit with the developer to establish the product's capabilities are compatible with the ST. An evaluator may perform testing to establish product compliance to the ST, but selection of this package is not intended to require that the developer incur lab costs. The scheme may perform minimal auditing of the ST and developer prior to including the product in its basic package products listing.

4.5.2 Enhanced-basic package SARs

4.5.2.1 Security target assessment (ASE)

The ST should be evaluated as per ASE activities defined in ISO/IEC 18045

4.5.2.2 Vulnerability Survey (AVA_VAN)

Developer action elements:

AVA_VAN.3.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.3.1C The TOE shall be suitable for testing.

The TOE shall be evaluated as per AVA_VAN.3 activities defined in ISO/IEC 18045 and ISO/IEC 15408-3:2008.

4.5.3 Moderate package SARs

4.5.3.1 Security target assessment (ASE)

The ST should be evaluated as per ASE activities defined in ISO/IEC 18045

4.5.3.2 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 shall be evaluated as per AVA_VAN.4 activities defined in ISO/IEC 18045 and ISO/IEC 15408-3:2008.

Annex A

(informative)

Security problem definition

A.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 standard are those of network eavesdropping, network attacks, physical access, and malicious or flawed software, as detailed in the following sections. Of note, this standard primarily considers threats that could impact 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, the goal is to protect the integrity of this user data. Another way to look at this standard'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 considered security-critical in that threats should not add undue risk to safety.

A.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.

A.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.

A.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 could have been prevented.

A.1.4 T.BAD_PEER (Malicious peer device)

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