IEEE SA
STANDARDS
ASSOCIATION

# IEEE/UL Standard for Wireless Diabetes Device Security Assurance Evaluation: Connected Electronic Product Security Evaluation Programs

IEEE Engineering in Medicine and Biology Society

Developed by the
IEEE Engineering in Medicine and
Biology Standards Committee

**IEEE Std 2621.1™-2022/UL 2621-1:2022**

STANDARDS

# IEEE/UL Standard for Wireless Diabetes Device Security Assurance Evaluation: Connected Electronic Product Security Evaluation Programs

Developed by the

**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 assurance evaluation program, with specific requirements and guidance relating to digital diabetes devices and solutions, such as insulin pumps is described 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 978-1-5044-8580-7 STD25338
Print: ISBN 978-1-5044-8581-4 STDPD25338

*IEEE prohibits discrimination, harassment, and bullying.*
*For more information, visit https://www.ieee.org/about/corporate/governance/p9-26.html.*

## 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

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

UL's Standards for Safety are copyrighted by ULSE Inc. Neither a printed nor electronic copy of a Standard should be altered in any way. All of UL's Standards and all copyrights, ownerships, and rights regarding those Standards shall remain the sole and exclusive property of ULSE Inc.

To purchase UL Standards, visit ULSE's Standards Sales site at:

http://www.shopulstandards.com/HowToOrder.aspx or call toll-free 1-888-853-3503.

## Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (https://standards.ieee.org/ipr/disclaimers.html), appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents."

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

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied

[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.

viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers 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.

[3] Available at: https://ieeexplore.ieee.org/browse/standards/collection/ieee.

## 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 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.

[4] Available at: https://standards.ieee.org/standard/index.html.
[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,** *Co-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
Karl Weber

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 2621.1-2022/UL 2621-1:2022, IEEE/UL Standard for Wireless Diabetes Device Security Assurance Evaluation: Product Security Evaluation Programs.

Today, with few exceptions, wireless digital [aka Internet of Things (IoT)] devices are generally not subjected to an independent security evaluation that could provide grounds for confidence to the device's users and other applicable stakeholders (e.g., insurers). The lack of independent security evaluation is one of the leading causes of IoT insecurity we observe today. In an illustrative example, attackers commandeered Internet-connected webcams, digital video recorders, printers, digital receivers, and routers, leveraging their security vulnerabilities to convert them into a powerful botnet that launched successful Internet distributed denial of service. Because these devices were not held to a minimum security standard, they lacked the basic security hygiene of proper authentication and in-field security patching. These kinds of failures put users and data at risk. The path forward is quite simple: the IoT needs a security evaluation program for these devices. While financial smartcards, mobile devices, and other products used by government agencies enjoy security evaluation programs, the vast majority of the IoT, including wireless medical devices, lacks such a comprehensive program that is institutionalized as part of product development, go-to-market, and regulatory approval processes (where applicable). Furthermore, some government security evaluation programs have suffered from inefficiency, making them inappropriate for the fast pace of IoT technological innovation. While government and regulatory entities may leverage and even mandate the use of other security standards, the intent of this standard is to define a security assurance evaluation program that is managed by independent, international industry standards and certification bodies.

## Audience and stakeholders

The following groups are the intended audience for this standard and have the following roles and responsibilities with respect to the standard, as follows:

a) Operators of product security assurance testing programs (called "schemes")

A "scheme" is an organization that manages a security assurance evaluation program described by this standard. The scheme may be an independent non-profit, a certification body (government or non-governmental organization), or any other group that is able to perform the tasks associated with managing an evaluation program described herein. For example, the scheme is responsible for determining which laboratories are appropriate for performing the testing needed for particular product families.

b) Government regulatory authorities

This standard recognizes, but does not intend to restate or replace, applicable laws and regulations, including laws and regulations regarding data privacy and security for wireless devices. 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.

Regulatory bodies may contribute guidance to this standard and associated assurance evaluation programs or act as a scheme. It is a goal of this standard that regulatory bodies will acknowledge the critical importance of higher security standards for many classes of IoT devices, encourage compliance and certification, and perhaps someday mandate compliance and certification. Until such time, however, as a standard is mandated, the goal is to establish a de-facto standard for IoT device security, in which the general public may expect and demand compliance and certification, not unlike the manner in which some other standards and marks are widely accepted for electrical devices and components.

c) Vendors and component suppliers for vendors

Product vendors, such as medical device manufacturers, may present their products and associated assurance evidence for evaluation and certification against this standard. At the lowest assurance level, the evidence provided is simply a statement of conformance without independent review from an authorized laboratory. For the higher assurance levels, evaluations are performed by scheme-accredited test laboratories, with evaluation fees depending on numerous factors, including complexity of product, complexity of product security requirements, availability of test laboratories, etc.

d) Test laboratories

The scheme may accredit test laboratories based on their skills in the art and science of security techniques and methodologies and their demonstrated compliance to ISO 17025.

e) Retailers, purchases, insurers

The standard may be used by organizations with "purchasing power" to hold suppliers to a higher standard for security and privacy.

f) Consumers

Consumers are the ultimate beneficiaries of this standard. By raising the assurance evaluation bar, this standard can help enable faster and safer adoption of innovative wireless technologies and help contribute to improved quality of life.

## The role of this standard in security/privacy risk management

Numerous sources of commercial best practice guidance and regulations in the area of product security promote the use of risk assessment as an overarching principle to properly and efficiently identify and mitigate risks to privacy and security that may arise through the use of those products. As devices are increasingly connected to networks, the risk associated with cyber threats grows. The standard aims to provide manufacturers, regulators, and consumers with an efficient, standardized approach to effectively manage risk attributable to cybersecurity threats. Specifically, the standard aims to provide, through developer attestation and (at higher assurance levels) technical evaluation of that attestation, grounds for confidence that the device can protect itself against applicable security threats, and where applicable, whether the user can achieve protection against associated privacy and security threats. Thus, the standard can become a valuable tool in the risk assessment arsenal of regulators, retailers, and manufacturers while also providing a basis for consumers to make more informed purchasing decisions to help manage risk. The following sections provide examples of how this standard is intended to help in the risk management mission.

## Identification of assets, threats, and vulnerabilities

The standard leverages ISO 15408 to help developers identify and document, using the ISO 15408 standardized framework, the threats applicable to their products and components.

The security assurance evaluation program described in this standard helps developers identify vulnerabilities by augmenting the developer secure development lifecycle with independent vulnerability assessment by qualified cybersecurity test laboratories.

## Assessment of the impact of threats and vulnerabilities on device functionality and end users

First, this standard helps to assess the impact of threats and vulnerabilities on device functionality and end users by requiring developers to consider relevant threats and how they might impact user privacy and security. Second, this standard helps assess the impact of vulnerabilities discovered during the security evaluation program. Finally, the standard also helps stakeholders (manufacturers, regulators, end users, insurers, and independent cybersecurity experts) balance the need for security with essential product performance. This balance is struck as part of the process of authoring protection profiles (PPs) and security targets (STs), since this balance is necessarily product specific: a specific control may be acceptable for one type of product and completely unacceptable for another type of product. The applicable stakeholder group weighs cybersecurity risk against the risk that a control may hamper essential product performance.

## Assessment of the likelihood of a threat and of a vulnerability being exploited

This standard helps to assess the likelihood of a vulnerability being exploited. As part of the vulnerability assessment requirement included in the PPs and STs, the security evaluator attempts to understand not only whether a vulnerability is exploitable but also what level of attack potential is required to exploit the vulnerability. Attack potential takes into consideration how much time is required to devise an exploit, what level of knowledge of the product's inner workings would be required, what kind of sophisticated equipment might be needed to exploit, etc. The attack potential helps developers assess the probability of a threat converting to active exploit based on this potential. For example, a low potential exploit (one that can be accomplished without sophisticated equipment or knowledge) is likely to have a higher probability of exploit in practice than a high potential exploit that is beyond the technical and economic reach of most attackers.

## Determination of risk levels and suitable mitigation strategies

This standard helps to determine suitable mitigation strategies; as part of the Protection Profile and Security Target authoring process, the applicable stakeholders (including evaluators and developers) should work together so that the security functional requirements are carefully chosen to mitigate security threats while balancing other requirements. For example, it may be determined that a wireless-connected device should use a simple pairing scheme (or one that is known to be not as secure as other pairing schemes) in order to meet usability requirements and to instead require documented physical security controls and user training, augmenting the technical pairing mechanism offered by the device, for an overall suitable security approach (as documented in the ST ).

## Assessment of residual risk and risk acceptance criteria

This is a central focus of a conformant security assurance program defined by this standard. During a security evaluation, the evaluator determines whether residual risks are acceptable relative to the assurance requirements specified in the ST. For example, if a vulnerability exploit requires an attack potential that is higher than what is required in the ST, the evaluator may indicate that the residual risk associated with this vulnerability is acceptable. The evaluation process should provide all relevant stakeholders, including the product manufacturer, its customers, healthcare providers, and regulators, with an independent expert assessment of these risks.

## ISO/IEC 15408

To be effective for security-critical electronic devices, security standards should delve deeply into the processes and techniques for developing and deploying security technologies that provide high assurance of protection. A consortium of national governments came together in the mid 1990s to create a framework for specifying security requirements—for any electronic product, software component, or system—and evaluating vendor claims of conformance to the requirements. The framework that was developed is ISO/IEC

15408[6], known informally as the Common Criteria (CC) ("Recognition of Common Criteria Certificates in the Field of Information Technology Security"), which remains arguably the most widely used and internationally accepted, generally applicable product security framework. CC has been utilized to specify a wide variety of security functionality over almost two decades. Requirements are specified in two dimensions: functional requirements cover security features of a product or component while assurance requirements provide the confidence those features actually do what they claim. CC is a powerful, scalable framework that permits comparability and consistency between the results of independent security evaluations that follow the standard's methodology.

Security functional requirements (SFRs) vary widely across products and product components, depending on their threat model, assets and functions under protection, and numerous other factors. For example, the SFRs for a network access point are likely to include the following:

- User authentication to help ensure the access point is only configured by authorized users
- Device authentication to help ensure that only authentic, trustworthy devices are able to connect to the access point
- Data-at-rest encryption and physical security to protect long-term private keys used for the various secure communications capabilities offered by the device

Security assurance requirements (SARs) depend on the overall assurance level desired for the product and its evaluation. Categories of requirements relevant to assurance may include:

- Semi-formal design and specification of device's security functionality
- Rigorous analysis of test coverage of device's security-related code
- Methodical vulnerability analysis of device security functions

## Protection profiles and security targets

CC provides for the creation of product-specific requirements specifications, against which individual commercial products or product components are evaluated. The two types of specifications are PPs and STs. A PP is intended to generalize the requirements for a class of similar products. STs, in contrast, provide requirements for a specific product instance or component. For example, if there are numerous manufacturers of connected diabetes devices, all of which have similar security requirements, then a PP can be authored to cover all connected diabetes devices. A specific vendor's diabetes product (or product family) should have its own ST. An ST can be tailored from the appropriate PP or can be created from scratch, without a preexisting PP. Evaluations are only performed against STs. PPs are not required as part of a conformant evaluation program but can be used when significant efficiency is to be gained from a common parent specification.

## Selecting security requirements for PPs and STs

The CC provides a large menu of common functional and assurance requirements, from which PP and ST authors may choose, based on product threat models and security capabilities. Whenever possible, requirements should be selected from this menu. However, CC allows for the use of extended requirements when a product has security needs and capabilities that are not well represented in the default menu.

PPs and STs applicable to this standard may be authored by any organization (e.g., a vendor, consortium of vendors, regulatory body, or scheme). However, the most effective PPs are those that are created by

[6] Information on references can be found in Clause 2.

representatives from a comprehensive set of stakeholders pertinent to the product area. These stakeholders convene to perform threat modeling of common products and derive the security objectives to meet the threats. The stakeholders should account for the expected sophistication of attackers when determining the assurance requirements and should carefully balance the needs of all stakeholders. For example, a PP developed for diabetes devices should include a convention of stakeholders representing a sample of diabetes product manufacturers, independent cybersecurity experts, applicable component suppliers, physician and nursing groups, applicable regulatory agencies (e.g., US Food and Drug Administration), and user/privacy groups.

This standard does not mandate the use of evaluated assurance levels. Rather, this standard defines custom assurance evaluation packages with varying levels of evaluation rigor depending on the product and its market needs.

## Custom security targets

While a scheme will likely recognize PPs for major classes of electronic products as well as popular components, developers whose products do not map well to PPs are also encouraged to evaluate and certify their component products against custom STs (approved by the applicable scheme) so that device manufacturers can efficiently incorporate them into a reduced scope and resource product evaluation. Component STs should be carefully defined so that they use at least the same assurance level as the devices that will contain them, with functionality claims consistent with the relevant parts of the PPs.

This standard also allows for scheme-approved custom STs (not derived from any scheme-approved PPs) for complete products, although this is generally discouraged unless the product fails to map to an existing scheme-approved PP. In the same way that the PP follows a multi-stakeholder, risk-based approach to deriving an appropriate set of security threats, objectives, and requirements, a custom ST should be carefully created to consider a maximum practical selection of stakeholder perspectives (e.g., product developer, regulators, evaluators, independent security experts, professional organizations, etc.). In addition, the development process for custom STs, like all other STs, should strive not to constrain product design and implementation freedom while defining, via a risk-based approach, the product's security objectives and 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 (this part)]
- IEEE Std 2621.2™/UL 2621-2:2022 (information security requirements for connected diabetes solutions)
- IEEE Std 2621.3™ /UL 2621-3:2022 (use of mobile devices in diabetes control contexts)

# Contents

1. Overview ........ 14
   1.1 Scope ........ 14
   1.2 Purpose ........ 14
   1.3 Word usage ........ 15

2. Normative references ........ 15

3. Definitions, acronyms, and abbreviations ........ 15
   3.1 Definitions ........ 15
   3.2 Acronyms and abbreviations ........ 16

4. Conformance ........ 16
   4.1 Use of ISO/IEC 15408 ........ 17
   4.2 Assurance packages ........ 17
   4.3 Laboratory Accreditation ........ 18
   4.4 Product Certification ........ 18
   4.5 Evaluated products list and product labeling ........ 19
   4.6 Protection profile (PP) and security target (ST ) approval ........ 19
   4.7 Assurance Maintenance ........ 19

# IEEE/UL Standard for Wireless Diabetes Device Security Assurance Evaluation: Connected Electronic Product Security Evaluation Programs

## 1. Overview

### 1.1 Scope

This standard defines a framework for a connected electronic product security evaluation program.

### 1.2 Purpose

The purpose of this standard is to provide grounds for confidence that connected electronic products deliver the security protections claimed by their developers and deemed necessary and sufficient by an appropriate set of stakeholders. This standard is initially targeted to wireless diabetes devices and their components (e.g., operating systems, network stacks, apps).

In order to realize this purpose, this standard shares the following objectives:

- Provide for security evaluations of electronic products performed to high standards, including the ability to achieve protection and an overall contribution toward enhanced safety, privacy, and security for electronic product stakeholders, including product manufacturers, resellers, users, and administrators
- Improve the availability of connected electronic products that have been independently evaluated and certified to meet such standards
- Reduce the use of ad hoc, unreliable, and low security assurance connected electronic product development and evaluation methods that can increase risk to electronic product stakeholders
- Continuously improve the efficiency (cost and time) of the security evaluation and certification of connected electronic products

### 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*).[7,8]

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*).

## 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—Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model.[9]

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

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

ISO/IEC 17025, Testing and calibration laboratories.

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.[10]

**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.

[7] The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations.

[8] The use of *will* is deprecated and cannot be used when stating mandatory requirements, *will* is only used in statements of fact.

[9] ISO/IEC publications are available from the ISO Central Secretariat (https://www.iso.org/). ISO/IEC publications are available in the United States from the American National Standards Institute (https://www.ansi.org/).

[10] *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.

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

**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 Target of Evaluation 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 include firmware written to read-only memory (ROM) or EEPROM whose reprogrammability is protected against unauthorized use.

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

**scheme**: A plan of action for determining conformity assessment.

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

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

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

**user**: An authorized operator of the Target of Evaluation. 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

| | |
|---|---|
| CC | Common Criteria |
| PP | protection profile |
| SAR | security assurance requirement |
| SFR | security functional requirement |
| ST | security target |

## 4. Conformance

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