P2621.1

Submitter Email: dklonoff@diabetestechnology.org
Type of Project: New IEEE Standard
Project Request Type: Initiation / New
PAR Request Date: 14 Jan 2020
PAR Approval Date: 04 Mar 2020
PAR Expiration Date: 31 Dec 2024
PAR Status: Active

1.1 Project Number: P2621.1
1.2 Type of Document: Standard
1.3 Life Cycle: Full Use

2.1 Project Title: Standard for Wireless Diabetes Device Security Assurance: Product Security Evaluation Program

3.1 Working Group: Healthcare Device Security Assurance Working Group(EMB/Stds Com/HDSecWG)
3.1.1 Contact Information for Working Group Chair:
Name: David Klonoff
Email Address: dklonoff@diabetestechnology.org
3.1.2 Contact Information for Working Group Vice Chair:
None
3.2 Society and Committee: IEEE Engineering in Medicine and Biology Society/Standards Committee(EMB/Stds Com)
3.2.1 Contact Information for Standards Committee Chair:
Name: Carole Carey
Email Address: c.carey@ieee.org
3.2.2 Contact Information for Standards Committee Vice Chair:
Name: Hasan Al-Nashash
Email Address: hnashash@aus.edu
3.2.3 Contact Information for Standards Representative:
Name: Carole Carey
Email Address: c.carey@ieee.org

4.1 Type of Ballot: Individual
4.2 Expected Date of submission of draft to the IEEE SA for Initial Standards Committee Ballot: Oct 2020
4.3 Projected Completion Date for Submittal to RevCom: Apr 2021

5.1 Approximate number of people expected to be actively involved in the development of this project: 25
5.2 Scope of proposed standard: This standard defines a framework for a connected electronic product security evaluation program,
which includes:
1. How to apply the ISO/IEC 15408 security evaluation framework in a security evaluation program defined by this standard.
2. Framework for authorizing independent testing labs to be used in the security evaluation program.
3. Framework for certifying results from authorized labs.
4. Framework for defining and approving new security requirements and changes to security requirements, via protection profiles and
security targets, to be used in the security evaluation program.
5. Framework for assuring continued maintenance of assurance post-certification.

5.3 Is the completion of this standard contingent upon the completion of another standard? No
5.4 Purpose: The purpose of this standard is to provide assurance 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).
5.5 Need for the Project: Medical devices used for monitoring and managing diabetes provide life-saving benefits to patients and effective implementation options to healthcare providers. These devices include

blood and continuous glucose monitors, insulin pumps, pens and other insulin delivery devices, and closed loop artificial pancreas systems and others. With ever-increasing connectivity and data exchange between these diabetes devices, other devices (such as smartphones), and the Internet, there is an increased risk to the safety and privacy of the patient and to the integrity of the healthcare provider. This standard, therefore, is needed to aid medical manufacturers in the development of more secure, and therefore safer, products as well as to provide the framework for enhancing assurance across the relevant stakeholder community, as described in section 5.6.

5.6 Stakeholders for the Standard: Device manufacturers, clinicians, regulators, certification bodies, independent cybersecurity/privacy experts, healthcare facilitators, test labs, software developers, and patients/consumers.

6.1 Intellectual Property

6.1.1 Is the Standards Committee aware of any copyright permissions needed for this project? Yes

Explanation: The basis of this standards will be the Diabetes Technology Society standard DTSec.

6.1.2 Is the Standards Committee aware of possible registration activity related to this project? No

---

7.1 Are there other standards or projects with a similar scope? Yes

Explanation: UL 2900

The UL 2900 series of standards consists of the following parts, under the general title 'Standard for Software

Cybersecurity for Network-Connectable Devices':

Part 1: General Requirements for Network-Connectable Devices

Part 2-1: Particular Requirements for Healthcare Systems

Part 2-2: Particular Requirements for Industrial Control Systems

Part 3: General Requirements for the Organization and Product Development Security Lifecycle Processes for

Network-Connectable Devices

7.1.1 Standards Committee Organization: UL

Project/Standard Number: UL2900

Project/Standard Date:

Project/Standard Title: Cybersecurity for Network Connected Diabetes Devices

7.2 Is it the intent to develop this document jointly with another organization? Yes

7.2.1 Organization: Underwriter Laboratories

Technical Committee Name: N/A

Technical Committee Number:

8.1 Additional Explanatory Notes : These standards were previously under one standard (P2721) but have now been separated into three separate but related standards:

2621.1 Defines a framework for a connected electronic product security evaluation program.
2621.2 Defines the security requirements, which compose a Protection Profile, for connected diabetes devices.
2621.3 Provides guidance for the safe use of consumer mobile devices in the control of diabetes-related medical devices.

IEEE and UL have signed an MOU for joint development

2.1 and 5.2: The connected devices used in diabetes might have different properties and different vulnerabilities than connected devices used for other diseases. We intend to build this standard for diabetes first. This standard might be useful as a template for connected devices for other diseases in the future. We feel that this project is more likely to be successful if we focus on diabetes devices rather than devices for all types of health conditions.

The working group has developed this standard following research and consultation with a multi-stakeholder community consisting of the US FDA, independent cybersecurity experts, consumer technology developers (e.g. smartphone developers, smartphone operating system developers, and smartphone chipset developers), diabetes device developers, medical research funding agencies, physicians, educators, consumers, regulatory experts, liability attorneys, policy experts, and more. This standard has been developed to identify issues and best practices relating to CMD use in medical contacts. The same stakeholder groups and other applicable interested parties should consider this standard in the design, development, evaluation, approval, management, deployment, and use of CMDs in medical control contexts. The core features of this standard were originally developed by Diabetes Technology Society as a standard and a guideline called DTSec and DtMoSt. Diabetes Technology Society then turned over these documents to IEEE and UL to be comanaged.

The recommendations contained in this standard are intended to supplement existing standards and guidance,

including (in the US, for example) FDA recognized standards such as ISO/IEC 62304 and FDA guidance such as the Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. These guidelines describe current consensus thinking of the aforementioned multi-stakeholder community membership on this topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited.

ISO/IEC 15408-1 2009 - Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model (Third edition 2009-12-15, Corrected version 2014-01-15)(Source Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model)
ISO/IEC 15408-2-2011 - Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components (Third edition 2008-08-15, Corrected version 2011-06-01)(Source Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components)
ISO/IEC 15408-3-2011 - Information technology Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components (Third edition 2008-08-15, Corrected version 2011-06-01)(Source Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components)