This is a PRELIMINARY DRAFT STANDARD and is not intended, nor should it be interpreted, to have any legal effect. This DRAFT reflects the input of Members of the Steering Committee and the Diabetes Technology Society and will be circulated for wider comment following additional internal revisions

Diabetes Technology Society

Standard for Connected Diabetes Device Security (DTSec)

December 28, 2015
Version 0.8

DTSEC-2015-08-000

Legal Notice:

Diabetes Technology Society (DTS) organized the development of this version of the Diabetes Technology Society Standard for Wireless Device Security (DTSec). As the holder of the copyright in the Diabetes Technology Society Standard for Wireless Device Security (DTSec), DTS retains the right to use, copy, distribute, translate or modify DTSec as it sees fit.

Foreword

This version of DTSec (v1.7) is a revised version based on suggestions from the DTSec Steering Committee and Advisors. This standard and related Protection Profiles, which are managed by the DTSec Working Group (DWG), consists of scope of work, Protection Profile, and Assurance committees, all working under the auspices of the Diabetes Technology Society. This draft document is not intended for official use.

This is a PRELIMINARY DRAFT STANDARD and is not intended, nor should it be interpreted, to have any legal effect. This DRAFT reflects the input of Members of the Steering Committee and the Diabetes Technology Society and will be circulated for wider comment following additional internal revisions

52
53

54 # Table of Contents

67
68

1. INTRODUCTION

The following section is non-normative, with the exception of statements that include the word "***shall***" in boldface italics.

The purpose of DTSec is to establish a standard used to provide a high level of assurance that electronic products deliver the security protections claimed by their developers and required by their users. While this standard is initially targeted to networked life-critical devices, such as insulin pump controllers, used in the treatment of diabetes, there is nothing inherent in this standard that precludes its application to any medical product or component contributing to the protection of high value assets, resources, and functions. Indeed, while the Diabetes Technology Society has a specific mission in diabetes-related electronic products, it is the express intent of this standard's authors that it can provide foundational work for effective cybersecurity standards across not only other medical device classes but other connected devices and the broader "Internet of Things."

In order to meet the goal above, participants in the creation of this standard share the following objectives:

1. Enhance the likelihood that security evaluations of critical medical products are performed to high standards, including the ability to achieve highly assured protection and an overall contribution towards enhanced safety, privacy, and security for electronic product stakeholders, including product manufacturers, regulators, patients, and caregivers;
2. Increase the availability of critical electronic products that have been independently evaluated and certified to meet such high standards;
3. Reduce the use of ad-hoc, unreliable, and low assurance electronic product development and evaluation methods that increase risk to electronic product stakeholders;
4. Continuously improve the efficiency (cost and time) of the evaluation and certification of critical electronic products.

Professional symposia that support DTSec:
Diabetes Technology Society Annual Conference
MEDSec (Medical Cybersecurity and Privacy: The Internet of Medical Things)

Scope

This section describes the scope of the DTSec standard.

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 glucose monitors and continuous glucose monitors, insulin pumps, pens and other insulin delivery devices, and closed loop artificial pancreas systems. With ever-increasing connectivity and data exchange between these diabetes devices, other devices (such as smart phones), and the Internet, there is an increased risk to the safety and privacy of the patient and to the integrity of the healthcare provider. The DTSec program calls for the specification of security requirements for wireless diabetes devices and following the general framework of establishing security standards for information and electronic systems (ISO/IEC 15408, described in the following section). These requirements are codified by the use of Protection Profiles and Security Targets (explained later in this document), but at a high level have the following objectives:

- To establish the general requirements for connected devices that meet the balanced needs for security and clinical application.
- To identify possible and potential threats related to the various components and interfaces of the connected devices, such as network, storage, software, connected peer devices, and cryptography.
- To define a set of generalized requirements that apply to families of similar devices (these are formed into the Protection Profile)
- To define a set of specific mandatory requirements, derived from the generalized requirements, corresponding to specific connected-diabetes device products and components (these requirements are formed into the Security Target).
- To outline additional optional functional requirements for manufacturers to consider to add to their toolbox for future development.

In addition to security functional requirements, the Protection Profiles and Security Targets specify assurance requirements to address the question of: how can I be sure that a wireless diabetes device actually delivers the security claimed in the functional requirements? Common assurance requirements are collected into an assurance package, described in more detail later in this document, and formally defined in the Protection Profiles and Security Targets themselves.

In addition to the program for creation and approval of security requirements documents, this standard also defines the assurance program for evaluating and certifying products against those requirements. The assurance program is defined later in this document.

In summary, the DTSec scope includes a program for specifying security requirements for wireless diabetes devices and a program for generating independent assurance (by technical evaluation) that products meet the specified requirements. The remainder of this standard document provides more detailed information about these items and specific mandatory guidance for how this standard is applied.

ISO/IEC 15408

To be effective for critical electronic devices, especially those that are network connected and may be subject to remote malicious attack, security standards must 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 electronics product, software component, or system - and evaluating vendor claims of conformance to the requirements. The framework that was developed is ISO/IEC 15408, known informally as the Common Criteria (CC), which remains the only 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. CC assurance requirements can be thought of as falling into two broad areas: product-independent, organizational requirements (e.g. life-cycle processes, configuration management controls, a process and common approach to design and specification, etc.) and product-dependent requirements (e.g. design and requirements artifacts specific to a particular system, functional test results, and vulnerability assessment).

Security functional requirements vary widely across products and product components, depending on their threat profile. For example, the security functional requirements for a wireless insulin controller may include:

- authentication to ensure the controller is only operated by authorized users

- device and software authentication to ensure that only authentic, trustworthy devices and their constituent software/firmware are used to administer insulin
- data integrity and confidentiality to protect against corruption or other unauthorized access to commands sent between controller and pump
- data confidentiality to safeguard the personal data (privacy) of patients and other persons

Protection Profiles and Security Targets

The 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 Protection Profiles (PP) and Security Targets (ST). PPs are intended to generalize the requirements for a wide range of similar products and represent the appropriate security and assurance requirements for a class of devices derived from a technical community of clinical and security experts. This enables the purchaser of a device to acquire a secure product by specifying that the device meet the requirements of the PP rather than detailing all requirements for each device purchase. STs, in contrast, provide specific requirements for a specific product or component from a specific manufacturer. For example, if there are numerous manufacturers of insulin pump controllers, all of which have similar security requirements, then a PP can be authored by a technical community of manufacturers and other stakeholders (e.g. caregivers, regulators, independent cybersecurity experts) to cover insulin pump controllers. A manufacturer can then tailor an ST from the PP. Evaluations are performed against STs. PPs ***shall*** be authored by DWG and used when significant efficiency is to be gained from a common security specification and to reduce the subsequent resources required to develop derived STs.

The CC provides a large menu of common functional requirements, from which PP and ST authors may choose. Whenever possible, requirements should be selected from this menu. PP authors also have the freedom under the CC to define "extended" requirements to address requirements not explicitly listed in the standard. For example, embedded medical electronics may have requirements not initially conceived by the CC standards authors targeting general IT systems. The complete selection of requirements for PPs and STs must be carefully made based on the device threat model, including the functional attack vectors (local/physical, local network, wide-area network, supply chain, etc.) and the motivation and sophistication of attackers to which the product's security capabilities must be resistant.

Security evaluation and certification performed under the auspices of this standard ***shall*** utilize international standard ISO/IEC 15408:2009 (general framework and specification of requirements) and ISO/IEC 18045:2005 (companion document to ISO 15408, covering evaluation methodology).).

ISO 15408 Assurance Packages

Assurance requirements can be grouped into a package that is reused across different PPs and STs. Standards bodies and developers can create customized assurance packages. For example, packages may vary the rigor of vulnerability assessment, depending upon the reasonably expected magnitude of anticipated threats threat (e.g. nation state vs. amateur hackers).

Each assurance requirement originates from a particular assurance component, where each component includes a selection of related requirements in increasing levels of rigor, corresponding to the needs of increasing assurance. DWG may create a package that adopts more rigorous requirements for testing and vulnerability assessment activities that are tightly coupled to device implementation. However, because medical device manufacturers often follow a mature, high quality software development life-cycle process, such as one compliant to IEC 62304, an international and widely adopted standard for medical device software lifecycle processes, compliance (and associated audit) to IEC 62304 may be used as a cost-effective replacement for evaluation of organizational lifecycle-related assurance requirements for device software development. DTSec assurance packages ***shall*** be defined and included within any Protection Profiles authored under this standard.

An additional approach to evaluation efficiency that should be considered in an evaluation program is a vendor's ability to demonstrate consistent evaluation success. For example, if a vendor successfully passes an evaluation and therefore certifies a product against a DTSec PP/ST, then subsequent versions of similar products, wherein the vendor asserts compliance to all requirements of the ST, may claim a de-facto certification subject to randomized auditing by DWG and/or its appointed subcontractor.

Security evaluation and certification for high-criticality products and components performed under the auspices of this standard ***shall*** target a custom assurance package that satisfies the aims of protection against moderate to high potential attack threats. The precise selection of custom assurance package depends on numerous factors, including relative criticality, system tolerance to faults, specific selection of assurance requirements, and more. Lower level assurance evaluations ***shall*** be limited to general-purpose products components not responsible for life-critical functions, or devices that are not exposed to such attack threats (e.g. non-networked devices used only within hospitals).

The primary initial audience for product evaluation is medical device manufacturers and their suppliers, although patients, doctors, regulators, device purchasers, and other stakeholders also will have an interest in the results of such evaluations. While DWG is expected to author PPs for major classes of diabetes-related medical devices with technical community input, suppliers of components that implement a subset of security functions required by these devices, such as SSL protocol, BTLE, and cryptographic libraries, are also encouraged to evaluate and certify these components against custom STs (approved by DWG) so that device manufacturers can efficiently incorporate them into a reduced scope and resource product evaluation. Component STs ***shall*** be carefully defined so that they use the same assurance level as the devices that will contain them, and functionality claims ***shall*** be consistent with the relevant parts of the PPs.

2. ASSURANCE PROGRAM

While a standardized documentary approach to specification and evaluation of security requirements is important, the actual evaluation of products against these requirements is the cornerstone of DTSec's approach to enhanced cybersecurity assurance. As such, DTSec governs the accreditation of independent testing labs that perform evaluations against this standard and the certification of lab results under this standard.

Lab Accreditation

DWG ***shall*** publicize a list of independent labs approved by DWG to perform evaluations under DTSec. Labs that wish to provide evaluation services under DTSec must apply and be accepted into the program by DWG.

Labs approved under DTSec ***shall*** be accredited against the ISO 17025 lab accreditation standard, under a scope that includes information technology security testing or similar designation. In addition, DWG reserves the right to accept or reject lab applications based on numerous factors, including but not limited to the lab's experience in information technology and vulnerability assessment, the reputation and international acceptance of the lab's ISO 17025 accrediting body, and the lab's prevailing evaluation costs and resource availability.

Labs approved under DTSec ***shall*** be competent to perform vulnerability assessment consistent with AVA_VAN[1] requirements at AVA_VAN.4 or higher leveling, as described in ISO 15408 and ISO 18045. In addition, the lab must be capable of handling vulnerability assessment at these levels for a wide range of device software and hardware environments that are typical in the medical device industry. For example, some devices will run on simple microcontrollers with basic operating systems and small applications, while others may include sophisticated web interfaces and general-purpose operating systems and applications. Since such competence may not be included within the scope of the lab's accreditation, the lab must demonstrate its suitability during the application process to DWG. It is the responsibility of DWG to mandate and take reasonable steps to maximize effectiveness and consistency of AVA_VAN implementations across labs; however, DWG recognizes that vulnerability assessment is a function of evaluator skill and time invested as well as specific device characteristics and that perfect consistency

[1] These are vulnerability analyses under the Common Criteria.

(even with the same lab across different devices) is not realistic. DWG requires that labs document their assessment work and make itself available to auditing and informal observation during evaluations by the DWG. Despite the acknowledged challenges in the world of consistent security evaluation, this difficulty should never be used as an excuse to lower the assurance bar for DTSec.

Product Certification

If a product successfully passes evaluation by a DTSec-approved lab, the lab must submit an Evaluation Technical Report to DWG. The report must provide enough detail to satisfy DWG that the evaluation of the product against the ST was performed to a high standard, especially with respect to AVA_VAN vulnerability assessment. A product ***shall*** not be considered certified under DTSec until the evaluation report is formally accepted by DWG and the product listed under the DTSec evaluated products list.

Evaluated Products List

Any products that have successfully passed an evaluation under DTSec and whose evaluation results have been certified by DWG shall be listed under a publicly disclosed DTSec evaluated products list. However, if certified products are subsequently reported to contain vulnerabilities that conflict with the applicable ST requirements, DWG reserves the right to remove those products from the evaluated products list until the vulnerabilities are remediated. DWG reserves the right to remove products from the evaluated products list if they suffer from a large volume of recurring vulnerabilities, even if all reported vulnerabilities have been remediated; similarly, a lab that has successfully evaluated a product that suffers from such recurring vulnerabilities may be subject to removal from the list of approved labs.

Protection Profile and Security Target Approval

DWG ***shall*** author and publish PPs and incorporate public review and feedback prior to their formal acceptance and use to derive any STs.

An ST ***shall*** be used for any evaluations performed under DTSec. Public review and formal publication under DTSec of STs are encouraged but not required. An ST ***shall*** be reviewed and approved by DWG before it may be used in any evaluation under DTSec.

Assurance Maintenance Program

When a product developer wishes to gain reuse of a product certification for new versions of the product (hardware and/or software changes), then the developer

must submit an assurance maintenance request form, which documents the differences between the certified product and the new, modified product. If the changes are sufficiently minor, DWG may accept the form without any further actions and simply append the new product version information to the applicable entry in the evaluated products list.

Product developers should notify DWG of high severity vulnerabilities that could be exploited to subvert the asserted security functional requirements in evaluated products. Developers should include a plan to mitigate such problems. If such vulnerabilities, whether reported by developers or third parties, are not adequately and promptly mitigated, DWG reserves the right to remove the product from the evaluated products list. Because the overall impact of vulnerabilities and their potential mitigations in specific products vary greatly, this standard does not include guidance for when DWG may take this action. DWG would consider the perspective of all stakeholders, including developers, regulators, patients, and caregivers.

DWG reserves the right to institute random audits of the developer by DWG personnel and/or DTSec-approved labs in order to obtain assurance that the new product satisfies the original requirements documented in the applicable ST or in an approved ST that has minor revisions from an ST that was previously applied in a full evaluation of the earlier revision product. Such audits aim to sample requirements compliance and require a small percentage of the cost and time of a full evaluation. If a product developer cannot support the audit activities for any reason or if the changes documented in the assurance maintenance request form are deemed sufficiently major by DWG, then DWG reserves the right to require a full revalidation of the new product. DWG and its accredited labs will enter into agreements as needed in order to meet confidentiality requirements of vendors bringing their products into evaluation against this standard.

This standard does not stipulate a lifetime or expiration for product evaluations; a product evaluation shall remain in effect as long as it continues to meet the assurance maintenance requirements defined herein.