Diabetes Technology Society

Standard for Wireless Diabetes Device Security (DTSec)

November 25, 2017
Version 2.0

DTSEC-2017-11-001

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 (2.0) is a revised version based on suggestions from the DTSec working groups, steering committee, and the public (following a public review cycle). 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 Diabetes Technology Society.

Table of Contents

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 for 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 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.

1.1 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 monitor systems 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. Following the general framework of establishing security standards for information and electronic systems (ISO/IEC 15408, described in the following section), the DTSec program calls for the specification of security requirements for wireless diabetes devices. 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 adding 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.

1.2 Role of DTSec in Medical Device Safety Risk Management

Numerous sources of commercial best practice guidance and regulations in the area of medical device safety promote the use of risk assessment as an overarching principle to properly and efficiently identify and mitigate risks to patient safety that may arise through the use of medical devices. It is commonly understood that cybersecurity threats are but one of the many factors that must be considered in this risk assessment. As medical devices are increasingly connected to networks, the risk associated with cyber threats grows. DTSec aims to provide manufacturers and regulators with an efficient, standardized approach to effectively manage safety risk attributable to cybersecurity threats. Specifically, the standard aims to provide, through evaluation, confidence that the medical device is able to protect itself against applicable security threats. Thus, DTSec becomes a valuable tool in the manufacturer's risk assessment arsenal.

As an example of how DTSec may fit into a nation's medical device regulatory guidance, consider recent FDA guidance described in *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* (issued October 2, 2014). The "General Principles" section within this guidance document lists five elements of a vulnerability and management approach in line with U.S. government regulations. For each element, we explain here how DTSec helps manufacturers meet the spirit of the guidance.

1. Identification of assets, threats, and vulnerabilities;

DTSec leverages ISO 15408 (described more later in this document) to help developers identify and document, using the ISO 15408 standardized framework, the threats applicable to medical device products and components.

The DTSec assurance-through-evaluation program (described in section 2 of this standard) helps developers identify vulnerabilities by augmenting the developer secure development lifecycle with independent vulnerability assessment by qualified cybersecurity test labs.

2. Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;

DTSec helps to assess the impact of threats and vulnerabilities on device functionality and end users/patients by requiring developers to consider relevant threats and how they might impact safe clinical use. For example, if a patient with diabetes makes clinical decisions based on the readings from a wirelessly connected glucose monitor, then the developer must consider how cybersecurity threats borne over the wireless connection could potentially corrupt the integrity of these readings, leading to unsafe clinical decisions. This assessment leads to the inclusion of appropriate mitigating controls (security functional requirements) in the Security Target specification.

DTSec also helps assess the impact of vulnerabilities discovered during the security evaluation program. For example, if a flaw in the wireless protocol is discovered, then evaluator will assess the exploitability of this vulnerability. If the vulnerability cannot be exploited to corrupt blood glucose data, this implies a reduced impact relative to a protocol vulnerability the evaluator would be able to exploit to corrupt blood glucose data.

DTSec also helps stakeholders (manufacturers, regulators, end users, healthcare providers, payers, and independent cybersecurity experts) balance the need for security with essential clinical performance. This balance is struck as part of the process of authoring Protection Profiles and Security Targets, 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 clinical performance. For example, while user authentication to a medical device may seem an obviously important protection against unauthorized tampering with the device, security functional requirements must ensure that such controls do not add undue safety risk by preventing the user from accessing life-critical functionality. Indeed, DTSec's focus on product-specific security requirements ensures that these risk inputs will be rigorously considered by all relevant stakeholders rather than ignored or undervalued in an environment that has relied solely on product developers "doing the right thing." Cybersecurity history teaches us that developers - whether because of economic pressures, lack of a complete picture of all risks, or other reasons - often do not strike the proper balance.

3. Assessment of the likelihood of a threat and of a vulnerability being exploited;

DTSec helps to assess the likelihood of a vulnerability being exploited. As part of the vulnerability assessment requirement included in the Protection Profiles and Security Targets, the security evaluator will attempt to understand not only whether a vulnerability is exploitable but also what level of attack potential is required to exploit. 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.

4. Determination of risk levels and suitable mitigation strategies;

DTSec helps to determine suitable mitigation strategies; as part of the protection profile and Security Target authoring process, the DWG, evaluators, and developers work together to ensure that the security functional requirements are carefully chosen to mitigate security threats while balancing overall safe clinical use. For example, it may be determined that a Bluetooth-connected diabetes device should use a simple pairing scheme (one that is not known to be as secure as other pairing schemes) in order to meet clinical usability requirements and to 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 Security Target).

5. Assessment of residual risk and risk acceptance criteria.

This is a central focus of the DTSec assurance program. During a security evaluation, the evaluator must determine whether residual risks are acceptable relative to the assurance requirements specified in the Security Target. For example, if a vulnerability exploit requires an attack potential that is higher than what is required in the Security Target, the evaluator will affirm that the residual risk associated with this vulnerability is acceptable. The evaluation process provides all relevant stakeholders, including the product manufacturer, its customers, healthcare providers, and regulators, with an independent expert assessment of these risks.

1.3 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 electronic 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

1.4 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.

STs may be derived from a single all-inclusive PP or from the combination of a base PP and one or more Extended Packages (EPs). For example, if a class of devices applies to multiple products that have varying assurance requirements, a base PP may be used to specify the common functional requirements, and multiple EPs may be used to specify the multiple different sets of assurance requirements. An ST may then claim conformance to both a base PP and the selected EP.

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).

1.5 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 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 Protection Profiles authored under this standard. If a combination of base and extended PPs is used to derive an ST, then the assurance package must be defined in exactly one of the PPs

used to derive the ST. For example, a base PP may omit assurance requirements entirely, relying on multiple extended PPs to include multiple different assurance packages.

Security evaluation and certification for products and components performed under the auspices of this standard ***shall*** target an assurance package that satisfies the aims of protection against levels of attack potential consistent with assessed security risk of that product or component. The precise selection of an assurance package depends on numerous factors, including relative criticality, system tolerance to faults, and specific selection of assurance requirements.

1.6 Custom STs and the role of DWG in ST Development

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.

This standard also allows for DWG-approved custom STs (not derived from any DWG-approved PPs) for complete CDD products, although this is generally discouraged unless the product fails to map to an existing DWG 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 ***shall*** be carefully created so as to consider a maximum practical selection of DWG stakeholder perspectives (e.g. product developer, regulators, evaluators, caregivers, 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.

1.7 Composition

This standard allows for the evaluation of products that are composed of multiple products, one or more of which may already have been evaluated under this standard and also may have been developed by different product manufacturers. For example, a closed loop "artificial pancreas" TOE may be composed of a CGM from one developer and an insulin pump from another developer. It is recommended, although, not

required, that any constituent products be evaluated independently prior to evaluation of the composed system. Doing so enables the creation of evidence (e.g. test results, analysis documentation) and resulting assurance that can be used not only for the standalone product but also reused for evaluation of the composed product. For example, if an insulin pump is evaluated first, then the ability of the insulin pump to defend itself against unauthorized access and unauthorized information flows from a CGM will already be established. This should dramatically reduce the lab resources required to evaluate a composed closed loop system that uses the same insulin pump, especially if the same lab is used for both evaluations because the lab will already have access and familiarity with shared evaluation artifacts that another lab must reproduce. Note, however, that a composed TOE must still be evaluated even if all of its constituent components have previously been evaluated, since the ST corresponding to the composed system may include requirements or other special considerations that preceding evaluations did not consider.

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.

2.1 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 (even with the same lab across different devices) is not realistic. DWG requires that labs document their assessment work and make themselves available to auditing and informal observation during evaluations by the DWG.

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

2.2 Product Certification

If a product 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 is listed under the DTSec evaluated products list.

2.3 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 to a level of acceptable residual risk, as originally intended and agreed upon in the ST by its developers and DWG. 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.

2.4 Protection Profile and Security Target Approval

DWG ***shall*** author and publish PPs, incorporating 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.

2.5 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, as determined via risk assessment performed by evaluator in coordination with the product developer and DWG, 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 advocates prompt mitigation of vulnerabilities (e.g. via an authorized software update if such updates are supported by the manufacturer) that may directly impact patient safety. Notification of DWG regarding vulnerabilities in evaluated products should not be treated as higher priority than the clinical mitigation required for patient safety.

Recognizing that threat actors and techniques rapidly evolve, DWG reserves the right to request the submission of an assurance maintenance request form to specifically address new threats that the DWG and/or applicable DTSec-approved labs feel may invalidate an active approval. The above process for product modifications will be used by DWG to determine, by working with appropriate stakeholders including the developer, whether product changes and re-evaluation are necessary.

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.