EDSA-301
ISA Security Compliance Institute —
Embedded Device Security Assurance –
Maintenance of ISASecure® certification

Version 2.1

December 2014

Revision history

version	date	changes
1.0	2010.08.04	Initial version published to http://www.ISASecure.org
2.1	2014.12.11	replace SDSA by SDLA and use SDLPA terminology, incorporate VIT in EDSA, add concept of confidence in evidence impact assessment

Contents

FOREWORD

This is one of a series of documents that defines ISASecure® certification for embedded devices, which is developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). The current list of documents related to ISASecure embedded device security assurance can be found on the ISCI web site http://www.ISASecure.org.

1 Scope

This document specifies the criteria for maintaining ISASecure® EDSA certification for an embedded device, as the device and the ISASecure EDSA criteria evolve over time. A product is considered to be an embedded device if it satisfies the definition provided in 3.1.4. This document covers certification situations where:

- a certified device has subsequently been modified; or
- the ISASecure certification criteria have changed; or
- both the device and the certification criteria have changed.

In these cases, an assessment is required in order to determine whether, and in what manner, a previous certification may be used as evidence toward a new certification. The requirements in this document address these topics.

A certification is called an *initial* certification if it *does not* take into account the results of a prior certification for the device or for a prior version of the device. The criteria for a device to earn an initial certification are defined in [EDSA-300].

In overview, in order to obtain an initial ISASecure EDSA certification, a supplier must pass a security development process lifecycle assessment (SDLPA) equivalent to that defined under the ISASecure SDLA (Security Development Lifecycle Assurance) development process certification. This evaluation will be at a level equal to the security level of the EDSA certification sought. Specifically, in order for an embedded device from a supplier to achieve ISASecure EDSA certification, either

- the supplier must hold an ISASecure SDLA certification; or
- the supplier passes an equivalent SDLPA assessment of their development process as part of the EDSA evaluation itself.

A supplier may apply for EDSA and SDLA certification in parallel.

ISASecure EDSA certification of embedded devices has three additional elements:

- Security Development Artifacts for embedded devices (SDA-E);
- Functional Security Assessment for embedded devices (FSA-E); and
- Embedded device robustness testing (ERT).

SDLPA is an evaluation of the embedded device supplier's security development process. SDA-E examines the artifacts that are the outputs of the supplier’s security development process for the embedded device to be certified. FSA-E examines the security capabilities of the device, while recognizing that in some cases security functionality may be allocated to other components of the device’s overall system environment.

ERT has two major elements - Communication Robustness Testing (CRT) and Vulnerability Identification Testing (VIT). CRT examines the capability of the device to adequately maintain essential functions while being subjected to normal and erroneous network protocol traffic at normal to extremely high traffic rates (flood conditions). VIT scans the device for the presence of known vulnerabilities.

This document specifies when and how the results of a previous certification may be used for certification of a modified embedded device, for a certification to a later version of the ISASecure criteria, or for a certification to a higher security level. It specifies the incremental evaluations that are performed when evidence from a prior certification evaluation does not fully apply to the new certification being sought. To specify this, the document discusses this topic in turn for each of the elements of ISASecure EDSA certification listed above.

2 Normative references

[EDSA-300] *ISA Security Compliance Institute Embedded Device Security Assurance – ISASecure Certification Requirements,* as specified at http://www.ISASecure.org

[EDSA-310] *ISA Security Compliance Institute Embedded Device Security Assurance –Requirements for embedded device robustness testing,* as specified at http://www.ISASecure.org

[EDSA-311] *ISA Security Compliance Institute Embedded Device Security Assurance – Functional security assessment for embedded devices,* as specified at http://www.ISASecure.org

[EDSA-312] *ISA Security Compliance Institute Embedded Device Security Assurance – Software development artifacts for embedded devices*, as specified at http://www.ISASecure.org

[SSA-420] *ISCI System Security Assurance – Vulnerability Identification Test Policy Specification*, as specified at http://www.ISASecure.org

[SSA-420] *ISCI System Security Assurance – Vulnerability Identification Testing Policy Specification*, as specified at http://www.ISASecure.org

[SDLA-312] *ISCI Security Development Lifecycle Assurance – Security development lifecycle assessment*, as specified at http://www.ISASecure.org

[SDLA-300] *ISCI Security Development Lifecycle Assurance – Requirements for ISASecure Certification and Maintenance of Certification,* as specified at http://www.ISASecure.org

3 Definitions and abbreviations

3.1 Definitions

.

3.1.1
allocatable
able to be met by other components

NOTE As used here, refers to security capabilities capable of being met by other components in a device's architectural context, although not directly provided by the device itself.

3.1.2
artifact
tangible output from the application of a specified method that provides evidence of its application

NOTE Examples of artifacts for secure development methods are a threat model document, a security requirements document, meeting minutes, internal test results.

3.1.3
certifier
chartered laboratory, which is an organization that is qualified to certify products or supplier development processes as ISASecure

NOTE This term is used when a simpler term that indicates the role of a "chartered laboratory" is clearer in a particular context.

3.1.4
embedded device
special purpose device running embedded software designed to directly monitor, control or actuate an industrial process

NOTE Attributes of an embedded device are: no rotating media, limited number of exposed services, programmed through an external interface, embedded OS or firmware equivalent, real-time scheduler, may have an attached control panel, may have a communications interface. Examples are: PLC, field sensor devices, SIS controller, DCS controller.

3.1.5
essential function

function or capability that is required to maintain health, safety, the environment and availability for the equipment under control

NOTE Essential functions include but are not limited to the safety instrumented function (SIF), the control function, and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions is commonly termed loss of protection, loss of control, and loss of view respectively. In some industries additional functions such as history may be considered essential.

3.1.6
evidence impact assessment

identification of that portion of the evidence from the certification evaluation of a product, which may be applied toward the certification of a modified version of the product, and of those aspects of the evaluation which must be performed on the modified product and new evidence created

3.1.7
initial certification

certification where the ISASecure certification process does not take into account any prior ISASecure certifications of a product under evaluation or of any of its prior versions

3.1.8
ISASecure version

identifier for the ISASecure certification criteria in force at a particular point in time, defined by the set of document versions that define the certification program, and identified by a three-place number, such as ISASecure EDSA 2.0.1

3.1.9
security level

measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner

NOTE Vulnerabilities can either be designed into the IACS, inserted at any time during its lifecycle or result from changing threats. Designed-in vulnerabilities may be discovered long after the initial deployment of the IACS, for example an encryption technique has been broken or an improper policy for account management such as not removing old user accounts. Inserted vulnerabilities may be the result of a patch or a change in policy that opens up a new vulnerability.

3.1.10
supported

provided by the entity under evaluation itself

NOTE This term is used when referring to security functionality. In particular, supported functionality need not be allocatable to external entities that exist in the environment of the entity under evaluation.

3.2 Abbreviations

The following abbreviations are used in this document

ASCI	Automation Standards Compliance Institute
CM	change management
CRT	communication robustness testing
ERT	embedded device robustness testing
EDSA	embedded device security assurance
FSA-E	functional security assessment for embedded devices
IACS	industrial automation and control system
ICMP	Internet control message protocol
ISCI	ISA Security Compliance Institute
SDA-E	security development artifacts for embedded devices
SDL	security development lifecycle
SDLA	security development lifecycle assurance
SDLPA	security development lifecycle process assessment
VIT	vulnerability identification testing

4 Overview

In this section we summarize the approach to maintenance of ISASecure EDSA certification as a device and the ISASecure EDSA certification requirements evolve over time. The intent of the overall approach is to leverage previous certification results wherever possible to achieve cost effectiveness, while maintaining the integrity of the certification result. Sections 5 - 9 provide more detailed requirements for various certification maintenance scenarios.

4.1 SDLPA certification element

In order to achieve any ISASecure EDSA certification, whether an initial certification or a subsequent certification, the supplier must either:

- at the time the EDSA certification is granted, hold an SDLA certification at a level greater than or equal to EDSA certification level sought; or

- pass an evaluation of the SDLA criteria at this level, as part of the evaluation for ISASecure EDSA certification.

Therefore, ultimately, the capability to obtain further ISASecure EDSA certifications throughout the life of a product will depend upon the supplier maintaining adherence to SDLA requirements for their development lifecycle process as specified in [SDLA-300].

However, once a specific version of an embedded device has achieved ISASecure EDSA certification, it retains this certification regardless of changes in the supplier's development process or the certification status of this process.

4.2 Modified devices

When a particular release of a device achieves, for example, ISASecure EDSA 1.0.0 certification, this particular device version retains this specific certification indefinitely. A device supplier is not *required* to update an embedded device certification for every field patch and new release of the device. The decision to certify a later device version is ultimately an optimization of end customer opinion and cost to the supplier. However, the device supplier is required to clearly communicate to the marketplace which version of their device meets the ISASecure criteria, and which version of the criteria it meets, as stated in Requirement ISASecure_ED.R3 of [EDSA-300].

If a device has achieved certification, and a modified version of that device is submitted for certification, the supplier may at their option request consideration for the prior certification evidence for any or all of the certification elements SDLPA, SDA-E, FSA-E, and ERT. For those elements for which consideration is requested, a well-defined evidence impact assessment is performed that ultimately determines which aspects of the certification evaluation will need to be carried out for the modified device. Given the scope of changes to the device and security development process, if such an assessment is determined not to support an update of the evaluation with confidence, the certifier may elect to perform any or all of the evaluation elements in full for the modified device. If an evidence impact assessment is performed and shows that the modifications to the device, its documentation and the supplier security development process would not affect the certification results for one or more of these elements, then no certification tests or evaluations will be necessary in order for the modified device to pass that element of certification. In other cases, partial evaluations may be sufficient. The nature of modifications together with the quality of the analysis of the modifications that is required to be submitted by the supplier to the certifier, are the major factors in determining the effort required to obtain a certification for a modified product. However, by policy, CRT is always run in its entirety on a device if any aspects of these test results may have been affected. Also, by policy, VIT is always run in its entirety on the modified device.

User documentation changes are evaluated along with changes to the device itself when a modified device is submitted for certification. However, a device that has had only user documentation changes is considered to retain its certification if the device itself has not changed.

Section 6 provides requirements for certification of modified devices.

4.3 Updated ISASecure criteria

As in the case of device modifications, a device supplier is not required to update an embedded device certification to the latest ISASecure version. Hence, for example, a device certified to ISASecure EDSA 1.0.0 is not required to obtain a certification to ISASecure EDSA 2.0.1. However, all devices going through certification after ISASecure EDSA 2.0.1 becomes available will be certified to that ISASecure EDSA version.

Consider the case where a device achieved certification under ISASecure EDSA 1.0.0, and this same device version is submitted for certification to the new certification version ISASecure EDSA 2.0.1. This certification process will consist of carrying out the defined delta between the two certification versions.

In most cases both the device and the ISASecure EDSA certification version will have changes. Consider the case where a device achieved certification under ISASecure EDSA 1.0.0, and a *modified* device version is submitted for certification to ISASecure EDSA 2.0.1. This certification process will be logically equivalent to first certifying this modified device to ISASecure EDSA 1.0.0 using the approach described in 4.2, and then carrying out the defined delta between the two certification versions on the modified device.

Section 7 provides requirements for certification to updated ISASecure EDSA certification criteria. Section 8 provides requirements for certifications when both the device and the certification criteria have been updated.

4.4 Certification to a higher security level

Once a device has achieved ISASecure EDSA certification at a specified security level, the device supplier may modify the device or available process evidence as deemed necessary, and then apply for a higher level certification. As noted in 4.1, the supplier must hold an ISASecure SDLA certification at least at this new security level, or undergo an evaluation to this level of SDLA criteria as part of the embedded device certification, to achieve an EDSA certification to a higher security level. Any device modifications are assessed to the original security level following the approaches outlined in 4.2. The certifier will evaluate the FSA-E and SDA-E certification criteria that apply for the new desired security level, but did not apply at the original security level. Finally, the certifier will rerun VIT and apply the pass/fail criterion for the new level. Section 9 provides requirements for this case.

5 EDSA certification elements for a modified device - SDLPA

This section addresses maintenance of certification for the SDLPA element of an EDSA embedded device certification. The SDLPA element allows for leveraging of certification effort across multiple products, in a manner distinct from the other EDSA certification elements.

The SDLPA element of an EDSA certification examines the existence of a documented SDL (Security Development Lifecycle) process for an organization. The related SDA-E element examines adherence to this process in the development of the candidate embedded device. Maintenance of SDA-E evidence that a modified device has adhered to the SDL process is discussed in later sections. This section discusses maintenance of SDLPA evidence for the continued existence of a documented process, when a modified embedded device is submitted for EDSA certification.

If a supplier submits multiple products for certification, it is likely that the assessment related to the existence of the SDL process, will be directly applicable to any number of these certifications. A supplier may choose to formalize this leverage by obtaining a separate ISASecure SDLA certification, which certifies the supplier's security development process independent of specific products. A supplier that applies for an initial or subsequent EDSA product certification, and holds a separate SDLA process certification, need take no further action to meet the SDLPA element of the EDSA product certification. If a supplier does not hold an ISASecure SDLA process certification, the certifier must revisit the SDLPA element of the EDSA evaluation when a modified embedded device is submitted for certification. However the certifier will take into consideration prior ISASecure process audit evidence from any product certification previously achieved by the supplier, as stated in [EDSA-300] Requirement ISASecure_ED.R6. For EDSA certification, this consideration applies whether multiple certifications represent several releases of the same embedded device model or several different products, which may be products of the same or different type (such as embedded devices and system products). The requirements in this section detail this approach.

The following submission to the EDSA certification process by the embedded device supplier supports the certifier in considering the applicability of evidence from prior ISASecure audits of the supplier's security development process, toward a later EDSA certification.

Requirement ISASecure_EDM.R1 – Submission of analysis of SDLA requirements

If an embedded device supplier does not hold an applicable ISASecure SDLA process certification, they present a modified device for EDSA certification where the embedded device previously achieved EDSA certification, and they request consideration for the evidence from that prior SDLPA assessment and/or any other prior ISASecure audits of the supplier's security development process, then the supplier SHALL submit the following to the EDSA certification process:

- an analysis of the SDLA matrix, that for each numbered requirement, considering the validation activity in the column labeled “Development Organization and SDL Validation Activity” in [SDLA-312], either:
    - States that no additional actions beyond those previously carried out to meet this requirement under prior ISASecure audits of their security development process, were required to meet this validation requirement for this EDSA certification, or
    - Briefly describes additional actions beyond those previously carried out to meet this requirement, which were carried out to meet this validation requirement for this certification.

NOTE Regardless of whether the device supplier holds an ISASecure SDLA process certification, a submission is always required of an analysis of the SDLA requirements with respect to potential changes to embedded device artifacts that are outputs from this process for a particular modified device presented for certification, per Requirement ISASecure _EDM.R3 below, related to the SDA-E evaluation element. Requirement ISASecure_EDM.R1 adds the requirement to analyze any potential changes related to evidence previously submitted regarding the existence of a documented SDL process, which is the SDLPA evaluation element. For example, the development group for the modified device may have changed its approach to meeting some EDSA SDLA requirements, or the modified device may have been developed by a different development group than previously, so that prior evidence that describes the SDL applicable to this device no longer applies. In either case it is possible that different process approaches and tools are in place, and therefore different evidence of compliance with SDLA requirements may be needed.

Requirement ISASecure_EDM.R2 – SDLPA certification element for EDSA after achieving first certification

A modified embedded device submitted for certification where that device has previously achieved EDSA certification SHALL pass the SDLPA element of the certification if either the first two or the third condition below are met:

- the certifier determines that the development process and tools as used in creating the submitted device are the same, equivalent or better than those used in creating the prior device that achieved certification;
- the certifier validates in the context of the submitted device, those requirements which they would judge would require additional supplier actions beyond that previously carried out to meet these SDLA requirements for the prior certification, and all are assessed as pass;
- the organization that will develop the modified device going forward holds an ISASecure SDLA certification at the time of application for the certification of the modified device, at greater than or equal to the security level of the EDSA certification sought.

The SDLPA report in the first case MAY include only a summary describing the certifier's conclusion of the first bullet above, a summary of the validations performed, plus a reference to the prior ISASecure audits of the security development process for this organization.

6 Requirements for certification of modified devices

The requirements in this section cover certifying a modified device, when a previous version of the device has already been certified.

6.1 Criteria for applying certification evidence from previous device version

The following requirements provide the general criteria under which evidence from prior certifications is considered applicable toward earning certification for a modified device. Specific requirements on how these criteria are evaluated follow in Section 6.3.

Requirement ISASecure_EDM.R3 – SDA-E certification element for a modified device

If an embedded device has been certified, then a modified version of the device SHALL on the basis of that prior evidence pass the SDA-E element of certification if:

- the certifier determines that an evidence impact assessment to determine whether the device modifications may have impacted each line item of the SDA-E can be performed with confidence (where a line item is a cell in the [SDLA-312] matrix, in the column applicable to product certifications, applicable to the security level of the EDSA certification); and
- the certifier carries out this assessment; and
- the certifier has evaluated at their discretion, any (and possibly all) of the artifacts associated with the potentially impacted SDA-E line items, and given them pass status.

The SDA-E report in this case MAY include only a summary of the evidence impact assessment relative to SDA-E, and the validations performed, plus a reference to the initial SDA–E evaluation for the device. If the certifier judges that such an evidence impact assessment cannot be performed with confidence, the certifier SHALL carry out a full SDA-E evaluation for the embedded device as described in [EDSA-312].

Requirement ISASecure_EDM.R4 – FSA-E certification elements for a modified device

If an embedded device has been certified, then a modified version of the device SHALL on the basis of that prior evidence pass the FSA-E element of certification if:

- the certifier determines that an evidence impact assessment for the prior FSA-E results for the embedded device can be performed with confidence; and

- the certifier carries out this assessment and shows that device modifications have either not impacted these results, or may have impacted few FSA-E line items in [EDSA-311] in a manner isolated from other line items; and

- the certifier has evaluated any potentially impacted FSA-E line items and given them pass status.

Device modifications SHALL be shown to have no impact on results for a line item of the FSA-E by showing:

- No architecture change, functionality change or significant new code has been incorporated related to a security feature referenced by the line item of the FSA-E.

In this case the certification report covering FSA-E MAY consist of only a summary of the FSA-E evidence impact assessment, results for those line items that were evaluated, and a reference to the initial certification report for the embedded device. If the certifier determines that an FSA-E evidence impact assessment cannot be performed with confidence, or that embedded device changes related to the FSA-E are widespread, then the certifier SHALL perform the full FSA-E for the embedded device and a full report SHALL be provided for that certification element.

NOTE It is well understood that security features do not stand alone and are inherently interrelated in providing coherent protection for a device. Therefore if there are sufficient changes to security functionality for an embedded device which it appears may interact, then the full FSA-E is likely to be performed on the modified device. This is because an evidence impact assessment attempting to isolate the line items affected by the modifications, will likely need to examine all FSA-E line items to gain confidence, which will make this assessment essentially equivalent to simply performing a full FSA-E.

Requirement ISASecure_EDM.R5 – CRT certification element for a modified device

If an embedded device has been certified, then a modified version of the device SHALL on the basis of that prior evidence pass the CRT element of certification if:

- the certifier determines that an evidence impact assessment for CRT results can be performed with confidence; and

- the certifier carries out such an assessment and shows that device modifications have not impacted CRT results.

Device modifications SHALL be shown to have no impact on CRT results by showing:

- No architectural modifications have been made to any network protocols, essential functions, or their interactions; and

- No significant new code has been incorporated for any network protocol, essential function, or their interactions; and

- Any changes to user documentation that impact mitigation guidance required due to CRT results are deemed appropriate.

If it is determined per these criteria that no aspects of CRT results have been affected, the certification report covering CRT MAY consist of only a summary of the CRT evidence impact assessment and a reference to the initial certification reports for the device. If either of the types of code changes in the first two bullets directly above has been made to the device itself, or if the certifier determines that such an assessment of changes cannot be done with confidence, the modified device SHALL undergo the full CRT certification element, for all applicable protocols, in order to achieve certification for this element and a full report SHALL be provided. If only user documentation changes per in the third bullet have taken place, then testing is not required, and the modified device SHALL pass CRT based upon an evaluation of the documentation changes that shows they meet the criteria in the third bullet above.

6.2 VIT assessment for a modified device

VIT is always rerun for a modified device, as detailed in the following requirements. The concept of "consideration for prior evidence" does not apply for the VIT certification element.

Requirement ISASecure_ EDM.R6 – VIT certification element for a modified device

If a embedded device has been certified, and a revised device later presented for certification, VIT SHALL be executed on the modified device such that the test meets the same requirements as for an initial certification, as described in [EDSA-310] and [EDSA-420]. In some cases it may be run by the supplier instead of the chartered laboratory. In particular, if any CRT tests are required for the certification of the revised device per Requirement ISASecure_EDM.R5, then VIT SHALL be performed by the chartered laboratory. If no CRT tests are required, the chartered laboratory MAY permit the supplier to perform VIT in accordance with the requirements in [EDSA-310] and [EDSA-420], and to submit the results. The chartered laboratory MAY rerun the test at their discretion.

Requirement ISASecure_ EDM.R7 – Requirements on supplier-executed VIT for modified device

If a supplier executes VIT toward certification of a revised device under the conditions in Requirement ISASecure_EDM.R6, this process SHALL meet the following requirements:

- supplier personnel responsible for the VIT SHALL have successfully completed a training class or 1 year of job experience demonstrating proficiency with the VIT tool to be used;
- the supplier SHALL run the test with a policy file provided by the chartered laboratory;
- the chartered laboratory SHALL witness execution of the VIT by the supplier, including starting the test, saving the report file, and signing of the report. This witnessing MAY be achieved remotely.
- the supplier SHALL submit as evidence of VIT:
    - documentation of the tested device configuration, that contains the same information the chartered laboratory would record if they performed the test;
    - the policy file used to run the test;
    - the command line that was executed to run the test; and
    - the full report from the VIT tool; and
- the VIT evidence submitted to the chartered laboratory SHALL be signed by a responsible representative of the supplier.

6.3 Evidence and assessment for criteria

If based upon the criteria in Section 6.1, a device supplier believes that some of the evidence used to certify a previous version of a device is applicable toward certification of a modified device, they may request consideration for this evidence. In this case, their submission of data toward certification of the modified device will include supporting evidence to demonstrate that the criteria stated in the requirements of 6.1 are met. This section specifies the nature of that supporting evidence and how the certifier carries out an evidence impact assessment relative to the evidence from the prior certification evaluation, based upon the suppliers' supporting evidence regarding device changes.

Requirement ISASecure_EDM.R8– Submission of device modification data

A device supplier applying for certification for a modified device, MAY request consideration for SDA-E, FSA-E and/or CRT evaluations done on a prior version of the device that achieved certification. If so, the applicant SHALL submit to the certification process:

- a high level description of modifications to the device since the previous certification;
- a mapping from the elements of this description to a detailed change log extracted from the CM system for the device software; and
- evidence that this extraction from the CM system constitutes all changes in the modified device; and
- a list of any third party sub components that had new CVE reports against them since the prior certification; whether or not addressed by the time of application for certification; and
- a list of any changes in third-party supplied sub components such as an OS service pack update; and
- a high level summary of any changes to user documentation related to device security.

Requirement ISASecure_EDM.R9 – Submission of analysis of device modifications

If a device supplier has submitted evidence per Requirement ISASecure_EDM.R8– Submission of device modification data, then they shall in addition submit the following to the certification process:

- If consideration is requested for prior SDA-E evidence,
    - an analysis of the SDA-E matrix, that for each numbered requirement, considering the validation activity in the column labeled “Applies for Component or System Certification” in [SDLA-312], either:
        - States that no additional actions beyond those previously carried out to meet this requirement for the prior certification are required to meet this validation requirement for this certification, or
        - Briefly describes additional actions beyond those previously carried out to meet this requirement for the prior certifications, which were carried out to meet this validation requirement for this certification.
- If consideration is requested for FSA-E: an analysis of the FSA -E matrix, that notes for each numbered line item in [EDSA-311] that applies to the security level for the EDSA certification, whether there is any change to the functionality or code described by this requirement, among the device modifications since the previous certification. If so, the applicant SHALL provide a mapping to the related code modifications at the CM level of detail (as reported under Requirement ISASecure_EDM.R8).
- If consideration is requested for CRT: an analysis of the modifications reported under Requirement ISASecure_EDM.R8 that SHALL state which if any of these changes modified the code implementing the protocols subject to ISASecure CRT or the usage of these protocols by the essential functions as defined in [EDSA-310], and SHALL include rationale for the conclusion that a modification did not occur.

Requirement ISASecure_EDM.R10 – Determination of no evidence impact for SDA-S line item

When performing an evidence impact assessment for a modified device where a prior version has been certified, the certifier SHALL determine that no modifications that may impact the assessment results for a particular line item of the SDA-E evaluation have occurred if:

- the analysis submitted of the SDA-E matrix as described under Requirement ISASecure_EDM.R9 reports no impact; and

- a certifier review of evidence submitted per Requirement ISASecure_EDM.R8 and Requirement ISASecure_EDM.R9 finds no indication of such an impact after consultation with the device supplier.

Requirement ISASecure_EDM.R11 – Determination of no evidence impact for FSA-E line item

When assessing modifications for a modified device where a prior version has been certified, the certifier SHALL determine that no modifications that may impact the assessment results for a specific FSA-E line item have taken place if:

- the analysis submitted of the FSA-E matrix as described under Requirement ISASecure_EDM.R9 reports no changes to functionality covered by this line item of the FSA-E since the last certification; and

- a certifier review of evidence submitted per Requirement ISASecure_EDM.R8 and Requirement ISASecure_EDM.R9 finds no indication of such changes after consultation with the device supplier.

Requirement ISASecure_EDM.R12 – Determination of no evidence impact for CRT

When performing an evidence impact assessment for a modified device where a prior version has been certified, the certifier SHALL determine that no modifications that may impact CRT results have taken place if

- the analysis submitted of changes to protocol or essential services code as described under Requirement ISASecure_EDM.R9 reports no changes to this code since the prior certification; and

- a certifier review of the evidence submitted per Requirement ISASecure_EDM.R8 and Requirement ISASecure_EDM.R9 finds no indication of such changes after consultation with the device supplier.

Requirement ISASecure_EDM.R13 – Criteria for granting a certification to a modified device

If an embedded device has been certified to security level *n*, then a modified version of the device SHALL be granted certification to the same level and ISASecure EDSA version if:

- criteria for passing the SDLPA element of certification are met per Requirement ISASecure_EDM.R2; and

- criteria for passing the SDA-E element of certification are met per ISASecure_EDM.R3 and Requirement ISASecure_EDM.R10

- criteria for passing the FSA-E element of the certification are met per ISASecure_EDM.R4 and Requirement ISASecure_EDM.R11; and

- criteria for passing CRT element of certification are met per Requirement ISASecure_EDM.R5 and ISASecure_EDM.R12; and

- criteria for passing the VIT element of certification are met per ISASecure_EDM.R6 and R7.

Alternatively, for each of the evaluation elements SDLPA, SDA-E, FSA-E, and CRT for which the supplier did not request consideration for the prior certification per Requirement ISASecure_EDM.R1 and Requirement ISASecure_EDM.R8, the certifier SHALL evaluate that element under the criteria for initial certification found in [EDSA-300].

7 Certification to updated ISASecure criteria

The requirements in this section cover certification of a device that holds a prior certification, to a later version of the ISASecure certification criteria. These requirements suffice in the case that the device itself has not undergone modifications as well. If it has, see Section 8.

Requirement ISASecure_EDM.R14 – SDLPA and SDA-E elements for certification to a later ISASecure EDSA version

A device that has been ISASecure EDSA certified SHALL pass the SDLPA and SDA-E elements of a certification to a later ISASecure EDSA version if:

- any new SDLA and SDA-E requirements added in this ISASecure EDSA version are assessed as pass for the device; and
- any changed SDLA and SDA-E requirements in this ISASecure EDSA version are assessed as pass for the device.

Requirement ISASecure_EDM.R15 – FSA-E element for certification to a later ISASecure EDSA version

A device that has been ISASecure EDSA certified SHALL pass the FSA-E element of a certification to a later ISASecure version if:

- any new FSA-E requirements added in this ISASecure version are assessed for the device as either supported or allocatable; and
- any changed FSA-E requirements in this ISASecure version are assessed for the device as either supported or allocatable.

Requirement ISASecure_EDM.R16 – ERT element for certification to a later ISASecure version

A device that has been ISASecure EDSA certified SHALL pass the ERT element of a certification to a later ISASecure version if:

- for any new protocols added in this ISASecure version, applicable tests as specified by the later ISASecure CRT specification are carried out and pass; and
- if there is a change in CRT test requirements for a previously certified protocol, then a full CRT for this protocol that meets the requirements of the later ISASecure specification version is carried out and passes; and
- the device passes VIT under the requirements in 6.2.

Requirement ISASecure_EDM.R17 – Criteria for granting a certification to a later ISASecure version

A device that has been ISASecure EDSA certified to level *n* SHALL be granted a certification to a later ISASecure version at this same level if:

- Certification criteria for passing SDLPA and SDA-E for level *n* are met per **Error! Reference source not found.**; and
- Certification criteria for passing the FSA-E for level *n* are met per Requirement ISASecure_EDM.R15 ; and
- Certification criteria for passing the ERT for level *n* are met per Requirement ISASecure_EDM.R16.

The certification report SHALL cover only the tests and assessments performed for the certification as defined by these requirements.

8 Certification when both device and ISASecure version have changed

It will be a common scenario that a device will have changed slightly by the time a new version of ISASecure EDSA certification criteria is released. Thus it will be useful to be able to certify a slightly modified device to a newer version of ISASecure, without repeating the overall process. The following requirement provides a means to achieve this. It states that requirements are met in this case for both certification of modified devices and certification to later ISASecure versions.

Requirement ISASecure_EDM.R18 – Certification of a modified device to a later ISASecure version

For a device that previously received an ISASecure certification, a certifier SHALL grant a recertification to a later ISASecure version for a modified device if the criteria in both Requirement ISASecure_EDM.R13 and Requirement ISASecure_EDM.R17 are met.

9 Certification to a higher ISASecure EDSA level

Once a device has achieved certification at ISASecure EDSA certification at level *n*, the supplier may modify the device or available process evidence as deemed necessary, and then apply for a higher level certification. The following requirement applies in this situation.

Requirement ISASecure_EDM.R19 – Certification of a device to a higher ISASecure level

For a device that previously received an ISASecure certification to level *n*, a certifier SHALL grant a certification to a higher ISASecure security level for a (possibly modified) device if:

- If the device has been modified, the criteria for granting a certification at the original level *n* for the modified device are met per Requirement ISASecure_EDM.R13; and

- The additional SDA-E and FSA-E requirements present at the desired new level certification that are not present at level *n* have been assessed as pass; and

- The supplier either passes an ISASecure SDLPA assessment for requirements at the new security level, or holds an ISASecure SDLA certification at the time of granting of the certification incorporating the new level; and

- VIT has passed for the new level, per ISASecure_EDM.R6 and R7.

In this case the certification report SHALL provide content per Requirement ISASecure_EDM.R13 as well as report on the new requirements assessed for the new certification level.