ISASecure-120

ISA Security Compliance Institute — ISASecure® certification programs

Certification process for relabeled products

Version 1.2

June 2023

A. DISCLAIMER

ASCI and all related entities, including the International Society of Automation (collectively, “ASCI”) provide all materials, work products and, information (‘SPECIFICATION’) AS IS, WITHOUT WARRANTY AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the SPECIFICATION, and the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION. Also, there is no warranty or condition of title, quiet enjoyment, quiet possession, correspondence to description, or non-infringement with regard to the SPECIFICATION.

Without limiting the foregoing, ASCI disclaims all liability for harm to persons or property, and users of this SPECIFICATION assume all risks of such harm.

In issuing and making the SPECIFICATION available, ASCI is not undertaking to render professional or other services for or on behalf of any person or entity, nor is ASCI undertaking to perform any duty owed by any person or entity to someone else. Anyone using this SPECIFICATION should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

B. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES

To the maximum extent permitted by applicable law, in no event shall ASCI or its suppliers be liable for any special, incidental, punitive, indirect, or consequential damages whatsoever (including, but not limited to, damages for loss of profits or confidential or other information, for business interruption, for personal injury, for loss of privacy, for failure to meet any duty including of good faith or of reasonable care, for negligence, and for any other pecuniary or other loss whatsoever) arising out of or in any way related to the use of or inability to use the SPECIFICATION, the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION, or otherwise under or in connection with any provision of this SPECIFICATION, even in the event of the fault, tort (including negligence), misrepresentation, strict liability, breach of contract of ASCI or any supplier, and even if ASCI or any supplier has been advised of the possibility of such damages.

C. OTHER TERMS OF USE

Except as expressly authorized by prior written consent from the Automation Standards Compliance Institute, no material from this document owned, licensed, or controlled by the Automation Standards Compliance Institute may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, except for non-commercial use only, provided that you keep intact all copyright and other proprietary notices. Modification of the materials or use of the materials for any other purpose, such as creating derivative works for commercial use, is a violation of the Automation Standards Compliance Institute’s copyright and other proprietary rights.

Revision history

version	date	changes
1.2	2023.06.29	Initial version published to https://www.isasecure.org/

Contents

List of tables

List of figures

List of requirements

FOREWORD

This is one of a series of documents that defines ISASecure® certification programs. This document describes the policies and procedures for claiming certification of products that have been certified under ISASecure product certification programs by one supplier, and are relabeled and resold by another supplier. The list of all ISASecure certification programs and documents can be found on the web site https://www.isasecure.org/.

1 Background and scope

ISCI (ISA Security Compliance Institute) operates the following certification programs:

- ISASecure® CSA (Component Security Assurance), product certification for control system components for conformance to IEC 62443-4-2 and IEC 62443-4-1

- ISASecure ICSA (IIoT Component Security Assurance), product certification for IIoT devices and IIoT gateways, based on IEC 62443-4-2 and IEC 62443-4-1 with exceptions and extensions for the IIoT environment

- ISASecure SSA (System Security Assurance), product certification for off-the-shelf control systems, for conformance to IEC 62443-3-3

- ISASecure SDLA (Security Development Lifecycle Assurance), process certification for an organization's secure product development lifecycle for conformance to IEC 62443-4-1.

In the future other product or process certification programs may be offered.

The present document in Sections 4 and 5 addresses the scenario in which an organization has been granted any ISASecure *product* certification, and this same product, with possibly cosmetic changes for branding purposes, is then resold by a second supplier under their brand. The second supplier is here referred to as the *brand owner*. Policies, procedures, and requirements are specified for a brand owner to obtain and claim certification of a relabeled product.

Situations will arise in which an OEM product may be sold by a different supplier, after incorporating some changes that are not cosmetic. However, the product may still be very similar to one already certified by the OEM supplier. Such a product does not fall under the scope of relabeled product certification. Guidance for that case is planned for a future specification.

2 Normative references

2.1 ISASecure specifications

The specifications that define the existing CSA, ICSA, SSA and SDLA certification programs are listed in:

[CSA-100] CSA-100 *ISCI Component Security Assurance – ISASecure certification scheme,* as specified at https://www.isasecure.org/

[ICSA-100] ICSA-100 *ISCI IIoT Component Security Assurance – ISASecure certification scheme,* as specified at https://www.isasecure.org/

[SSA-100] SSA-100 *ISCI System Security Assurance – ISASecure certification scheme,* as specified at https://www.isasecure.org/

[SDLA-100] SDLA-100 *ISCI Security Development Lifecycle Assurance – ISASecure certification scheme*, as specified at https://www.isasecure.org/

Likewise, the documentation for all ISASecure certifications will include a 100-series document that lists all specifications that define that certification program.

Following are additional specifications for the CSA, ICSA, SSA and SDLA certification programs that are specifically referenced in the present document.

[CSA-204] CSA-204 *ISCI Component Security Assurance – Instructions and Policies for Use of the ISASecure Symbol and Certificates*, as specified at https://www.ISASecure.org

[ICSA-204] ICSA-204 *ISCI IIoT Component Security Assurance – Instructions and Policies for Use of the ISASecure Symbol and Certificates*, as specified at https://www.ISASecure.org

[SSA-204] SSA-204 *ISCI System Security Assurance – Instructions and Policies for Use of the ISASecure Symbol and Certificates*, as specified at https://www.isasecure.org/

[CSA-300] CSA-300 *ISCI Component Security Assurance – ISASecure certification requirements*, as specified at https://www.isasecure.org/

[ICSA-300] ICSA-300 *ISCI IIoT Component Security Assurance – ISASecure certification requirements*, as specified at https://www.isasecure.org/

[SSA-300] SSA-300 *ISCI System Security Assurance – ISASecure certification requirements*, as specified at https://www.isasecure.org/

[CSA-301] CSA-301 *ISCI Component Security Assurance – Maintenance of ISASecure certification,* as specified at https://www.isasecure.org/

[ICSA-301] ICSA-301 *ISCI IIoT Component Security Assurance – Maintenance of ISASecure certification,* as specified at https://www.isasecure.org/

[SSA-301] SSA-301 *ISCI System Security Assurance – Maintenance of ISASecure certification,* as specified at https://www.isasecure.org/

[CSA-312] CSA-312 *ISCI Component Security Assurance – Security development artifacts for components*, as specified at https://www.isasecure.org/

[ICSA-312] CSA-312 *ISCI IIoT Component Security Assurance – Security development artifacts for IIoT components*, as specified at https://www.isasecure.org/

[SSA-312] SSA-312 *ISCI System Security Assurance – Security development artifacts for systems*, as specified at https://www.isasecure.org/

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

[SDLA-312] SDLA-312 *ISCI Security Development Lifecycle Assurance – Security Development Lifecycle Assessment*, as specified at https://www.isasecure.org/

[ISDLA-312] ISDLA-312 *ISCI Security Development Lifecycle Assurance – Security Development Lifecycle Assessment for ICSA*, as specified at https://www.isasecure.org/

2.2 International standards

NOTE The following pairs of references that have the same document number 62443-m-n, provide the same technical standard, as published by the organizations ANSI/ISA and IEC.

[ANSI/ISA-62443-3-3] ANSI/ISA−62443−3−3 (99.03.03) - 2013, *Security for industrial automation and control systems Part 3-3: System security requirements and security levels*

[IEC 62443-3-3] IEC 62443−3−3:2013 *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*

[ANSI/ISA-62443-4-1] ANSI/ISA-62443-4-1-2018 *Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements*

[IEC 62443-4-1] IEC 62443-4-1:2018 *Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements*

[ANSI/ISA-62443-4-2] ANSI/ISA-62443-4-2-2018 *Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components*

[IEC 62443-4-2] IEC 62443-4-2:2019 *Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components*

3 Definitions and abbreviations

3.1 Definitions

3.1.1
brand owner
organization that resells an OEM product under its own brand name

3.1.2
certification
third party attestation related to products, processes, or persons that conveys assurance that specified requirements have been demonstrated

NOTE Here, this refers to either a successful authorized evaluation of a product or a process to ISASecure criteria. This outcome permits the product supplier or organization performing the process to advertise this achievement in accordance with certification program guidelines.

3.1.3
certification body
an organization that performs certification

3.1.4
control system
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.5
cosmetic change
change to appearance with no change to functionality

3.1.6
file with executable content
file which includes a description of processor instructions and for which, if triggered, those instructions are carried out by directly reading the contents of the file

NOTE 1 An .exe file, a .dll file, a Python script (or script in any real-time interpreted language) and a Docker container image are all files with executable content by this definition. C source code is not a file with executable content.

NOTE 2 The definition does not specify the mechanism used to carry out the processor instructions – it may be the processor itself and/or an interpreter program.

3.1.7
functional security assessment
assessment of a defined list of security features for a control system, embedded device, or other control system component

3.1.8
industrial automation and control system
collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure, and reliable operation

3.1.9
OEM product
product which an OEM supplier manufactures and sells to other organizations for the purpose of resale under a brand name of the reselling organization

NOTE Such an “other organization” is referred to here as a brand owner, see 3.1.1.

3.1.10
OEM supplier
manufacturer of an assembly or product

NOTE 1 OEM is a common term used to identify a position in the supply chain.

NOTE 2 The assembly or product might be regarded as a component by a customer.

3.1.11
relabeled product
OEM product being sold by a brand owner under their brand

3.1.12
update
incremental hardware or software change in order to address security vulnerabilities, bugs, reliability or operability issues

3.1.13
upgrade
incremental hardware or software change in order to add new features

3.2 Abbreviations

The following abbreviations are used in this document.

ANSI	American National Standards Institute
ASCI	Automation Standards Compliance Institute
CSA	Component Security Assurance
dll	dynamic link library (file extension)
DM	defect management
EDR	embedded device requirement
exe	executable file (file extension)
FSA	functional security assessment
IACS	industrial automation and control system(s)
ICSA	IIoT Component Security Assurance
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
ISO	International Organization for Standardization
OEM	original equipment manufacturer
PLC	programmable logic controller
SDA	security development artifacts
SDL	security development lifecycle
SDLA	Security Development Lifecycle Assurance
SDLPA	Security development lifecycle process assessment
SM	security management
SSA	System Security Assurance
VIT	vulnerability identification testing

4 Overview of the certification process for relabeled products

This section provides an informal overview of the ISASecure certification process for relabeled products. Section 5 provides the formal description of this process, in a series of numbered requirements.

The terms *OEM product*, *OEM supplier*, *relabeled product*, and *brand owner* are used throughout this document and defined in 3.1.

4.1 Scope of application

At a high level, a relabeled product is eligible to use the product certification process for relabeled products specified in the present document, if:

- an OEM supplier has achieved certification for an OEM product associated with the relabeled product; and

- differences between the relabeled product and the associated OEM product are cosmetic only; and
- any cosmetic changes to the OEM product to create the relabeled product that will be sold to the end customer by the brand owner, are present in the product as sold by the OEM supplier to the brand owner; and
- the security context for the relabeled product is the same as that presented (as required under IEC 62443-4-1) as an artifact for the certification of the associated OEM product.

NOTE The third bullet rules out application of the process in this document if the brand owner carries out any branding or other changes to the product after it receives the product from the OEM supplier.

The two use cases to which this process applies are pictured in Figure 1 and Figure 2. Figure 1 depicts the case in which the OEM supplier builds a fully custom and branded product specifically for the brand owner, and achieves certification for this product. Although the brand owner is delivering a physically identical product to that which achieved certification under the OEM supplier, in order for the brand owner to advertise a certified product, the brand owner must obtain its own certification for the product. This is required because the brand owner is necessarily involved in supporting its customers for maintenance of security of the product after the sale, and therefore requires a certification for the product that at a minimum, addresses those lifecycle processes.

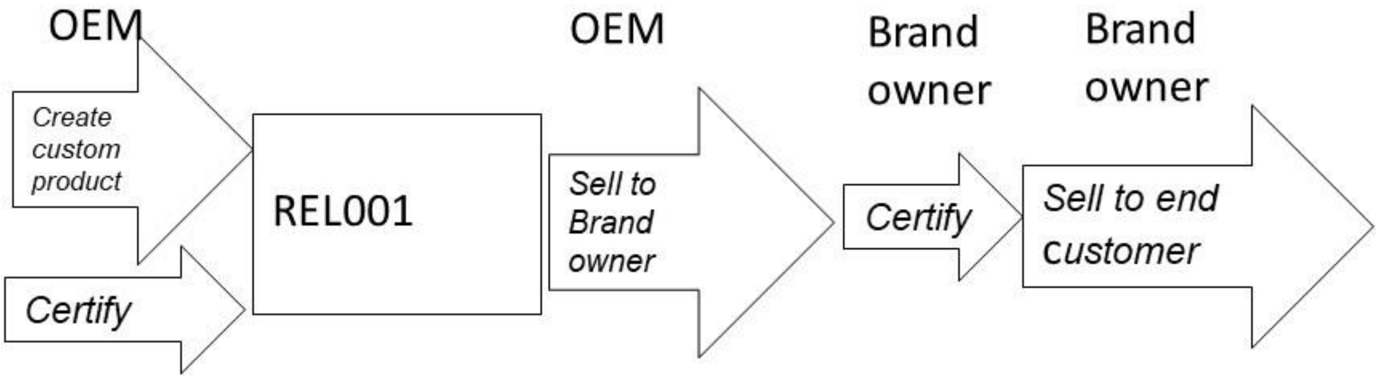


Figure 1. Use case 1: OEM certifies fully customized product

In the second use case shown in Figure 2, the OEM supplier also delivers a branded product to the brand owner. The difference is that the OEM has certified a generic product, and not the customized version. In this case, the generic product is not built specifically for the brand owner. In order to advertise a certified product, in this situation, the brand owner also must obtain a certification for the branded product.

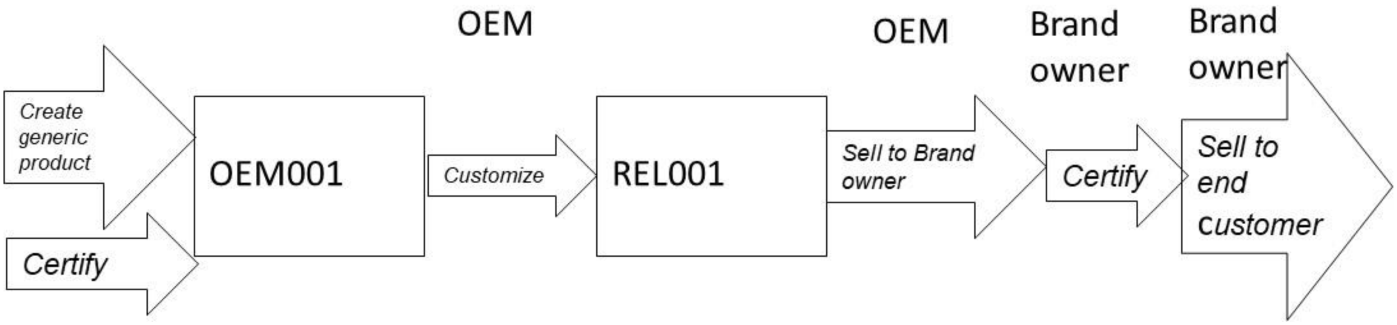


Figure 2. Use case 2: OEM certifies generic product then makes cosmetic customizations

4.2 ISASecure product certification background

The following summary of criteria for ISASecure product certification, is provided as background for understanding the certification process for relabeled products.

Each ISASecure product certification has the following elements (as specified in CSA-300, ICSA-300, or SSA-300):

- Security Development Lifecycle Process Assessment (**SDLPA**) – supplier holds an ISASecure SDLA (Security Development Lifecycle Assurance) certification

- Security Development Artifacts (**SDA**) – artifacts from the specific product development are assessed for conformance with IEC 62443-4-1

- Functional Security Assessment (**FSA**) – product functional capabilities are assessed for conformance to requirements for the certification program (for example, conformance to IEC 62443-4-2 for CSA)

- Vulnerability Identification Testing (**VIT**) – a Nessus vulnerability scan is performed on the product and meets a specified threshold for vulnerabilities found.

4.3 Process overview

Figure 3 illustrates the streamlined process offered under ISASecure, for a relabeled product to achieve certification as sold by a brand owner, where the OEM supplier for that product has previously achieved ISASecure certification for the associated OEM product. This process is called the “ISASecure certification process for relabeled products.”

The three boxes highlighted in yellow at the left of Figure 3, show the process for verifying and documenting that the relabeled product meets the eligibility criteria listed above in 4.1 (further defined in Section 5). The certification body collects a specified set of information regarding the OEM product and associated relabeled product, and verifies eligibility based upon that information. If the relabeled product is eligible, the certification process for relabeled products may continue.

The process further requires that the brand owner holds an ISASecure SDLA certification, which may be limited in scope to address those lifecycle practices for the relabeled product in which the brand owner participates. This is represented by the boxes labeled “process scoping” and “SDLPA” in Figure 3. A minimum set of IEC 62443-4-1 requirements in which the brand owner will necessarily participate is defined in the present document (Section 6 Appendix). Examples of requirements in this minimum set are:

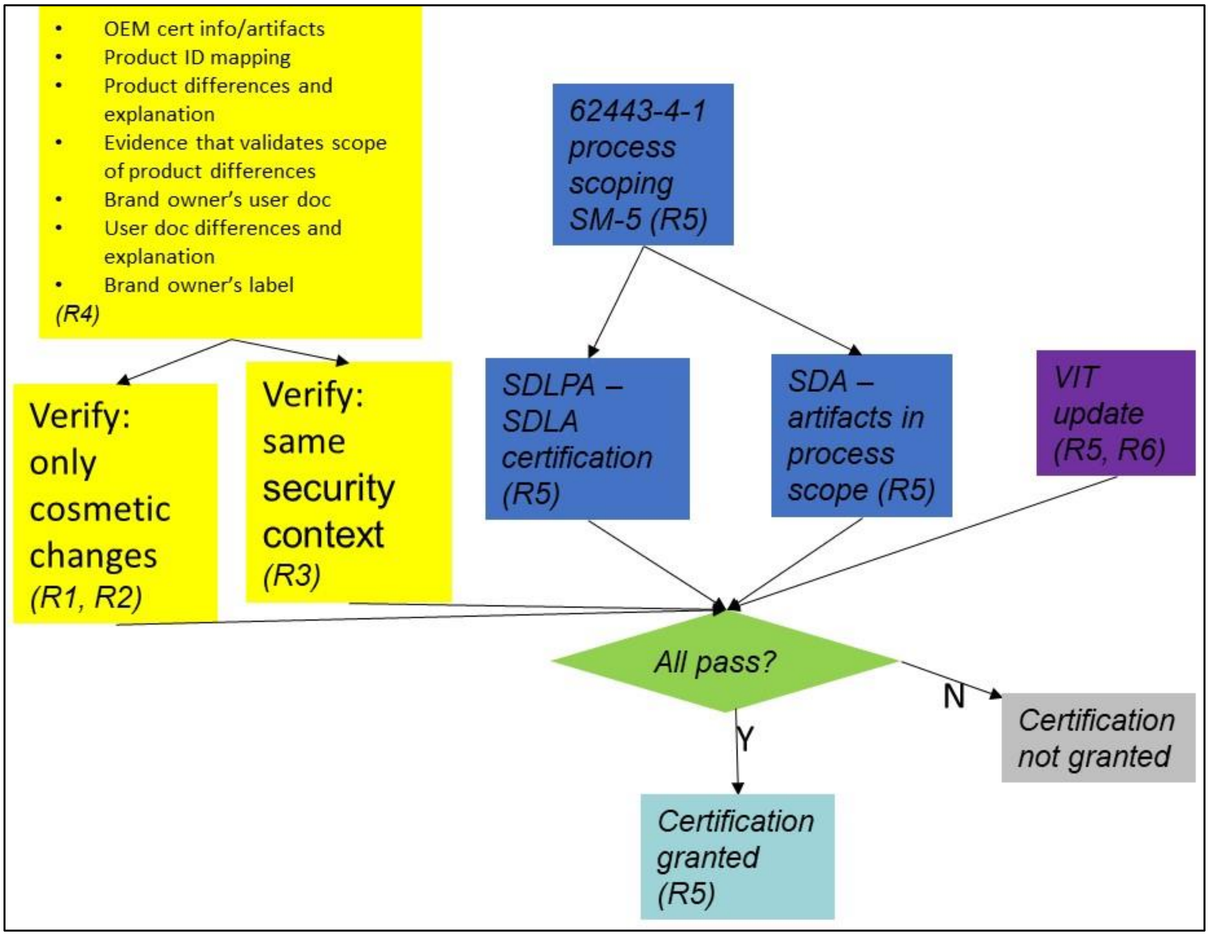
- SM-9 *Security requirements for externally provided components*, which requires a security risk management process for the overall resale process

- DM-1 *Receiving notifications of security related issues*, which will apply at a minimum for security issues about the product reported to the brand owner by the brand owner’s customers or other external sources.

Conformance to additional SDLA requirements may be required under this limited SDLA certification, for example, if the brand owner participates in investigating security issues in the field or delivering security updates to their customers.

For the brand owner’s certified lifecycle practices, artifacts from these practices as carried out for the relabeled product are examined under the SDA element of the certification process. This is shown in the box labeled SDA in Figure 3.

Finally, ISASecure certification requires a vulnerability scan of a product within a specified length of time of issuance of the ISASecure certificate. The certification body, the brand owner, or the OEM supplier can carry out this scan in support of the certification process, on the relabeled product. This is shown in the box labeled “VIT update” in Figure 3.



- OEM cert info/artifacts
- Product ID mapping
- Product differences and explanation
- Evidence that validates scope of product differences
- Brand owner's user doc
- User doc differences and explanation
- Brand owner's label
(R4)
62443-4-1 process scoping SM-5 (R5)
Verify: only cosmetic changes (R1, R2)
Verify: same security context (R3)
SDLPA – SDLA certification (R5)
SDA – artifacts in process scope (R5)
VIT update (R5, R6)
All pass?
N
Y
Certification not granted
Certification granted (R5)

Figure 3. ISASecure initial certification process for relabeled products

The major simplifications of the certification process for the brand owner, gained due to the existing certification of the OEM product are:

- The FSA element of certification is fully satisfied by the OEM certification. Therefore, it does not appear as a separate activity in the figure.
- The majority of the requirements of the SDLPA and SDA elements of certification are satisfied by the OEM certification. The SDLA certification for the brand owner may be limited in scope, since no further development is performed on the product by the brand owner.

The requirements for the ISASecure certification process for relabeled products, are described formally in the following Section 5. Requirement numbers in that section correspond to the labels “Rn” shown in Figure 3.

5 Requirements for certification of relabeled products

The following requirements apply when a brand owner is selling a relabeled product, where the OEM supplier holds an ISASecure certification for the associated OEM product.

Requirement RELABEL.R1 – Cosmetic changes only A relabeled product SHALL differ only by cosmetic changes from its associated OEM product to be eligible for the certification process for relabeled products. This judgment SHALL be made by the certification body for the relabeled product based upon product comparison information required from the OEM supplier and the brand owner per this specification. User documentation SHALL also differ only by cosmetic changes.

Requirement RELABEL.R2 – Limitations on cosmetic changes A change SHALL NOT be classified as cosmetic for the purposes of eligibility for the certification process for relabeled products, if it changes the manner in which any FSA requirement is met. For a change to software to be classified as cosmetic, it SHALL meet the definition of cosmetic (3.1.5), and SHALL be implemented in the product sold by the OEM supplier to the brand owner. Further, evidence SHALL be provided that any differences between the certified OEM product and the product sold by the brand owner, in the as-delivered list of files with executable content (3.1.6), and to any content of those files, consist of cosmetic changes only. For those files with executable content declared to be exactly the same in the two products, this shall be demonstrated using a hash function. Otherwise, evidence SHALL be provided to demonstrate that changes are cosmetic only. An example of such a demonstration would be a comparison of build instructions for both products showing any differences, and then further comparison of any files that differ within those instructions.

NOTE 1 For example, if the brand owner uses a different external physical case for the product, this is not a cosmetic change if the case incorporates different piece parts than the certified OEM product, via which the product meets the CSA requirement FSA-EDR 3.11 *Physical tamper resistance and detection*.

NOTE 2 For example, to meet this requirement regarding files with executable content, a cosmetic change to software can be implemented using a configuration file that does not change any files with executable content, or by a change to a file with executable content that is demonstrated to be cosmetic only.

Requirement RELABEL.R3 – Same security context A relabeled product SHALL have the same security context used to support the certification of its associated OEM product, to be eligible for the certification process for relabeled products.

Requirement RELABEL.R4 – Product information required for certification of relabeled product The following product information SHALL be submitted when applying for certification of a relabeled product under the certification process for relabeled products:

- From OEM supplier
  - ISASecure certificate number of OEM product
  - Associated artifacts and analyses related to the OEM product certification required for the certification body to carry out the certification process for relabeled products
- Declared by both OEM supplier and brand owner:
  - Mapping of product identifiers between OEM product and relabeled product (which defines the OEM product "associated with" a relabeled product)
  - Documented comparison of certified OEM product and relabeled product – any cosmetic differences and an explanation of them
  - Evidence that demonstrates the following items are the same in the certified OEM product and relabeled product:
    - Code – except for cosmetic changes as described in Requirement RELABEL.R1 and RELABEL.R2

        - Factory-set configuration - except for cosmetic changes as described in Requirement RELABEL.R1 and RELABEL.R2
        - Interfaces
        - Hardware components
    - Explanation of any differences between the user documentation to be delivered with the relabeled product, and the OEM user documentation used to support the OEM's certification for the OEM product
- From the brand owner
    - Attestation that only the mapped OEM product is used to create brand owner products that are given the identifier of the relabeled product
    - Brand owner's user documentation for the relabeled product
    - For physical devices, image of label on relabeled product showing brand owner name, address, product name and identifier.

NOTE 3 This requirement implies the certification process for relabeled products requires that some artifacts and analyses related to the OEM product certification be releasable to the certification body performing the certification of the relabeled product. The certification body for the relabeled product is not required to be the same organization as the certification body that granted the OEM product certification.

Requirement RELABEL.R5 – Certification criteria for relabeled product

A product certification SHALL be granted for a product eligible for the certification process for relabeled products, and where the brand owner has applied for certification under this process as described in requirements RELABEL.R1 – R4, if the criteria under the certification elements shown in Table 1 are met.

Table 1. Certification criteria for relabeled product

Element	Certification Criteria
SDLPA	Brand owner SHALL hold an ISASecure SDLA certification for SDL (Security Development Lifecycle) processes they perform for the relabeled product, and the documented scope of the process includes the relabeled product. See Table 2 for minimum SDL requirements that SHALL be evaluated, and required aspects that SHALL be included in validating conformance to the SDL requirements.
SDA	Certification body SHALL assess SDA artifacts in SDLA-312 (column titled "Component or System Validation Activity") for all SDLA requirements in scope for the brand owner's SDLA certification. The results SHALL meet the criterion for passing SDA described in the relevant certification program document describing SDA (e.g., CSA-312, ICSA-312, SSA-312).
FSA	OEM certification for associated OEM product SHALL BE in valid status.
VIT	The relabeled product SHALL meet ISASecure program certification criterion for VIT, except that VIT on the relabeled product MAY be performed by either the certification body, the OEM supplier, or the brand owner. The VIT certification criterion is described in SSA-420, which applies to all ISASecure product certification programs, with additional specifications for ICSA provided in ICSA-300.

Requirement RELABEL.R6 – VIT performed by brand owner or OEM supplier If VIT is performed by the OEM supplier or the brand owner (as permitted under Requirement RELABEL.R5), the test and reporting process SHALL conform to the "requirements for supplier-executed VIT" found in ISASecure specifications for maintenance of certification (for CSA, ICSA, and SSA, these are CSA-301, ICSA-301, and SSA-301, respectively).

Requirement RELABEL.R7 – Certificate format The certificate of product certification issued under the ISASecure certification process for relabeled products, SHALL use the same format as specified in document series 204 (e.g., CSA-204, ICSA-204, SSA-204) for ISASecure product certifications.

Requirement RELABEL.R8 – Contents and response to product update reporting Product update reporting as referenced under Requirement RELABEL.R9 SHALL consist of the following information. The brand owner and the OEM supplier jointly report the following information to the certification body once per year and report in a timely manner if the attestations listed cannot be made, for any update to the relabeled product (as defined in 3.1.12) offered in the marketplace by the brand owner.

- Mapping of most recent update version of the relabeled product offered in the marketplace by the brand owner, to its associated OEM product update version

- Documented comparison between the associated OEM product and relabeled product as updated – attestation that all differences are cosmetic, and description of any cosmetic differences and an explanation of them

- Attestation and rationale that the security context for the updated associated OEM product remains the same as that for the relabeled product update

- Explanation of any differences between the user documentation to be delivered with the relabeled product update, and the OEM user documentation delivered with the OEM product update, and attestation that all differences are cosmetic

- Description of any changes to brand owner SDL process scope and rationale provided under IEC 62443-4-1 requirement SM-5 for the SDLA certification of the brand owner, since the initial certification of the relabeled product, or since the most recent report to the certification body under this requirement.

If there has been no version change since the most recent interaction with the certification body regarding the relabeled product, that will likewise be reported. In that case, only the first and last bullet items in the above list are required.

Upon receipt of such a report, the certification body SHALL advise the OEM and brand owner in a timely manner whether the certification of the relabeled product can be maintained under the product certification process for relabeled products, and what actions are necessary to do so.

NOTE 4 Comparison information for the OEM and relabeled product and for their documentation, for updated product versions, are likely to be a minor modification of the information provided for the initial certification of the relabeled product. The report for a year can, if desired, meet this requirement by explaining any new differences since the prior year and providing a reference to that prior report.

NOTE 5 Product upgrades (defined in 3.1.13) are addressed in Requirement RELABEL.R11.

Requirement RELABEL.R9 – Maintenance of certification for product and updates A brand owner MAY claim ISASecure certification of a relabeled product under the ISASecure certification process for relabeled products, as long as:

- an ISASecure accredited certification body has granted a certificate to that effect to the brand owner, indicating conformance to the certification process and criteria defined in the present document; and

- the brand owner maintains their SDLA certification, where the relabeled product remains under that SDL process; and

- the associated OEM product certification is in valid status; and

- product update reporting is provided as defined under Requirement RELABEL.R8.

The brand owner claim of certification MAY under these conditions include product updates by the OEM under the OEM product certification, that have been relabeled.

The certification body for a relabeled product SHALL proactively monitor the status of the associated OEM product certification, independently of and in addition to status information provided to the certification body by the brand owner. If the associated OEM product certification is withdrawn or in suspended status, the certification body for the relabeled product SHALL respectively withdraw the certification for the relabeled product or place it in suspended status. If product update reporting is not up to date, the certification body SHALL withdraw the certification for the relabeled product.

Requirement RELABEL.R10 – Relabeled product certification dependency on OEM product certification A brand owner SHALL NOT claim ISASecure certification of a relabeled product, if the OEM supplier no longer holds a valid certification for the associated OEM product mapped to this relabeled product under the declarations submitted to comply with Requirement RELABEL.R4 or Requirement RELABEL.R8. In this case the brand owner SHALL request that the certification body for the relabeled product withdraw that certification in accordance with RELABEL.R9.

Requirement RELABEL.R11 – Certification of upgrades A brand owner MAY apply to a certification body for ISASecure certification of an upgrade to a relabeled product that is associated with an upgraded OEM product for which the OEM supplier has achieved certification, The certification body SHALL grant this certification using the same process described above for initial certification of the relabeled product, but considering instead the two upgraded products. Further, for the SDA evaluation as described in Table 1, the brand owner MAY submit an analysis of each SDA line item that demonstrates continued conformance to that requirement for the upgraded relabeled product. This analysis MAY be considered by the certification body in their SDA evaluation.

NOTE 6 Product upgrade is defined in 3.1.13.

6 Appendix – SDLA requirements applicable for brand owners

The following table lists minimum SDLA requirements in scope for the SDLA certification required for a brand owner to be granted a product certification under the certification process for relabeled products. It is referenced by Requirement RELABEL.R5.

Table 2. Minimum SDLA requirements

ID	IEC 62443-4-1 requirement	SDLA requirement	Include in scope of validation
SM-4	Security expertise	SDLA-SM-4	Limited to security processes performed by brand owner, which include at a minimum, processes in fulfillment of requirements in this table, and any additional processes identified under SM-5.
SM-5	Process scoping	SDLA-SM-5	Requires documented rationale that justifies the scope of SDLA certification. For many requirements this justification may be that the OEM supplier is fully responsible for meeting the requirement. Process states that this SDL applies only to relabeled products where the associated OEM product holds an ISASecure certification.
SM-7	Development environment security	SDLA-SM-7	Verify protection of product after it leaves custody of OEM supplier, or provide evidence that the product is never in brand owner custody at any time before it is in the custody of the customer.
SM-9	Security requirements for externally provided components	SDLA-SM-9	Security risks of receiving and reselling OEM product are addressed. These include risks that the product delivered to the brand owner's customer may have unknown differences from the certified OEM product that impact security, and the risk that the OEM product may at some point no longer be certified. Related to the latter risk, include processes to track the certification status of the associated OEM product, and to monitor product updates by the OEM as defined in RELABEL.R8.

ID	IEC 62443-4-1 requirement	SDLA requirement	Include in scope of validation
SM-10	Custom-developed components from third-party suppliers	SDLA_SM-10	If generic (not relabeled) OEM product was certified (as in Figure 2), verify that OEM actions to create relabeled product sold to brand owner, fall in scope of the OEM supplier's SDLA certification. If relabeled product was certified by the OEM supplier, this requirement is met, and risks have been addressed under SM-9.
SM-12	Process verification	SDLA-SM-12	Limited to security processes performed by brand owner
SM-13	Continuous improvement	SDLA-SM-13	Limited to security processes performed by brand owner. An example would be improvement of process for reporting to the OEM, security defects reported to the brand owner by their customers.
DM-1	Receiving notifications of security-related issues	SDLA-DM-1	May be limited to notifications from relabeled product users and other external sources.
DM-3	Assessing security related issues	SDLA-DM-3	Verify that bug tracking system is in place that supports brand owner's role in defect management and security update management. This may be achieved via access to the bug tracking system for the OEM supplier.
DM-6	Periodic review of security defect management practice	SDLA-DM-6	Limited to aspects of brand owner participation in practices governed by IEC 62443-4-1 requirements with identifiers DM-nnn in scope per SM-5.