# CSA-102
# ISA Security Compliance Institute – Component Security Assurance –

**Baseline document versions and errata for CSA 1.0.0 specifications**

Version 2.4

December 2022

### 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 |
|---|---|---|
| 1.1 | 2019.12.14 | Initial version published to https://www.ISASecure.org |
| 1.2 | 2020.07.17 | Add erratum for CSA-311 FSA-CR 2.1 |
| 1.3 | 2020.09.11 | Add erratum for CSA-311 FSA-CR 2.9 RE(1) |
| 1.6 | 2021.03.07 | Add errata for CSA-311 CCSC 3, FSA-CR 2.1 RE(3), and FSA-CR 2.1 RE(4); For SDLA-312 v5.5, consider accessible points of entry in threat model |
| 1.9 | 2021.10.26 | Modify existing errata for CSA-311 CSSC 3 and FSA-CR 2.1; add erratum for CSA-311 FSA-CR 2.1 RE(1); change Table 1 baseline version of CSA-200 to v4.8 |
| 1.10 | 2022.02.11 | Add errata for CSA-311 FSA-CR 2.7 and FSA-CR 3.8 to clarify meaning of “session” |
| 2.2 | 2022.05.27 | Change baseline version of SDLA-312 to v5.7 and reference errata as issued on that document; correct typo in CSA-311 requirement ID FSA-EDR 2.4B; add erratum for CSA-311 CR 1.2 to verify incoming as well as outgoing authentication capability |
| 2.4 | 2022.12.28 | In CSA-200 section 4.2 clarify ISCI policy for certificate status and posting (5.3.1, 5.3.2, 5.3.3 in present document); in CSA-300 address certifier review of supplier submissions (5.5.2) and add requirement ISASecure_C.R6 clarifying meaning of independent test (5.5.3); in CSA-301 address case of known vulnerability found after initial certification and not fixed (5.6.1); in present document section 4: change baseline version of CSA-311 from v1.11 to v2.3, change baseline version of SSA-420 from v3.2 to v4.5, change baseline version of SDLA-312 from v5.7 to v6.3 (incorporation of SDLA errata, no net effect on CSA); remove errata on CSA-311 v1.11; format for unique section number and title per erratum |
|  |  |  |
|  |  |  |

# Contents

# FOREWORD

This is one of a series of documents that defines the ISASecure® CSA (Component Security Assurance) certification program for software applications, embedded devices, host devices, and network devices. These are the component types defined by the standard IEC 62443-4-2, that are used to build control systems. ISASecure CSA is developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). A description of the program and the current list of documents related to ISASecure CSA, as well as other ISASecure certification programs, can be found on the web site https://www.ISASecure.org.

# 1 Scope

This document lists baseline versions and all approved changes to all ISASecure CSA 1.0.0 specifications published at https://www.ISASecure.org. These changes are thus to be considered part of those specifications. This document is updated periodically as additional minor changes are identified. Major changes to any of the CSA specifications will result in a new issue of the relevant specification. This document maintains a list of changes which of themselves do not merit a new version of the specification which is changed. These changes may address typographical errors, cut and paste errors, or technical inaccuracies which are clearly non-controversial in the context of the overall intent of the specification.

When any specification is reissued with a new version number, errata tracked in this document are incorporated, and this document is revised and reissued to remove those errata. Clause 4 specifies the version numbers of the documents to which the errata in this document apply.

# 2 Normative references

All documents listed below in Table 1 are normative references for this document.

Errata on [SSA-420 and [SDLA-312] are provided separately in the following normative documents.

[SSA-102] *ISCI System Security Assurance – Baseline document versions and errata for SSA 4.0.0 Specifications*, as specified at https://www.ISASecure.org

[SDLA-102] *ISCI Security Development Lifecycle Assurance – Baseline document versions and errata for SDLA 3.0.0 Specifications*, as specified at https://www.ISASecure.org

# 3 Definitions and abbreviations

Definitions and abbreviations for the terms used in this document are found in the documents for which errata are described, which are those document versions listed in Clause 4.

# 4 Baseline document versions and index to errata

This clause lists all ISASecure CSA 1.0.0 baseline documents that may be the subject of errata, and indicates for each document whether errata in the present document apply to the document. The table below provides the sub clause reference in the present document that lists specific modifications for these errata. Note that errata on SSA-420 and SDLA-312 may affect CSA, and are published separately in SSA-102 and SDLA-102, respectively.

**Table 1 - ISASecure CSA Baseline and Errata Index**

| **Document ID** | **Document Title** | **Baseline Version** | **Errata** | **Reference in this document** |
|---|---|---|---|---|
| CSA-100 | *ISCI Component Security Assurance - ISASecure certification scheme* | 4.3 | Yes | 5.2 |
| CSA-200 | *ISCI Component Security Assurance – ISASecure CSA chartered laboratory operations and accreditation* | 4.8 | Yes | 5.3 |

| Document ID | Document Title | Baseline Version | Errata | Reference in this document |
|---|---|---|---|---|
| CSA-204/205 | *ISCI Component Security Assurance – Instructions and Policies for Use of the ISASecure® Symbol and Certificate (205 is editable certificate template)* | 3.3 | No | 5.4 |
| CSA-300 | *ISCI Component Security Assurance – ISASecure certification requirements* | 4.2 | Yes | 5.5 |
| CSA-301 | *ISCI Component Security Assurance – Maintenance of ISASecure certification* | 3.2 | Yes | 5.6 |
| CSA-311 | *ISCI Component Security Assurance – Functional security assessment for components* | 2.3 | No | 5.7 |
| CSA-312 | *ISCI Component Security Assurance – Security development artifacts for components* | 3.2 | No | 5.8 |
| SSA-420 | *ISCI System Security Assurance – Vulnerability Identification Testing Specification* | 4.5 | No | 5.9 |
| SDLA-312 | *ISCI Security Development Lifecycle Assurance – Security development lifecycle assessment* | 6.3 | No | 5.10 |

# 5 Errata by document

## 5.1 General

This clause lists all errata that apply to the documents indicated in Table 1 of the present document.

## 5.2 CSA-100 ISASecure certification scheme

The following errata apply to CSA-100 version 4.3.

### 5.2.1 Add reference to CSA-102

In clause 2, add the sentence “A list of baseline document version numbers and errata on the baseline documents is published in [CSA-102].” In 2.3.1, after [CSA-303], add the reference “[CSA-102] *ISCI Component Security Assurance – Baseline document versions and errata for CSA 1.0.0 specifications*, as specified at https://www.ISASecure.org.”

### 5.2.2 CSA-102 not shown in Figure 1

In 4.5.1, note 2, add text as in italics to the note:

“The figure depicts all documents in Section 2 with the exception of *the baseline/errata document [CSA-102],* the application form [ISASecure-202], the editable certificate template [CSA-205], and the policy document [ISASecure-117] which describes the transition from the prior ISASecure EDSA program to CSA.”

### 5.3 CSA-200 Chartered laboratory operations and accreditation

The following errata apply to the specification CSA-200 v4.8.

#### 5.3.1 Posting certificate status

Replace the following existing sentence in section 4.2, with the paragraph and note following:

Existing sentence: "At the request of a component supplier, components that are issued certifications are registered on this same ISCI website."

Replacement paragraph and note: "A chartered laboratory reports new certificates and status changes (terminations and withdrawals) to ISCI (see Requirement_CSA.R39.) Certificates granted and status changes are posted on the ISCI website. ISCI will post certificates and status changes upon receipt from a chartered laboratory, except that for certificates granted, a supplier may request that posting be delayed up to 90 days. ISCI will provide a facility via which a product user may determine if a CSA certification has been granted, terminated, or withdrawn.

NOTE A supplier may request a delay in posting a certificate granted to receive advantageous timing for planned announcements."

#### 5.3.2 Refer to CSA-301 regarding validity of certification

Replace Requirement_CSA.R38 by the following text:

**"Requirement_CSA.R38 Withdrawal or termination of certification** A CSA product certification SHALL remain valid for a product and its updates, or be withdrawn in accordance with [CSA-301] Requirement ISASecure_CM.R2.

The certification body SHALL terminate a certification if the supplier reports to them that the product has left support status under the ISASecure SDLA-certified SDL process, or if the supplier otherwise requests termination of the certification for any reason.

If the certifier determines the supplier has not participated in good faith in the certification process, the certifier SHALL withdraw the certification."

#### 5.3.3 Notification of certification status change

Replace Requirement_CSA.R39 by the following text and note:

**"Requirement_CSA.R39 Notification of certification status change** The chartered laboratory SHALL inform ISCI of any withdrawal or termination of an ISASecure product certification at the time it occurs. The chartered laboratory SHALL inform the supplier that ISCI posts certificates granted, upon receipt from the chartered laboratory, except that the supplier may request a delay of up to 90 days from the grant date for posting of certificates granted.

NOTE The action to terminate or withdraw a certificate that is granted, but not yet posted on the ISCI website, will not be posted by ISCI."

### 5.4 CSA-204/204 Symbol and certificate

No errata apply to the specifications CSA-204 version 3.3 or CSA-205 version 3.3.

### 5.5 CSA-300 ISASecure certification requirements

The following errata apply to the specification CSA-300 version 4.2.

#### 5.5.1 Certifier carries out VIT

In Table 1, in the row for VIT-C, replace existing text in the requirement column "The system passes VIT-C, per the pass/fail criteria for capability security level *n*," with the text "The certifier carries out and the component passes VIT-C, per the pass/fail criteria for capability security level *n*."

### 5.5.2 Certifier review of supplier submissions

In 5.2, after item g) at the end of ISASecure_C.R4, as a part of that requirement, add the following text: “The certifier SHALL in the course of certification activities, review the supplier submissions upon which these activities depend. The review SHALL verify completeness and consistency of these submissions with definitions in the CSA specifications and with the product as presented for certification. The supplier SHALL make revisions to these submissions if found necessary in this review.”

### 5.5.3 Meaning of validation by independent test

Add the following additional requirement after ISASecure_C.R5:

**“Requirement ISASecure_C.R6 – Validation by independent test**

If a validation activity for a requirement in [CSA-311] specifies that validation by independent test is required (identified by a “Yes” in the column titled “Validation by Independent Test Required (Yes/No)”) this means that the assessor SHALL BE fully responsible for the testing described. In particular this SHALL include responsibility for the appropriateness and quality of the test, and witnessing the execution of the test. The assessor MAY at their discretion use tools created by the supplier and assistance from supplier personnel in carrying out the test.”

## 5.6 CSA-301 Maintenance of ISASecure certification

The following errata apply to the specification CSA-301 version 3.2.

### 5.6.1 Known vulnerability found and not fixed

- Add the following two terms and definitions, and accompanying notes, to section 3.1:

**“fix (for a product security issue)**
modification of a product and/or its documented security guidance to address a security issue, such that the resulting product version would meet certification criteria specified for initial product certification

NOTE 1 This definition is based upon the usage of the term in IEC 62443-4-1 requirement DM-4, part a).

NOTE 2 Changes that eliminate a security issue may or may not fall under this definition of “fix.” For example, recommending use of the user’s choice of an external firewall to protect against exploitation of a critical vulnerability is not a “fix.” Since the firewall is not part of the product, the product still has a critical vulnerability and so does not meet initial certification criteria. On the other hand, incorporating a specific firewall into the product and satisfying IEC 62443-4-1 requirements for that firewall as a third party component. would count as a fix. As a second example, suppose that a flawed security capability was removed from the product and replaced by instructions for integration with an external system to achieve the security capability. This would be considered a fix if IEC 62443-4-2 explicitly permitted the capability to be achieved by integration into a system, but would not be a fix if IEC 62443-4-2 did not permit this.”

**“version (of component)**
well defined release of a component, typically identified by a release number”

- At the end of requirement ISASecure_CM.R2, add this paragraph to that requirement:

“After initial certification, it is possible that previously unknown vulnerabilities may become known in the product version initially certified, or in one of its updates. It is possible that the severity of such a vulnerability exceeds the risk threshold established for the product per SDLA-312 requirement SDLA-DM-4, or that the vulnerability prevents the product from meeting one or more functional requirements for certification. In these situations, if the supplier concludes that it is infeasible or impractical to fix the issue with a product update, the supplier SHALL inform the certifying chartered laboratory, who SHALL withdraw the certification. The certification body SHALL reasonably coordinate with the supplier so that the supplier may communicate with product users before the certification is withdrawn, but in all cases SHALL withdraw the certification at most 90 days after being informed by the supplier that the vulnerability will not be fixed by a product update. The supplier SHALL communicate with product users regarding the vulnerability as required by IEC 62443-4-1 Requirement DM-5 Disclosing security-related issues.”

## 5.7 CSA-311 Functional security assessment for components

No errata apply to the specification CSA-311 version 2.3.

### 5.8 CSA-312 Security Development Artifacts

No errata apply to the specification CSA-312 version 3.2.

### 5.9 SSA-420 Vulnerability Identification Testing

Any errata for SSA-420 are found in the document [SSA-102].

### 5.10 SDLA-312 Security development lifecycle assessment

Any errata for SDLA-312 are found in the document [SDLA-102].

— — — — — —