# SDLA-204

# ISA Security Compliance Institute —
# Security Development Lifecycle Assurance –

## Instructions and Policies for Use of the ISASecure Symbol and Certificate

Version 1.1

May 2014

## Revision history

| version | date | changes |
|---|---|---|
| 1.1 | 2014.05.27 | Initial version published to http://www.ISASecure.org |
| | | |
| | | |

# Contents

# Foreword

This is one of a series of documents that defines ISASecure certification for control systems, which is developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). Certifications available include ISASecure Embedded Device Security Assurance (EDSA) for embedded devices, ISASecure System Security Assurance (SSA) for systems and ISASecure Security Development Lifecycle Assurance (SDLA) which addresses control system supplier development processes. This specification is one of the series of documents that describes requirements for ISASecure SDLA certification. The current list of documents related to ISASecure certification programs can be found on the web site http://www.ISASecure.org.

# 1 Scope

This document describes the procedure and conditions which govern the use of the ISASecure symbol and certificate by organizations that hold the ISASecure SDLA (Security Development Lifecycle Assurance) certification for their security development process. This document also describes symbol and certificate use by ISASecure SDLA chartered laboratories and any references to their ASCI license by such laboratories. The reference [SDLA-100] describes the overall ISASecure SDLA program.

Separate documents cover this topic for the ISASecure EDSA and ISASecure SDLA certification programs (EDSA-204 and SSA-204). The intent of the requirements is the same across all ISASecure programs. However, there are some topics unique to each program addressed in each program-specific document..

# 2 Normative references

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

[ISASecure-202] *ISCI ISASecure Certification Programs – Application and Contract for Chartered Laboratories*, internal ISCI document

[SDLA-205] *ISCI Security Development Lifecycle Assurance – Certificate Document Format,* as specified at http://www.ISASecure.orghttp://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

NOTE The following international standards apply to the ISASecure certification and testing processes, as specified in [ISASecure-111].

[ISO/IEC 17065] ISO/IEC 17065.2012, "*Conformity assessment—requirements for bodies certifying products, processes and services*", October 2012

[ISO/IEC Guide 65] ISO/IEC Guide 65, "*General Requirements for Bodies Operating Product Certification Systems*", 1996

[IAF Guide 65 Guidance] IAF Guidance on the Application of ISO/IEC Guide 65:1996**,** "*General Requirements for Bodies operating Product Certification Systems* ***",*** IAF GD 5:2006 Issue 2 Application date: 8 December 2007

[ISO/IEC 17011] ISO/IEC 17011, "*Conformity assessment – General requirements for accreditation bodies accrediting conformity assessment bodies*", 01 September 2004

[ISO/IEC 17000] ISO/IEC 17000 "*Conformity assessment — Vocabulary and general principles*"

[ISO/IEC 28] ISO/IEC Guide 28, "*Conforming assessment – Guidance on a third-party certification system for products,*" 2004

[ISO/IEC 23] ISO/IEC Guide 23 "*Methods of indicating conformity with standards for third-party certification systems,"* 1982

# 3 Definitions and abbreviations

## 3.1 Definitions

As a general rule, definitions of ISO/IEC 17000 are applicable.

**3.1.1**
**accreditation**
third party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks

NOTE For ISASecure certification programs, accreditation is an assessment and recognition process via which an organization is granted chartered laboratory status or CRT laboratory status.

**3.1.2**
**accreditation body**

third party that performs attestation, related to a conformity assessment body, conveying a formal demonstration of its competence to carry out specific conformity assessment

**3.1.3**
**accreditation body logo**
logo used by an accreditation body to identify itself

**3.1.4**
**accreditation certificate**
formal document or a set of documents issued by an accreditation body, stating that accreditation has been granted for the defined scope

**3.1.5**
**accreditation symbol**
symbol issued by an accreditation body to be used by chartered laboratories to indicate their accredited status

**3.1.6**
**conformity assessment body**
body that performs conformity assessment services and that can be the object of accreditation

NOTE Examples are a laboratory, inspection body, product certification body, management system certification body and personnel certification body. This is an ISO/IEC term and concept.

**3.1.7**
**control system**
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

**3.1.8**
**chartered laboratory**
organization chartered by ASCI to evaluate products or processes under one or more ISASecure certification programs and to grant certifications under one or more of these programs

NOTE A chartered laboratory is the conformity assessment body for the ISASecure certification programs.

**3.1.9**
**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.

**3.1.10**
**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

**3.1.11**
**ISASecure symbol**
graphic or text affixed or displayed to designate that ISASecure certification has been achieved

NOTE The ISASecure symbol is the mark of conformity for an ASCI certification scheme. The symbol or mark is licensed by ASCI to chartered laboratories for the use by suppliers that have achieved requirements for a particular type of ISASecure certification and by chartered laboratories to signify conformance to the ISASecure certification requirements.

**3.1.12**
**ISASecure version**
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 3-place number such as ISASecure SDLA 2.6.1

**3.1.13**
**SDLA certification pending**
formal status of a candidate for SDLA certification, via which ISCI confirms that the organization has made significant progress toward meeting SDLA requirements

**3.1.14**
**termination**
discontinuation of certified status upon request by the certified client

### 3.2 Abbreviations

The following abbreviations are used in this document.

| | |
|---|---|
| ASCI | Automation Standards Compliance Institute |
| EDSA | embedded device security assurance |
| IACS | industrial automation and control system(s) |
| IAF | International Accreditation Forum |
| ISCI | ISA Security Compliance Institute |
| ISA | International Society of Automation |
| IEC | International Electrotechnical Commission |
| ISO | International Organization for Standardization |
| SDLA | Security Development Lifecycle Assurance |
| SSA | System Security Assurance |

## 4 ISASecure symbol and references

### 4.1 General

The ISASecure symbol is defined as the sequence of letters “ISASecure,” where the first four letters only are capitalized. It has specified uses in its text and graphical form. The graphical form of the ISASecure symbol shall be displayed only in the appropriate form, size, and color detailed on the ISASecure website: http://www.ISASecure.org.

When displayed in isolation such as on letterhead, the ISASecure symbol shall always be accompanied by the trademark notation, as in ISASecure$^{TM}$. When used within a document that has several occurrences of the symbol, such as a brochure or press release, the first occurrence shall have the trademark notation. In addition, in this case, the document shall also include the statement:

***ISASecure™*** is a Trademark of ASCI. All rights reserved.

A chartered laboratory and/or its clients shall neither use the ISASecure symbol in any misleading manner, nor shall imply in use of the symbol or in any reference that ASCI or ISCI approves of its products or development processes.

In particular, a chartered laboratory and/or its clients shall not use the ISASecure symbol in any way that might mislead the reader regarding the status of a chartered laboratory or the certification of a client's products or security development lifecycle process. All references that contain the ISASecure symbol shall clearly define the particular ISASecure certification program to which they are related, which in the present case would be the ISCI SDLA certification program.

### 4.2 Use by chartered laboratory

An ISASecure SDLA chartered laboratory may use the ISASecure symbol in text or graphical form. When an ISASecure chartered laboratory displays the ISASecure symbol in printed or online documentation, its license number (chartered laboratory identification, in five-digit format) issued by ASCI shall be printed centrally under the ISASecure symbol. Its accreditation number may also appear. ISCI shall maintain one license number for each organization, and track those ISASecure programs for which the laboratory is accredited, in association with that number.

In particular, the ISASecure symbol may be displayed on organizational stationery/letterhead by a chartered laboratory only if the mark or title of the chartered laboratory is also shown, along with its license number.

The following is an example of correct use of the ISASecure symbol by a chartered laboratory:

ISASecure$^{TM}$ SDLA

Accreditation Number: WWWWW

License Number: XXXXX

A chartered laboratory is entitled to use the phrase, "An ISASecure Chartered Laboratory – Accreditation number WWWWW, License Number XXXXX" in combination with the ISASecure symbol.

To request approval to use the phrase “An ISASecure Chartered Laboratory – Accreditation number:WWWWW, License Number XXXXX” the chartered laboratory shall:

a) Submit a request to use the wording to the ASCI Managing Director; and

b) Submit a pictorial representation of how the wording is to appear

c) Submit a pictorial representation of how the wording is to appear in conjunction with the accreditation body’s mark/symbol, the ISASecure symbol or any other mark or symbol of conformity.

The ASCI Managing Director shall respond within 30 days as to whether the use of the wording as proposed by the laboratory is acceptable.

The chartered laboratory shall bear responsibility for obtaining any required copyrights and for monitoring the use of the wording and ensuring that the wording is not misused.

Chartered laboratories are entitled to incorporate the ISASecure symbol in public material that refers to accredited services, provided that the conditions in this procedure are met. Chartered laboratories are also entitled to make general reference to the ASCI license provided they ensure that ASCI recognition is not implied for parts of any ISASecure program for which they are not accredited.

Any use of the ISASecure symbol by the chartered laboratory that might contravene the conditions set out in this procedure will be considered a misuse of the symbol and subject to legal action which may include withdrawal of the ASCI license, or publication of the transgression or other action deemed necessary by ASCI to maintain the integrity of its mark.

### 4.3 Use by organization holding SDLA certification

An ISASecure SDLA certified organization may use the text form of the ISASecure symbol, and is not permitted to use its graphical form to represent this certification. The graphical version of the ISASecure symbol may be used only to represent achievement of ISASecure product certifications for specific products, such as ISASecure EDSA or ISASecure SSA.

When an organization that holds an SDLA certification displays the (text version of the) ISASecure symbol in printed or online documentation, the certification number issued by the certification body (chartered laboratory) shall be printed centrally under the ISASecure symbol. The ISASecure version and certification level shall also appear.

The following is an example of correct use of the ISASecure symbol by an SDLA certified organization:

ISASecure$^{TM}$ SDLA 1.0.1

Certification Level: 1

Certification number: YYYYY

When used in context to describe a certified organization, the following phrase shall be used:

*An ISASecure SDLA certified development organization*

When used in context to describe an organization that has been granted the status of  ISASecure SDLA certification pending, as described in [SDLA-300], the following phrase shall be used:

*development organization has achieved "ISASecure SDLA Certification Pending" status*

The graphical form of the ISASecure symbol shall not be used to depict pending status (or SDLA certification, as stated above).

An organization that has achieved pending status shall not imply that it has achieved or is assured of achieving SDLA certification.

At this time, an assertion in publicly available information that a specific product or version was developed under an ISASecure SDLA certified process, is not permitted. An assertion that a general class of products is developed under an ISASecure SDLA certified process, is permitted.

This last form of usage to describe products is subject to audit by the chartered laboratory that certified the organization, to confirm the assertions made. An organization shall not make any assertions that state that a process which is in SDLA certification pending status,  was used to develop a class of products.

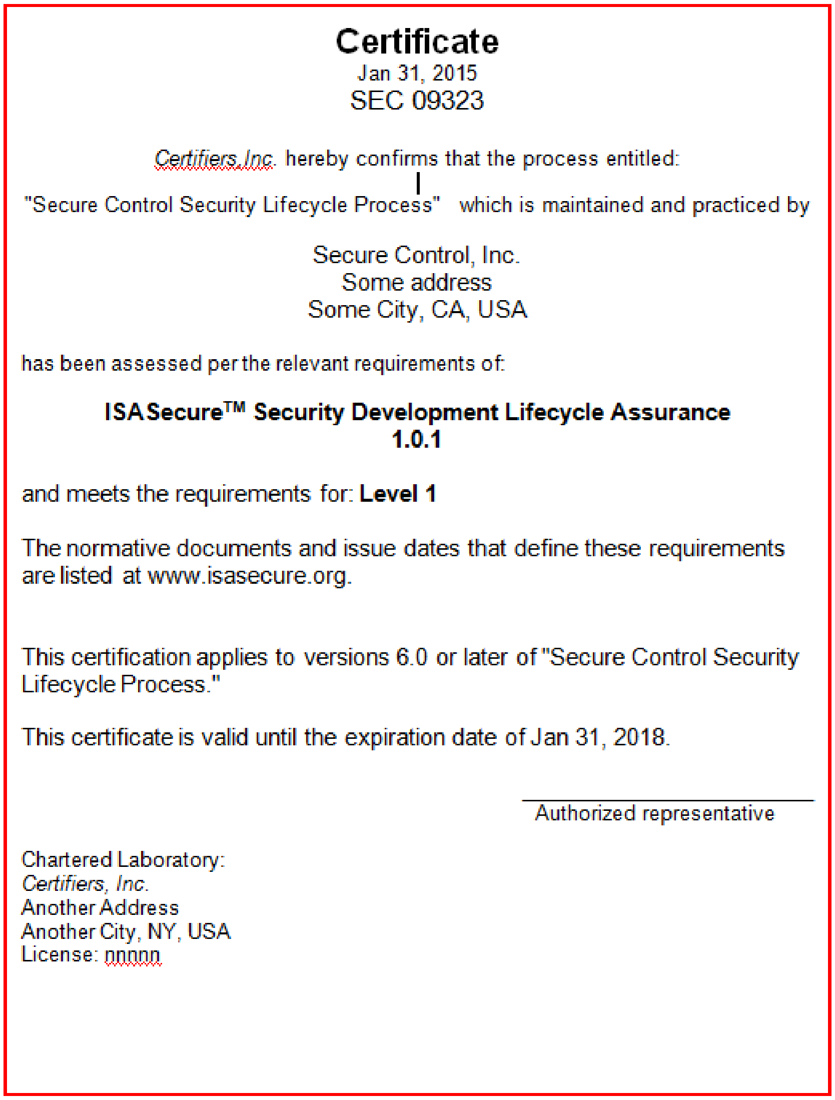
An organization shall not allow a reference to its SDLA certification to be used in such a way as to imply that the certification body certifies any of its products, or that any of its products conform with ISASecure product certification criteria.

As specified in [ISO/IEC 17065], the chartered laboratory agreement with its client will state that upon withdrawal, or termination of certification, the client "discontinues its use of all advertising matter that contains any reference thereto." Therefore a reference in advertising matter to an SDLA certification or pending SDLA certification status previously held, is not permitted.

Also as specified in [ISO/IEC 17065], the consequences of transgressions by clients of a chartered laboratory related to use of the ISASecure symbol are managed by the chartered laboratory.

## 5 Certificates

The certification certificate issued by a chartered laboratory to its clients must be the one recognized by the ASCI program. The document [SDLA-205] posted on the ISASecure website contains the approved certificate format in an editable form suitable for use as a template. Figure 1 illustrates this format. The wording and relative placement of the information shall be used. If alterations are made to the approved certificate, prior to its use, the ASCI Managing Director must approve the certification certificate used by the chartered laboratory. A typical example would be addition of the logo of the chartered laboratory organization to the certificate. The graphical form of the ISASecure logo shall not appear on an ISASecure SDLA certificate.



**Certificate**
Jan 31, 2015
SEC 09323

*Certifiers,Inc.* hereby confirms that the process entitled:

"Secure Control Security Lifecycle Process" which is maintained and practiced by

Secure Control, Inc.
Some address
Some City, CA, USA

has been assessed per the relevant requirements of:

**ISASecure™ Security Development Lifecycle Assurance**
**1.0.1**

and meets the requirements for: **Level 1**

The normative documents and issue dates that define these requirements are listed at www.isasecure.org.

This certification applies to versions 6.0 or later of "Secure Control Security Lifecycle Process."

This certificate is valid until the expiration date of Jan 31, 2018.

Authorized representative

Chartered Laboratory:
*Certifiers, Inc.*
Another Address
Another City, NY, USA
License: nnnnn

**Figure 1 - Example Certificate**

## 6 Change in accreditation status

Upon withdrawal or suspension of the chartered laboratory accreditation, a chartered laboratory shall immediately cease to issue certificates and any other materials displaying the ISASecure symbol, license or containing reference to ASCI recognition.

## 7 Modification of the ISASecure symbol

Upon any modifications to the ISASecure symbol, ASCI must immediately inform chartered laboratories of its changes and proper use. The effective date for the use of the new symbol must be published on the website: http://www.ISASecure.org.

## 8 Use of accreditation certificates and symbol

Chartered laboratory use of the accreditation certificates issued by the accreditation body and the associated symbols must follow the policies and procedures of the accreditation body.

— — — — — —