ISASecure-115

ISA Security Compliance Institute — ISASecure® certification programs

Policy for transition to SDLA 2.0.0, EDSA 2.1.0 and SSA 2.1.0

Version 1.5

September 2018

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, INFORMATON, 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.

Revision history

version	date	changes
1.4	2018.02.09	Initial version published to http://www.ISASecure.org
1.5	2018.09.07	Add section 7 to permit EDSA chartered laboratories to obtain provisional recognition as SDLA chartered laboratories in a timely manner

Contents

FOREWORD

This is one of a series of documents that defines ISASecure® certification programs. This document describes the ISCI policy for transition of certification operations to the updated certification versions ISASecure SDLA 2.0.0 (Security Development Lifecycle Assurance), ISASecure EDSA 2.1.0 (Embedded Device Security Assurance), and ISASecure SSA 2.1.0 (System Security Assurance). The list of ISASecure certification programs and documents for these program versions, and for their prior versions, can be found on the web site http://www.ISASecure.org.

1 Background and scope

ISCI (ISA Security Compliance Institute) operates a process certification program for control system supplier security development lifecycle processes called ISASecure® SDLA certification (Security Development Lifecycle Assurance). The prior version of this program was called SDLA 1.0.0. An updated version of this program has been modified to align with the approved standard published as ANSI/ISA-62443-4-1 and IEC 62443-4-1. This new version of the ISASecure certification program is called SDLA 2.0.0.

ISCI also operates product certification programs for embedded devices, called ISASecure EDSA (Embedded Device Security Assurance) and for control systems, called ISASecure SSA (System Security Assurance). The prior versions of these programs were denoted EDSA 2.0.0 and SSA 2.0.0. These programs refer to the specification [SDLA-312] used in common with the ISASecure SDLA certification. The revised versions of these programs that refer to SDLA 2.0.0 specifications are called EDSA 2.1.0 and SSA 2.1.0.

In addition to the change to refer to SDLA 2.0.0 specifications, EDSA 2.1.0 and SSA 2.1.0 incorporate modifications to the process for maintaining certificates over time. The present document provides an overview of these upcoming requirements for organizations planning their transition to these programs.

This document specifies the timeline and related policies for transition of certification operations to SDLA 2.0.0, EDSA 2.1.0 and SSA 2.1.0.

2 Normative references

The standard with which SDLA 2.0.0, EDSA 2.1.0, and SSA 2.1.0 align is:

[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*

SSA 2.0.0 and SSA 2.1.0 also align with the standard:

[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*

An ISASecure certification program version program is defined by a set of associated specification documents and document versions. The documents associated with the six programs named in Clause 1 are published at http://www.ISASecure.org.

The present document refers specifically to:

[SDLA-200] *ISCI Security Development Lifecycle Assurance – ISASecure SDLA Chartered laboratory operations and accreditation,* 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

[EDSA-301] *ISCI Embedded Device Security Assurance – Maintenance of ISASecure certification,* as specified at http://www.ISASecure.org

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

3 Definitions and abbreviations

3.1 Definitions

3.1.1
accreditation
for ISASecure certification programs, assessment and recognition process via which an organization is granted chartered laboratory or CRT laboratory status

NOTE The CRT laboratory accreditation program is not otherwise referenced in, nor impacted by, the present document, since ISCI CRT laboratories are not certification bodies.

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 a specific conformity assessment

3.1.3
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.

3.1.4
certification body
an organization that performs certification

3.1.5
chartered laboratory
organization chartered by ASCI to evaluate products or development 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. ASCI is the legal entity representing ISCI.

3.1.6
combined assessment
three-factor ISASecure product certification assessment that consists of certifier robustness testing (ERT or SRT), evaluation of security functionality (FSA) and process assessment (SDA/SDLPA), which may support an initial certification, or a “delta” certification for a modified product in accordance with the ISASecure EDSA-301 or SSA-301 documents

3.1.7
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.

3.1.8
control system
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

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
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

3.1.12
release
any software/hardware delivered by the supplier to the customer

3.1.13
update
incremental hardware or software change in order to address security vulnerabilities, bugs, reliability or operability issues

3.1.14
upgrade
incremental hardware or software change in order to add new features

3.1.15
version (of ISASecure certification)
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 SDLA 2.6.1

3.1.16
version (of product)
identifier for a release, usually numerical

NOTE For a system, may incorporate many individual component versions.

3.2 Abbreviations

The following abbreviations are used in this document.

ANSI	American National Standards Institute
ASCI	Automation Standards Compliance Institute
CRT	communication robustness testing
DCS	distributed control system
EDSA	embedded device security assurance
ERT	embedded device robustness testing
FSA	functional security assessment
IACS	industrial automation and control system(s)
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
OS	operating system
PLC	programmable logic controller
SDA	security development artifacts
SDL	security development lifecycle
SDLPA	security development lifecycle process assessment
SDLA	security development lifecycle assurance
SIS	safety instrumented system
SRT	system robustness testing
SSA	system security assurance

4 Transition policies

The following policies apply to ISASecure chartered laboratories, which are the certification bodies for the ISASecure certification programs.

[SDLA-312] as referred to here, contains the list of security development lifecycle process requirements that are evaluated for SDLA, EDSA, and SSA certification. It is revised under SDLA 2.0.0 for alignment with [ANSI/ISA-62443-4-1]. We refer to the prior and revised versions of this document as *[SDLA-312] for SDLA 1.0.0*, and *[SDLA-312] for SDLA 2.0.0*.

Figure 1 in 4.3 below summarizes the transition policy information explained in 4.1 and 4.2.

Note that these policies address the following evaluation activities:

- Evaluation of SDL (security development lifecycle) process documentation toward SDLA process certification
- Evaluation of products performed as audit samples to show SDL compliance, toward SDLA process certification
- Evaluation of a product performed toward EDSA or SSA certification of that product.

4.1 Transition of process certification (SDLA)

For an initial certification audit or a recertification audit for SDLA process certification, the transition is a one year period after the publication of SDLA 2.0.0 specifications. Specifically, after this one year period, a supplier's documented SDL must conform to [SDLA-312] for SDLA 2.0.0. Where conformance to an SDL is audited for selected products as part of an SDLA evaluation, products falling under the SDL process that started SDL activity after this one year period, SHALL conform to [SDLA-312] for SDLA 2.0.0. If a product audited under the SDLA evaluation started SDL activities sooner, then it MAY conform to [SDLA-312] for either SDLA 1.0.0 or SDLA 2.0.0, as long as the product was released less than three years after the publication date of SDLA 2.0.0. Otherwise, products audited under the SDLA evaluation SHALL conform to [SDLA-312] for SDLA 2.0.0.

This policy is expressed in column 3 of Figure 1 in 4.3.

4.2 Transition of product certifications (EDSA and SSA)

A transition period of one year after the publication of SDLA 2.0.0 specifications is allowed for product certifications. Specifically, the specification [SDLA-312] for SDLA 2.0.0 SHALL be used for an ISASecure evaluation of any product under EDSA or SSA, where the SDL activity for that product release started after this one year period. Such products SHALL be certified to EDSA 2.1.0 or SSA 2.1.0.

[SDLA-312] for either SDLA 1.0.0 or SDLA 2.0.0 MAY be used for a product certification (EDSA or SSA), for products that started SDL activity less than one year after the publication of SDLA 2.0.0, as long as the product is submitted for certification in a timely fashion. A "timely fashion" is defined as less than three years after publication of SDLA 2.0.0. Such products MAY be certified to either the 2.0.0 or 2.1.0 versions of EDSA or SSA. Otherwise, [SDLA-312] for SDLA 2.0.0 SHALL be used; such products SHALL be certified to the 2.1.0 versions of EDSA or SSA.

These policies apply whether or not an applicant for product certification holds an SDLA certification. They apply for initial certifications as well as subsequent certifications performed under maintenance of certification in accordance with [EDSA-301] or [SSA-301].

This policy is expressed in last two columns of Figure 1 found in sub clause 4.3 below.

4.3 Transition Policy - Summary

The following table summarizes the policy for transition of ISASecure certification evaluations to the EDSA 2.1.0, SSA 2.1.0, and SDLA 2.0.0 specifications. It organizes for clarity the policies stated in the above sub clauses 4.1 and 4.2that apply to products.

In the table, the first two columns shaded in grey categorize products that are assessed under any ISASecure certification (EDSA, SSA, or SDLA), into three disjoint "time frame groups," one time frame group per row. The last three columns indicate which version of the EDSA, SSA, and SDLA certification documents SHALL be applied, for each time frame group, in three situations. These situations are:

- A supplier is undergoing a process assessment or selected product audit toward SDLA certification (column 3)
- A supplier who holds an SDLA certification is undergoing a product assessment for an EDSA or SSA certification, (column 4)
- A supplier who does not hold an SDLA certification is undergoing an EDSA or SSA certification (column 5)

These situations are enumerated for clarity, even though the specification version indicated in the table is the same in all of these situations. The specification version to be used depends only upon the time frame group of products being considered.

Figure 1. Transition Policy Summary

Release starts development activities under organizations' SDL	Release completed AND (if product certification) application submitted for certification	SDLA version that applies for SDLA certification assessment	EDSA, SSA, and SDLA version that applies for EDSA or SSA certification if supplier is SDLA certified	EDSA, SSA, and SDLA version that applies for EDSA or SSA certification if supplier is not SDLA certified
One year or more after publication of SDLA 2.0.0	Any time	SDLA 2.0.0	EDSA 2.1.0 SSA 2.1.0 SDLA 2.0.0	EDSA 2.1.0 SSA 2.1.0 SDLA 2.0.0
Less than one year after publication of SDLA 2.0.0	Less than three years after publication of SDLA 2.0.0	SDLA 1.0.0 OR SDLA 2.0.0	EDSA 2.0.0 or EDSA 2.1.0 SSA 2.0.0 or SSA 2.1.0 SDLA 1.0.0 or SDLA 2.0.0	EDSA 2.0.0 or EDSA 2.1.0 SSA 2.0.0 or SSA 2.1.0 SDLA 1.0.0 or SDLA 2.0.0
Less than one year after publication of SDLA 2.0.0	Three years or more after publication of SDLA 2.0.0	SDLA 2.0.0	EDSA 2.1.0 SSA 2.1.0 SDLA 2.0.0	EDSA 2.1.0 SSA 2.1.0 SDLA 2.0.0

5 Maintenance of certification

5.1 Policy

The policy in this section describes how EDSA and SSA certificates are maintained over time. It supersedes information found in other published EDSA 2.1.0 and SSA 2.1.0 specifications, which will be aligned with this policy. The policy applies for all certifications carried out under EDSA 2.1.0 or SSA 2.1.0.

For prior certification versions EDSA 2.0.0 and SSA 2.0.0, certificates applied to a specific product version, and were valid indefinitely. For EDSA 2.1.0 and SSA 2.1.0, the following policy applies.

- Certification applies to a product version and its updates (as clarified next), rather than to a single product version.
- A supplier shall reach agreement with the chartered laboratory on a policy that can be applied based upon examining product version numbers, that determines whether a new product version falls under an existing certificate, or requires a new certification. The intent of the policy is that upgrades (see 3.1.14) require a new certification, and updates (see 3.1.13) do not.

- In order to obtain a certification for a product, a supplier shall hold an ISASecure SDLA certification of a security development lifecycle process that applies to development of product updates going forward.

- A supplier shall inform the certifying chartered lab when the certified product has transitioned to a minimal or no support status, such that the certified SDL process for security management no longer applies.

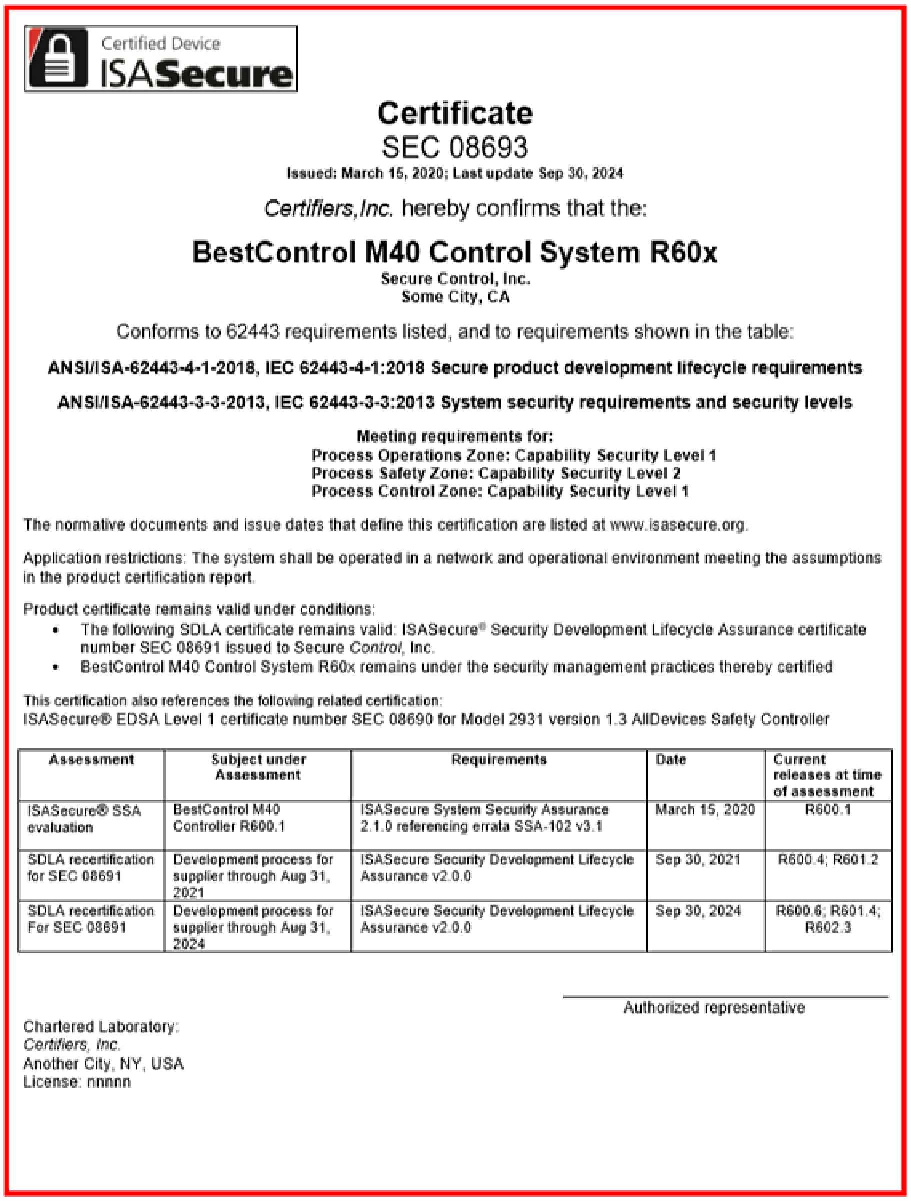
- A supplier earns a product certification using the same approach as for EDSA 2.0.0 or SSA 2.0.0, by passing a combined assessment for a specific product version (see 3.1.6).

- Once a supplier holds an EDSA 2.1.0 or SSA 2.1.0 certification, that certificate remains valid as long as:

    - The product remains in a support status such that a certified SDL process for security management still applies; AND

    - The supplier retains their SDLA certification.

A grace period of one year shall apply before a product certificate would become invalid due to loss of SDLA certification. A certificate will be updated to record combined and SDL assessments passed, related to the product. It will also record the current product versions at the time of each assessment, as illustrated in Figure 2 below. When first issued, the certificate will have a single row in the table of assessments.



Certified Device ISASecure

Certificate

SEC 08693

Issued: March 15, 2020; Last update Sep 30, 2024

Certifiers,Inc. hereby confirms that the:

BestControl M40 Control System R60x

Secure Control, Inc.
Some City, CA

Conforms to 62443 requirements listed, and to requirements shown in the table:

ANSI/ISA-62443-4-1-2018, IEC 62443-4-1:2018 Secure product development lifecycle requirements

ANSI/ISA-62443-3-3-2013, IEC 62443-3-3:2013 System security requirements and security levels

Meeting requirements for:
Process Operations Zone: Capability Security Level 1
Process Safety Zone: Capability Security Level 2
Process Control Zone: Capability Security Level 1

The normative documents and issue dates that define this certification are listed at www.isasecure.org.

Application restrictions: The system shall be operated in a network and operational environment meeting the assumptions in the product certification report.

Product certificate remains valid under conditions:

- The following SDLA certificate remains valid: ISASecure® Security Development Lifecycle Assurance certificate number SEC 08691 issued to Secure *Control*, Inc.
- BestControl M40 Control System R60x remains under the security management practices thereby certified

This certification also references the following related certification:
ISASecure® EDSA Level 1 certificate number SEC 08690 for Model 2931 version 1.3 AllDevices Safety Controller

Assessment	Subject under Assessment	Requirements	Date	Current releases at time of assessment
ISASecure® SSA evaluation	BestControl M40 Controller R600.1	ISASecure System Security Assurance 2.1.0 referencing errata SSA-102 v3.1	March 15, 2020	R600.1
SDLA recertification for SEC 08691	Development process for supplier through Aug 31, 2021	ISASecure Security Development Lifecycle Assurance v2.0.0	Sep 30, 2021	R600.4; R601.2
SDLA recertification For SEC 08691	Development process for supplier through Aug 31, 2024	ISASecure Security Development Lifecycle Assurance v2.0.0	Sep 30, 2024	R600.6; R601.4; R602.3

Authorized representative

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

Figure 2. Example SSA 2.1.0 Certificate

5.2 End user perspective

For the end user considering a product purchase or installation of a new product version, the existence of valid ISASecure certificate means that a specific version of the product passed a combined assessment, and that the overall security development process for the supplier passed an assessment within the last three years. It also means that updates for the product remain under the certified SDL. When judging the assurance provided by the certificate for a later product version that is not shown on the certificate, the end user will consider the length of time since the last combined assessment and the last SDLA recertification, the nature and extent of subsequent changes to the product, and the anticipated support status of the product. The end user will also consider the supplier's version numbering policy for identifying upgrades, to consider when a later upgrade version may undergo a new combined assessment.

5.3 Supplier perspective

A supplier that intends to certify products to EDSA or SSA 2.1.0, will obtain an SDLA certification for an SDL process that applies to those products. The supplier will formulate and agree on a policy with their product certifier, for identifying updates to products, versus upgrades that would require new certifications. The policy will be based upon the version numbering of the product releases. For example, a supplier that versions products using the format a.b.c, might have a policy that every change to the "b" digit indicates a new certification, as those releases represent an upgrade. In this example, a certificate might be issued for version 6.x.y, where x and y represent placeholders that can be any digit.

6 Informative guidance for ISASecure program participants

ISCI provides information to assist ISASecure program participants in understanding the differences between SDLA 1.0.0 and SDLA 2.0.0. [SDLA-312] for SDLA 2.0.0 includes a mapping from SDLA 2.0.0 requirements to SDLA 1.0.0 requirements. Thus, one may identify requirements that were brought forward from [SDLA-312] for SSA 1.0.0 to [SDLA-312] for SDLA 2.0.0. Requirements for which no mapped SDLA 1.0.0 requirement is shown, are new for SDLA 2.0.0.

7 Provisional recognition as SDLA chartered laboratory

Upon request, ISCI will automatically grant provisional SDLA 2.0.0 chartered lab status to any organization that holds accreditation as an EDSA chartered laboratory as of Sep 1, 2018. In accordance with [SDLA-200], this means that these organizations may perform SDLA 2.0.0 certifications and issue ISASecure SDLA 2.0.0 certificates, on a interim basis, for 18 months following this granting of provisional status.

This policy is an exception to the process defined in [SDLA-200] for achieving provisional chartered laboratory status.