EDSA-100

ISA Security Compliance Institute — Embedded Device Security Assurance –

ISASecure certification scheme

Version 1.1

June 2010

Revision history

version	date	author	changes
1.1	2010.06.06	C. Muehrcke	Initial version published to http://www.ISASecure.org

Contents

Foreword

NOTE This is one of a series of documents that defines ISASecure certification for embedded devices, which is developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). This is the highest level document that describes the overall certification scheme and the scope for all other related documents. A description of the ISASecure program and the current list of documents related to ISASecure embedded device security assurance can be found on the web site http://www.ISASecure.org.

1 Scope

The ISASecure certification program has been developed by an industry consortium called the ISA Security Compliance Institute (ISCI) with a goal to accelerate industry wide improvement of cyber security for Industrial Automation and Control Systems (IACS). The ISCI ISASecure EDSA (embedded device security assurance) certification program achieves this goal by offering a common industry-recognized set of device and process requirements that drive device security, simplifying procurement for asset owners, and device assurance for equipment vendors. An embedded device that is certified to meet these requirements can display the ISASecure symbol.

This document provides an overview of the operation of the certification program, the roles of all organizations that participate in carrying out the program, and the documents that define these roles as well as the technical aspects of the program.

2 Normative references

NOTE Section 4.4 provides a diagrammatic and expository overview of the ISASecure EDSA documents and their relationships.

2.1 Accreditation/recognition

2.1.1 Chartered laboratory operations and accreditation

NOTE The following documents describe how to achieve chartered laboratory status and operate as an ISASecure EDSA certifier.

[EDSA-200] *ISCI Embedded Device Security Assurance – ISASecure EDSA chartered laboratory operations and accreditation,* as specified at http://www.ISASecure.org

[EDSA-202] *ISCI Embedded Device Security Assurance – Application and Contract for Chartered Laboratories*, as specified at http://www.ISASecure.org

2.1.2 CRT tool recognition program

NOTE The following documents describe how to attain ISASecure EDSA recognition for a tool used to carry out communication robustness testing.

[EDSA-201] *ISCI Embedded Device Security Assurance –Recognition process for communication robustness testing tools,* as specified at http://www.ISASecure.org

[EDSA-203] *ISCI Embedded Device Security Assurance - Application and Contract for CRT Tool Recognition,* see http://www.ISASecure.org

2.2 ISASecure symbol and certificates

NOTE The following documents describe the ISASecure symbol and certificates and how they are used.

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

[EDSA-205] *ISCI Embedded Device Security Assurance – Certificate Document Format,* as specified at http://www.ISASecure.org

2.3 Technical specifications

NOTE This section includes the specifications that define technical criteria for evaluating an embedded device for ISASecure EDSA certification.

2.3.1 General technical specifications

NOTE The following document is the overarching technical specification for ISASecure EDSA certification.

[EDSA-300] *ISCI Embedded Device Security Assurance – ISASecure Certification Requirements,* 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

[EDSA-303] *ISASecure EDSA Sample Report*, as published at http://www.ISASecure.org

2.3.2 CRT specifications

NOTE The first document in this list is the overarching technical specification that defines how tests are carried out for ISASecure EDSA CRT. The list of protocol-specific ISASecure EDSA technical test specifications that follow it, refer to [EDSA-310] for requirements that are common across all protocols.

[EDSA-310] *ISCI Embedded Device Security Assurance – Common requirements for communication robustness testing of IP based protocol implementations,* as specified at http://www.ISASecure.org

[EDSA-401] *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of two common "Ethernet" protocols,* as specified at http://www.ISASecure.org

[EDSA-402] *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF ARP protocol over IPv4,* as specified at http://www.ISASecure.org

[EDSA-403] *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF IPv4 network protocol,* as specified at http://www.ISASecure.org

[EDSA-404] *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF ICMPv4 network protocol,* as specified at http://www.ISASecure.org

[EDSA-405] *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF UDP transport protocol over IPv4 or IPv6,* as specified at http://www.ISASecure.org

[EDSA-406] *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF TCP transport protocol over IPv4 or IPv6,* as specified at http://www.ISASecure.org

2.3.3 Functional security assessment

NOTE The following document provides the technical evaluation criteria for FSA.

[EDSA-311] *ISCI Embedded Device Security Assurance – Functional security assessment,* as specified at http://www.ISASecure.org

2.3.4 Software development security assessment

NOTE The following document provides the technical evaluation criteria for SDSA.

[EDSA-312] *ISCI Embedded Device Security Assurance – Software development security assessment*, as specified at http://www.ISASecure.org

2.4 Internal ISCI operations

NOTE The following document describes internal ISCI operations for ISASecure EDSA.

[EDSA-101] *ISCI Embedded Device Security Assurance – Certification scheme operation,* internal ISCI document

2.5 External references

External references are documents that are maintained outside of the ISASecure EDSA program and are used by the program.

2.5.1 International standards for certification programs

NOTE The following international standards apply to the ISASecure EDSA certification and testing processes.

[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 17025] ISO/IEC 17025, "*General requirements for the competence of testing and calibration laboratories****",*** 15 December 1999

2.5.2 International standards for accreditation programs

NOTE The following international standard applies to the ISASecure EDSA chartered laboratory accreditation processes.

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

2.5.3 ASCI operations

NOTE Some evaluation criteria in this document are used for chartered laboratory accreditation.

[ASCI Lab] *ASCI Chartered Testing Laboratory 2009 Approval Process*, as specified at http://www.ISASecure.org

3 Definitions and abbreviations

3.1 Definitions

3.1.1
accreditation
for ISASecure EDSA, assessment and recognition process via which an organization is granted chartered 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
ASCI conformance program
a program managed by ASCI that offers evaluation of products or processes to a standard or other consensus specification

3.1.4
certifier
chartered laboratory, which is an organization that is qualified to certify embedded devices as ISASecure

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

3.1.5
certificate
a document that signifies that a person, product or organization has met the criteria defined under a specific evaluation program

NOTE For ISASecure EDSA, there are certificates for certified devices, recognized CRT tools and chartered laboratories.

3.1.6
certification

third party attestation related to products, processes, or persons that conveys assurance that specified requirements have been demonstrated. For ISASecure EDSA, this is an authorized evaluation of an embedded device to the ISASecure EDSA criteria, which, when successful, permits the device vendor to advertise this achievement in accordance with certification program guidelines

3.1.7
certification scheme

the overall definition of and process for operating a certification program

3.1.8
certified device

a well-defined version of an embedded device that has undergone an evaluation by a chartered laboratory, has met the ISASecure EDSA criteria and has been granted certified status by the chartered laboratory

3.1.9
chartered laboratory

organization chartered by ASCI to evaluate devices under the ISASecure EDSA certification program and to grant certifications

NOTE A chartered laboratory is the conformity assessment body for the ISASecure EDSA program.

3.1.10
communication robustness testing

tests that determine the extent to which an embedded device maintains its essential functions under adverse network traffic conditions

3.1.11
conformity assessment

demonstration that specified requirements relating to a product, process, system, person or body are fulfilled

3.1.12
conformity assessment body

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

NOTE This is an ISO/IEC term and concept. For ISASecure EDSA, the conformity assessment body is a chartered laboratory.

3.1.13
device vendor

organization that is responsible for compliance of an embedded device with ISASecure requirements

3.1.14
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.

3.1.15
end user

organization that purchases, uses or is impacted by the security of embedded devices

3.1.16
“Ethernet”

IEEE802.3 as Ethernet II or IEEE 802.3 Type 1 plus IEEE 802 SNAP

3.1.17
functional security assessment
assessment of a defined list of security features for an embedded device

3.1.18
pass
meet the criteria for passing an EDSA evaluation as defined within the technical EDSA specifications

3.1.19
provisional chartered status
an interim, temporary accreditation status during which a chartered laboratory is authorized to evaluate embedded devices and grant ISASecure EDSA certifications.

NOTE Provisional accreditation requirements ensure that the laboratory is organized and prepared to carry out ISASecure certifications in a competent, impartial and confidential manner.

3.1.20
recognized CRT tool
a test tool that has been evaluated by ISCI and determined to meet applicable requirements for carrying out ISASecure EDSA communication robustness testing

3.1.21
software development security assessment
an assessment of the software development process which produced a particular embedded device, from the point of view of the security of a device so produced

3.1.22
symbol
graphic affixed or displayed to designate that ISASecure certification has been achieved

NOTE An earlier term for symbol is “mark.”

3.1.23
tool supplier
provider of a test tool to support communication robustness testing

3.1.24
version (of embedded device)
a well defined release of an embedded device, typically identified by a release number

3.1.25
version (of ISASecure certification)
the ISASecure certification criteria in force at a particular point in time, defined by the set of document versions that define the certification program, and identified by a year and release number, such as ISASecure EDSA 2010.2.

3.2 Abbreviations

The following abbreviations are used in this document.

ASCI	Automation Standards Compliance Institute
ARP	address resolution protocol
CRT	communication robustness testing
EDSA	embedded device security assurance
FSA	functional security assessment
IACS	industrial automation and control system(s)
IETF	Internet engineering task force
IAF	International Accreditation Forum
ICMPv4	internet control message protocol version 4
IEEE	Institute of Electrical and Electronic Engineers
IPv4	internet protocol version 4
ILAC	International Laboratory Accreditation Cooperation
ISA99	ISA committee developing the S99 standard for IACS security
ISCI	ISA Security Compliance Institute
SDSA	software development security assessment
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
TCP	transmission control protocol
UDP	user datagram protocol

4 ISASecure EDSA certification program

4.1 Technical ISASecure EDSA evaluation criteria

ISASecure EDSA is a certification program for embedded devices, where a product is considered to be an embedded device if it satisfies the definition provided in 3.1.14. ISASecure certification of embedded devices has three elements:

- Communication robustness testing (CRT);
- Functional Security Assessment (FSA); and
- Software Development Security Assessment (SDSA).

CRT examines the capability of the device to adequately maintain essential services while being subjected to normal and erroneous network protocol traffic at normal to extremely high traffic rates (flood conditions). These tests include specific tests for susceptibility to known network attacks. The FSA examines the security capabilities of the device, while recognizing that in some cases security functionality may be allocated to other components of the device’s overall system environment. Finally, the SDSA examines the process under which the device was developed.

The program offers three certification levels for a device, offering increasing levels of device security assurance. These certifications are called ISASecure EDSA Level 1, ISASecure EDSA Level 2, and ISASecure EDSA Level 3.

All levels of certification include the three certification elements above. SDSA and FSA requirements increase in rigor for levels 2 and 3 while CRT criteria are the same regardless of certification level. Figure 1 illustrates this concept.

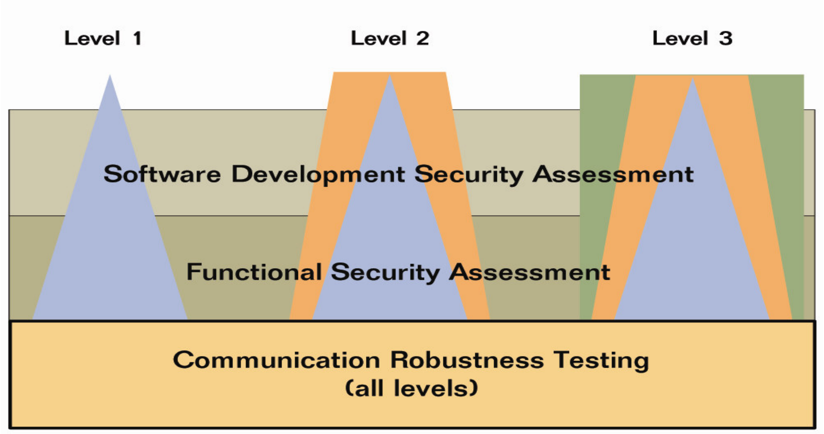
Level 1
Level 2
Level 3
Software Development Security Assessment
Functional Security Assessment
Communication Robustness Testing
(all levels)

Figure 1 - Structure of ISASecure Embedded Device Certifications

4.2 Certified embedded devices

The vendor for an embedded device that has been evaluated under the ISASecure EDSA certification program and shown to meet these technical criteria may display the ISASecure symbol and a certificate granting certification, in accordance with program procedures. Certification applies to a particular version of an embedded device, and references an ISASecure certification version. The ISASecure certification version number includes the year that the ISASecure version was released by ISCI, and a sequence number within that year. For example, device model 234, version 1.9 might be certified to ISASecure 2010.2 Level 1, which is the second ISASecure version released in 2010. The program defines procedures to maintain certification for the next version of the device, to later versions of the ISASecure evaluation program and to higher certification levels.

Subject to permission of each device vendor, ISCI will post the names of certified devices on its web site http://www.ISASecure.org.

4.3 Organizational roles

The following organizations participate in the ISASecure EDSA program. A term in parentheses following a description indicates the term used for this role in [ISO/IEC Guide 65].

- **End users** define procurement criteria for embedded devices, and may request an ISASecure device certified to a particular level

- **Device vendors** apply for certification of their embedded devices (supplier)

- **Chartered laboratories** accept applications from device vendors for device certification, evaluate devices, and grant device certifications to device vendors (conformity assessment body)

- **CRT tool suppliers** provide test tools that allow chartered laboratories to carry out CRT, and allow device vendors to test their devices in advance of formal evaluation for certification

- **ISCI** defines, maintains and manages the overall ISASecure EDSA certification program, grants recognition to qualified CRT tools, interprets the ISASecure EDSA specifications and maintains a web site for publishing program documentation, as well as lists of chartered laboratories, recognized CRT tools and certified devices

- **ASCI**, as the legal entity representing ISCI, grants chartered laboratory status to applicant organizations based on successful accreditation to criteria defined by ISCI

- The **EDSA accreditation body** evaluates candidates for chartered laboratory status and determines if they meet program accreditation criteria (accreditation body)

ISCI is organized as an interest area within ASCI (Automation Standards Compliance Institute), a not-for-profit 503 (c) (6) corporation owned by ISA. Descriptions of the governance and organizational structure for ASCI are found on the ISASecure website: http://www.ISASecure.org.

The EDSA accreditation body will be an organization recognized by IAF/ILAC.

Information related to device evaluations is private to chartered laboratories performing these evaluations, and is not disclosed to ASCI/ISCI, except as explicitly permitted by the device vendor or for cause in ASCI/ISCI's role as manager of the certification program.

4.4 Certification program documentation

4.4.1 Overview of documentation

Figure 2 shows the documents that define the ISASecure EDSA certification program. An arrow represents a referential dependency of a document on the contents of another document. Refer to Section 2 for the detailed bibliographic listing of these documents.

NOTE 1 [EDSA-200] and [EDSA-201] contain references to all related technical specifications. To retain readability, these references are not shown as arrows in the figure.

NOTE 2 The figure depicts all documents in Section 2 with the exception of the application forms [EDSA-202] and [EDSA-203] and certificate format document [EDSA-205].

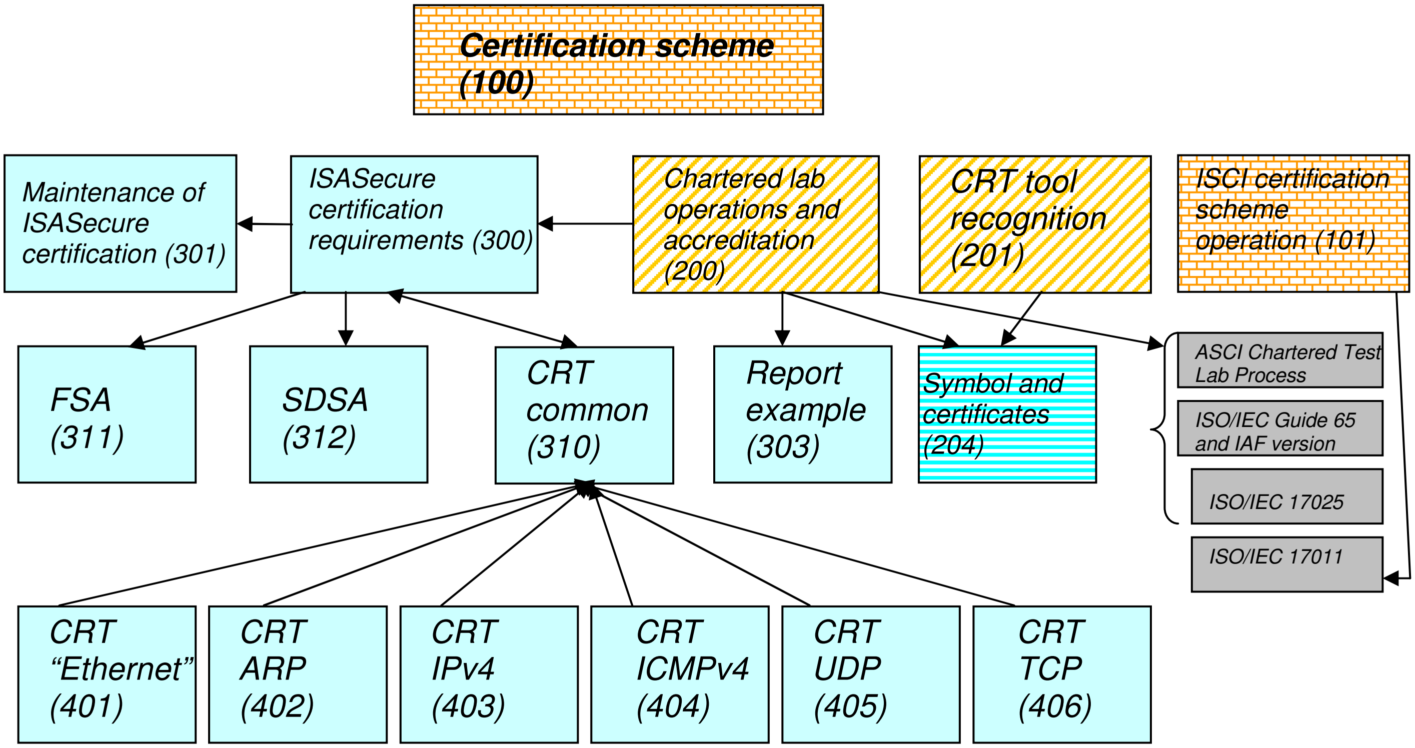
Certification scheme (100)
Maintenance of ISASecure certification (301)
ISASecure certification requirements (300)
Chartered lab operations and accreditation (200)
CRT tool recognition (201)
ISCI certification scheme operation (101)
FSA (311)
SDSA (312)
CRT common (310)
Report example (303)
Symbol and certificates (204)
ASCI Chartered Test Lab Process
ISO/IEC Guide 65 and IAF version
ISO/IEC 17025
ISO/IEC 17011
CRT "Ethernet" (401)
CRT ARP (402)
CRT IPv4 (403)
CRT ICMPv4 (404)
CRT UDP (405)
CRT TCP (406)

Figure 2 - ISASecure EDSA Documents

There are five major categories of ISASecure EDSA program documents:

- **Technical specifications**, shown in solid light blue, that describe the technical criteria applied to determine whether a device will be certified

  NOTE ISASecure EDSA program development has followed and leveraged the parallel ISA99 standards effort underway for embedded device cyber security requirements. When the ISA-99.04.01 standard is completed, the ISASecure Embedded Device certification technical specifications will be updated to serve as a compliance program for that standard.

- **Accreditation/recognition**, shown in gold diagonal stripe, that describe how an organization can become a chartered laboratory or a tool supplier can obtain recognition for a CRT tool

- **Symbol and certificates**, shown in blue horizontal stripe, covers the topic of proper usage of the ISASecure symbol and certificates

- **Structure,** shown in an orange brick pattern, used to describe and operate the overall program. The present document falls in this category.

- **External references**, shown in solid dark grey, are documents that exist outside of this particular program that are referenced by ISASecure EDSA program documents.

The following sections describe the documents in each category in further detail.

4.4.2 Technical specifications

The brief document [EDSA-300] *ISCI EDSA - ISASecure Certification Requirements,* defines at a high level the criteria for device certification, which simply stated, is to pass CRT, FSA, and SDSA. It points to the detailed documents on these three topics as shown in Figure 2. The documents [EDSA-311] and [EDSA-312] define the technical evaluation criteria for a device to pass FSA and SDSA, respectively, for each certification level.

The reference section of [EDSA-300] maintains the current list of protocol-specific CRT specifications, which defines the set of protocols that will be tested under CRT. At launch of the program, there are six such specifications, for “Ethernet”, ARP, IPv4, ICMPv4, UDP and TCP. These are documents numbered EDSA 401-406, shown at the bottom of the figure. An example is [EDSA-404] *ISCI EDSA – Testing the robustness of implementations of the IETF ICMPv4 network protocol*. Additional protocols and related documents will be added for CRT in the future.

The CRT common specification [EDSA-310], *ISCI EDSA – Common requirements for communication robustness testing of IP based protocol implementations*, contains test requirements that apply in common to CRT for all protocols. Hence individual protocol-specific test specifications all refer to this document. It should be pointed out that the approach taken for these specifications was to write each protocol-specific specification such that it could be understood as a stand alone document. Hence there is conceptual material that is similar across all of these specifications. However, details of common requirements are not repeated in each protocol-specific document, but rather presented in the common specification and referenced in the individual specifications.

The CRT common specification [EDSA-310] refers to [EDSA-300] for the list of required protocols to be tested, in order to define the pass criteria for CRT. This structure was chosen so that all ISASecure EDSA technical specifications could be listed in one technical document, which is [EDSA-300].

The document [EDSA-301] *ISCI EDSA – Maintenance of ISASecure Certification*, describes the certification criteria and process for a modified device, where a previous version has already achieved certification. It also covers the process for upgrading a certification to a later ISASecure version (for example 2010.2 Level 1 to 2011.1 Level 1), or to a higher level.

These documents are used by:

- End users, to understand the meaning of various levels of ISASecure certification

- Device vendors, to understand the criteria against which their devices will be evaluated

- Chartered laboratories, to define evaluation processes and criteria

- Tool suppliers and ISCI, as the end reference for technical requirements for achieving CRT tool recognition

- The EDSA accreditation body, as the end reference for technical readiness assessment requirements when evaluating candidate organizations for chartered laboratory status.

The device evaluation report template/example [EDSA-303] will be followed by chartered laboratories. It provides end users and device vendors with an understanding of the type of information that will be provided to device vendors following all device evaluations, and will be publicly available for a certified device.

4.4.3 Accreditation/Recognition

ISASecure EDSA chartered laboratories and CRT tool suppliers implement the technical aspects of the certification program. The accreditation/recognition documents define how they obtain this role.

[EDSA-200] *ISCI EDSA – ISASecure EDSA chartered laboratory operations and accreditation* describes the accreditation criteria and process that an organization will follow to become a chartered laboratory. A candidate organization initially attains provisional chartered status which allows it full rights to evaluate devices and grant ISASecure EDSA certifications. To be granted full status as a chartered laboratory for the ISASecure EDSA program, a laboratory shall attain within a specified time frame the following internationally recognized accreditations, performed by the EDSA accreditation body:

- accredited to ISO/IEC 17025, with technology scope of accreditation covering testing to ISASecure EDSA CRT specifications; and

- accredited to IAF ISO/IEC Guide 65, with technology scope of accreditation covering ISASecure EDSA certification.

[EDSA-200] details the requirements for both provisional and full chartered laboratory status, including interpretations of the above international standards for the ISASecure EDSA program, and the process for technical readiness assessment. This document is used by:

- organizations that are candidate chartered laboratories, to understand the accreditation requirements and process

- the EDSA accreditation body, as the source for program specific requirements for the Guide 65 and ISO/IEC 17025 accreditations listed above.

The ISASecure EDSA certification program requires the use of test tools for CRT. In particular a chartered laboratory must use a CRT tool recognized by ISCI. [EDSA-201] *ISCI EDSA – Recognition process for communication robustness testing tools* details how a tool supplier applies for and maintains recognition of their test tool for use within the program. Specifically, this document details which aspects of the test requirements in [EDSA-310] and [EDSA-401] through [EDSA-406] must be addressed by a CRT tool, and how a tool supplier will demonstrate these capabilities to ISCI in order to become a recognized ISASecure EDSA CRT tool. Thus this document is used by:

- a tool supplier, to understand tool recognition requirements

- ISCI, as the technical and process guide for its CRT tool recognition program

- Chartered laboratories, to understand the requirements that will be met by all recognized CRT tools, since the laboratory potentially must meet the balance of ISASecure EDSA CRT requirements by other means.

4.4.4 Symbol and certificates

The document [EDSA-204] *ISCI EDSA – Instructions and Policies for Use of the ISASecure Symbol and Certificates* describes the format and correct usage for the ISASecure symbol and certificates. The ISASecure symbol is used by device vendors to indicate a certified embedded device. It is also used by chartered laboratories and suppliers of recognized CRT tools to indicate their authorized participation in the ISASecure program.

Three types of ISASecure certificates are issued: for certified devices, chartered laboratories and recognized CRT tools.

The supporting document [EDSA-205] *ISCI EDSA – Certificate Document Format* is a convenient shorter document that contains certificate format templates only.

The documents in this category as they apply to certified devices are used by:

- device vendors, to understand requirements for symbol and certificate usage
- end users, to understand the meaning of a symbol or certificate displayed by a vendor
- chartered laboratories, to create certificates for certified devices
- chartered laboratories, to monitor for correct use of the symbol and device certificates by client device vendors as required by [EDSA-200].

These documents as they apply to chartered laboratories and CRT tools are used by:

- chartered laboratories and tool suppliers, to understand requirements for symbol and certificate usage
- device vendors, to understand the meaning of the symbol or certificate displayed by a chartered laboratory
- chartered laboratories and device vendors, to understand the meaning of the symbol or certificate as displayed by a tool supplier
- ASCI/ISCI, to create certificates for chartered laboratories and CRT tools
- ISCI, to monitor for correct use of the symbol and certificates for chartered laboratories and recognized CRT tools.

4.4.5 Structure

Documents in the Structure category are the present document [EDSA-100] and [EDSA-101] *ISCI EDSA – Certification scheme operation.* [EDSA-100] is a publicly available reference to the structure of the overall ISASecure EDSA program. [EDSA-101] is an internal ASCI/ISCI document that describes its operating procedures for the program. This includes procedures for processing applications from candidates for chartered laboratory status or CRT tool recognition, organizational responsibilities, conflict of interest policies, document control procedures, and record keeping.

4.4.6 External references

[ISO/IEC Guide 65] is an international standard that contains requirements for operating a product certification program. [IAF Guide 65 Guidance] is an established elaboration of [ISO/IEC Guide 65]. [ISO/IEC 17025] is an international standard that presents requirements for product testing programs. The requirements in this document apply to the CRT element of ISASecure EDSA. To obtain chartered status, chartered laboratories will demonstrate adherence to the requirements in these three standards as part of the accreditation process.

[ISO/IEC 17011] is an international standard that applies to the accreditation process itself. Thus this document is used by the EDSA accreditation body and ASCI to define their accreditation operations for the ISASecure EDSA certification program.

[ASCI Lab] *ASCI Chartered Testing Laboratory 2009 Approval Process* adds additional requirements to the accreditation process that are common across all ASCI conformance programs, including ISASecure EDSA. The portions of this document that are relevant to the ISASecure EDSA program are referenced by [EDSA-200].