EDSA-200

ISA Security Compliance Institute — Embedded Device Security Assurance –

ISASecure EDSA chartered laboratory operations and accreditation

Version 1.3

September 2010

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
1.2	2010.06.07	Initial version published to http://www.ISASecure.org
1.3	2010.09.21	Table 3 changes for requirement numbers and modified requirements due to revisions to CRT specs EDSA-310 and 401 through 406

Contents

List of requirements from other ISASecure EDSA specifications

List of tables

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). A description of this 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). An organization that performs evaluations and grants certifications under the ISASecure EDSA (Embedded Device Security Assurance) program for embedded devices is referred to as a *ISASecure EDSA chartered laboratory*, or (more briefly) a *chartered laboratory*. This document specifies the criteria and processes that define:

- Requirements on the operations of a chartered laboratory (Section 6); and
- How a chartered laboratory is accredited to begin and continue ISASecure device certification operations (Section 7).

ISCI has based its certification program approach on:

- International standards for conformity assessment programs
- General specifications for operation of ISA compliance programs
- Specifications developed for the ISASecure EDSA program.

This document provides a complete reference to these sources, and interprets applicable general specifications and standards for the ISASecure EDSA program.

2 Normative references

[EDSA-201] *ISCI Embedded Device Security Assurance –Recognition process for communication robustness testing tools,* 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

[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

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

NOTE The following document is the overarching technical specification for ISASecure EDSA CRT (communication robustness testing). The UDP-specific specification that follows it is also explicitly referenced in the present document. The list of all protocol-specific ISASecure EDSA technical test specifications is maintained in the normative references clause of [EDSA-300].

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

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

NOTE The following document applies to all ISA compliance testing programs.

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

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

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

3 Definitions and abbreviations

3.1 Definitions

3.1.1
accreditation
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
applicant
device vendor that has submitted an embedded device to a chartered laboratory for evaluation for ISASecure EDSA certification

3.1.4
allocatable

able to be met by other components

NOTE As used here, refers to security capabilities capable of being met by other components in a device’s architectural context, although not directly provided by the device itself.

3.1.5
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.

3.1.6
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.

3.1.7
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.

3.1.8
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.

3.1.9
preliminary visit

process used to evaluate whether an organization is ready for a formal assessment toward accreditation, and to identify nonconformances and the organization’s competency

NOTE This is a concept from [ISO/IEC 17011].

3.1.10
symbol

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

NOTE An earlier term for symbol is “mark.”

3.2 Abbreviations

The following abbreviations are used in this document.

ASCI	Automation Standards Compliance Institute
ARP	address resolution protocol
BS	Bachelor of Science
CE	computer engineering
CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional
CRT	communication robustness testing
CS	computer science
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
ICMP	Internet control message protocol
IEEE	Institute of Electrical and Electronic Engineers
ILAC	International Laboratory Accreditation Cooperation
ISCI	ISA Security Compliance Institute
SDSA	software development security assessment
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
NA	not applicable

4 Background

4.1 Technical ISASecure EDSA certification elements

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 3.1.8. 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.

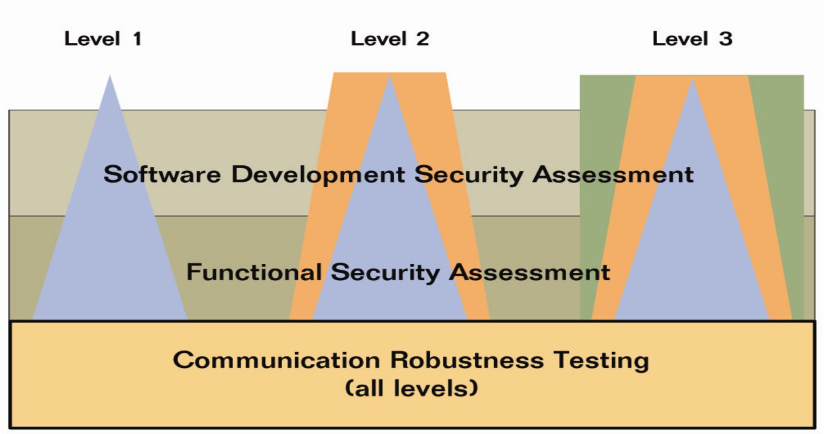
Level 1
Level 2
Level 3
Software Development Security Assessment
Functional Security Assessment
Communication Robustness Testing
(all levels)

Figure 1 - Structure of ISASecure Embedded Device Certifications

In addition to requirements for initial certification, ISASecure EDSA specifies requirements for maintaining certification when a certified device and/or ISASecure criteria are modified, as described in [EDSA-301].

4.2 ISASecure EDSA certification program implementation

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.

ASCI chartered laboratories are organizations that are accredited to evaluate embedded devices under the ISASecure EDSA program. ASCI grants accredited laboratories the right to process ISASecure EDSA certifications for embedded devices on its behalf and issue certificates for devices meeting the EDSA certification requirements. Device certification is determined by the chartered laboratory's tests, functional audits and process audits, which measure adherence to the ISASecure EDSA requirements for CRT, FSA and SDSA. The list of ASCI chartered laboratories is posted on the ISCI website at http://www.ISASecure.org. At the request of device vendors, devices that are issued certifications are registered on this same ISCI website.

The ISASecure EDSA certification program requires the use of test tools for communication robustness testing. These tools are used by chartered laboratories to perform CRT and by device vendors in preparation for certification. Test tools must be evaluated for consistency and fairness to ensure that they are appropriate for use by ASCI chartered test laboratories. ISCI operates a test tool recognition program to support these objectives. The program is described in document [EDSA-201].

5 Summary of operations and accreditation requirements

ISASecure EDSA will operate as an internationally recognized certification program. To meet this standard, the chartered laboratory operations and accreditation requirements are designed to comply with accepted international standards applicable to product certification and testing.

The operations of ISASecure EDSA chartered test laboratories shall be in compliance with the applicable requirements in:

- ASCI Chartered Testing Laboratory 2009 Approval Process [ASCI Lab]
- ISO/IEC Guide 65 [ISO/IEC Guide 65]
- IAF Guidance on the Application of Guide 65 [IAF Guide 65 Guidance]
- ISO/IEC 17025 [ISO/IEC 17025]

The first document in this list applies to ISCI (and all interest area groups that are organized under ASCI). The last three documents are international standards that apply generally to organizations that carry out tests and audits in support of product certification.

This document organizes the requirements from the above documents into a unified set of categories. Where required, it interprets those requirements for ISASecure EDSA and adds additional requirements. Of particular note are interpretations for:

- qualifications for chartered laboratory personnel (6.3.2);
- requirements on the certification application process (6.6.2);
- technical criteria for the certification decision (6.10.2;)
- complaint appeals (6.5.2);
- publication of certification status (6.6.2); and
- monitoring use of the ISASecure symbol (6.12.2).

Accreditation of a chartered laboratory consists of an assessment of the organization against the general requirements in the above documents and the specific requirements in Section 6 of this document, together with an assessment of technical readiness for performing ISASecure EDSA evaluations. Technical readiness assessment is based upon review of laboratory processes and procedures as well as review of artifacts from FSA and CRT audits carried out by the laboratory on a device. To be recognized as a chartered laboratory for the ISASecure EDSA program, a laboratory shall attain the following accreditations, performed by an IAF/ILAC 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 65, with technology scope of accreditation covering ISASecure EDSA certification.

The laboratory accreditation process consists of two steps. In the first step, an IEC assessor who is qualified with respect to the above two accreditations will complete a preliminary visit. Provisional chartered status is granted if the assessor’s report from the preliminary visit shows that the laboratory meets a defined subset of the requirements for full accreditation, including technical readiness. Provisional accreditation requirements ensure that the laboratory is organized and prepared to carry out ISASecure certifications in a competent, impartial and confidential manner. The set of requirements for provisional chartered laboratory status is defined in Section 7.2.

In the second step, laboratories must obtain full accreditation within 18 months of receiving provisional status, or they will be terminated from the ISASecure EDSA certification program. This is achieved via a formal assessment by the IEC assessor against the full requirements for the accreditations listed above.

The additional requirements to attain full chartered laboratory status require a formally documented and implemented management and quality system.

Once a laboratory has attained provisional chartered status, ASCI grants that laboratory the right to perform device evaluations and grant ISASecure EDSA certifications. These rights continue as long as the laboratory attains fully accredited chartered laboratory status in the required time frame and maintains this status.

6 Requirements on operations of chartered laboratories

6.1 Overview

This section specifies all requirements on the operation of chartered laboratories. It provides specific interpretations for some of the general requirements in the four source references listed in Section 5, and defines additional requirements that are specific to the ISASecure EDSA program. It should be noted that there are duplicate requirements as well as unique requirement contributions in the four source documents listed above.

The subset of these requirements that apply for provisional chartered laboratory status is discussed in Section 7.2. All ISASecure EDSA specific requirements called out in Section 6 of this document will apply for provisional chartered laboratories with the exception of those in 6.4.2.

The requirements on chartered laboratory operations listed in [ASCI Lab] apply to ISASecure EDSA as specified in this document. However, the application process described in [ASCI Lab] is not used for ISASecure EDSA chartered laboratories. A candidate organization for provisional chartered laboratory status shall follow the application process in [EDSA-202] in order to apply to ASCI for provisional chartered laboratory status, and in addition shall follow the application process specified by the accreditation body.

6.2 Management system elements

6.2.1 General requirements

The following requirements shall be implemented by a chartered laboratory. The chartered laboratory may subcontract as defined in these requirements. The subcontracting of the certification decision by the laboratory to another organization is not allowed per ISO/IEC requirements.

- ✓ *ASCI Chartered Testing Laboratory 2009 Approval Process I. Capability E. Quality Assurance and F. Records, also III Independence*
- ✓ ISO/IEC Guide 65 Section 4
- ✓ IAF ISO/IEC Guide 65 Section 4
- ✓ ISO/IEC 17025 Section 4

6.2.2 ISASecure EDSA specific requirements

The general confidentiality requirement in 4.10.2 of ISO/IEC Guide 65 states that information gained from an evaluation may not be available to a third party without consent of the device vendor. This means in particular that neither ASCI nor ISCI shall have access to information generated during ISASecure EDSA evaluations, except by permission of the device vendor. ISCI as a matter of course publishes the names of products that have been certified on its web site. This shall be done with permission of the device vendor.

The requirement in 4.2.1 of ISO/IEC 17025 for adequate documentation of procedures instructions, etc. shall be interpreted as follows for CRT: Laboratory documentation that provides guidance for CRT shall provide sufficient detail to ensure compliance with the requirements of [EDSA-310] and of the protocol-specific CRT specifications, when used in conjunction with a recognized CRT tool.

6.3 Personnel

6.3.1 General requirements

Chartered laboratory procedures shall address the general requirements as specified in:

- ✓ *ASCI Chartered Testing Laboratory 2009 Approval Process Section I. Capability G. Personnel*
- ✓ ISO/IEC Guide 65 Section 5
- ✓ IAF ISO/IEC Guidance on ISO/IEC Guide 65 Section 5
- ✓ ISO/IEC 17025 Section 5.2

6.3.2 ISASecure EDSA specific requirements

6.3.2.1 FSA/SDSA auditors

The above general requirements include written descriptions of personnel qualifications for positions related to evaluation of devices. The minimum qualifications that a chartered laboratory sets for auditors that carry out the FSA and SDSA shall include those specified in Table 1:

Table 1 - FSA/SDSA auditor qualifications

Category of qualification / experience	FSA auditor	SDSA auditor
Formal education	• BS Electrical Engineering **OR** • BS Computer Engineering (CE) OR • BS Computer Science (CS) OR • BS Chemical Engineering with CE or CS minor OR • Equivalent science or engineering degree	• BS Electrical Engineering **OR** • BS Computer Engineering OR • BS Computer Science OR • BS Chemical Engineering with CE or CS minor OR • Equivalent science or engineering degree
Professional certification*	• CISA, CISSP or equivalent	• CISA, CISSP or equivalent
Work experience post BS degree	• Min 8 years experience	• Min 8 years experience
Relevant development work experience	• Min 4 year detailed system level product development involvement for IACS **OR** • Min 4 years of systems integration experience for IACS **OR** • Min 6 years system level product Test of IACS • Experience includes 2 years with software security-related responsibilities	• Min 4 year software development experience for IACS **AND** • Min 2 year involvement with software process improvement activities • Experience includes 2 years with software security-related responsibilities • Experience includes 2 years with technical management responsibilities

Category of qualification / experience	FSA auditor	SDSA auditor
Relevant auditing work experience	• Min 1 year experience performing technical product audit OR 2 years in position in which has been audited on 3 or more products	• Min 1 year experience performing software process audit OR 2 years in position in which software process has been audited on 3 or more products
Relevant industry specific knowledge	• General knowledge of at least two different IACS **AND** • General knowledge of application of IACS and roles and duties of employees at sites using IACS **AND** • Moderate level knowledge of networking and communication protocols **AND** • Able to independently read and interpret requirement specifications for IACS products **AND** • Able to independently read and understand user installation and configuration documents for IACS products **AND** • Knowledge of methods used to protect communications and detect / prevent communication attacks	• General knowledge of end-end software development life cycle **AND** • General knowledge of IACS architectures
Knowledge of security standards	S99 Standard plus at least one of: • Common Criteria • ISO 27001	S99 Standard plus at least one of: • Common Criteria • ISO 27001

*Requirement applies 6 months after ISCI launch of the EDSA certification program.

6.3.2.2 CRT Testers

The minimum qualifications that a chartered laboratory sets for individuals that oversee the technical aspects of CRT testing and interpretation of results shall include those specified in Table 2:

Table 2 - CRT tester qualifications

Category of qualification / experience	CRT tester
Formal education	• BS Electrical Engineering **OR** • BS Computer Engineering **OR** • BS Computer Science **OR** • BS Chemical Engineering with CE or CS minor **OR** • Equivalent science or engineering degree **OR** • 4 years work experience in testing of IACS may be substituted for degree
Work experience post BS degree	• Min 5 years experience
Relevant development work experience	• Min 4 year detailed system level product development involvement for IACS **OR** • Min 4 years of Systems Integration experience for IACS **OR** • Min 3 years System Level Product Test for IACS

Category of qualification / experience	CRT tester
	• Experience includes 1 year with software security-related responsibilities • Experience includes 2 years involvement with networking technologies
Relevant test work experience	• Min 1 year experience performing testing on IACS
Relevant industry specific knowledge	• Successful completion of training class or 1 year experience in job demonstrating proficiency with CRT tool to be used **AND** • General knowledge of at least two different IACS **OR** detailed knowledge of one IACS **AND** • Moderate level knowledge of networking and communication protocols **AND** • Able to independently read and understand user installation and configuration documents for IACS Products **AND** • Knowledge of methods used to protect communications and detect / prevent communication attacks
Knowledge of security standards	S99 Standard plus at least one of: • Common Criteria • ISO 27001

6.4 Changes to certification requirements

6.4.1 General requirements

The chartered laboratory procedures must address the requirements as specified in:

✓ ISO/IEC Guide 65 Section 6

6.4.2 ISASecure EDSA specific requirements

For ISASecure, changes in technical certification requirements are initiated by ISCI, not the laboratory. Hence ISCI keeps the chartered laboratories informed of upcoming changes to technical certification criteria. The chartered laboratory in turn shall have processes to keep interested parties informed of these changes and other types of changes to certification requirements (such as changes to legal agreements associated with the certification process).

When technical changes in certification criteria occur, existing certifications to the previous criteria remain in place, since the certification applies to a particular product version. Hence no products can lose certification due to lack of communication of new technical requirements. However, vendors can do more effective planning related to future devices based upon timely information about upcoming changes (of all types) to the certification program requirements.

6.5 Appeals, complaints and disputes

6.5.1 General requirements

Chartered laboratory procedures shall address the requirements as specified in

✓ *ASCI Chartered Testing Laboratory 2009 Approval Process Section IV. Report and Complaint Procedures B. Complaints*

✓ ISO/IEC Guide 65 Section 7

✓ IAF ISO/IEC Guide 65 Section 7

- ✓ ISO/IEC 17025 Section 4.8

6.5.2 ISASecure EDSA specific requirements

The published chartered laboratory procedure for handling complaints shall include the provision that complaints may be appealed to ISCI by the party bringing the complaint, if the internal laboratory resolution procedure does not offer a resolution satisfactory to them. Appealed complaints first go to the ISCI Technical Steering Committee. They may be further appealed to the ISCI governing board, then to ASCI board of directors.

An appealed complaint may request a ruling on whether the ISASecure specifications were correctly applied by the chartered laboratory in a specific instance. Such a complaint shall not be escalated to the ASCI board of directors, but is resolved within ISCI. This ruling could impact:

- Whether the certification process is applicable to a particular product that has applied for certification
- Whether or not a certification was granted
- Adequacy of the device evaluation process by the chartered laboratory.

ISCI or ASCI shall not accept certification applications, process, grant or revoke certifications. This is the role of a chartered laboratory. ISCI can assist in interpretation of the ISASecure EDSA specifications toward this end.

6.6 Application for certification

6.6.1 General requirements

The procedures shall address the requirements as specified in:

- ✓ *ASCI Chartered Testing Laboratory 2009 Approval Process Section I. Capability 8. Testing, evaluation and processing, items C7-C8.*
- ✓ ISO/IEC Guide 65 Section 8
- ✓ ISO/IEC 17025 Section 4.4, Contract Review of Testing Services

6.6.2 ISASecure EDSA specific requirements

The ISASecure specification [EDSA-300] contains requirements that device vendors must meet in order to apply for ISASecure EDSA certification for a device. That document is intended as a reference for vendors applying for certification of a device.

These requirements are numbered R1, R2, and R4, and are repeated below.

This document requires that a chartered laboratory incorporate these three requirements into their certification application process for device vendors:

Requirement ISASecure_ED.R1 – Application for a certification level

When a device vendor applies for certification of an embedded device, the certification applicant SHALL specify the maximum level for which they would like to achieve device certification. The levels possible are 1, 2, or 3. The certifier SHALL award certification to a device at the highest level less than or equal to this maximum level for which the device qualifies, without requiring the device vendor to reapply for certification.

Requirement ISASecure_ED.R2 – Prior certifications

When applying for ISASecure certification of an embedded device, the certification applicant SHALL specify one of:

- this is an initial certification
- this device or an earlier version has achieved an ISASecure certification, which is offered as evidence toward this certification.

As discussed in [EDSA-301], the certifier may perform an analysis to determine the extent to which the evidence offered from a prior certification is applicable to the new certification. The certifier shall have the option to require an initial certification if in its judgment such an analysis would not be cost effective.

Requirement ISASecure_ED.R4 – ISASecure application requirements for an initial certification

Items specified as follows SHALL be submitted to the certification process by an applicant for an initial certification:

a) technical items as required by the specifications listed in Clause 2 of [EDSA-300]; and

b) administrative and potentially additional technical items defined by the certifier.

A chartered laboratory shall include the following in its signed agreement with a certification applicant:

Requirement ISASecure_ED.R3 – Publication of embedded device certification status

ISCI, the certifier, and the device vendor SHALL publish certification status information for certified devices in a public venue. Information provided SHALL include the most granular version identifier of the device to which the ISASecure EDSA certification applies, and the version of the certification achieved, designated by the year and release, such as ISASecure EDSA 2010.2.

6.7 Preparation for evaluation/testing

6.7.1 General requirements

Chartered laboratory procedures shall address the requirements as specified in:

- ✓ ISO/IEC Guide 65 Section 9
- ✓ IAF ISO/IEC Guide 65 Section 9
- ✓ ISO/IEC 17025 Section 4.4

6.7.2 ISASecure EDSA specific requirements

Individuals assigned responsibility for an FSA audit, SDSA audit and oversight of CRT shall have at a minimum the qualifications listed in 6.3.2.

6.8 Evaluation

6.8.1 General requirements

Chartered laboratory procedures shall address the requirements as specified in:

- ✓ *ASCI Chartered Testing Laboratory 2009 Approval Process Section I. Capability A. Testing facilities, B. Testing equipment and C. Testing, evaluation and processing procedures*

- ✓ ISO/IEC Guide 65 Section 10
- ✓ ISO/IEC 17025 Section 5 – Technical Requirements

6.8.2 ISASecure EDSA specific requirements

An initial evaluation of an embedded device shall be carried out in accordance with all technical specifications for CRT, FSA and SDSA as listed in Clause 2 of [EDSA-300].

[EDSA-301] specifies the method for carrying out a device evaluation when evidence from a prior certification is accepted toward a new certification for a newer device version.

For the SDSA, the following requirement from [EDSA-300] applies to the evaluation process:

Requirement ISASecure_ED.R3 – Consideration for prior SDSA

A certifier SHALL consider the applicability of SDSA evaluation evidence and results for a certified device, to certifications for any later devices from the same organization.

The evaluation and testing process shall use an ISCI recognized test tool for CRT. The process for recognition of test tools is defined in [EDSA-201]. The chartered laboratory shall verify that the software version and hash of the tool software is as specified for the recognized tool on the ISASecure web site at http://www.ISASecure.org.

The laboratory shall have a procedure to verify identical device configurations as required by [EDSA-310], if portions of CRT are carried out on different physical devices.

ISO/IEC 17025 5.4.2 on selection of test methods, specifies using the latest version of the standards upon which tests are based. The latest versions of ISASecure specifications shall be identified on the ISASecure web site.

ISO/IEC 17025 5.4.4 and 5.4.5 discuss the definition of procedures for and validation of non-standard test methods. The test methods and criteria for monitoring upward essential services for CRT are non-standard test methods that are agreed with each certification applicant before the start of CRT. They are subject to the requirements in these ISO/IEC 17025 sub clauses.

ISO/IEC 17025 5.5 on the topic of accuracy, appropriate use, maintenance and calibration specifically applies to the CRT test tool, in particular the functional component of this tool that measures jitter.

6.9 Evaluation report

6.9.1 General requirements

The chartered laboratory shall address the requirements on evaluation reports as specified in:

- ✓ *ASCI Chartered Testing Laboratory 2009 Approval Process Section I Reports and Complaint Procedures, A. Reports.*
- ✓ ISO/IEC Guide 65 Section 11
- ✓ ISO/IEC 17025 Section 5.10 – Testing Report

6.9.2 ISASecure EDSA specific requirements

The overall evaluation report shall follow the format of the ISASecure EDSA sample report [EDSA-303].

Detailed reporting on CRT results for an embedded device shall be carried out in accordance with the requirements on CRT reporting in all technical specifications for CRT as listed in Clause 2 of [EDSA-300].

ISO/IEC Guide 65 Section 11b) states that in the case of a nonconformance such that certification is not granted, that the report from the chartered laboratory shall advise the certification applicant of the additional testing and assessment that needs to take place once the item is remedied. For ISASecure EDSA, if the FSA or SDSA does not pass, those items in the FSA or SDSA that may require reassessment shall be specified. If the CRT element does not pass, all CRT tests shall be performed on a modified device presented again for certification in order to pass this element.

6.10 Decision on certification

6.10.1 General requirements

The chartered laboratory shall address the requirements on the decision to certify an embedded device in:

- ✓ ISO/IEC Guide 65 Section 12
- ✓ IAF ISO/IEC Guide 65 Section 12

6.10.2 ISASecure EDSA specific requirements

The following defines the technical criteria that a chartered laboratory shall use for granting an initial ISASecure EDSA certification:

Requirement ISASecure_ED.R5 – Criteria for granting an initial certification

An initial ISASecure EDSA certification for level *n* SHALL be granted for an embedded device if:

- for all levels, the CRT pass criteria are met as defined in [EDSA-310];
- all FSA criteria in [EDSA-311] applicable to level *n* are assessed as either supported or allocatable; and
- all SDSA criteria in [EDSA-312] applicable to level *n* are assessed as pass.

[EDSA-301] specifies the technical criteria that the laboratory shall use for granting certification when evidence from a prior certification is accepted as evidence toward a new certification for a different version of the same device.

The form of letter or certification document provided when a device passes certification shall meet the format requirements in [EDSA-205].

6.11 Surveillance

An ISASecure EDSA certification states that a specific version of an embedded device meets established security criteria. ISCI does not require a chartered laboratory to verify periodically that devices shipped by the vendor that are labeled with the version number that has been certified, are in fact that version. There are however, requirements for the chartered laboratory to monitor the use of the ISASecure symbol as described in Section 6.12.

6.12 Use of the ISASecure symbol

6.12.1 General requirements

The procedures for use of the ISASecure symbol on a device shall address the requirements as specified in:

- ✓ *ASCI Chartered Testing Laboratory 2009 Approval Process Section II Control Programs, A. Listing and Labeling.*

- ✓ ISO/IEC Guide 65 Section 14
- ✓ IAF ISO/IEC Guide 65 Section 14

6.12.2 ISASecure EDSA specific requirements

The interpretation of the above requirements for ISASecure entails that the chartered laboratory shall monitor the use of the ISASecure symbol by the device vendor to insure appropriate use, and take appropriate action if the symbol is used incorrectly.

[EDSA-204] provides detailed instructions and policies regarding use of the ISASecure symbol. The agreement that the chartered laboratory signs with the certification applicant shall acknowledge and require adherence to this information.

6.13 Complaints to embedded device vendors

6.13.1 General requirements

A chartered laboratory shall include the following in its signed agreement with a device vendor: that the vendor has a process for meeting the requirements regarding complaints they receive, as specified in:

- ✓ ISO/IEC Guide 65 Section 15

These requirements address handling and disclosure of complaints known to the vendor of a certified device, regarding the compliance of that device with the ISASecure EDSA requirements.

6.13.2 ISASecure EDSA specific requirements

In addition, the signed agreement between the laboratory and the device vendor shall include the following broader provision. Any complaint known to the vendor of a certified device that is determined to affect product security shall be brought to the attention of the chartered laboratory that granted a certification for the device. The laboratory shall evaluate the impact on the product conformance to the ISASecure requirements.

The chartered laboratory process for handling such reports from a vendor shall include a process to advise ISCI if a modification to the ISASecure specifications should be considered based upon this event. This process shall be contingent upon approval from the device vendor to disclose to ISCI any information concerning their device, whether or not it is attributed to their device.

7 Accreditation of chartered laboratories

7.1 Overview

Accreditation of a chartered laboratory involves an assessment of the organization against the requirements in the following documents, and an assessment of technical readiness for performing ISASecure EDSA evaluations.

- ASCI Chartered Testing Laboratory 2009 Approval Process [ASCI Lab]
- ISO/IEC Guide 65 [ISO/IEC Guide 65]
- IAF Guidance for ISO/IEC Guide 65 [IAF Guide 65 Guidance]
- ISO/IEC 17025 [ISO/IEC 17025]
- Section 6 this document, all ISASecure specific requirements subsections

Technical readiness assessment is based upon review of documented laboratory processes and procedures as well as review of artifacts from sample FSA and CRT audits carried out by the laboratory on a device supplied by ISCI, as described in Section 7.3. To be recognized as a chartered laboratory for the ISASecure EDSA program, a laboratory shall attain the following accreditations, performed by an IAF/ILAC recognized 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 65, with technology scope of accreditation covering ISASecure EDSA certification.

The second accreditation will require compliance with the IAF Guidance on ISO/IEC Guide 65 in addition to Guide 65.

These internationally recognized accreditations shall be obtained by a laboratory within 18 months of obtaining a provisional chartered laboratory status, as described in Section 5. The following section discusses requirements for attaining provisional chartered laboratory status.

7.2 Provisional chartered laboratory status

The goal for provisional accreditation is that the laboratory that attains provisional chartered status is organized and prepared to carry out ISASecure certifications in a competent, impartial and confidential manner. The attainment of full, internationally recognized chartered laboratory status requires in addition, a formally documented and implemented management and quality system that sustains and improves these operations.

ASCI will grant a laboratory provisional chartered status based on the results of a preliminary visit at the laboratory by a qualified IEC assessor for the 17025 and Guide 65 accreditations listed in Section 7.1. Provisional chartered status is granted if the preliminary visit shows that the laboratory complies with a defined subset of the requirements in the five documents listed in Section 7.1, as well as technical readiness per Section 7.3. All ISASecure specific requirements in Section 6 of this document except 6.4.2 are mandatory to receive provisional chartered status.

The subset of requirements for provisional chartered status covers the following topics:

- **organization** – legal entity status, organizational structure and management in place, roles, responsibility for and disclosure of subcontractors, financial resources, liability coverage
- **impartiality** – impartiality to customers, conflict of interest eliminated at an individual and organizational levels, adherence to restrictions on performing certification-related services or activities
- **confidentiality protection** – formal processes in place to protect confidentiality of certification information from all third parties, including ASCI and ISCI
- **technical expertise and resources** - personnel (and potentially contractors) of the laboratory meet the qualifications listed in Section 6.3.2, adequate supervision of personnel, appropriate test laboratory facilities and tools
- **due care –** transparency of work to customer, control of customer-supplied equipment, adequate storage and backup of technical records, complaint process, process for resolution of nonconforming work, adequate legal agreement with customers, ASCI approved certification document format

Annex A identifies the detailed subset of requirements from each of the first four normative accreditation reference documents that cover the above topics for provisional chartered laboratory status. Annex B organizes these requirements within the topical areas listed above rather than by source document.

In summary, to attain provisional chartered status a preliminary visit must show that the laboratory meets the following requirements:

1. all requirements in Annex B of this document (which cover the topics above)
2. all ISASecure specific requirements in Section 6 of this document except 6.4.2
3. technical readiness as described in 7.3.

The preliminary visit for a candidate laboratory toward provisional chartered laboratory status is performed by an IEC assessor that has been qualified by an IAF/ILAC recognized accreditation body. Application for a preliminary visit is made as required by the accreditation body. [EDSA-202] provides the ASCI application process and forms for provisional chartered laboratory status based on this preliminary visit.

During the period when a chartered laboratory is operating in provisional status, ASCI shall be made aware of the laboratory's plans for internationally recognized accreditation by an IAF/ILAC organization. ASCI shall have the option to perform an interim review and update its evaluation for provisional accreditation of the laboratory 9 months after it is received. Once a chartered laboratory has achieved accreditation by an IAF/ILAC organization, that organization determines the requirements and frequency for maintenance audits to maintain accredited status.

7.3 Technical readiness assessment

The technical readiness assessment for accreditation focuses on CRT and FSA. The evaluation consists of assessment of evidence supplied by the candidate laboratory per the evaluation criteria in Table 3. The requirements numbered UDP.nn in this table are from [EDSA-405]. The requirements numbered CRT.nn are from [EDSA-310].

Table 3 - Evidence for technical readiness

ID	Evidence supplied by candidate laboratory	Evaluation criteria
1	Vendor statement of test tools and versions in use for CRT, description of robustness testing methodology	• CRT tool and version for robustness test is recognized by ISCI • Appropriate tool is in place for interface surface test • Robustness testing methodology complies with UDP.R6, UDP.R8, UDP.R10 and similar requirements for other protocols
2	CRT processes/procedures	• Comply with coverage of various phases of testing per CRT.R50 • Comply with CRT.R2 on how protocols for test are selected; CRT.R3 on test order; CRT.R5 on criteria for pass; and CRT.R6 on use of multiple DUTs; • Comply with CRT.R25 on documentation and reporting of discussions with customers on anomalies; CRT.R26 on reporting conditional branches of test execution; • Comply with set up procedure for interface surface test per CRT.R29-31; and for individual protocol tests

ID	Evidence supplied by candidate laboratory	Evaluation criteria
		• Comply with CRT.R39 regarding requirement for TD measurement jitter relative to device cycle time and monitoring coverage for various device outputs • Comply with CRT.R51 on handling of redundant configuration devices • Comply with interface surface test requirements CRT.R32-37 and CRT.R41 • Comply with CRT.R59 regarding mixing types of PDUs • Comply with CRT.R60 for how pass of CRT is defined • Comply with CRT.R61 regarding repeating failures before giving failed status • Comply with CRT.R63 for setting pseudo random seed value if used • Instructions for evaluation report creation comply with CRT.R65-69
3	Mapping that maps each interface surface test requirement in [EDSA-310] Sections 8.1-8.5 to a portion of a test procedure	• Mapping is complete and accurate
4	Mapping that maps each table in Section 7 of each CRT protocol-specific specification to a portion of test procedure	• Mapping is complete and accurate
5	Application form and instructions to be given to vendors submitting devices	• Application requests all items required per [EDSA-310] Section 6 • Application requests information about proprietary protocol extensions per UDP.R4 and parallel requirements for other protocols
6	Intermediate artifacts, paperwork and final evaluation report for an ISCI-supplied sample device (with application also filled out by ISCI), covering CRT and FSA, and including a mock up of SDSA results. Artifacts include procedure for non-standard tests created for the sample	• Results of FSA are as expected • Results of interface surface test are as expected and indicate compliance with procedures • Results of robustness tests are as expected and indicate compliance with procedures • Report of test configurations for tests meet requirements CRT.R29-31 and CRT.R48-49 in appropriate protocol tests

ID	Evidence supplied by candidate laboratory	Evaluation criteria
	device to monitor upward essential services per ISO/IEC 17025 5.4.4 and validation of these tests per 5.4.5.	• Records of control signal generated for testing meet requirements of CRT.R39 • Check for reporting of pseudo random seed value per CRT.R63 • Artifacts that describe test method to monitor upward essential services comply with CRT.R40 • Evaluation report and detailed CRT report meet requirements per Section 6.9 of this document • Evaluation report complies with UDP.R12 and similar requirements for other protocols. • Evidence meets [ASCI Lab] IV.A.1, I.C.1, I.C.2
7	Evidence demonstrating that interface surface test result and robustness test result requested by ISCI can be reproduced based on information in evaluation report; document steps used to reproduce these	• Verify that steps for creation of reproduced result required only information in the evaluation report; and that results are same as initial results

Note that in Step 6, a mock up of the SDSA results is requested since an SDSA cannot be carried out without involvement of the device vendor. In the case of this sample evaluation, the device vendor for the sample device will not be involved in the process.

Annex A Requirements for provisional chartered laboratory status, by reference

A.1 ISO/IEC Guide 65

The candidate for provisional status as an ISASecure EDSA chartered laboratory will be required to demonstrate compliance with the requirements designated in Table 4 below from [ISO/IEC Guide 65].

Table 4 - ISO/IEC Guide 65 requirements for provisional accreditation

Clause	Title	Required for Provisional Accreditation	Comments
4.	Certification body	▨	▨
4.1	General provisions	all	4.1.3, 4.1.4 demonstrated by technical readiness assessment
4.2	Organization	all except k	
4.3	Operations	all	Demonstration addressed by technical readiness assessment
4.4	Subcontracting	all	
4.5	Quality system		
4.6	Conditions and procedures for granting, maintaining, extending, suspending and withdrawing certification	all	
4.7	Internal audits and management reviews		
4.8	Documentation		
4.9	Records		
4.10	Confidentiality	all	
5.	Certification body personnel	5.1.1	
6.	Changes in the certification requirements		
7.	Appeals, complaints and disputes	all	
8.	Application for certification	all	
9.	Preparation for evaluation	9.3	
10.	Evaluation		
11.	Evaluation report	all	
12.	Decision on certification	all	
13.	Surveillance		
14.	Use of licences, certificates and marks of conformity	all	
15.	Complaints to suppliers	all	

A.2 IAF Guidance on ISO/IEC Guide 65

The candidate for provisional accreditation as an ISASecure EDSA chartered laboratory will be required to demonstrate compliance with the requirements designated in Table 5 below from [IAF Guide 65 Guidance]. Note that mandatory requirements in that document (as in the other standards referenced here) are designated by the use of “shall.”

Table 5 - IAF Guidance on ISO/IEC Guide 65 requirements for provisional accreditation

Clause	Title	Required for Provisional Accreditation	Comments
4.	Certification body	▨	▨
4.1	General provisions	G4.1.1; G4.1.2	All of remaining requirements are the responsibility of ASCI

4.2	Organization	G4.2.3;
		G4.2.18;
		G4.2.19;
		G4.2.22;
		G4.2.30
			Some of remaining requirements are the responsibility of ASCI, others are not mandatory

4.3	Operations	4.3.1	Topic addressed by technical readiness assessment. Other mandatory requirements in this section apply to ASCI, and not to the chartered laboratory.

4.4	Subcontracting	G4.4.2;
		G4.4.3;
		G4.4.4	

4.5	Quality system		Not in ISO/IEC Guide 65 requirements for provisional accreditation
4.6	Conditions and procedures for granting, maintaining, extending, suspending and withdrawing certification		Suspension of certification is not applicable for ISASecure EDSA
4.7	Internal audits and management reviews		Not in ISO/IEC Guide 65 requirements for provisional accreditation
4.8	Documentation		Not in ISO/IEC Guide 65 requirements for provisional accreditation

Clause	Title	Required for Provisional Accreditation	Comments
4.9	Records		No requirements in this section of guidance
4.10	Confidentiality		No requirements in this section of guidance
5.	Certification body personnel		Record keeping as specified here not required for provisional accreditation
6.	Changes in the certification requirements		Not in ISO/IEC Guide 65 requirements for provisional accreditation
7.	Appeals, complaints and disputes	G.7.3	Remaining requirements are not mandatory
8.	Application for certification		No requirements in this section of guidance
9.	Preparation for evaluation		No mandatory requirements in this section of guidance
10.	Evaluation		No requirements in this section of guidance
11.	Evaluation report		No requirements in this section of guidance

12.	Decision on certification	G.12.4;
		G.12.5;
		G.12.6
			Remaining requirements are not mandatory or apply to ASCI and not to the chartered laboratory

13.	Surveillance		Not in ISO/IEC Guide 65 requirements for provisional accreditation
14.	Use of licences, certificates and marks of conformity		Requirements are not mandatory or apply to ASCI and not to the

Clause	Title	Required for Provisional Accreditation	Comments
			chartered laboratory
15.	Complaints to suppliers		No requirements in this section of guidance

A.3 ISO/IEC 17025

The candidate for provisional status as an ISASecure EDSA chartered laboratory will be required to demonstrate compliance with the requirements designated in below from [ISO/IEC 17025].

Table 6 - ISO/IEC 17025 requirements for provisional accreditation

Clause	Title	Required for Provisional Accreditation	Comments
4.	Management requirements	▨	▨
4.1	Organization	4.1.1; 4.1.4; 4.1.5b,c,f,g,h	
4.2	Management system	4.2.1	Addressed by technical readiness assessment, therefore CRT process and procedure documentation shall exist to meet the evaluation criteria defined in Section 7.3 of this document
4.3	Document control		
4.4	Review of requests, tenders and contracts		
4.5	Subcontracting	4.5.1-4.5.3	
4.6	Purchasing		
4.7	Service to clients	4.7.1	
4.8	Complaints	all	
4.9	Control of nonconforming work	4.9.1	
4.10	Improvement		
4.11	Corrective action		
4.12	Preventive action		

4.13	Control of records	4.13.1.2;
		4.13.1.3;
		4.13.1.4
		Scope limited to technical records	

4.14	Internal audit		
4.15	Management review		
5.	Technical	▨	▨
5.1	General	all	Addressed by technical readiness assessment
5.2	Personnel	5.2.1; 5.2.3	
5.3	Accommodation and environmental conditions	all	

Clause	Title	Required for Provisional Accreditation	Comments
5.4	Test and calibration methods and method validation	5.4.1; 5.4.2; 5.4.4; 5.4.5	Addressed by technical readiness assessment; 5.4.4 and 5.4.5 shall be addressed as noted in Section 6.8.2 of this document
5.5	Equipment	5.1.1; 5.1.2	Addressed by technical readiness assessment
5.6	Measurement traceability	5.6.2.2.2	Addressed by mappings required in technical readiness assessment
5.7	Sampling		Not applicable
5.8	Handling of test and calibration items	5.8.1; 5.8.2	
5.9	Assuring the quality of test and calibration results		
5.10	Reporting the results	all	Addressed by technical readiness assessment

A.4 ASCI Chartered Testing Laboratory 2009 Approval Process

The candidate for provisional status as an ISASecure EDSA chartered laboratory will be required to demonstrate compliance with the requirements designated in Table 7 from [ASCI Lab].

Table 7 - ASCI Chartered Testing Laboratory 2009 Approval Process requirements for provisional accreditation

Section	Title	Required for Provisional Accreditation	Comments
I.A.	Capability - Testing Facilities	all	
I.B.	Capability - Test Equipment	1	
I.C.	Capability - Testing, Evaluation and Processing Procedures	1; 2	Addressed by technical readiness assessment
I.D	Capability - Calibration Program		No application seen for ISASecure EDSA.
I.E.	Capability - Quality Assurance		
I.F.	I. Capability F. Records (including Specifications Library)		
I.G.	Capability - Personnel	1; 4	
II.A.	Control Programs - Listing and Labeling	2; 3; 4	II.A.1 is applicable to ASCI; II.A.2 shall be part of laboratory agreement with vendor client
II.B.	Control Programs - Follow up and Field Inspections		Not applicable. The initial assessment of the manufacturer (device vendor) described in this section is superseded by the SDSA. Follow up inspections are not required by the ISASecure EDSA program. See rationale in Section 6.11 of this document.
III	Independence	all	
IV.A.	Report and Complaint Procedures-Reports	1; 3	Demonstration for IV.A.1 addressed by technical readiness assessment

Section	Title	Required for Provisional Accreditation	Comments
IV.B.	Report and Complaint Procedures - Complaints	1	Documented policy aspect of IV.B.2 is required by other standards

Annex B Requirements for provisional chartered laboratory status, by topic

The candidate for provisional accreditation as an ISASecure EDSA chartered laboratory will be required to demonstrate compliance with the requirements designated in Table 8 below, and with all ISASecure specific requirements in Section 6 of this document except 6.4.2, in addition to passing a technical readiness assessment per Section 7.3. The requirements below comprise the same total set of requirements listed in all documents analyzed in Annex A, except that those requirements that are addressed by the technical readiness assessment (as noted in Annex A) have been removed.

Table 8 - Requirements for provisional accreditation not covered by technical readiness assessment

Topic	Document	Required for Provisional Accreditation
Organization	ASCI Chartered Testing Laboratory 2009 Approval Process	
	ISO/IEC Guide 65	4.2 b,c,d, f,g,h,i,n; 4.4; 12.1; 12.2
	IAF Guidance on Application of ISO/IEC Guide 65	G.4.4.2; G.4.4.3; G.4.4.4
	ISO/IEC 17025	4.1.1; 4.1.5f; 4.1.5h; 4.5.1; 4.5.2; 4.5.3
Impartiality	ASCI Chartered Testing Laboratory 2009 Approval Process	III.
	ISO/IEC Guide 65	4.1.1; 4.1.2; 4.2a,e,l,m,n,o; 9.3
	IAF Guidance on Application of ISO/IEC Guide 65	G.4.1.1; G.4.2.3; G.4.2.18; G.4.2.19; G.4.2.22; G.4.2.30
	ISO/IEC 17025	4.1.4; 4.1.5b
Confidentiality	ASCI Chartered Testing Laboratory 2009 Approval Process	IV.A.3
	ISO/IEC Guide 65	4.10
	IAF Guidance on Application of ISO/IEC Guide 65	
	ISO/IEC 17025	4.1.5c
Technical Personnel and Resources	ASCI Chartered Testing Laboratory 2009 Approval Process	I.A.1 – I.A.6; I.B.1; I.G.1; I.G.4
	ISO/IEC Guide 65	4.2j; 5.1.1; 9.3
	IAF Guidance on Application of ISO/IEC Guide 65	G.12.4
	ISO/IEC 17025	4.1.5g; 5.2.1; 5.2.3; 5.3
Due Care	ASCI Chartered Testing Laboratory 2009 Approval Process	I.A.7; II.A.2 – II.A.4; IV.B.1
	ISO/IEC Guide 65	4.2p; 4.6; 7; 8; 11; 12.3; 12.4; 14; 15
	IAF Guidance on Application of ISO/IEC Guide 65	G.4.1.2; G.7.3; G.12.5; G.12.6
	ISO/IEC 17025	4.7.1; 4.8; 4.9.1; 4.13.1.2; 4.13.1.3; 4.13.1.4; 5.8.1; 5.8.2

Annex C Mapping from sources for general requirements to this document

In this section we show the coverage of the ISO/IEC Guide 65 and 17025 international standards, and the ASCI chartered laboratory process, as called out in this document. Each mapping table is preceded by a summary statement regarding the coverage shown by that mapping.

C.1 ISO/IEC Guide 65 1996 coverage

As shown in Table 9, all sections of [ISO/IEC Guide 65] are called out as requirements in this document, with the exception of clause 13 regarding surveillance. The reason for this omission is noted below.

Table 9 - Mapping from ISO/IEC Guide 65 to this document

	Reference in ISO/IEC Guide 65	Reference this document	Comments
4.	Certification body	6.2	
5.	Certification body personnel	6.3	
6.	Changes in the certification requirements	6.4	
7.	Appeals, complaints and disputes	6.5	
8.	Application for certification	6.6	
9.	Preparation for evaluation	6.7	
10.	Evaluation	6.8	
11.	Evaluation report	6.9	
12.	Decision on certification	6.10	
13.	Surveillance	NA	There are no requirements under this topic. The rationale for this is discussed in Section 6.11 of this document.
14.	Use of licenses, certificates and marks of conformity	6.12	
15.	Complaints to suppliers	6.13	

C.2 IAF ISO/IEC 65 Guidance coverage

As shown in Table 10, all sections of [IAF Guide 65 Guidance] are called out as requirements in this document, with the exception of Clause 13. Clause 13 has no associated requirements in this document for the reasons referenced below.

Table 10 - Mapping from IAF Guidance on ISO/IEC Guide 65 to this document

	Reference in IAF ISO/IEC 65	Reference this document	Comments
4.	Certification body	6.2	
5.	Certification body personnel	6.3	
6.	Changes in the certification requirements		No requirements in this clause of standard
7.	Appeals, complaints and disputes	6.5	
8.	Application for certification		No requirements in this clause of standard
9.	Preparation for evaluation	6.7	
10.	Evaluation		No requirements in this clause of standard
11.	Evaluation report		No requirements in this clause of standard
12.	Decision on certification	6.10	
13.	Surveillance	NA	There are no requirements under this topic. The rationale for this is discussed in Section 6.11.
14.	Use of licenses, certificates and marks of conformity	6.12	
14.	Complaints to suppliers		No requirements in this clause of standard

C.3 ISO/IEC 17025 coverage

All requirements in ISO/IEC 17025 are referenced in this document. As shown in Table 11, the requirements clauses 4 and 5 of ISO/IEC 17025 are called out in their entirety in this document, respectively in 6.2 which covers management elements and in 6.8 which covers evaluation. In addition, some sub clauses of those clauses are called out in more specific sections as shown below.

Table 11 - Mapping from ISO/IEC 17025 to this document

	Reference in ISO/IEC 17025 document	Reference this document
4.	4. Management requirements	6.2
4.1	4.1 Organization	6.2
4.2	4.2 Management system	6.2
4.3	4.3 Document control	6.2
4.4	4.4 Review of requests, tenders and contracts	6.6, 6.7
4.5	4.5 Subcontracting	6.2
4.6	4.6 Purchasing	6.2
4.7	4.7 Service to clients	6.2
4.8	4.8 Complaints	6.5
4.9	4.9 Control of nonconforming work	6.2
4.10	4.10 Improvement	6.2
4.11	Corrective action	6.2
4.12	Preventive action	6.2
4.13	Control of records	6.2
4.14	Internal audit	6.2

	Reference in ISO/IEC 17025 document	Reference this document
4.15	Management review	6.2
5.	Technical	6.8
5.1	General	6.8
5.2	Personnel	6.3
5.3	Accommodation and environmental conditions	6.8
5.4	Test and calibration methods and method validation	6.8
5.5	Equipment	6.8
5.6	Measurement traceability	6.8
5.7	Sampling	6.8
5.8	Handling of test and calibration items	6.8
5.9	Assuring the quality of test and calibration results	6.8
5.10	Reporting the results	6.9

C.4 ASCI Chartered Testing Laboratory 2009 Approval Process coverage

As shown in Table 12, all sections of the ASCI Chartered Testing Laboratory 2009 Approval Process are called out as requirements in this document, with the exception of II.B Follow up and field inspections and I.D. Calibration Program, which do not apply to the ISASecure EDSA program.

Table 12 - Mapping from ASCI Chartered Testing Laboratory 2009 Approval Process to this document

	Reference in ASCI Chartered Testing Laboratory 2009 Approval Process document	Reference this document	Comments
I.A.	Capability - Testing Facilities	6.8	
I.B.	Capability - Test Equipment	6.8	
I.C.	Capability - Testing, Evaluation and Processing Procedures	6.8	
I.C 7-8	Capability - Testing, Evaluation and Processing Procedures C7-C8	6.6	
I.D.	Capability - Calibration Program		No application seen for ISASecure EDSA.
I.E.	Capability - Quality Assurance	6.2	
I.F.	Capability - Records (including Specifications Library)	6.2	
I.G.	Capability - Personnel	6.3	
II.A.	Control Programs - Listing and Labeling	6.12	
II.B.	Control Programs - Follow up and Field Inspections		Not applicable. The initial assessment of the manufacturer (device vendor) described in this section is superseded by the SDSA. Follow up inspections are not required by the ISASecure EDSA program. See rationale in Section 6.11.
III.	Independence	6.2	
IV.A.	Report and Complaint Procedures - Reports	6.9	
IV.B	Report and Complaint Procedures - Complaints	6.4	