Security Certification Scheme

QD-005
December 21, 2015
Version 2 Revision 1

Confidential Information
All rights reserved. No parts of this procedure may be re-used without the prior written permission of the authors.
1 Contents

2 Purpose of the Document:................................................................................................... 3

3 Scope: .................................................................................................................................. 3

4 Definitions (list abbreviations and definitions) ................................................................. 3

4.1 Definitions ..................................................................................................................... 3

4.2 Abbreviations .............................................................................................................. 4

5 Reference Material ........................................................................................................... 5

5.1 Normative references ................................................................................................. 5

6 Responsibility and Authority:.......................................................................................... 5

7 Certification Scheme ....................................................................................................... 5

7.1 Requirements .............................................................................................................. 5

7.2 Activities ..................................................................................................................... 5

7.3 Client Requirements ................................................................................................. 6

7.4 Certification Body Requirements .............................................................................. 6

7.5 Statement of Conformity ........................................................................................... 6

7.6 Surveillance Audits .................................................................................................... 6

7.7 Personnel ................................................................................................................... 6

7.8 Retention of Records ................................................................................................. 6

7.9 Integrity and Consistency ........................................................................................... 6

7.10 Certification Marks .................................................................................................... 7

7.11 Scheme Resources .................................................................................................... 7

7.12 Certification Results and Reporting ........................................................................ 7

7.13 Scheme Description ................................................................................................... 7

7.14 Complaints and Appeals .......................................................................................... 7

7.15 Fraudulent Claim of Certification ............................................................................. 7

7.16 Update and Maintenance of the Functional Safety Scheme ....................................... 7

8 Document Status: Draft ................................................................................................ 9

9 Revisions ......................................................................................................................... 9

10 Approvals ....................................................................................................................... 9
2 Purpose of the Document:

exida strives to operate the most useful and relevant functional safety and cybersecurity certification program in the world. These programs go beyond referenced international standards to add additional requirements defined in this Scheme. This document describes the Security Certification Scheme used by exida. It provides the needed details to understand the scope and normative documents that form the basis of the certification.

3 Scope:

The scope covers all the steps in the Security Certification Scheme. It will apply to any process, product or collection of products that use software to perform their required functionality. The presumption is that the software can be corrupted in some way so as to prevent or alter the designed functionality of the product.

4 Definitions (list abbreviations and definitions)

4.1 Definitions

4.1.1 accreditation
assessment and recognition process via which an organization is granted Certification Body status by a nationally recognized Accreditation Body which is a member of the International Accreditation Forum (IAF)

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

4.1.3 certifier
an organization that is qualified to perform cybersecurity assessment evaluation

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

4.1.5 certification
the process of an impartial third party evaluation, review, decision, attestation, and surveillance as specified by the certification scheme and it is requirements in order to provide assurance that the specified requirements have been demonstrated

4.1.6 certification scheme
certification system (4.1.7) related to specified products, services, or processes to which the same specified requirements, specific rules and procedures apply as specified by the certification scheme document and its referenced normative documents.
[Source: IEC 17067]

4.1.7 certification system
rules, procedures and management for carrying out certification
4.1.8 certified device
a well-defined version of a product or collection of products that have undergone an evaluation and have been granted certified status

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

4.1.10 device vendor
an organization that applies for certification and is responsible for compliance of a device per the defined scheme

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

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

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

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

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

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

4.2 Abbreviations
The following abbreviations are used in this document.

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>address resolution protocol</td>
</tr>
<tr>
<td>CRT</td>
<td>communication robustness testing</td>
</tr>
<tr>
<td>EN</td>
<td>European Norm</td>
</tr>
<tr>
<td>EUC</td>
<td>Equipment under Control</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet engineering task force</td>
</tr>
<tr>
<td>IAF</td>
<td>International Accreditation Forum</td>
</tr>
<tr>
<td>ICMPv4</td>
<td>internet control message protocol version 4</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronic Engineers</td>
</tr>
<tr>
<td>Ipv4</td>
<td>internet protocol version 4</td>
</tr>
<tr>
<td>ILAC</td>
<td>International Laboratory Accreditation Cooperation</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
</tbody>
</table>
5 Reference Material

5.1 Normative references

5.1.1 International standards for certification programs


5.1.2 International standards for accreditation programs

6 Responsibility and Authority:
The Managing Director of exida and his appointee are responsible for the content and maintenance of the scheme and this document. This is an informative document and is not meant to be an operating procedure.

7 Certification Scheme

7.1 Requirements

exida will obtain a list of required normative standards for each security certification job. The requirements against which a product or system is evaluated are then obtained from the Security Case for each referenced standard. The specific requirements and interpretations in each Security Case are formulated by those personnel deemed competent to perform as an Evaluating Assessor per OP 1020 (Competency, Training, and Awareness).

7.2 Activities

Certification assessment functions including Evaluation (Selection and Determination of characteristics), Review, Decision of certification, Attestation, and Surveillance are specified in OP1023 (Certification Procedure).
7.3 Client Requirements

Requirements that must be met by the client are specified in the Certification Agreement and in the applicable Security Case set for each project. This includes:

- All information required to perform the determination of characteristics (testing, test witnessing, analysis of design, inspection, design appraisal, assessment of services or processes, etc.,
- All requirements and restrictions on usage of the certification mark,
- All requirements for how non-conformities with certifications requirements are dealt with and resolved,
- All conditions for continuing surveillance, and
- Certificate withdrawal requirements including discontinuation of advertising and product marking.

7.4 Certification Body Requirements

exida and any other Certification Body shall be accredited per ISO/IEC 17065 by a national Accreditation Body who is a member of IAF which has a Multilateral Recognition Agreement. The Certification Body shall utilize competent personnel as specified OP 1020 (Competency, Training, and Awareness). All competency evaluations shall be done by the Scheme Owner, exida.

7.5 Statement of Conformity

The Statement of Conformity (e.g. the Certificate) shall contain the information described in the applicable exida Certificate Template. Reference templates are stored in the exida Quality US groove space.

7.6 Surveillance Audits

Surveillance audits are required as specified in OP 1030 (Surveillance Audits).

7.7 Personnel

All personnel assigned by exida.com LLC to perform certification tasks shall be employed by exida.com LLC or shall be under contract to exida.com LLC per OP1023.

7.8 Retention of Records

All data shall be retained per OP1027 (Control of Data).

7.9 Integrity and Consistency

Integrity shall be maintained by the use impartiality analysis. All certification projects shall utilize a hazard and risk analysis approach to evaluate impartiality per OP 1035 (Impartiality). Consistency shall be obtained by the use of the applicable Security Case on each project.
7.10 Certification Marks
All certification marks are shown in the Certification Agreement. These marks are the intellectual property of exida.

7.11 Scheme Resources
This Scheme is reviewed annually as part of exida's internal quality review process. Management and Quality personnel are required for this task. An Advisory Board must be established and must hold regular meetings (at least once per year) to review scheme issues.

7.12 Certification Results and Reporting
Certification results shall be expressed per OP 1032 (Report Procedure). Successful results (Certificate and assessment Report) will be posted on the exida website in order that the validity of a certificate may be verified by the public.

7.13 Scheme Description
A simple to understand description of the Security Scheme will be posted on the exida website. This should include a presentation and one or more web seminars.

7.14 Complaints and Appeals
Scheme complaints and appeals shall be processed following OP 1003 (Complaints, Appeals).

7.15 Fraudulent Claim of Certification
exidaWhen the Certification Body discovers fraudulent claims of certification, a message must be sent to the company perpetrating the fraud stating that the fraudulent certificates must be immediately stopped. An announcement on the certification list warning potential consumers of the fraudulent certificate shall be placed on the exida website.

7.16 Update and Maintenance of the Functional Safety Scheme
This document is reviewed annually as part of exida's internal quality review process. All suggestions for improvement will be reviewed with the Advisory Board. Client input is continuously sought and incorporated after review with the Advisory Board, allowing the scheme to rapidly adjust to the needs of the user community and enhance the overall robustness of the certification process.

7.17 Financial Support and Fees
exida does not receive any outside financial support. exida is wholly dependent on fees from services and products.

Fees for each work item are documented in the proposal. Customers are invoiced at the completion of each work item. If Travel is anticipated for the completion of this project, travel costs and out of pocket expenses will be invoiced at cost plus 10%.
All amounts payable to *exida* are payable in full without making any deduction or withholding. If Customer Company is prohibited by law from making payments free of deductions or withholdings, Customer Company will pay such amounts to *exida* as may be necessary to ensure that the actual amount received by *exida* after deduction or withholding and after any payment of any additional Taxes or other charges due as a consequence of the payment of such additional amounts will equal the amount that would have been received by *exida* if such deductions or withholdings were not required.
8 Document Status: Released

9 Revisions

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision</th>
<th>Author</th>
<th>Changes</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>V0</td>
<td>R5</td>
<td>David Johnson</td>
<td>review with WMG</td>
<td>29 Apr 2015</td>
</tr>
<tr>
<td>V1</td>
<td>R1</td>
<td>William Goble</td>
<td>Edits to clarify requirements</td>
<td>24 Jul 2015</td>
</tr>
<tr>
<td>V2</td>
<td>R1</td>
<td>Steven Close</td>
<td>Add Section 7.17</td>
<td>21 Dec 2015</td>
</tr>
</tbody>
</table>

10 Approvals

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision</th>
<th>Approved By</th>
<th>Approval email</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1</td>
<td>R1</td>
<td>William Goble</td>
<td></td>
<td>7/28/2015</td>
</tr>
<tr>
<td>V1</td>
<td>R1</td>
<td>Mike Medoff</td>
<td></td>
<td>7/28/2015</td>
</tr>
<tr>
<td>V2</td>
<td>R1</td>
<td>William Goble</td>
<td>Verbal</td>
<td>12/21/2015</td>
</tr>
</tbody>
</table>