# EDSA-102
# ISA Security Compliance Institute – Embedded Device Security Assurance –
**Errata for EDSA Specifications**

Version 1.2

April 2011

**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 | 2011.04.05 | initial version published to http://www.ISASecure.org |
| | | |
| | | |

# Contents

# Foreword

NOTE This document is one of a series of robustness test specifications for embedded devices. The full current list of documents related to embedded device security assurance can be found on the web site of the ISA Security Compliance Institute, http://www.ISASecure.org.

## 1 Scope

This errata document lists approved changes to all ISASecure EDSA specifications published at http://www.ISASecure.org. These changes are thus to be considered part of those specifications. This document is updated periodically as additional minor changes are identified. Major changes to any of the EDSA specifications will result in a new issue of the relevant specification. This document maintains a list of changes which of themselves do not merit a new version of the specification which is changed. These changes may be typographical errors, cut and paste errors, or technical inaccuracies which are clearly non- controversial in the context of the overall intent of the specification.

When any specification is reissued with a new version number, errata tracked in this document are incorporated, and this document is revised and reissued to remove those errata. Clause 4 specifies the version numbers of the documents to which the errata in this document apply.

## 2 Normative references

A bibliography of all published EDSA specifications is provided in the following highest level document.

[EDSA-100] *ISA Security Compliance Institute – Embedded device security assurance – ISASecure Certification Scheme,* as specified at http://www.ISASecure.org

Errata in the following EDSA specifications are listed in the subsequent sections of this document:

[EDSA-310] *ISA Security Compliance Institute – Embedded device security assurance – Common requirements for communication robustness testing of IP-based protocol implementations,* as specified at http://www.ISASecure.org

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

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

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

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

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

[EDSA-405] *ISA Security Compliance Institute 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] *ISA Security Compliance Institute 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

## 3 Definitions and abbreviations

Definitions and abbreviations for the terms used in this document are found in the documents for which errata are described, which are those document versions listed in Clause 4.

## 4 Index to Errata

This clause lists all ISASecure EDSA specifications that may be the subject of errata, and indicates for each specification whether errata apply to this specification. If so, the table below provides the section in this document that lists specific modifications for these errata.

**Table 1 - ISASecure EDSA Errata Index**

| Document ID | Document Title | Version | Errata | Reference in this document |
|---|---|---|---|---|
| EDSA-100 | *ISA Security Compliance Institute – Embedded device security assurance – ISASecure Certification Scheme* | 1.1 | None | |
| EDSA-200 | *ISCI Embedded Device Security Assurance – ISASecure EDSA chartered laboratory operations and accreditation* | 1.3 | None | |
| EDSA-201 | *ISCI Embedded Device Security Assurance – Recognition process for communication robustness testing tools* | 1.21 | None | |
| EDSA-202 | *ISCI Embedded Device Security Assurance – Application and Contract for Chartered Laboratories* | 1.0 | None | |
| EDSA-204 | *ISCI Embedded Device Security Assurance – Instructions and Policies for Use of the ISASecure Symbol and Certificates* | 1.3 | None | |
| EDSA-205 | *ISCI Embedded Device Security Assurance – Certificate Document Format* | 2.0 | None | |
| EDSA-300 | *ISCI Embedded Device Security Assurance – ISASecure Certification Requirements* | 1.0 | None | |
| EDSA-301 | *ISCI Embedded Device Security Assurance – Maintenance of ISASecure Certification* | 1.0 | None | |
| EDSA-310 | *ISCI Embedded Device Security Assurance – Common requirements for communication robustness testing of IP based protocol implementations* | 1.7 | Yes | 5.4 |
| EDSA-311 | *ISCI Embedded Device Security Assurance – Functional security assessment* | 1.4 | Yes | 5.2 |

| Document ID | Document Title | Version | Errata | Reference in this document |
|---|---|---|---|---|
| EDSA-312 | *ISCI Embedded Device Security Assurance – Software development security assessment* | 1.4 | Yes | 5.3 |
| EDSA-401 | *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of two common "Ethernet" protocols* | 2.01 | Yes | 5.5 |
| EDSA-402 | *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF ARP protocol over IPv4* | 2.31 | Yes | 5.6 |
| EDSA-403 | *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF IPv4 network protocol* | 1.31 | Yes | 5.7 |
| EDSA-404 | *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF ICMPv4 network protocol* | 1.3 | Yes | 5.8 |
| EDSA-405 | *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF UDP transport protocol over IPv4 or IPv6* | 2.6 | Yes | 5.9 |
| EDSA-406 | *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF TCP transport protocol over IPv4 or IPv6* | 1.41 | Yes | 5.10 |

# 5 Errata by document

## 5.1 General

This clause lists all errata that apply to the documents in Table 1.

## 5.2 EDSA-311 Functional Security Assessment

The following erratum applies to the specification EDSA-311.

- **Modify requirement for disabling non-access-controlled services:** In the Comments/Clarifications column of FSA-AC-2.1.11, add the words "able to be" so that the text now reads: "All services should either be secured by access control or *able to be* disabled for normal operation (services that must be disabled also need to be documented for the user)." This corrects an editorial error that occurred when moving this text from the ballot comment form to this document.

## 5.3 EDSA-312 Software Development Security Assessment

The following errata apply to the specification EDSA-312.

- **Modify requirement for SRS assignment of a Security Assurance Level:** In the Comments/Clarifications column of SDSA-SRS-5, change the text to read: "The scheme used to define security assurance level is not designated by this specification. Possible examples are an ISASecure EDSA certification level, an ISA 99.01.01 Security Assurance Level or a vendor-defined

scheme." In the existing document this requirement refers to ISA 99.01.01 only. This restriction was not intended.

- **Fill in missing ISASecure level:** Set the ISASecure level column for SDSA-SPV-1.8: Security Bug Severity, to "All." The level designation was missing.

### 5.4 EDSA-310 Common CRT

The following errata apply to the specification EDSA-310 version 1.7.

- **Clarify location of list of CRT protocols:** Modify CRT.R1b) to read: "protocol specific robustness testing per the requirements of Clause 9 for all protocols *for which specifications are* listed in [EDSA-300] *Clause 2*, that are applicable to the device, where applicability is defined in Requirement CRT.R2." The text in italics has been added since the location of the protocol list in EDSA-300 was unclear.

- **Remove restriction to digital outputs:** Item c) under Requirement CRT.30 states that the following is included in the CRT test setup:

  "a testing device which is a monitoring component that is capable of receiving the digital control output of the DUT and collecting data to support the calculation of jitter on the signal received in ms, to the accuracy stated in CRT.R39."

  The word "digital" is deleted from this sentence, to be consistent with CRT.R39, since digital, analog and discrete outputs are all monitored by CRT testing.

### 5.5 EDSA-401 "Ethernet"

The following errata apply to the specification EDSA-401 version 2.01.

- **Clarify requirement sources and precedence:** The following statement is inserted before the notes in Clause 1, Scope: "Requirements are comprised of all the numbered Requirements in this document and any immediately following clarifying information, together with the tables in Clause 7 that describe individual tests. In the event of a conflict between these, the tables in Clause 7 take precedence."

- **Correct protocol description:** Figure 1 – IEEE 802.3 frame structure with IEEE 802.2 Type 1 and IEEE 802 SNAP states that the SNAP header should start with 0xAA0003. This is not correct. It should start with 0xXX 0xYY 0x03, where 0xXX and 0xYY are in {0xAA, 0xAB}.

- **Remove ramp down requirement on high load test procedure:** Table 2 – "Ethernet".T08: Maintenance of service under high load, including network saturation: Raw DPDU flood, in the Test procedure row, states that the TD "then gradually reduces its sending rate to zero." This ramp-down portion of the test procedure in quotes is not required and is deleted from the specification.

### 5.6 EDSA-402 ARP

The following errata apply to the specification EDSA-402 version 2.31.

- **Clarify requirement sources and precedence:** The following statement is inserted before the notes in Clause 1, Scope: "Requirements are comprised of all the numbered Requirements in this document and any immediately following clarifying information, together with the tables in Clause 7 that describe individual tests. In the event of a conflict between these, the tables in Clause 7 take precedence."

- **Clarify meaning of Results row:** Insert this sentence before Table 2: "If the Results row in a table does not indicate "Pass/Fail," this means that the test provides security-relevant information about the DUT to be included in the test report, but cannot cause a device to fail certification as long as related documentation of compensating controls is provided by the vendor as indicated."

- **Typographical error:** Table 3 – ARP.T01: DUT cache poisoning, in the Test description and the Test procedure rows, the first instance of "ARP request DPDUs" is changed to correctly read "ARP reply DPDUs."

- **Remove ramp down requirement on high load test procedure:** Table 4 – ARP.T10: Maintenance of service under high load, including network saturation, in the Test procedure row, states that the TD "then gradually reduces its sending rate to zero." This ramp-down portion of the test procedure in quotes is not required and is deleted from the specification.

### 5.7 EDSA-403 IPv4

The following errata apply to the specification EDSA-403 version 1.31.

- **Clarify requirement sources and precedence:** The following statement is inserted before the notes in Clause 1, Scope: "Requirements are comprised of all the numbered Requirements in this document and any immediately following clarifying information, together with the tables in Clause 7 that describe individual tests. In the event of a conflict between these, the tables in Clause 7 take precedence."

- **Remove conformance requirement:** In requirement IPv4.R10, item b) is removed. This is a conformance requirement and thus not appropriate in the specification.

- **Clarify test scenario intent:** In 6.7.3, the fourth bullet states: "NPDU sequences where an unfragmented NPDU is sent after sending a fragmented NPDU with the same source and destination IPv4 addresses, same protocol type and same value of the NPDU's identification field."

  This is clarified by adding the phrase "most but not all of," so that it reads as follows:

  "NPDU sequences where an unfragmented NPDU is sent after sending most but not all of a fragmented NPDU with the same source and destination IPv4 addresses, same protocol type and same value of the NPDU's identification field."

- **Clarify meaning of Results row:** Insert this sentence before Table 8: "If the Results row in a table does not indicate "Pass/Fail," this means that the test provides security-relevant information about the DUT to be included in the test report, but cannot cause a device to fail certification as long as related documentation of compensating controls is provided by the vendor as indicated."

- **Remove ramp down requirement on high load test procedure**: Table 5 – IPv4.T14: Maintenance of service under high load, including network saturation: Raw NPDU flood, in the Test procedure row, states that the TD "then gradually reduces its sending rate to zero." This ramp-down portion of the test procedure in quotes is not required and is deleted from the specification.

### 5.8 EDSA-404 ICMPv4

- **Clarify requirement sources and precedence:** The following statement is inserted before the notes in Clause 1, Scope: "Requirements are comprised of all the numbered Requirements in this document and any immediately following clarifying information, together with the tables in Clause 7 that describe individual tests. In the event of a conflict between these, the tables in Clause 7 take precedence."

- **Remove ramp down requirement on high load test procedure:** Table 6 – ICMPv4.T08: Maintenance of service under high load, including network saturation: Raw ICMPv4 NPDU flood**,** in the Test procedure row, states that the TD "then gradually reduces its sending rate to zero." This ramp-down portion of the test procedure in quotes is not required and is deleted from the specification.

### 5.9 EDSA-405 UDP

The following errata apply to the specification EDSA-405 version 2.6.

- **Clarify requirement sources and precedence:** The following statement is inserted before the notes in Clause 1, Scope: "Requirements are comprised of all the numbered Requirements in this document and any immediately following clarifying information, together with the tables in Clause 7 that describe individual tests. In the event of a conflict between these, the tables in Clause 7 take precedence."

- **Correct acronym expansion:** Section 3.2, Abbreviations, states that the acronym TPDU is short for "transmission-layer PDU." This is not correct. The correct expanded form is "transport-layer PDU," as in ISO/IEC 7498-1, *OSI Basic Reference Model*.

- **Remove ramp down requirement on high load test procedure:** Table 7 – UDP.T09: Maintenance of service under high load, including network saturation: Raw TPDU flood, in the Test procedure row, states that the TD "then gradually reduces its sending rate to zero." This ramp-down portion of the test procedure in quotes is not required and is deleted from the specification.

### 5.10 EDSA-406 TCP

The following errata apply to the specification EDSA-406 version 1.41.

- **Clarify requirement sources and precedence:** The following statement is inserted before the notes in Clause 1, Scope: "Requirements are comprised of all the numbered Requirements in this document and any immediately following clarifying information, together with the tables in Clause 7 that describe individual tests. In the event of a conflict between these, the tables in Clause 7 take precedence.

- **Remove extra word:** TCP.R12 states the following, which has the extraneous word "either" not found in parallel requirements in the other CRT protocol specifications:

  **"**Load stress testing SHALL use either a deterministic selection process (e.g., an offline test case generator or a seeded pseudo-random selection process), that tests series of valid messages, with the latter including malformed messages."

  The corrected text has the term "either" removed from this statement.

- **Correct terminology usage:** The term "denigrate" was used incorrectly to refer to aspects of the protocol that have been superseded. This occurs in Figure 3 and in 4.2.6.3 (two instances). Denigrate is replaced by the originally intended term "deprecate" in these locations.

- **Clarify meaning of Results row:** Insert this sentence before Table 6: "If the Results row in a table does not indicate "Pass/Fail," this means that the test results provide security-relevant information about the DUT to be included in the test report, but cannot cause a device to fail certification."

- **Correct reference to industry tests:** Requirement TCP.R5 – Unpredictability of DUT's initial sequence numbers, and Table 8 – TCP.T01: Statistical analysis of initial sequence number values, in the Test procedure row, refer to *dieharder* tests 100, 101, 102. These test numbers are incorrect. The correct test numbers are 1, 2, and 3.

- **Correction to test description and procedure:** In Table 17 – TCP.T11: Defense against peer dishonoring of the DUT's TCP received window edges, replace the existing Test Description by: "The TD establishes a TCP connection with the DUT, then sends TCP TPDUs for the connection that do not honor the DUT's receive window edges by responding with TCP TPDUs containing payload octets with impermissible sequence numbers, combining this with occasional reset of the connection." Also replace the Test Procedure by: "The TD sends otherwise valid TCP TPDUs whose payloads contain invalid sequence numbers that do not honor the DUT's receive window edges with respect to prior TPDUs of the same TCP connection. The TD MAY monitor for any response from the DUT." This table mistakenly had repeated information from TCP.T10.

- **Removal of rate-based "flood" references from text of Table 25:** In Table 25 – TCP.T19: Maintenance of service under high load: Unused open connection flood, delete the last two sentences of the "Test description" row that read: "The TPDU flood rate is selected to be a high load test, not a saturation test. See [CRT.Rate_limiting] for additional requirements." These statements are incorrect since this test is based on the number of concurrent connections rather than a traffic rate.

- **Remove protocol compliance aspect of high load test**: Table 29 – TCP.T23: Maintenance of service under high load: FIN flood, in the Remarks row, states:

"During this flood the TD attempts to use those TCP connections whose FIN TPDUs are spoofed as part of the attack, as well as to establish and use other TCP connections, to survey the DUT's behavior with non-null traffic on those TCP connections"

In the above, "attempts to use" should be replaced by "MAY attempt to use," yielding the corrected text:

"During this flood the TD MAY attempt to use those TCP connections whose FIN TPDUs are spoofed as part of the attack, as well as to establish and use other TCP connections, to survey the DUT's behavior with non-null traffic on those TCP connections"

- **Remove ramp down requirement on high load test procedure:** Table 10 – TCP.T24: Maintenance of service under high load, including network saturation: Raw TPDU flood, in the Test procedure row, states that the TD "then gradually reduces it sending rate to zero." This ramp-down portion of the test procedure in quotes is not required and is deleted from the specification.

— — — — — —