DNV·GL

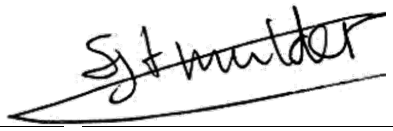
IEC 62351-3 SECURITY EXTENTION AILUX S.R.L.

# Pre-test outcome overview of IEC 62351-3 implementation in Ailux RTU62351 ver 5.3.02.05 tested as controlled station

Ailux S.R.L

**Report no.:** 18-2556
**Date:** 2018-05-29

| | | |
|---|---|---|
| Project name: | IEC 62351-3 security extention Ailux S.R.L. | DNV GL - Energy |
| Report title: | Pre-test outcome overview of IEC 62351-3 implementation in Ailux RTU62351 ver 5.3.02.05 tested as controlled station | Energy Advisory<br>P.O. Box 9035<br>6800 ET ARNHEM |
| Customer: | Ailux S.R.L | The Netherlands |
| Contact person: | Stefano Pini | |
| Date of issue: | 2018-05-29 | Tel: +31 26 356 9111 |
| Project No.: | 10097680 | Registered Arnhem 09006404 |
| Organisation unit: | INC | |
| Report No.: | 18-2556 | |

| Prepared by: | Verified by: | Approved by: |
|---|---|---|
|  |  |  |
| D. Colangelo | T. Levels | S.J.T. Mulder |



DNV GL Distribution:

☐ Unrestricted distribution (internal and external)

☐ Unrestricted distribution within DNV GL Group

☒ Unrestricted distribution within DNV GL contracting party

☐ No distribution (confidential)

Keywords:

IEC62351-3 server side

| Rev. No. | Date | Reason for Issue | Prepared by | Verified by | Approved by |
|---|---|---|---|---|---|
| 0 | 2018-05-29 | First issue | D. Colangelo | T. Levels | S.J.T. Mulder |

# Table of contents


1 PURPOSE OF THIS DOCUMENT ..... 2
1.1 Remarks & Recommendations following from the test 2

2 PRE-TEST OUTCOME OVERVIEW IEC CD 62351-100-3 ..... 3
2.1 Configuration Parameters 3
2.2 Normal Procedure 4
2.3 Resiliency test 7

# 1 PURPOSE OF THIS DOCUMENT

On behalf of Ailux S.R.L. DNV GL performed a compliance pre-test on device RTU62351 (further referred as Device Under Test, DUT), with software version 5.3.02.05. The purpose of this document is to describe the pre-test outcome of the type test according to IEC 62351-3 implementation in the DUT.

The type test was executed following IEC FDIS AMD 62351-3:2018 applied to IEC 60870-5-104 at DNV GL, Arnhem from 14th March to 16th March 2018.

The pre-test outcome overview does not form any basis for an Attestation of Conformance and does not constitute part of a Conformance Test report. The purpose of the pre-test is to support a manufacture to better prepare their devices in view of a Conformance Test trial.

The Attestation of Conformance is primarily of interest to product marketers and customers, as a proof of independent verification of minimized interoperability risks.

## 1.1 Remarks & Recommendations following from the test

The following remarks apply:

# 2 PRE-TEST OUTCOME OVERVIEW IEC CD 62351-100-3

The test result charts described in this chapter are based on test procedures as described in IEC CD 62351-100-3 document. A full description of the test cases is presented in that document.

## 2.1 Configuration Parameters

| **Configuration Parameters** | | √……. indicates the Test Case has PASSED<br>FAIL…… indicates the Test Case has FAILED<br>N.A……. indicates that Configuration Value is NOT SUPPORTED by the device<br>Empty……. indicates the Test Case was NOT PERFORMED<br>Black Box… indicates the Test Case is NOT APPLICABLE in the normative | |
|---|---|---|---|
| **Test** | **No.** | **Description** | **Result** |
| Configuration Parameters | 6.1.1 | Station Type (Client, Server) | ✓ |
| | 6.1.2 | TCP IP Port to be used for secure communication | ✓[1] |
| | 6.1.3 | TLS Versions | ✓[2] |
| | 6.1.4 | TLS Cipher Suites | ✓ |
| | 6.1.5 | Public Key Lengths | ✓[3] |
| | 6.1.6 | Certificates Revocation Check methods | ✓[4] |
| | 6.1.7 | Certificate Revocation Check Interval | |
| | 6.1.8 | TLS Session Renegotiation Interval | ✓[5] |
| | 6.1.9 | TLS Session Resumption Interval | ✓[6] |
| | 6.1.10 | Number of CA supported | ✓[7] |
| | 6.1.11 | Maximum certificate size | ✓[8] |

[1] The secure TCP is a fixed value.
[2] Pre-test has been performed for TLSv 1.2
[3] The value is indicated in PICS
[4] The value is indicated in PICS
[5] The value is indicated in PICS
[6] The value is indicated in PICS
[7] The value is indicated in PICS
[8] The value is indicated in PICS

## 2.2 Normal Procedure

| Verification of Procedures<br>IEC 62351-3 requirements | | Record the test cases result on the right for each configuration value supported (see clause 6):<br>√……. indicates the Test Case has PASSED<br>FAIL…… indicates the Test Case has FAILED<br>N.A……. indicates that Configuration Value is NOT SUPPORTED by the device<br>Empty……. indicates the Test Case was NOT PERFORMED<br>Black Box… indicates the Test Case is NOT APPLICABLE in the normative | Station Type | |
|---|---|---|---|---|
| | | | Client Station | Server Station |
| **Test** | **No.** | **Description** | **Result** | |
| Normal Procedure | 7.1.1 | The DUT (Client only) initiates the TCP/IP connection to the Server using remote station TCP/IP port specified for secure communication. | N.A | |
| | 7.1.2 | The DUT (Server only) accepts the TCP/IP connection on TCP/IP port specified for secure communication. | | ✓ |
| | 7.1.3 | The DUT (Client only) performs the Initial TLS Handshake upon the connection is established and no previous TLS Session was established. | N.A | |
| | 7.1.4 | The DUT performs Session Renegotiation at the Configured interval for Session Renegotiation, in an ongoing TLS Session. | N.A | ✓ |
| | 7.1.5 | If CRL certificate check method is supported, at least one TLS renegotiation is synchronized (performed immediately after) the CRL update. | | |
| | 7.1.6 | If OCSP certificate check method is supported, the TLS Session Renegotiation is performed at the Configured interval for Certificate Revocation check. | | |
| | 7.1.7 | The DUT supports at least minumum number fo root CAs (has the corresponding number of root CA certificates installed locally). | N.A | ✓ |
| | 7.1.8 | The DUT accepts any Remote Station certificate from one or more authorized CA locally configured, after successful validation. | N.A | ✓ |
| | 7.1.9 | The DUT accepts one or more specific Remote Station certificate (locally configured) from one or more authorized CA (locally configured). | N.A | ✓ |
| | 7.1.10 | During the initial handshake<br>the DUT (Client only) correctly provides the Trusted CA Indication in the ClientHello message. | N.A | |
| | 7.1.11 | During the initial handshake,<br>the DUT (Server only), in the ServerHello message, correctly provides a certificate selected from the Certificate Chain specified in the Trusted CA Indication of the last ClientHello message received. | | |
| | 7.1.12 | During the initial handshake,<br>the DUT performs Mutual Authentication with the Remote Station. | N.A | ✓ |
| | | Record the test cases result on the right for each configuration value supported (see clause 6): | Station Type | |

| Verification of Procedures<br>IEC 62351-3 requirements | | √……. indicates the Test Case has PASSED<br>FAIL…… indicates the Test Case has FAILED<br>N.A…… indicates that Configuration Value is NOT SUPPORTED by the device<br>Empty……. indicates the Test Case was NOT PERFORMED<br>Black Box… indicates the Test Case is NOT APPLICABLE in the normative | Client Station | Server Station |
|---|---|---|---|---|
| **Test** | **No.** | **Description** | **Result** | |
| Normal Procedure<br>*(continued)* | 7.1.13 | During the initial handshake,<br>the Message Authentication Code (MAC) option, with the specific algorithm indicated in the cipher suites selected, is correctly supported. | N.A | ✓ |
| | 7.1.14 | During the initial handshake,<br>the TLS Session Extension defined in RFC5746 is correctly supported. | N.A | ✓ |
| | 7.1.15 | During the initial handshake,<br>the DUT accepts certificates size less than or equal to the maximum certificate size supported. | N.A | ✓ |
| | 7.2.16 | During the initial handshake,<br>the process of accessing the CRL does not cause an established TCP/IP connection or a TLS session to be terminated if the received certificate is valid. | | |
| | 7.2.17 | During the initial handshake,<br>the process of accessing the OCSP responder does not cause an established TCP/IP connection or a TLS session to be terminated if the received certificate is valid. | | |
| | 7.1.18 | During the session renegotiation,<br>the DUT (Client only) correctly provides the Trusted CA Indication in the ClientHello message. | | |
| | 7.1.19 | During the session renegotiation,<br>the DUT (Server only), in the ServerHello message, correctly provides a certificate selected from the Certificate Chain specified in the Trusted CA Indication of the last ClientHello message received. | | |
| | 7.1.20 | During the session renegotiation,<br>the DUT performs Mutual Authentication with the Remote Station. | N.A | ✓ |
| | 7.1.21 | During the session renegotiation,<br>the Message Authentication Code (MAC) option, with the specific algorithm indicated in the cipher suites selected, is correctly supported. | N.A | ✓ |
| | 7.1.22 | During the session renegotiation,<br>the TLS Session Extension defined in RFC5746 is correctly supported. | N.A | ✓ |

| Verification of Procedures<br>IEC 62351-3 requirements | | Record the test cases result on the right for each configuration value supported (see clause 6):<br>√……. indicates the Test Case has PASSED<br>FAIL…… indicates the Test Case has FAILED<br>N.A……. indicates that Configuration Value is NOT SUPPORTED by the device<br>Empty……. indicates the Test Case was NOT PERFORMED<br>Black Box… indicates the Test Case is NOT APPLICABLE in the normative | Station Type | |
|---|---|---|---|---|
| | | | Client Station | Server Station |
| **Test** | **No.** | **Description** | **Result** | |
| Normal Procedure<br>*(continued)* | 7.1.23 | During the session renegotiation,<br>the DUT accepts certificates size less than or equal to the maximum certificate size supported. | **N.A** | ✓ |
| | 7.1.24 | During the session renegotiation,<br>the process of accessing the CRL does not cause an established TCP/IP connection or a TLS session to be terminated if the received certificate is valid. | | |
| | 7.1.25 | During the session renegotiation,<br>the process of accessing the OCSP responder does not cause an established TCP/IP connection or a TLS session to be terminated if the received certificate is valid. | | |
| | 7.1.26 | The DUT is able to perform the TLS Session Resumption (initiated by the Hello Request message from the server or the Client Hello message from the client) upon the TCP/IP connection is re-established if a previous TLS Session was dropped within the Configured interval for Session Renegotiation | **N.A** | ✓ [9] |
| | 7.1.27 | The DUT is able to perform the TLS Session Resumption (initiated by the Hello Request message from the server or the Client Hello message from the client) at the Configured interval for Session Resumption, in an ongoing TLS Session. | **N.A** | ✓ |

[9] The resumption was tested only when initiate by the client because after the re-establish of TCP connection the client always sends a clientHello

## 2.3 Resiliency test

| Verification of Procedures<br>IEC 62351-3 requirements | | Record the test cases result on the right for each configuration value supported (see clause 6):<br>√……. indicates the Test Case has PASSED<br>FAIL…… indicates the Test Case has FAILED<br>N.A…… indicates that Configuration Value is NOT SUPPORTED by the device<br>Empty……. indicates the Test Case was NOT PERFORMED<br>Black Box… indicates the Test Case is NOT APPLICABLE in the normative | Station Type | |
|---|---|---|---|---|
| | | | Client Station | Server Station |
| **Test** | **No.** | **Description** | **Result** | |
| Resiliency Test | 7.2.1 | During the initial handshake,<br>the DUT is not able to access to the CRL to verify the revocation of the certificate received and the certificate received is valid. | | |
| | 7.2.2 | During the initial handshake,<br>The DUT is not able to access to the OCSP responder to verify the revocation of the certificate received and the certificate received is valid. | | |
| | 7.2.3 | During the initial handshake,<br>the CRL is not updated (validity time expired). | | |
| | 7.2.4 | During the initial handshake,<br>the Remote Station proposes TLS version 1.1. | N.A | ✓ |
| | 7.2.5 | During the initial handshake,<br>the Remote Station proposes TLS version 1.0. | N.A | ✓ |
| | 7.2.6 | During the initial handshake,<br>the Remote Station proposes TLS version prior to 1.0. | N.A | ✓ |
| | 7.2.7 | During the initial handshake,<br>the Remote Station proposes none of the mandatory TLS cipher suites and none implemented in the DUT. | N.A | ✓ |
| | 7.2.8 | During the initial handshake,<br>the Remote Station does not provide the certificate | N.A | ✓ |
| | 7.2.9 | During the initial handshake,<br>the DUT receives a Remote Station's certificate having size longer than the maximum certificate size supported | N.A | ✓ |

| Verification of Procedures<br>IEC 62351-3 requirements | | Record the test cases result on the right for each configuration value supported (see clause 6):<br>√……. indicates the Test Case has PASSED<br>FAIL…… indicates the Test Case has FAILED<br>N.A……. indicates that Configuration Value is NOT SUPPORTED by the device<br>Empty……. indicates the Test Case was NOT PERFORMED<br>Black Box… indicates the Test Case is NOT APPLICABLE in the normative | Station Type | |
|---|---|---|---|---|
| | | | Client Station | Server Station |
| **Test** | **No.** | **Description** | **Result** | |
| | 7.2.20 | During the initial handshake,<br>the DUT receives a Remote Station's certificate with a not valid signature. | N.A | ✓ |
| | 7.2.21 | After sending a HelloRequest message to the Client, the DUT (Server only) does not receive the TLS Session Renegotiation request from the Client. | | ✓ [10] |
| | 7.2.22 | During the session renegotiation,<br>The DUT is not able to access the CRL to verify the revocation of the certificate received and the certificate received is valid. | | |
| | 7.2.23 | During the session renegotiation,<br>The DUT is not able to access to the OCSP responder to verify the revocation of the certificate received and the certificate received is valid. | | |
| | 7.2.24 | During the session renegotiation,<br>the CRL is not updated (validity time expired). | | |
| | 7.2.25 | During the session renegotiation,<br>the Remote Station proposes TLS version 1.1. | N.A | ✓ |
| | 7.2.26 | During the session renegotiation,<br>the Remote Station proposes TLS version 1.0. | N.A | FAIL [11] |
| | 7.2.27 | During the session renegotiation,<br>the Remote Station proposes TLS version prior to 1.0. | N.A | ✓ |

[10] The DUT waits a time equal to the renegotiation interval before showing the security alert.

[11] After raising the security alert, the DUT closes the connection which is against the current test procedures.

| Verification of Procedures<br>IEC 62351-3 requirements | | Record the test cases result on the right for each configuration value supported (see clause 6):<br>√……. indicates the Test Case has PASSED<br>FAIL…… indicates the Test Case has FAILED<br>N.A……. indicates that Configuration Value is NOT SUPPORTED by the device<br>Empty……. indicates the Test Case was NOT PERFORMED<br>Black Box… indicates the Test Case is NOT APPLICABLE in the normative | Station Type | |
|---|---|---|---|---|
| | | | Client Station | Server Station |
| **Test** | **No.** | **Description** | **Result** | |
| Resiliency Test | 7.2.10 | During the initial handshake,<br>the DUT receives a Remote Station's certificate referring to a CA for which the certificate is not installed in the DUT. | N.A | ✓ |
| | 7.2.11 | During the initial handshake,<br>the DUT receives a Remote Station's certificate referring to a CA for which the certificate is installed in the DUT but the Remote Station's individual certificate is not specifically configured in the DUT. | | |
| | 7.2.12 | During the initial handshake,<br>the DUT is not able to provide a certificate selected from the Certificate Chain specified in the Trusted CA Indication of the last ClientHello message received. | | |
| | 7.2.13 | During the initial handshake,<br>the DUT receives a Remote Station's certificate NOT belonging to any of the Certificate Chains selected in the Trusted CA Indication of the last ClientHello message transmitted. | | |
| | 7.2.14 | During the initial handshake,<br>the DUT receives an expired Remote Station's certificate. | N.A | ✓ |
| | 7.2.15 | During the initial handshake,<br>the DUT receives a revoked Remote Station's certificate. | N.A | ✓ |
| | 7.2.16 | During the initial handshake,<br>the DUT receives a Remote Station's certificate with a public key length equal to the minimum required. | N.A | ✓ |
| | 7.2.17 | During the initial handshake,<br>the DUT receives a Remote Station's certificate with a public key length shorter than the minimum required. | N.A | ✓ |
| | 7.2.18 | During the initial handshake,<br>the DUT receives a Remote Station's certificate specifying an unsupported signature algorithm. | N.A | ✓ |
| | 7.2.19 | During the initial handshake,<br>the DUT receives a Remote Station's certificate specifying a signature algorithm with unsupported signature parameters (e.g curve) | | |

| Verification of Procedures<br>IEC 62351-3 requirements | | Record the test cases result on the right for each configuration value supported (see clause 6):<br>√……. indicates the Test Case has PASSED<br>FAIL…… indicates the Test Case has FAILED<br>N.A……. indicates that Configuration Value is NOT SUPPORTED by the device<br>Empty……. indicates the Test Case was NOT PERFORMED<br>Black Box… indicates the Test Case is NOT APPLICABLE in the normative | Station Type | |
|---|---|---|---|---|
| | | | Client Station | Server Station |
| **Test** | **No.** | **Description** | **Result** | |
| Resiliency Test | 7.2.28 | During session renegotiation,<br>the Remote Station proposes none of the mandatory TLS cipher suites and none implemented in the DUT. | N.A | ✓ |
| | 7.2.29 | During session renegotiation,<br>the Remote Station does not provide the certificate | N.A | ✓ |
| | 7.2.30 | During session renegotiation,<br>the DUT receives a Remote Station's certificate having size longer than the maximum certificate size supported. | N.A | ✓ |
| | 7.2.31 | During session renegotiation,<br>the DUT receives a Remote Station's certificate referring to a CA for which the certificate is not installed in the DUT. | N.A | ✓ |
| | 7.2.32 | During session renegotiation,<br>the DUT receives a Remote Station's certificate referring to a CA for which the certificate is installed in the DUT but the individual Remote Station certificate's is not specifically configured in the DUT. | | |
| | 7.2.33 | During session renegotiation,<br>the DUT (Server only) is NOT able to provide a certificate selected from the Certificate Chain specified in the Trusted CA Indication of the last ClientHello message received. | | |
| | 7.2.34 | During session renegotiation,<br>the DUT (Client only) receives a Remote Station's certificate NOT belonging to any of the Certificate Chains selected in the Trusted CA Indication of the last ClientHello message transmitted. | | |
| | 7.2.35 | During session renegotiation,<br>the DUT receives an expired Remote Station's certificate. | N.A | ✓ |
| | 7.2.36 | During session renegotiation,<br>the DUT receives a revoked Remote Station's certificate. | N.A | ✓ |
| | 7.2.37 | During session renegotiation,<br>the DUT receives a Remote Station's certificate with a public key length equal to the minimum required. | N.A | ✓ |

| Verification of Procedures<br>IEC 62351-3 requirements | | Record the test cases result on the right for each configuration value supported (see clause 6):<br>√……. indicates the Test Case has PASSED<br>FAIL…… indicates the Test Case has FAILED<br>N.A……. indicates that Configuration Value is NOT SUPPORTED by the device<br>Empty……. indicates the Test Case was NOT PERFORMED<br>Black Box… indicates the Test Case is NOT APPLICABLE in the normative | Station Type | |
|---|---|---|---|---|
| | | | Client Station | Server Station |
| **Test** | **No.** | **Description** | **Result** | |
| Resiliency Test | 7.2.38 | During session renegotiation,<br>the DUT receives a Remote Station's certificate with a public key length shorter than the minimum required. | N.A | ✓ |
| | 7.2.39 | During session renegotiation,<br>the DUT receives a Remote Station's certificate specifying an unsupported signature algorithm. | N.A | ✓ |
| | 7.2.40 | During session renegotiation,<br>the DUT receives a Remote Station's certificate specifying a signature algorithm with unsupported signature parameters (e.g. curve) | | |
| | 7.2.41 | During session renegotiation,<br>the DUT receives a Remote Station's certificate with a NOT valid signature. | N.A | ✓ |

## About DNV GL

Driven by our purpose of safeguarding life, property and the environment, DNV GL enables organizations to advance the safety and sustainability of their business. We provide classification and technical assurance along with software and independent expert advisory services to the maritime, oil and gas, and energy industries. We also provide certification services to customers across a wide range of industries. Operating in more than 100 countries, our 16,000 professionals are dedicated to helping our customers make the world safer, smarter and greener.