INTERNATIONAL HYDROGRAPHIC ORGANIZATION

TEST DATA IMPLEMENTATION GUIDE

(Part of Appendix 1 of S-63 Edition 1.0)

Edition 1.1 - July 2004

Published by the
International Hydrographic Bureau
4, Quai Antoine 1er
B.P 445 - MC 98011 MONACO Cedex
Principality of Monaco
Tel: +(377) 93 10 81 00
Telefax: +(377) 93 10 81 40
E-mail: info@ihb.mc
Web: www.iho.shom.fr

Page intentionally left blank

CONTENTS

Page intentionally left blank

1 Introduction

The publication "S-63—IHO Data Protection Scheme" describes the IHO recommended standard for the protection of ENC information. It defines security constructs and operating procedures that must be followed to ensure that the data protection scheme is operated correctly and to provide specifications that allow participants to build compliant systems.

This document is S-63 Appendix 1. It defines a recommended set of test definitions and test data which can be used by developers of Data Server and Data Client applications to understand the security constructs defined in S-63 and test if their application is compliant with the standard.

1.1 Intended Audience

This document is aimed at two main audiences: data servers (VARs, RENCs etc.) and ECDIS manufacturers. These organisations should use the tests described in this document to verify that their software is S63 compliant.

1.2 References

[1] S63 Edition 1.0: IHO Data Protection Scheme, International Hydrographic Bureau

[2] S57 edition 3.1: IHO Transfer Standard for Digital Hydrographic Data, International Hydrographic Bureau

1.3 Maintenance of the S-63 Test Data

The S-63 Appendix 1 will be maintained by the IHO DPSWG. More test data can be included in the future based on user feedback to provide a complete test platform to verify correctness and compliance with the standard, or for end-user applications to identify erroneous situations. The current version of the document is expected to provide a complete test sample for compliance testing.

The S-63 Appendix 1 will be maintained independent of the IHO S-63 main document and new versions will be published on the IHO website.

Questions related to the use of the test data can be posted at the *Open Ecdis Forum* (www.openecdis.org).

1.4 Change History

Version	Date	Change
1.0	Oct-2003	First version of document
1.1	Jul-2004	Added chapter 4.4 and test 7.2, and corrected some test descriptions and testdata.

2 Index of Tests

This section contains an index of all the tests contained within this document. The index provides an indication of the type and purpose of each test. All tests are mandatory, and all tests must be passed in order to gain accreditation for the software in question. If the software fails any of the tests described in this document then it will not be accredited.

Test ID	Test Type	Test Description
1.1	User Permit	User Permit Generation
1.2	User Permit	User Permit Verification & Decryption
1.3	User Permit	Identify Unregistered HW_ID in User Permit
1.4	User Permit	Identify Incorrect M_KEY used in User Permit generation
1.5	User Permit	Identify Incorrect Checksum in User Permit
2.1	Cell Permit	Generate Cell Permit
2.2	Cell Permit	Decrypt Cell Permit
2.3	Cell Permit	Decrypt Erroneous Cell Permit
2.4	Cell Permit	Check Expiry Date in Cell Permit
3.1	Certificate	Data Server Authenticate SA Public Key
3.2	Certificate	Data Client Uses Correct SA Public Key File
3.3	Certificate	Data Client Authenticate SA Public Key
3.4	Certificate	Data Client Identifies Erroneous SA Public Key
3.5	Certificate	Make Data Server Self-Signed Key (SSK)
3.6	Certificate	Authenticate Data Server Certificate in ENC Signature File
3.7	Certificate	Identify Erroneous Data Server Certificate in ENC Signature File
4.1	Digital Signature	Sign ENC File
4.2	Digital Signature	Authenticate ENC signature
4.3	Digital Signature	Identify Erroneous ENC signature
5.1	Encryption/Decryption	Encrypt ENC Base Cells and Update Files
5.2	Encryption/Decryption	Decrypt ENC Base Cells and Update Files
5.3	Encryption/Decryption	Encrypt Next Edition of ENC with Next Cell Key
5.4	Encryption/Decryption	Decrypt Next Edition of ENC with Next Cell Key
5.5	Encryption/Decryption	Decrypt Erroneous ENC
6.1	Compression	Compress ENC
6.2	Compression	Decompress ENC
6.3	Compression	Decompress Corrupted ENC
7.1	Multiple Data Servers	Test Installation of cells from Multiple Data Servers
7.2	Multiple Data Servers	Test installation of an exchange set containing multiple data server signatures

3 Glossary

This document uses the following terms:

Data server	The VAR or RENC that supplies the ENC data.
Data server application	The VAR or RENC software that is used to prepare ENC data and the keys required to access it.
Data client	The mariner who uses the data to navigate
Data client application	ECDIS system that displays the data for the mariner

4 Organisation of the Test Definitions and Test data

4.1 Test Definitions

The test definitions offers high level functionaltests which are recommended to test for compliance with all security constructs defined in S-63. It does not replace unit testing in software development, but offer structured input to functional software testing.

The test definitions are organised in functional categories and defined in chapter 5. Test definitions for the Scheme Administrator functionality has not been included in the document since only the IHB will require these test scenarios.

Each test definition indicates whether the test is applicable for Data Server or Data Client applications. Note that a test is relevant for all applications if the type of application is omitted.

There are test definitions for both good and erroneous test conditions to ensure a robust application and reflect operational conditions.

Note that the IEC will be responsible for defining applicable ECDIS type approval tests which will complement this document.

4.2 Test Data

A range of test data has been developed to support the test definitions. The test data is documented alongside the test(s) to which it relates.

4.2.1 Provision of Test Data to Developers

All the test data is organised in a ZIP file and will extract into a directory structure where each test data will be located in a separate directory. Note that some of the test data sets are used in multiple test definitions.

Note that the test data can also be used by the developers for unit testing or other test situations for their application.

4.3 Conditions of Use for the Test data

The ENC information included in the test data has been made available to the recipient solely for the purpose of testing their application and verifying compliance with the S-63 standard. The material is supplied under the conditions shown below. If the recipient does not agree to bound by these conditions then the material should not be used and it should be destroyed.

The test data currently includes ENC information from the:

- Norwegian Hydrographic Service
- UK Hydrographic Office

The test data is NOT to be used for navigation.

4.4 Encoding of Data Server Origin in Cell Permit Files

The DPSWG has identified problems linking a cell permit issued by a Data Server to its corresponding ENC service. A Data Client application will experience problems when it attempts to decrypt an ENC with the incorrect cell permit in a multi supplier environment.

The *Guidance Notes for OEMs and Data Servers* version 2 available on the IHO web site describes how a Data Server Identifier is encoded in the reserved field in each permit record (each line) of the meta permit file defined in chapter 5.3.4 of the S-63 standard.

The permit files included with the S-63 testdata have been made available in the original format and in the new and recommended extended format defined in the *Guidance Notes for OEMs and Data Servers*. Since the naming convention for the meta permit files are identical, the extended meta permits are stored in a separate directory.

A developer should consult the *Guidance Notes for OEMs and Data Serves* for further recommendations on the management of cell permits and the encoding of Data Server origins in permit files.

5 Test Definitions

5.1 Default test data parameters

Many of the tests require a default set of parameters to be used. Unless specified elsewhere, the following default parameters are used throughout the test definitions and in the test data:

Manufacturer ID (M_ID)	=	10	(or 3130 hexadecimal)
Manufacturer Key (M_KEY)	=	10121	(or 3130313231 hexadecimal)
Hardware ID (HW_ID)	=	12345	(or 3132333435 hexadecimal)

This is the official manufacturer information issued by the Scheme Administrator (IHB) to be used for test purposes. A Data Server shall never deliver an official ENC service to an organisation with these parameters. The OEM shall request valid M_ID and M_KEY information from the Scheme Administrator (IHB) in accordance with the request procedure defined in the S-63 security scheme, chapter 11.

The official IHO Scheme Administrator Certificate is used in the test data unless a different certificate is specified in the test description.

5.2 User Permit Tests

5.2.1 Test 1.1 – User Permit Generation

Test ID	**1.1**
Test Name	***User Permit Generation***
Description	**Data client** applications must be able to generate a valid User Permit to uniquely identify the end-user ECDIS system based on the manufacturer and hardware information defined in the associated test data set.
Applicability	**Data client** applications (i.e. ECDIS equipment) should perform this test.
Input Data Location	The input data for this test can be found in the following directory on the CD: **S-63 TEST 1.1**
Input Data	**M_ID** = 10 (or 3130 hexadecimal) **M_KEY** = 10121 (or 3130313231 hexadecimal) **HW_ID** = 12345 (or 3132333435 hexadecimal)
Expected Output	The **user permit** generated by the ECDIS equipment should be: 66B5CBFDF7E4139D5B6086C23130

Actual Output	
Pass/Fail	
S-63 reference	This test references section 4.3.1 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.2.2 Test 1.2 – User Permit Verification & Decryption

Test ID	**1.2**
Test Name	***User Permit Verification & Decryption***
Description	Data server applications must be able to extract the HW_ID from a correctly-generated user permit.
Applicability	Data servers should perform this test.
Input Data Location	The input data for this test can be found in the following directory on the CD: **S-63 TEST 1.1**
Input Data	**User permit** = 66B5CBFDF7E4139D5B6086C23130 **M_ID** = 10 (ASCII) or 3130 (hexadecimal) **M_KEY** = 10121 (ASCII) or 3130313231 (hexadecimal)
Expected Output	The data extracted from this user permit should be: **HW_ID** = 12345 (ASCII) or 3132333435 (hexadecimal)
Actual Output	
Pass/Fail	
S-63 reference	This test references section 4.3.2 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.2.3 Test 1.3 – Identify Unregistered HW_ID in User Permit

Test ID	**1.3**
Test Name	***Identify unregistered HW_ID in user permit***
Description	Data server applications must be able to identify an incorrectly-generated user permit and react accordingly. This test checks the data server response to a user permit containing an unregistered HW_ID.
Applicability	Data servers should perform this test.
Input Data Location	The input data for this test can be found in the following directory on the CD: **S-63 TEST 1.3/ERRONEOUS HW_ID**
Input Data	**User permit** = EE9B0BCC4FF891EF45194F8B3130 Only the following manufacturer and hardware information shall be registered as valid with the Data Server: **M_ID** = 10 (ASCII) or 3130 (hexadecimal) **M_KEY** = 10121 (ASCII) or 3130313231 (hexadecimal) **HW_ID** = 12345 (ASCII) or 3132333435 (hexadecimal)
Expected Output	The **HW_ID** encoded in this user permit is: **HW_ID** = 23456 (ASCII)or 3233343536 (hexadecimal) This HW_ID should not be registered with the data server. The data server application must raise a clear and appropriate error message to indicate that the HW_ID is invalid, and discontinue any further operation on the user permit in question.
Actual Output	
Pass/Fail	
S-63 reference	This test references section 4.3.2 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.2.4 Test 1.4 – Identify Incorrect M_KEY used in User Permit generation

Test ID	**1.4**
Test Name	***Identify incorrect M_KEY used in user permit generation***
Description	Data server applications must be able to identify an incorrectly-generated user permit and react accordingly. This test checks the data server response to a user permit containing an incorrect checksum.
Applicability	Data servers should perform this test.
Input Data Location	The input data for this test can be found in the following directory on the CD: **S-63 TEST 1.3/ERRONEOUS M_KEY**
Input Data	**User permit** = C911B3EAB6B8A070A393B6D13130 Only the following manufacturer and hardware information shall be registered as valid with the Data Server: **M_ID** = 10 (ASCII) or 3130 (hexadecimal) **M_KEY** = 10121 (ASCII) or 3130313231 (hexadecimal) **HW_ID** = 12345 (ASCII) or 3132333435 (hexadecimal)
Expected Output	The **M_KEY** used to encrypt the HW_ID in this user permit is: **M_KEY** = 10122 (ASCII) or 3130313232 (hexadecimal) When decrypting the HW_ID in this user permit, the data server should attempt to use the expected M_KEY value 10121 (ASCII) which matches the M_ID of 10. This operation should fail because the HW_ID in the user permit has actually been encrypted using an incorrect M_KEY value of 10122 (ASCII). The data server application must raise a clear and appropriate error message and discontinue any further operation on the user permit in question.
Actual Output	
Pass/Fail	

S-63 reference	This test references sections 4.3.2 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.2.5 Test 1.5 – Identify Incorrect Checksum in User Permit

Test ID	**1.5**
Test Name	***Identify incorrect checksum in user permit***
Description	Data server applications must be able to identify an incorrectly-generated user permit and react accordingly. This test checks the data server response to a user permit containing an incorrect checksum.
Applicability	Data servers should perform this test.
Input Data Location	The input data for this test can be found in the following directory on the CD: **S-63 TEST 1.3/ERRONEOUS CHECKSUM**
Input Data	**User permit** = 66B5CBFDF7E4139DECCECCEC3130
Expected Output	This user permit contains an invalid checksum. The data server application must raise a clear and appropriate error message to indicate that the checksum is invalid, and discontinue any further operation on the user permit in question.
Actual Output	
Pass/Fail	
S-63 reference	This test references sections 4.3.2 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.3 Cell Permit Tests

5.3.1 Test 2.1 – Generate Cell Permit

Test ID	**2.1**
Test Name	***Generate cell permit***
Description	Data server applications must be able to generate a valid cell permit for a given user permit. The data server application should be able to extract the HW_ID from the user permit, and use the HW_ID to encrypt the cell keys in the user permit. This test checks that the data server can do this correctly.
Applicability	Data servers should perform this test.
Input Data Location	The input data for this test can be found in the following directories on the CD: **S-63 TEST 1.1** (user permit) **S-63 TEST 2.1** (cell permits)
Input Data	**User permit** = 66B5CBFDF7E4139D5B6086C23130 **M_ID** = 10 (ASCII) or 3130 (hexadecimal) **M_KEY** = 10121 (ASCII) or 3130313231 (hexadecimal) **HW_ID** = 12345 (ASCII) or 3132333435 (hexadecimal) **Subscription expiry date**: 24.08.2004 **Service indicator**: 0 (applicable only for Meta Permit file) **Reserved**: 0 (applicable only for Meta Permit file) **No comments provided** (applicable only for Meta Permit file)
Expected Output	A correct cell permit and a correct meta permit file containing a copy of the cell permit must both be created. The meta permit file must contain all the expected meta-data for the cell in question, and this meta-data must be correct.
Actual Output	
Pass/Fail	

Cell Name	Cell Edition	Cell Key	Cell Key
NO4D0512	3	9C467D359D	27737811B4
NO5F1615	4	A370962ACO	3488379F47

S-63 reference	This test references sections 5.2, 5.3 and 5.4.1 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.3.2 Test 2.2 – Decrypt Cell Permit

<table>
<tr><td>Test ID</td><td>2.2</td></tr>
<tr><td>Test Name</td><td>Decrypt cell permit</td></tr>
<tr><td>Description</td><td>Data client applications must be able to extract the encrypted cell keys from a cell permit and then decrypt the cell keys. The cell keys are then used to decrypt the S57 cell that the data client wishes to gain access to.

The data client application should be able to get cell permits from both cell permit files and meta permit files.

This test checks that the data client application can do this correctly.</td></tr>
<tr><td>Applicability</td><td>Data client applications should perform this test.</td></tr>
<tr><td>Input Data Location</td><td>The input data for this test can be found in the following directories on the CD:
S-63 TEST 1.1 (user permit)
S-63 TEST 2.1 (cell permits)
S-63 TEST 5.1 (Encrypted ENC cells using cell permits in TEST 2.1)
S-63 TEST 2.2 (cell permits)
S-63 TEST 5.3 (Encrypted ENC cells using cell permits in TEST 2.2)</td></tr>
<tr><td>Input Data</td><td>User permit = 66B5CBFDF7E4139D5B6086C23130
M_ID = 10 (ASCII) or 3130 (hexadecimal)
M_KEY = 10121 (ASCII) or 3130313231 (hexadecimal)
HW_ID = 12345 (ASCII) or 3132333435 (hexadecimal)

<table><tr><th>Cell Name</th><th>Cell Edition</th><th>Cell Key 1</th><th>Cell Key 2</th></tr><tr><td>NO4D0512</td><td>3</td><td>9C467D359D</td><td>27737811B4</td></tr><tr><td>NO5F1615</td><td>5</td><td>3488379F47</td><td>D45EF0F7E7</td></tr></table>
Subscription expiry date: 24.08.2004
Service indicator: 0 (applicable only for Meta Permit file)
Reserved: 0 (applicable only for Meta Permit file)
No comments provided (applicable only for Meta Permit file)</td></tr>
<tr><td>Expected Output</td><td>A valid cell key must be extracted from the cell permit. This cell key must be used to decrypt the ENC cell in question, rendering that cell readable.</td></tr>
<tr><td>Actual Output</td><td></td></tr>
</table>

Pass/Fail	
S-63 reference	This test references sections 5.2, 5.3, 5.4.2 and 5.4.4 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.3.3 Test 2.3 – Decrypt Erroneous Cell Permit

<table>
<tr><td>Test ID</td><td>2.3</td></tr>
<tr><td>Test Name</td><td>Decrypt erroneous cell permit</td></tr>
<tr><td>Description</td><td>Data client applications must be able to identify an error in a cell permit. Errors must be identified in permits contained in both cell permit files and meta permit files.

This test checks that the data client application can do this correctly.</td></tr>
<tr><td>Applicability</td><td>Data client applications should perform this test.</td></tr>
<tr><td>Input Data Location</td><td>The input data for this test can be found in the following directories on the CD:
S-63 TEST 1.1 (user permit)
S-63 TEST 2.3 (erroneous cell permit)
S-63 TEST 5.1 (Encrypted ENC cells)

Note that the first cell permit in TEST 2.3 is a broken version of first cell permit in TEST 2.1. It has an incorrect checksum.
The second cell permit in TEST 2.3 is the same as the second cell permit in TEST 2.1. It should work fine.</td></tr>
<tr><td>Input Data</td><td>Cell permit file/meta permit file containing a cell key with an incorrect checksum.
User permit = 66B5CBFDF7E4139D5B6086C23130
M_ID = 10 (ASCII) or 3130 (hexadecimal)
M_KEY = 10121 (ASCII) or 3130313231 (hexadecimal)
HW_ID = 12345 (ASCII) or 3132333435 (hexadecimal)

<table>
<tr><th>Cell Name</th><th>Cell Edition</th><th>Cell Key 1</th><th>Cell Key 2</th></tr>
<tr><td>NO4D0512</td><td>3</td><td>N/A</td><td>N/A</td></tr>
<tr><td>NO5F1615</td><td>4</td><td>A370962ACO</td><td>3488379F47</td></tr>
</table>

Subscription expiry date: 24.08.2004
Service indicator: 0 (applicable only for Meta Permit file)
Reserved: 0 (applicable only for Meta Permit file)
No comments provided (applicable only for Meta Permit file)</td></tr>
<tr><td>Expected Output</td><td>The data client application must raise a clear and appropriate error message to indicate that the checksum is invalid, and discontinue any further operation on the cell permit in question.</td></tr>
<tr><td>Actual Output</td><td></td></tr>
</table>

Pass/Fail	
S-63 reference	This test references sections 5.2, 5.3, 5.4.2 and 5.4.4of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.3.4 Test 2.4 – Check Expiry Date in Cell Permit

Test ID	**2.4**
Test Name	***Check expiry date in cell permit***
Description	Data client applications must be able to tell whether the user has a valid subscription to a particular ENC cell which has not expired. If the expiration date on the cell permit has passed then the user must not be able to use the cell permit to decrypt the cell. The expiration date may be contained in either the cell permit or the meta permit file. This test checks that the data client application can do this correctly.
Applicability	Data client applications should perform this test.
Input Data Location	The input data for this test can be found in the following directory on the CD: **S-63 TEST 2.4**
Input Data	The test data set contains cell permits for the ENC data defined in the directory **S-63 Test 5.1** plus the manufacturer and hardware information defined in directory **S-63 Test 1.1**. All the parameters remain the same except for the subscription expiration date in the cell permit which has been changed to 14.02.2002.
Expected Output	The data client application must raise a clear and appropriate error message to indicate that the user does not have a valid subscription to the ENC cell in question, and discontinue any further operation on the ENC cell.
Actual Output	
Pass/Fail	
S-63 reference	This test references sections 9.2.1 and 9.2.2 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.4 Certificate Tests

5.4.1 Test 3.1 – Data Server Using Valid Data Server Certificate

Test ID	**3.1**
Test Name	***Data server using valid data server certificate***
Description	Encrypted ENC cells supplied by data servers are signed by the data server upon dispatch. The data server signature should contain a signature from the SA public key to verify the data servers identity and *bona fides*. A data server application must always verify its data server signature against the SA public key before using it to sign its ENC data. This test checks that the data server application uses a correct data server public key that has been signed by the SA public key when signing ENC files.
Applicability	Data servers should perform this test.
Input Data Location	The input data for this test can be found in the following directory on the CD: **S-63 TEST 3.1 – Valid & invalid data server certificates**
Input Data	There are two data server certificates provided. One is valid, and one is corrupt.
Expected Output	When using the correct data server certificate, the data server application should sign the ENC cells with the certificate as expected. When using the incorrect data server certificate, the data server application must raise a clear and appropriate error message to indicate that the data server certificate is corrupt and cannot be used to sign ENC cells.
Actual Output	
Pass/Fail	
S-63 reference	This test references sections 9.2.1 and 9.2.2 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.4.2 Test 3.2 - Data Client Uses Correct SA Public Key File

Test ID	**3.2**
Test Name	***Data client uses correct SA public key file***
Description	Confirm that the data client application is not using the **IHO.crt** file on the media to authenticate the Data Server Certificate in the Cell signatures. **Note that the application shall not use SA Public Key directly from media provided by the service provider. The SA Public Key shall always be installed in a separate, independent operation and be subject to carefully controlled operating procedures.** This test ensures that the data client application uses the pre-installed SA public key to verify data server signatures on ENC files, and not the SA public key supplied with the ENC distribution media.
Applicability	Data client applications should perform this test.
Input Data Location	The input data for this test can be found in the following directory on the CD: **S-63 TEST 3.2– Valid & Erroneous IHO.crt files**
Input Data	Two IHO.crt files will be supplied, one is valid and the other is corrupt. The valid one should be stored in the secure area on the data client system. The corrupt one should be burnt onto a test CD containing some sample ENC cells.
Expected Output	When the data client application comes to validate the ENC cells on the CD, the outcome will depend on which IHO.crt is used by the data client application. The data client application should be able to validate the ENC cells on the media correctly because it is using the IHO.crt file from the secure area, which is correct. If the data client cannot validate the ENC cells it is because it is using the IHO.crt file from the media, which is wrong.
Actual Output	
Pass/Fail	
S-63 reference	This test references sections 6.2 and 6.6.4 of the S63 standard
Test Developed by	UKHO

5.4.3 Test 3.3 – Data Client Authenticates SA Public Key on CD Against Installed SA Public Key

Test ID	**3.3**
Test Name	***Data client authenticates SA public key on CD against installed public key***
Description	Data client applications must have a copy of the SA public key installed in a secure area as part of a separate, independent operation before the application is released to the user. The application must not use SA public key from any media supplied by the user. The application must only read the SA public key from the pre-installed secure area. This test ensures that the data client application can verify that the pre-installed SA public key matches the SA public key supplied on the ENC media.
Applicability	Data client applications should perform this test.
Input Data Location	The input data for this test can be found in the following directory on the CD: **S63 TEST 3.3 – Valid & Erroneous SA Public Key Files**
Input Data	The test data set contains a copy of the SA public key issued by IHB for use with the S-63 standard, plus an invalid IHO.crt file which is corrupt. The valid one should be stored in the secure area on the data client system. The corrupt one should be burnt onto a test CD containing some sample ENC cells. The public keys are available in two formats: • .CRT files - compliant with X.509 • .TXT files - text files as defined in S-63
Expected Output	When the data client application comes to validate the ENC cells on the CD, it should also check the SA public key on the CD against the SA public key that is stored in the secure area on the data client system. If the SA public key on the CD is different from the SA public key that is stored in the secure area on the data client system, then the data client application should warn the user that the two keys are different. This is a non-fatal error.

Actual Output	
Pass/Fail	
S-63 reference	This test references sections 6.2 and 6.6.4 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.4.4 Test 3.4 – Data Client Identifies Erroneous SA Public Key

Test ID	**3.4**
Test Name	***Data client identifies erroneous SA public key***
Description	Encrypted ENC cells supplied by data servers are digitally signed by the data server upon dispatch. The data server signature should contain a signature from the SA public key to verify the data servers identity and *bona fides*. On receipt of an ENC cell, the data client application must always verify the SA public key that is supplied with the data server signature before checking the data server digital signature itself. Data client applications must have a copy of the SA public key installed in a secure area as part of a separate, independent operation before the application is released to the user. The application must not read the SA public key from any media supplied by the user. The application must only read the SA public key from the pre-installed secure area.
Applicability	Data client applications should perform this test.
Input Data Location	The input data for this test can be found in the following directory on the CD: **S63 TEST 3.3 – Valid & Erroneous SA Public Key Files**
Input Data	The test data set contains one set of valid SA public key files, and one set of public key files which are different from the official SA public key. The file format is valid, but the file content is erroneous. The public keys are available in two formats: • .CRT files - compliant with X.509 • .TXT files - text files as defined in S-63
Expected Output	The data client application must raise a clear and appropriate error message to indicate that the digital signature provided with the ENC cell by the data server does not contain a valid SA public key. The application must then discontinue any further processing on the ENC cell in question.
Actual Output	
Pass/Fail	

S-63 reference	This test references sections 6.2 and 6.6.4 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.4.5 Test 3.5 – Make Data Server Self-Signed Key (SSK)

Test ID	**3.5**
Test Name	***Make data server self-signed key***
Description	Encrypted ENC cells supplied by data servers are digitally signed by the data server upon dispatch. The data server signature should contain a signature from the SA public key to verify the data servers identity and *bona fides.* The data server application must be able to generate a self-signed key that can then be dispatched to the IHO to be signed with the SA public key.
Applicability	Data servers should perform this test.
Input Data Location	The input data for this test can be found in the following directories on the CD: **S-63 TEST 3.5**
Input Data	The test data set contains files required to produce a Data Server Self Signed Key (SSK). The following text files are included: • DATA SERVER PRIVATE KEY.TXT – generated by the data server and used to sign its public key • DATA SERVER PUBLIC KEY.TXT – generated by the data server • DATA SERVER SSK.TXT – generated by the data server and is the data servers public key signed with the data servers private key
Expected Output	The data server application should create an SSK in the correct format. Because the SSK generation process involves a random element (the 'k' parameter,) no two SSKs will ever be the same. However, it is possible to check that the general format of an SSK is correct, and the SSK produced by the data server application should have the same format as the sample SSK included with the test data set.
Actual Output	
Pass/Fail	
S-63 reference	This test references sections 6.4 and 6.6.1 of the S63 standard

Test Developed by	Electronic Chart Centre AS

5.4.6 Test 3.6 – Authenticate Data Server Certificate in ENC Signature File

Test ID	**3.6**
Test Name	***Authenticate data server certificate in ENC signature file***
Description	Encrypted ENC cells supplied by data servers are digitally signed by the data server upon dispatch. The data server signature should contain a signature from the SA public key to verify the data servers identity and *bona fides.* The data client application must be able to extract and validate the data server certificate supplied with an ENC cell.
Applicability	Data client applications should perform this test.
Input Data Location	The input data for this test can be found in the following directories on the CD: **S-63 TEST 3.1 – SA Public Key** **S-63 TEST 3.5 – Data Server Public Key** **S-63 TEST 5.1 – Sample ENC files with signatures**
Input Data	Various signed ENC cell files plus the SA public key.
Expected Output	The data client should be able to extract and validate a digital signature attached to an ENC cell file. All the ENC signature files should generate the same DATA SERVER PUBLIC KEY.TXT file that is stored in the **TEST 3.5** directory.
Actual Output	
Pass/Fail	
S-63 reference	This test references sections 6.6.5 and 7.2.1 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.4.7 Test 3.7 - Identify Erroneous Data Server Certificate in ENC Signature File

Test ID	**3.7**
Test Name	***Identify erroneous data server certificate in ENC signature file***
Description	Encrypted ENC cells supplied by data servers are digitally signed by the data server upon dispatch. The data server signature should contain a signature from the SA public key to verify the data servers identity and *bona fides.* The data client must be able to verify that the data server signature belonging to an ENC file is correct. This ensures that the ENC file was produced by a recognised and accredited data server.
Applicability	Data client applications should perform this test.
Input Data Location	The input data for this test can be found in the following directories on the CD: **S-63 TEST 3.1 – SA Public Key** **S-63 TEST 3.6 - Erroneous Data Server Certificates in the ENC signature files for the test data in directory S-63 Test 5.1.** **S-63 TEST 5.1 – Sample ENC files with signatures**
Input Data	Various signed ENC cell files, plus the SA public key. In addition, the **TEST 3.6** data set contains erroneous data server certificates stored in ENC signature files for the exchange set defined in directory **S-63 Test 5.1**. These data server certificates cannot be authenticated with the SA Public key because the last hexadecimal characters in the data server public key parameter are corrupted. The following files are included in the dataset: • Erroneous signature file NOLD0512.000 • Erroneous signature file NOMF1615.000 • Erroneous signature file NOMF1615.001
Expected Output	The data client application must raise a clear and appropriate error message to indicate that the digital signature provided with the ENC cell by the data server cannot be authenticated. The application must then discontinue any further processing on the ENC cell in question.
Actual Output	
Pass/Fail	

S-63 reference	This test references sections 6.6.5 and 7.2.1 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.5 Digital Signature Tests

5.5.1 Test 4.1 – Sign ENC File

Test ID	**4.1**
Test Name	***Sign ENC file***
Description	Encrypted ENC cells supplied by data servers must be digitally signed by the data server upon dispatch. The data server signature should contain a signature from the SA public key to verify the data servers identity and *bona fides.* The data server application must be able to sign the ENC base data files and update files that it produces. The signature must be applied to the ENC base and update files after they have been compressed and encrypted. This test ensures that the data server signatures applied to ENC base data are in the correct format. Note that due to the random "k" parameter that is input to the DSA signature algorithm, it is not possible to create two identical ENC signature files for the same ENC data file. This makes it impossible to directly cross-check a signature for an ENC file produced by the data server against a sample signature. However, it is possible to check the format of a signature against the format of a sample signature.
Applicability	Data servers should perform this test.
Input Data Location	The input data for this test can be found in the following directories on the CD: **S-63 TEST 3.2 – Data Server Key Information** **S-63 TEST 5.1 - Unencrypted ENC files and signature files for the corresponding encrypted ENC files**
Input Data	Various ENC cell files plus data server keys.
Expected Output	Valid ENC signature files for the ENC cell files
Actual Output	
Pass/Fail	
S-63 reference	This test references sections 7.2.1 and 7.3.1 of the S63 standard

Test Developed by	Electronic Chart Centre AS

5.5.2 Test 4.2 – Authenticate ENC signature

Test ID	**4.2**
Test Name	***Authenticate ENC signature***
Description	Encrypted ENC cells must be digitally signed by data servers. An ENC signature file contains a signature/certificate pair. A data client application must be able to authenticate the data server certificate contained in the ENC signature file using the installed SA public key. If verified correctly, the data server public key shall be extracted from the data server certificate and used to authenticate the ENC signature.
Applicability	Data client applications should perform this test.
Input Data Location	The input data for this test can be found in the following directories on the CD: **S-63 TEST 3.1 – SA Public Key** **S-63 TEST 5.1 - Unencrypted ENC files and signature files for the corresponding encrypted ENC files**
Input Data	Various ENC signature files. See section 5.6.1 for details
Expected Output	The data server signatures within ENC signature files can be validated successfully
Actual Output	
Pass/Fail	
S-63 reference	This test references sections 7.2.1 and 7.3.2 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.5.3 Test 4.3 – Identify Erroneous ENC signature

Test ID	**4.3**
Test Name	***Identify erroneous ENC signature***
Description	Encrypted ENC cells supplied by data servers must be digitally signed by the data server upon dispatch. The data server signature should contain a signature from the SA public key to verify the data servers identity and *bona fides.* The data client application must be able to authenticate the signature that is applied to an ENC file against the contents of the file to ensure that the ENC signature actually applies to the ENC data in question.
Applicability	Data client applications should perform this test.
Input Data Location	The input data for this test can be found in the following directories on the CD: **S-63 TEST 4.3 – data set with erroneous ENC signatures**
Input Data	The test data set contains erroneous ENC signatures for the ENC files included in the exchange set. The last few hexadecimal characters of each ENC signature element have been corrupted. The dataset contains the following files: • CATALOG.031 • README.TXT • NO4D0512.000 (Encrypted ENC base cell file) • ERRONEOUS NOLD0512.000 (Signature file to base cell) • NO5F1615.000 (Encrypted ENC file) • ERRONEOUS NOMF1615.000 (Signature file to base cell) • NO5F1615.001 (Encrypted ENC update file) • ERRONEOUS NOMF1615.001 (Signature to update file) These files have been encrypted using the parameters defined in **S-63 Test 2.1**
Expected Output	The data client application must raise a clear and appropriate error message to indicate that the digital signature provided with the ENC file by the data server cannot be validated against the ENC cell. The application must then discontinue any further processing on the ENC cell in question.
Actual Output	
Pass/Fail	
S-63 reference	This test references sections 7.2.1 and 7.3.2 of the S63 standard

Test Developed by	Electronic Chart Centre AS

5.6 Encryption/Decryption Tests

5.6.1 Test 5.1 - Encrypt ENC Base Cells and Update Files

Test ID	**5.1**
Test Name	***Encrypt ENC base cells and update files***
Description	ENC files are compressed and encrypted by the data server before being digitally signed and released. This test checks that the data server application correctly encrypts ENC base cells and update files.
Applicability	Data servers should perform this test.
Input Data Location	The input data for this test can be found in the following directories on the CD: **S-63 TEST 5.1**
Input Data	The test data set contained in the directory **S-63 TEST 5.1** contains matching pairs of encrypted and the corresponding unencrypted versions of an S57 exchange set stored in two separate subdirectories. The UNENCRYPTED directory consists of: • CATALOG.031 • README.TXT • NO4D0512.000 • NO5F1615.000 • NO5F1615.001 The ENCRYPTED directory consists of: • CATALOG.031 • README.TXT • NO4D0512.000 (Encrypted ENC base cell file) • NOLD0512.000 (Signature file to base cell) • NO5F1615.000 (Encrypted ENC file) • NOMF1615.000 (Signature file to base cell) • NO5F1615.001 (Encrypted ENC update file) • NOMF1615.001 (Signature to update file) The files have been encrypted using the parameters defined in directory **S-63 TEST 2.1**.
Expected Output	The encrypted ENC files generated by the data server application should be identical to the encrypted ENC files provided in the test data

	should be identical to the encrypted ENC files provided in the test data set.
Actual Output	
Pass/Fail	
S-63 reference	This test references sections 8.2.1 and 8.2.3 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.6.2 Test 5.2 - Decrypt ENC Base Cells and Update Files

Test ID	**5.2**
Test Name	***Decrypt ENC base cells and update files***
Description	ENC files are compressed and encrypted by the data server before being digitally signed and released. This test checks that the data client application correctly decrypts ENC base cells and update files.
Applicability	Data client applications should perform this test.
Input Data Location	The input data for this test can be found in the following directories on the CD: **S-63 TEST 5.1 with cell permits from directory S-63 TEST 2.1** **S-63 TEST 5.3 with cell permits from directory S-63 TEST 2.2**
Input Data	The test data set contained in the directory **S-63 TEST 5.1** contains matching pairs of encrypted and the corresponding unencrypted versions of an S57 exchange set stored in two separate subdirectories. The UNENCRYPTED directory consists of: • CATALOG.031 • README.TXT • NO4D0512.000 • NO5F1615.000 • NO5F1615.001 The ENCRYPTED directory consists of: • CATALOG.031 • README.TXT • NO4D0512.000 (Encrypted ENC base cell file) • NOLD0512.000 (Signature file to base cell) • NO5F1615.000 (Encrypted ENC file) • NOMF1615.000 (Signature file to base cell) • NO5F1615.001 (Encrypted ENC update file) • NOMF1615.001 (Signature to update file) These files have been encrypted using the parameters defined in directory **S-63 TEST 2.1**. The test data set contained in the directory **S-63 TEST 5.3** contains matching pairs of encrypted and the corresponding unencrypted versions of an S57 exchange set stored in two separate subdirectories.

	The UNENCRYPTED directory consists of: • CATALOG.031 • README.TXT • NO4D0512.000 (same base cell as in directory S-63 TEST 5.1) • NO5F1615.000 (next edition of base cell in directory S-63 TEST 5.1) The ENCRYPTED directory consists of: • CATALOG.031 • README.TXT • NO4D0512.000 (Encrypted ENC base cell file) • NOLD0512.000 (Signature file to base cell) • NO5F1615.000 (Encrypted ENC file) • NOMF1615.000 (Signature file to base cell) These files have been encrypted using the parameters defined in directory **S-63 TEST 2.2**.
Expected Output	The encrypted ENC files should be decrypted successfully with the appropriate Cell Keys/User Permits. All decrypted ENC base cell and update files should be identical to the unencrypted ENC files in the test data.
Actual Output	
Pass/Fail	
S-63 reference	This test references sections 8.2.2 and 8.2.4 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.6.3 Test 5.3 - Encrypt Next Edition of ENC with Next Cell Key

Test ID	**5.3**
Test Name	***Encrypt next edition of ENC with next cell key***
Description	ENC files are compressed and encrypted by the data server before being digitally signed and released. When the next edition of an encrypted ENC base cell and its associated update files are released into the market, they must be encrypted with the next edition of the cell key. Cell key 2 must now become the new cell key 1. A new cell key 2 must be assigned and used to encrypt the next edition of the cell in the future. This test checks that the data server application correctly encrypts new editions of ENC base cells and update files with cell key 2 instead of cell key 1.
Applicability	Data servers should perform this test.
Input Data Location	The input data for this test can be found in the following directories on the CD: **S-63 TEST 5.3**
Input Data	Various ENC data files.
Expected Output	The encrypted ENC files should be identical to the encrypted ENC files provided in the test data set.
Actual Output	
Pass/Fail	
S-63 reference	This test references sections 5.2.3, 8.2.1 and 8.2.3 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.6.4 Test 5.4 - Decrypt Next Edition of ENC with Next Cell Key

Test ID	**5.4**
Test Name	***Decrypt Next Edition of ENC with Next Cell Key***
Description	ENC files are compressed and encrypted by the data server before being digitally signed and released. When the next edition of an encrypted ENC base cell and its associated update files are released into the market, they must be encrypted with the next edition of the cell key. Cell key 2 must now become the new cell key 1. A new cell key 2 must be assigned and used to encrypt the next edition of the cell in the future. This test checks that the data client application correctly decrypts new editions of ENC base cells and update files with cell key 2 instead of cell key 1. Note that the application can decrypt the next edition of an ENC cell by either: • Using Cell Key 1 from a Cell Permit issued with that edition of the ENC (ref. test data in directory **S-63 TEST 2.2**) • Using Cell Key 2 from a Cell Permit issued with the previous edition of the ENC (ref. test data in directory **S-63 TEST 2.1**)
Applicability	Data client applications should perform this test.
Input Data Location	The input data for this test can be found in the following directories on the CD: **S-63 TEST 5.3 with cell permits from directory S-63 TEST 2.2** **S-63 TEST 5.1 with Cell Permits from directory S-63 TEST 2.1** The data client application can test the feature by using Cell Key 2 from the Cell Permits provided in directory S-63 Test 5.1 or Cell Key 1 from the Cell Permits provided in directory S-63 Test 5.2
Input Data	Various encrypted ENC data files
Expected Output	All decrypted ENC base cell and update files generated by the data client application should be identical to the unencrypted ENC files in the test data.
Actual Output	

Pass/Fail	
S-63 reference	This test references sections 5.2.3, 8.2.2 and 8.2.4 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.6.5 Test 5.5 - Decrypt Erroneous ENC

Test ID	**5.5**
Test Name	***Decrypt Erroneous ENC***
Description	ENC files are compressed and encrypted by the data server before being digitally signed and released. In addition to querying the status of the decryption, the data client application must also verify the CRC value of the decrypted ENC before accepting the ENC as being useable. Data client applications must be able to detect when the decryption of an ENC file and/or the CRC check has failed.
Applicability	Data client applications should perform this test.
Input Data Location	The input data for this test can be found in the following directories on the CD: **S-63 TEST 5.5**
Input Data	The test data set contains erroneous encrypted ENC base cell and update files and will not work with the Cell Keys defined in the directory **S-63 TEST 2.1**. The erroneous files come from the encrypted exchange set defined in directory **S-63 TEST 5.1** but the first bytes in each ENC file have been modified. The following erroneous files are included: • ERRONEOUS NO4D0512.000 (Encrypted ENC base cell file) • ERRONEOUS NO5F1615.000 (Encrypted ENC file) • ERRONEOUS NO5F1615.001 (Encrypted ENC update file) Note that the signature files included in the directory S-63 TEST 5.1 will not work with these encrypted ENC files.
Expected Output	The data client application should report erroneous decryption for all ENC base and update files in the dataset. The ENC files in question should not be accepted by the system.
Actual Output	
Pass/Fail	
S-63 reference	This test references sections 5.2.3, 8.2.2 and 8.2.4 of the S63 standard
Test Developed	Electronic Chart Centre AS

by	

5.7 Compression Tests

5.7.1 Test 6.1 - Compress ENC

Test ID	**6.1**
Test Name	***Compress ENC***
Description	ENC files are compressed and encrypted by the data server before being digitally signed and released. The ZIP algorithm must be used for the compression step. Data server applications must be able to successfully compress ENC files.
Applicability	Data servers should perform this test.
Input Data Location	The input data for this test can be found in the following directories on the CD: **S-63 TEST 6.1**
Input Data	The test data set contains compressed and uncompressed versions of three ENC base and update files stored in two separate subdirectories. The UNCOMPRESSED directory consists of: • NO4D0512.000 • NO5F1615.000 • NO5F1615.001 The COMPRESSED directory consists of: • NO4D0512.000.ZIP • NO5F1615.000.ZIP • NO5F1615.001.ZIP
Expected Output	Compressed ENC files generated by the data server application. Note that the compressed files can be different to what is provided in the test data set depending on how the zip parameters are defined. The client application is able to determine the proper decompression setting.
Actual Output	
Pass/Fail	
S-63 reference	This test references section 9.1.4.1 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.7.2 Test 6.2 - Decompress ENC

Test ID	**6.2**
Test Name	***Decompress ENC***
Description	ENC files are compressed and encrypted by the data server before being digitally signed and released. The ZIP algorithm is used for the compression step. Data client applications must be able to successfully uncompress ENC files so that they become S-57 compliant. In addition to querying the status of the decompression, the data client application must also verify the CRC value of the decompressed ENC.
Applicability	Data client applications should perform this test.
Input Data Location	The input data for this test can be found in the following directories on the CD: **S-63 TEST 6.1**
Input Data	Various compressed ENC data files. See section 5.7.1.
Expected Output	The decompressed ENC files generated by the data client application should be identical to the ENC files provided in the test data set.
Actual Output	
Pass/Fail	
S-63 reference	This test references section 9.1.4.2 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.7.3 Test 6.3 – Decompress Corrupted ENC

Test ID	**6.3**
Test Name	***Decompress corrupted ENC***
Description	ENC files are compressed and encrypted by the data server before being digitally signed and released. The ZIP algorithm is used for the compression step. Data client applications must be able to successfully uncompress ENC files so that they become S-57 compliant. In addition to querying the status of the decompression, the data client application must also verify the CRC value of the decompressed ENC.
Applicability	Data client applications should perform this test.
Input Data Location	The input data for this test can be found in the following directories on the CD: **S-63 TEST 6.2**
Input Data	The test data set contains erroneous compressed ENC base and update files. The first bytes in each file have been modified. The test data consist of the following files: • ERRONEOUS NO4D0512.000.ZIP • ERRONEOUS NO5F1615.000.ZIP • ERRONEOUS NO5F1615.001.ZIP
Expected Output	The data client application must raise a clear and appropriate error message to indicate that the ENC file cannot be decompressed correctly. The application must then discontinue any further processing on the ENC cell in question.
Actual Output	
Pass/Fail	
S-63 reference	This test references section 9.1.4.2 of the S63 standard
Test Developed by	Electronic Chart Centre AS

5.8 Multiple Data Server Tests

The following set of test cases simulates multiple Data Servers providing ENCs for use on a vendor ECDIS. The tests have been developed with a single Scheme Administrator signing SSKs for two Data Servers and those signatures are included in the test data sets.

The aim of the tests is to ensure that the correct authentication paths are followed within the vendor software and that the S63 implementation is consistent in the presence of multiple ENC data servers even when those data servers are distributing some of the same ENC cells.

5.8.1 Test 7.1 – Test installation of cells from multiple data servers

Test ID	**7.1**
Test Name	***Test installation of cells from multiple data servers***
Description	Data client applications must be able to load data from two different ENC data servers correctly.
Applicability	Data clients should perform this test.
Input Data Location	The input data for this test can be found in the following directory on the CD: **S-63 TEST 7.1**
Input Data	The test uses data produced by two different data servers. There are two sets of ENC cells with their associated permits in the test data set. There is also a document called **"Test 7.1 Checklist.doc"** included with the test data set which describes the layout of the test data in detail.
Expected Output	The data client application should correctly load all cells and updates from both data servers and consistently apply the updates as supplied.
Actual Output	
Pass/Fail	
S-63 reference	This test references sections 5.2, 5.3 and 5.4 of the S63 standard
Test Developed by	UKHO

5.8.2 Test 7.2 – Test installation of an exchange set containing multiple data server signatures

Test ID	**7.2**
Test Name	***Test installation of an exchange set containing multiple data server signatures***
Description	A single exchange set may contain multiple data server signatures. In this case it will include ENCs which have been encrypted and signed by different Data Servers. Data Client applications must be able to successfully authenticate the Data Server certificates from the ENC signatures using the installed SA key installed on the system.
Applicability	Data Client applications should perform this test.
Input Data Location	The input data for this test can be found in the following directories on the CD: **S-63 TEST 7.2**
Input Data	The test data set contains a single exchange set containing two ENC cells with associated update files. The cell NO4H0711 has been digitally signed by the S-63 testdata Data Server, while the cell NO5E0811 has been digitally signed by Primar Stavanger. The Data Server certificates have been issued by IHB. The ENC data is also made available unencrypted. The required permit files are provided in a separate directory for the following Data Client application: **User Permit** = 66B5CBFDF7E4139D5B6086C23130 **M_ID** = 10 (ASCII) or 3130 (hexadecimal) **M_KEY** = 10121 (ASCII) or 3130313231 (hexadecimal) **HW_ID** = 12345 (ASCII) or 3132333435 (hexadecimal)
Expected Output	The data client application should correctly: 1. authenticate the Data Server certificates from the ENC base and update file signatures using the SA key installed on the system. 2. validate the ENC signatures against the Data Server public key (extracted from the signature file) and the ENC contents. 3. load all cells and updates issued by the two Data Servers and consistently apply the updates as supplied.
Actual Output	
Pass/Fail	

S-63 reference	This test references section 6.6.6, 6.6.5, 7.3.2 and 5.4.2 of the S63 standard
Test Developed by	Electronic Chart Centre AS