

# IHO Data Protection Scheme (Preview PR)

**Edition 1.2.1 – March 2020**

**IHO**



International  
Hydrographic  
Organization

Published by the  
International Hydrographic Organization  
4b quai Antoine 1<sup>er</sup>  
Principauté de Monaco  
Tel: (377) 93.10.81.00  
Fax: (377) 93.10.81.40  
[info@ihodata.net](mailto:info@ihodata.net)  
[www.ihodata.net](http://www.ihodata.net)

© Copyright International Hydrographic Organization 2020

This work is copyright. Apart from any use permitted in accordance with the Berne Convention for the Protection of Literary and Artistic Works (1886), and except in the circumstances described below, no part may be translated, reproduced by any process, adapted, communicated or commercially exploited without prior written permission from the International Hydrographic Organization (IHO). Copyright in some of the material in this publication may be owned by another party and permission for the translation and/or reproduction of that material must be obtained from the owner.

This document or partial material from this document may be translated, reproduced or distributed for general information, on no more than a cost recovery basis. Copies may not be sold or distributed for profit or gain without prior written agreement of the IHO Secretariat and any other copyright holders.

In the event that this document or partial material from this document is reproduced, translated or distributed under the terms described above, the following statements are to be included:

"Material from IHO publication [reference to extract: Title, Edition] is reproduced with the permission of the IHO Secretariat (Permission No ...../...) acting for the International Hydrographic Organization (IHO), which does not accept responsibility for the correctness of the material as reproduced: in case of doubt, the IHO's authentic text shall prevail. The incorporation of material sourced from IHO shall not be construed as constituting an endorsement by IHO of this product."

"This [document/publication] is a translation of IHO [document/publication] [name]. The IHO has not checked this translation and therefore takes no responsibility for its accuracy. In case of doubt the source version of [name] in [language] should be consulted."

The IHO Logo or other identifiers shall not be used in any derived product without prior written permission from the IHO Secretariat.

## Contents

Foreword.....	v
1 Terms and definitions.....	1
1.1 Glossary of S-63 Data Protection Scheme Terms.....	1
1.2 Chart Related Terms.....	1
1.3 Organisations.....	2
1.4 Computing Terms.....	2
2 Introduction.....	2
2.1 General Description.....	3
2.2 Participants in the Scheme.....	3
2.3 References.....	4
2.4 Compatibility with Previous Versions.....	5
2.5 Document Structure.....	5
2.6 Maintenance.....	6
2.7 Support.....	6
3 Data Compression.....	6
3.1 Overview.....	6
3.2 Compression Algorithm.....	7
3.3 Compressed Files.....	7
4 Data Encryption.....	7
4.1 What Data is encrypted?.....	7
4.2 How is it encrypted?.....	7
5 Data Licencing.....	8
5.1 Introduction.....	8
5.2 The Userpermit.....	8
5.3 The Cell Permit.....	10
6 Data Authentication.....	14
6.1 Introduction to Data Authentication and Integrity Checking.....	14
6.2 Digital Certificates (SA Authentication).....	17
6.3 Digital Signatures (Verify Data Integrity).....	18
6.4 Data Authentication File Formats.....	20
7 Data Management.....	24
7.1 Introduction.....	24
7.2 ENC Product Listing (PRODUCTS.TXT).....	25
7.3 Serial File (SERIAL.ENC).....	29
7.4 The S-57 Catalogue File (CATALOG.031).....	31
7.5 ENC Update Management.....	32
7.6 The S-57 Readme File (README.TXT).....	34
8 Directory and File Structure.....	34
8.1 Introduction.....	34
8.2 S-57 File Management.....	34
8.3 File Structure.....	35
8.4 Folder and File Naming.....	35
8.5 Exchange Set Media.....	35
9 Scheme administrator processes.....	37
9.1 Data Protection Scheme Administrator.....	37
9.2 Scheme Administrator Processes.....	37
9.3 Create Top Level Key Pair.....	38
9.4 Create and Issue SA Digital Certificate (X509v3).....	39
9.5 Process Applications from Data Servers & OEMs.....	39
9.6 S-63 Test Data.....	41
9.7 Scheme Administrator – Security QA Procedures.....	42
10 Data server processes.....	43
10.1 Overview.....	43
10.2 Data Server Processes.....	43
10.3 Certification Processes.....	44
10.4 Data Management Processes.....	49
10.5 Encryption, Compression and ENC Signing Processes.....	49
10.6 Licensing Processes.....	52

10.7	Security QA Procedures – Data Server.....	56
11	OEM and Data Client Processes.....	57
11.1	Data Clients.....	57
11.2	Original Equipment Manufacturers (OEMs).....	57
11.3	OEM & Data Client Processes.....	58
11.4	Create Data Client Userpermit.....	59
11.5	ENC Cell Permit Installation.....	60
11.6	ENC Authentication and Integrity Checks.....	62
11.7	Decrypt ENC Base Cell and Update Files.....	66
11.8	Data Client Permanent Warnings.....	70
11.9	QA Procedures – Data Client.....	70
11.10	QA Procedures – Manufacturers (OEMs).....	71
12	S-63 Error Codes and Explanations.....	71
	Annex A Data Server Certificate Request Procedure.....	75
A.1	Purpose.....	75
A.2	Responsibility.....	75
A.3	Definitions.....	75
A.4	Procedure.....	75
A.5	Quality Metrics.....	78
	Annex B Manufacturer Information Request Procedure.....	80
B.1	Purpose.....	80
B.2	Responsibility.....	80
B.3	Definitions.....	80
B.4	Procedure.....	80
B.5	Quality Metrics.....	83
	Annex C ENC Update Status Report.....	85
C.1	Purpose.....	85
C.2	Use and Responsibility.....	85
C.3	Report Definitions.....	85
	Appendix 1 Data Protection Scheme Test Data.....	93
1.1	Introduction.....	93
1.2	Organisation of the Test Definitions and Test data.....	93
	Appendix 2 Large Media Support.....	95
2.1	Introduction.....	95
2.2	Media Overview.....	95
2.3	Media File Formats.....	96
2.4	Media Management (Data Servers).....	98
2.5	Media Management (Data Clients).....	99

## Foreword

Copyright infringement and data piracy are pervasive problems of the digital era. Electronic Navigational Charts (ENC) are not exempt from these issues. As well as the economic impact, the unofficial distribution of nautical information also gives rise to significant safety concerns. As a result, the publishers of official nautical information have sought to protect their data and provide the mariner with a certificate of authenticity through the adoption of a security scheme.

In September 2000, IHO Member States were polled on their views on developing a single IHO Recommended Security Scheme (RSS) (see: IHO Circular Letter 38/2000). Responses indicated that a large majority of the Member States wished to have their ENC data encrypted and agreed that the IHO should adopt a single RSS (see: IHO CL 15/2001 Rev.1). A majority of the Member States responding also supported the adoption of the Primar Security Scheme as the IHO RSS, as it was at the time the de facto standard for ENC protection and the majority of ECDIS manufacturers had already developed the necessary decryption facilities in their systems.

The IHO Committee on Hydrographic Requirements for Information Systems (CHRIS, now HSSC: Hydrographic Services and Standards Committee), at its 13<sup>th</sup> meeting (Athens, Greece, September 2001), revisited the issue of an RSS and agreed that a small advisory expert group investigate the implications of IHO becoming the security scheme administrator for an RSS and assuming responsibility for the maintenance of an RSS.

The Data Protection Scheme Working Group (DPSWG) reported back to the IHO Secretariat in January 2002 that there were no technical implications to the IHO Secretariat becoming the security scheme administrator and that the level of effort to administer the security scheme would be limited and within the IHO Secretariat resources. The DPSWG further provided a plan to develop an IHO RSS Version 1, based on the Primar Security Scheme. This Report was endorsed by CHRIS Members in February 2002 and the DPSWG was tasked to develop Version 1 of an IHO RSS.

The results were presented to CHRIS, at its 14<sup>th</sup> meeting (Shanghai, China, August 2002), which recommended that the ENC Security Scheme, as developed by the DPSWG, be submitted to IHO Member States for adoption as an IHO RSS, and that the role as Security Scheme Administrator be transferred to the IHO Secretariat. These proposals (see: IHO CL 44/2002) were approved by a majority of Member States (see: IHO CL 66/2002). As a result, Edition 1.0 of the IHO Data Protection Scheme was adopted in October 2003 as Publication S-63.

The 18<sup>th</sup> CHRIS meeting (Cairns, Australia, September 2006) tasked the DPSWG to develop a revised edition of S-63 with the following guidance:

- There would be no introduction of new features; changes would be kept to a minimum.
- Published S-63 guidelines would be included in the standard.
- S-63 would be reorganized to group issues relevant to the IHO Secretariat as Scheme Administrator, to Data Servers, and to OEMs, respectively.
- There would be a more precise description of the correct implementation of the IHO standard.

Accordingly, a draft Edition 1.1 of S-63 was prepared by DPSWG and endorsed by CHRIS at its 19<sup>th</sup> meeting (Rotterdam, Netherlands, November 2007). This was subsequently endorsed by Member States and adopted in March 2008. Edition 1.1 included supporting documentation, test data and a method to supply ENCs using “Large Media Support”.

In April 2012, small changes were made to Edition 1.1 to remove the hexadecimal limitation of M\_ID in order to extend the number of possible M\_ID values that the scheme is able to accommodate. This resulted in the publication of edition 1.1.1 of S-63.

In November 2014 an additional annex was added to Edition 1.1.1 to provide a normative reference for the ENC update status report. This report reflects functionality required by edition 4 of the ECDIS type approval standard IEC61174, section 4.4.2 and Annex L. No other substantive changes were made to S-63 as a result of this additional annex, only clarifications for users of the data protection scheme on how the report is formatted and the definitions of its various fields. This resulted in this Edition 1.2.0 of S-63. A minor clarification has been added providing guidance to more formally structure the README.TXT file at section 6.6, resulting in this Edition 1.2.1 of S-63.

Changes to this Standard, as well as any further developments, will continue to be coordinated by the ENCWG under HSSC Guidance.

## 1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

### 1.1 Glossary of S-63 Data Protection Scheme Terms

**Blowfish**

Encryption algorithm used by the protection scheme

**Cell Key**

Key used to produce encrypted ENC, and required to decrypt the encrypted ENC information.

**Cell Permit**

Encrypted form of Cell key, created specifically for a particular user.

**Data Client**

Term used to represent an end-user receiving the encrypted ENC information. The Data Client will be using a software application (e.g. ECDIS) to perform many of the operations detailed within the scheme. Typically, an ECDIS user.

**Data Server**

Term used to represent an organisation producing encrypted ENCs or issuing Cell Permits to end-users.

**M\_ID**

The unique identifier assigned by the SA to each manufacturer. Data Servers use this to identify which M\_KEY to use when decrypting the userpermit.

**M\_KEY**

ECDIS manufacturer's unique identification key provided by the Scheme Administrator to the OEM. It is used by OEMs to encrypt the HW\_ID when creating a userpermit.

**HW\_ID**

The unique identifier assigned by an OEM to each implementation of their system. This value is encrypted using the OEM's unique M\_KEY and supplied to the data client as a userpermit. This method allows data clients to purchase licences to decrypt ENC cells.

**SA**

Scheme Administrator

**SHA-1**

Secure Hash Algorithm [[NIST FIPS 180-1 fpd](#)]

**SSK**

Self Signed Key (Self Signed Certificate File)

**User Permit**

Encrypted form of HW-ID uniquely identifying the ECDIS system

### 1.2 Chart Related Terms

**ECDIS**

Electronic Chart Display and Information System as defined by IMO

**ENC**

Electronic Navigational Chart as defined by the ENC Product Specification. [[S-57](#)]

**S-57**

Transfer standard for ENC defined by IHO

**SENC**

System-ENC (This is the internal format that OEMs convert to when importing data)

### 1.3 Organisations

**ECC**

Electronic Chart Centre AS ([www.ecc.as](http://www.ecc.as))

**HO**

Hydrographic Office (e.g. Data Server)

**IHO**

International Hydrographic Organisation

**IMO**

International Maritime Organisation

**RENC**

Regional ENC Coordinating Centre integrating ENCs from several HOs into a single service (e.g. Data Server)

**UKHO**

United Kingdom Hydrographic Office ([www.ukho.gov.uk](http://www.ukho.gov.uk))

### 1.4 Computing Terms

**CRC**

Cyclic Redundancy Check

**Dongle**

Sometimes referred to as a hard lock device, It is a hardware device supplied by the OEMs that has the unique system identifier (HW\_ID) stored securely within.

**XOR**

Exclusive OR

## 2 Introduction

The publication “S-63 IHO Data Protection Scheme”, later referred to as ‘the scheme’, describes the 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 S-63 compliant systems and distribute data in a secure and commercially viable manner.

The Data Protection Scheme was prepared by the International Hydrographic Organisation’s (IHO) Data Protection Scheme Advisory Group (DPSWG). The S-63 standard is based on the protection scheme developed and operated by Primar and Primar-Stavanger as part of their protected ENC service. The Electronic Chart Centre AS and United Kingdom Hydrographic Office were the original contributing organisations.

The Standard was adopted as the official IHO standard, by the IHO member states in December 2002 (IHO CL 66, 2002). It defines the roles and responsibilities for protecting ENC data produced by National Hydrographic Offices and distributed to customers with ECS/ECDIS systems.

## 2.1 General Description

This document specifies a method of securing ENC information and maintaining the integrity of an ENC service with multiple data services serving a large customer base. The purpose of data protection is threefold:

- 1) **Piracy Protection:** To prevent unauthorised use of data by encrypting the ENC information.
- 2) **Selective Access:** To restrict access to ENC information to only those cells that a customer has been licenced for.
- 3) **Authentication:** To provide assurance that the ENC data has come from approved sources

Piracy protection and selective access are achieved by encrypting the ENC information and providing cell permits to decrypt them. Data Servers will encrypt ENC data provided by producer nations before supplying it to the Data Client. The encrypted ENC is then decrypted by the ECS/ECDIS prior to being reformatted and imported into the systems SENC. Authentication is provided by means of digital signatures within the data.

The scheme does not specifically address how ENC or SENC information can be protected once it is within an end-user application. This is the responsibility of the OEMs.

The scheme allows for the mass distribution of encrypted ENCs on hard media (e.g. CD-ROM or DVD) and can be accessed and used by all customers with a valid licence containing a set of permits. Selective access to individual cells is supported by providing users with a licenced set of permits containing the encrypted cell keys. This licence is created using a unique hardware identifier of the system and is unique to each Data Client. Consequently licences cannot be exchanged between individual Data Clients.

The scheme uses a compression algorithm to reduce the size of the dataset. Unencrypted ENC data contains many repeating patterns of information, e.g. coordinate information. Compression is therefore always applied before the ENC information is encrypted and uncompressed after the decryption on the data client system (normally an ECS/ECDIS).

## 2.2 Participants in the Scheme

There are several types of users of the scheme, these are as follows:

- The Scheme Administrator (SA), of which there is only one.
- The Data Server (DS), of which there can be many.
- The Data Client (DC), of which there are many.
- The Original Equipment Manufacturer (OEM) of which there are many.

A more detailed explanation of these terms is given below.

### 2.2.1 Scheme Administrator

The Scheme Administrator (SA) is solely responsible for maintaining and coordinating the scheme. The SA role is operated by the IHO Secretariat on behalf of the IHO member states.

The SA is responsible for controlling membership of the scheme and ensuring that all participants operate according to defined procedures. The SA maintains the top level digital certificate used to operate the S-63 Data Protection Scheme and is the only body that can certify the identity of the other participants of the scheme.

The SA is also the custodian of all documentation relating to the S-63 Data Protection Scheme.

### 2.2.2 Data Servers

Data Servers are responsible for the encrypting and signing ENC data in compliance with the procedures and processes defined in the scheme. Data Servers issue ENC licences (permits) so that Data Clients, with valid user permits, can decrypt ENC data.

Data Servers will use the M\_KEY and HW\_ID information, as supplied by the SA, to issue encrypted ENC cell keys to each specific installation. Even though the cell keys used to encrypt each cell are identical, they will be encrypted using the unique HW\_ID and therefore cannot be transferred between other ECDIS from the same manufacturer.

Hydrographic Offices, Value Added Resellers and RENC organisations are examples of Data Servers.

### 2.2.3 Data Clients

Data Clients are the end users of ENC information and will receive protected information from the Data Servers. The Data Client's software application (OEM System) is responsible for authenticating the ENC digital signatures and decrypting the ENC information in compliance with the procedures defined in the scheme.

Navigators with ECDIS/ECS systems are examples of Data Clients.

The scheme does not impede agents or distributors from providing data services to their customers. Agreements and structures to achieve this are outside the scope of this document. This document contains only the technical specifications to produce S63 compliant data services and systems.

### 2.2.4 Original Equipment Manufacturers (OEM)

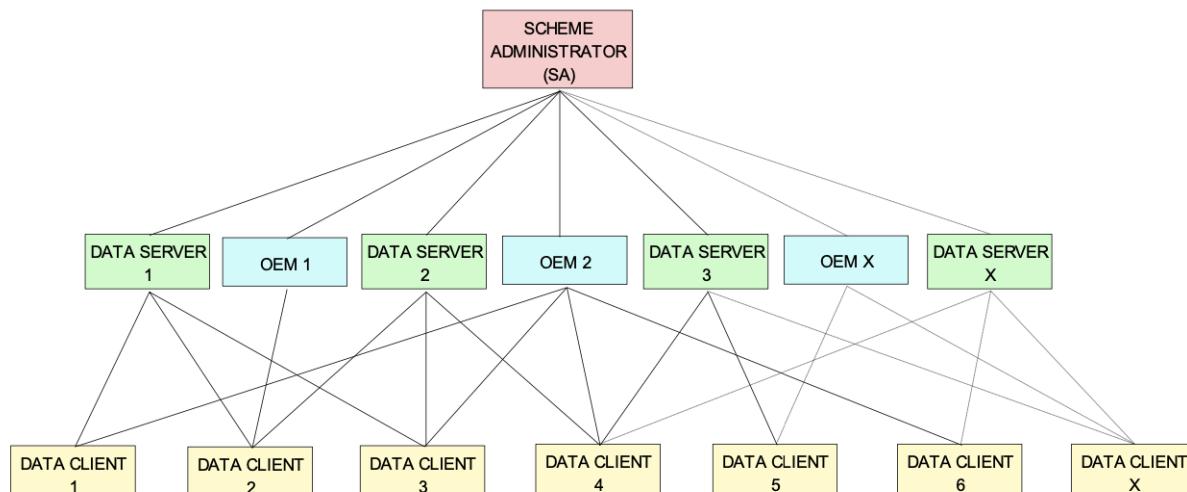
OEMs subscribing to the IHO S-63 DPS must build a software application according to the specifications set out in this document and self-verify and validate it according to the terms mandated by the SA. The S-63 standard contains test data for the verification and validation of OEM applications. The SA will provide successful OEM applicants with their own unique manufacturer key and identification (M\_KEY and M\_ID).

The manufacturer must provide a secure mechanism within their software systems for uniquely identifying each end user installation. The scheme requires each installation to have a unique hardware identifier (HW\_ID).

The software application will be able to decrypt the cell keys using the HW\_ID stored in either the hard lock or soft lock devices attached to or programmed within the application to subsequently decrypt and uncompress the ENC data. The CRC value contained within the ENC [S-57](#) can then be verified to establish the integrity of the underlying S57 data.

### 2.2.5 S-63 Participant Relationships

The Scheme Administrator (SA), of which there can only be one, authenticates the identity of the other participants within the scheme. All Data Servers and System Manufacturers (OEMs) must apply to the SA to become participants in the scheme and, on acceptance, are supplied with proprietary information unique to them. Data Clients are customers of Data Servers and OEMs where Data Servers supply data services and OEMs the equipment to decrypt and display these services.



**Figure 2-1 — IHO S-63 Data Protection Scheme Relationships**

## 2.3 References

- [1] S-57 edition 3.1.0: IHO Transfer Standard for Digital Hydrographic Data, International Hydrographic Organization (<https://ihonet/uploads/user/pubs/standards/s-57/31Main.pdf>).

- [2] NIST FIPS 186 fpd: Digital Signature Standard (DSS), National Institute of Standards and Technology, (<https://csrc.nist.gov/pubs/fips/186/final>).
- [3] NIST FIPS 180-1 fpd: Secure Hash Standard, National Institute of Standards and Technology, (<https://csrc.nist.gov/pubs/fips/180-1/final>).
- [4] ITU-T X.509 (11/1988): The Directory – Authentication framework, International Telecommunication Union (<https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=2999&lang=en>).
- [5] ZIP File Format Specification, PKWare Inc.
- [6] DES Modes of Operation, FIPS Pub 81 ([www.itl.nist.gov/fipspubs/fip81.htm](http://www.itl.nist.gov/fipspubs/fip81.htm))
- [7] IETF RFC 1423: Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers, D. Balenson, RFC Publisher (<https://www.rfc-editor.org/info/rfc1423>).
- [8] Blowfish encryption algorithm, B. Schneier, Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204. ([www.counterpane.com](http://www.counterpane.com))
- [9] ISO/IEC 13239:2002: Information technology — Telecommunications and information exchange between systems — High-level data link control (HDLC) procedures, International Organization for Standardization and International Electrotechnical Commission (<https://www.iso.org/standard/37010.html>).

## 2.4 Compatibility with Previous Versions

This version of S-63 uses the same algorithms and the same file formats and contents as the security scheme operated by Primar, Primar-Stavanger and IHO S-63 Version 1.0. This version of the S-63 standard has been amended to provide better definitions and explanation on the operation of the protection scheme.

A defined test data set has been produced and should be used by OEMs to verify and validate implementations of the S-63 Data Protection Scheme during self certification.

Version 1.1 of the standard has been produced in light of experience gained by Data Servers and ECS/ECDIS Manufacturers during the operation of the scheme under version 1.0. This version attempts to more clearly define the standard by removing duplication and possible ambiguity. It also contains additional mechanisms that will enable manufacturers to make their systems more intuitive for users of ECS/ECDIS. The following list refers to the revisions within the standard.

- 1) Removal of unnecessary duplication
- 2) Specification of how and under what conditions certain files must be used.
- 3) Removal of the permit dependency on the cell edition.
- 4) Additional information to enable Data Clients to manage ENC data more effectively and efficiently.
- 5) Identification of a loading strategy to enable more efficient loading of encrypted ENCs.

It is the responsibility of Data Servers to provide services that are backwardly compatible

## 2.5 Document Structure

The main body of the document can generally be broken down into four parts. The first part details the components that are fundamental to the scheme and describes their purpose and construction. The second identifies how all the components come together within an S-63 ENC Exchange Set. The third outlines the roles and responsibilities of each type of user participating in the scheme. Finally there is a section that defines the various error and warning messages that must be displayed on the data client when defined conditions occur.

### Main Document:

- 1) Scheme Components:

- Section 2: Data Compression
  - Section 3: Data Encryption
  - Section 4: Data Licensing
  - Section 5: Data Authentication
  - Section 6: Data Management
- 2) Exchange Set Format and Structure
- Section 7 Directory and File Structures
- 3) S-63 Participant Processes
- Section 8: Scheme Administrators Processes
  - Section 9: Data Server Processes
  - Section 10: OEM & Data Client Processes
- 4) S-63 Error and Warning Messages
- Section 11 S-63 Error Codes and Explanations

**Additional Sections:**

- S-63 Annex A: Data Server Certificate Request Procedure
- S-63 Annex B: Manufacturer Information Request Procedure
- S-63 Annex C: ENC Update Status Report

**Appendices:**

- Appendix 1: Contains a definition of available test data which can be used to develop full compliance with all aspects of the Data Protection Scheme.
- Appendix 2: Defines how encrypted ENC exchange sets provided by Data Servers will be stored using mass storage devices such as DVD or USB memory sticks.

## 2.6 Maintenance

Changes to this standard will conform to the “*Principles and procedures for making changes to IHO standards and specifications*”, as approved by the 18<sup>th</sup> CHRIS meeting (Cairns, Australia, Sept. 2006).

## 2.7 Support

Support in using and implementing this standard is provided to users by members of the IHO DPSWG, via the IHO Secretariat ([info@ihonet.int](mailto:info@ihonet.int)). In addition an inventory of frequently asked questions (FAQ) is maintained by the IHO Secretariat on the ECDIS section of the IHO website ([www.ihonet.int](http://www.ihonet.int)).

## 3 Data Compression

### 3.1 Overview

An ENC file will, because of its structure, contain repeating patterns of information. Examples of this are the consecutive numbering of the feature object identifier (FOID) or small variations in the co-ordinate information within an ENC file. ENC data therefore responds well to compression with reductions in size of between 30% and 60% reducing greatly the cost of transfer of ENC data to its final destination. Only the ENC files (base and update) are compressed. The ENC files are always compressed before they are encrypted as the effectiveness of any compression algorithm relies on the existence of structured data contents.

### 3.2 Compression Algorithm

The security scheme uses the ZIP algorithm<sup>1</sup> [ZIP File Format Specification](#) to compress and uncompress ENC data. It is identical to the algorithm used in many commercial applications e.g. WinZip, PKZIP. Potential Data Servers and OEMs should be aware that in the past errors have occurred when Data Servers compress data and it is interpreted by popular implementations of the ZIP algorithm as “text” data. If the data is uncompressed with incorrect parameters it can corrupt the ENC file leading to failing integrity checks. Data Servers and OEMs are advised to carefully implement compression/un-compression within their systems.

### 3.3 Compressed Files

The security scheme compresses only the ENC base cell and update files. No other files within the S-57 Exchange Set will be compressed.

## 4 Data Encryption

### 4.1 What Data is encrypted?

Only one encryption algorithm is used within the Scheme. Only the data within the ENC Base or Update Cell files inside an S-57 Exchange Set, i.e. text or image files are left unencrypted. The scheme encrypts the complete content of the ENC Base or Update data files. Other information within the Scheme that is encrypted includes the OEM System HW\_ID which is encrypted and provided to the Data Client in the form of a userpermit.

The cell keys used to encrypt the ENC data files are themselves encrypted by the Data Server and supplied to Data Clients as cell permits. Information about the encryption algorithm is available in [Clause 4.2.3](#).

### 4.2 How is it encrypted?

Each single ENC cell file is encrypted using a unique Cell Key. The same Cell Key is used to encrypt all updates issued for the cell. The scheme however, allows for the cell keys to be incremented and changed at the discretion of the Data Server. The Cell Keys are delivered to Data Clients in the form of cell permits.

#### 4.2.1 Encryption of ENC Information

The ENC information (base cells and updates) are encrypted using a 40-bit key.

#### 4.2.2 Encryption of Other Protection Scheme Information

The Userpermit and the Cell permit contents are encrypted using a 48-bit key.

#### 4.2.3 Encryption Algorithm – Blowfish

The scheme encrypts all information referenced in [Clause 4.1](#) using the Blowfish algorithm [Blowfish encryption algorithm](#). The algorithm is unpatented and available in the public domain ([www.counterpane.com](http://www.counterpane.com)). Blowfish is a block cipher algorithm that operates on 64 bit (8 byte) quantities. It requires that the data sources must be padded if they are not a multiple of 8 bytes. The protection scheme uses the “DES in CBC Mode” padding algorithm defined in [IETF RFC 1423](#) whenever any data sources must be padded. This complies with the ECB (Electronic Code Book) mode of DES [NIST FIPS 81](#).

---

<sup>1</sup> [http://en.wikipedia.org/wiki/ZIP\\_%28file\\_format%29](http://en.wikipedia.org/wiki/ZIP_%28file_format%29)

## 5 Data Licencing

### 5.1 Introduction

Data Clients do not buy ENC data but are licenced to use it. Licensing is the method that Data Servers use to give Data Clients selective access to up-to-date ENC cells for a given period of time.

To operate the scheme effectively there must be a means where Data Client systems can unlock the encrypted ENC cells. To unlock the data the Data Clients system must have access to the cell keys that were used to encrypt the ENC cells. These keys are supplied to the Data Client, encrypted, in a permit file containing a set of cell permits. It is these cell permits that contain the encryption keys.

To make each set of cell permits exclusive the cell keys must be encrypted using something that is unique to the Data Clients system. OEMs assign a unique identifier (HW\_ID) to each of their systems and provide an encrypted copy of this, in the form of a userpermit, to each Data Client. The HW\_ID is stored in the userpermit encrypted.

OEMs encrypt the HW\_ID with their own unique manufacturer key (M\_KEY) so that a HW\_ID cannot be duplicated by another manufacturer. Data Servers have access to the OEM M\_KEYs and can therefore decrypt the HW\_ID stored in the userpermit. Data Servers encrypt their cell keys with the manufacturers HW\_ID when producing a set of cell permits. This makes them unique to the Data Client and as such not transferable between Data Client systems.

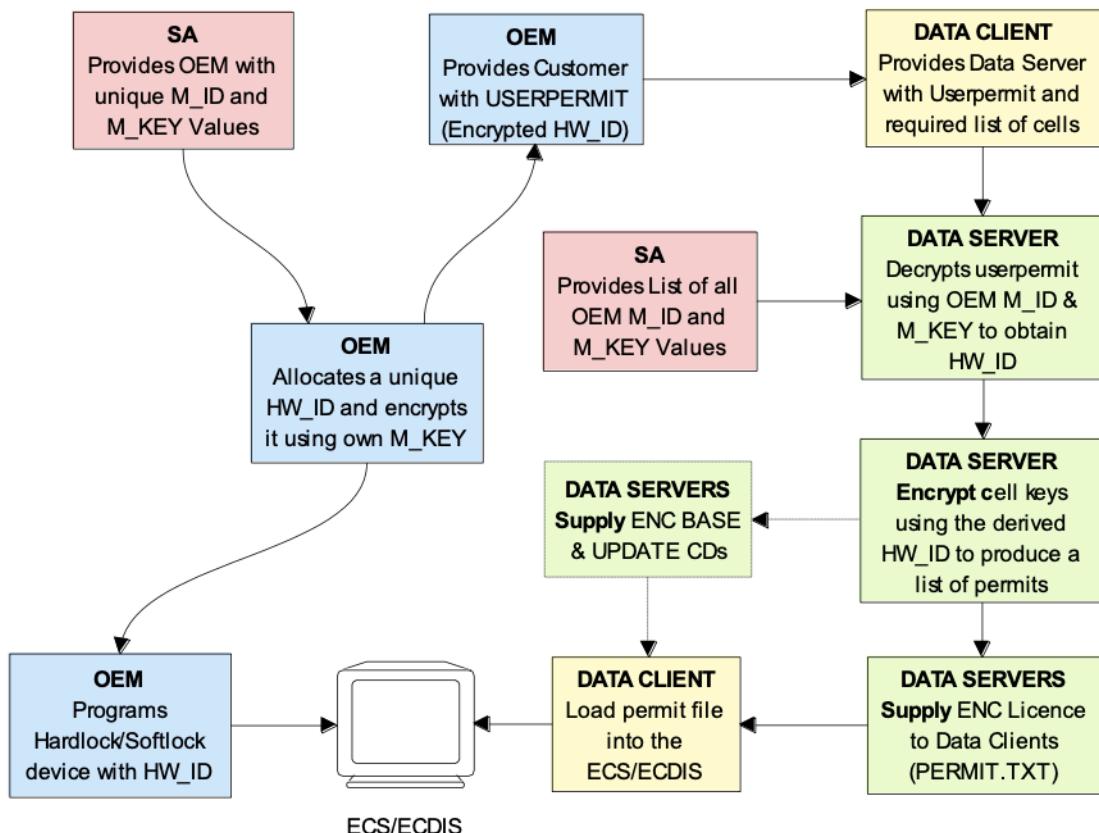


Figure 5-1 — High Level ENC Licensing Diagram

### 5.2 The Userpermit

The userpermit is created by OEMs and supplied to Data Clients as part of their system so that they can obtain the necessary access to encrypted ENCs from Data Servers. The following section defines the composition and format of the userpermit.

All Data Clients with systems capable of using data, protected with the S-63 scheme, must have a unique hardware identification (HW\_ID) built into their end-user system. Such a HW\_ID is often implemented as a dongle or by other means ensuring a unique identification for each installation.

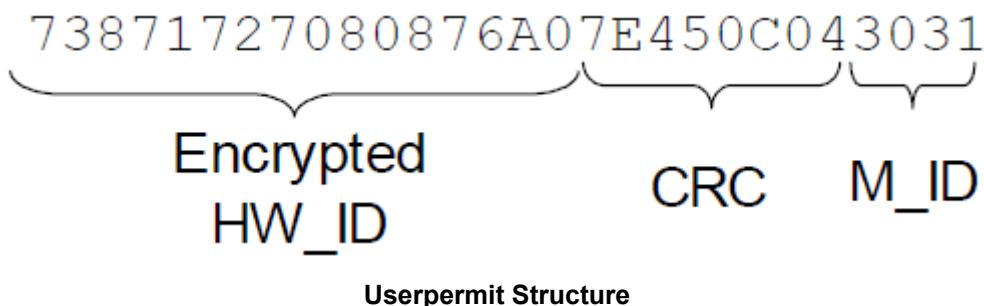
The HW\_ID is unknown to the Data Client, but the OEM will provide a userpermit that is an encrypted version of the HW\_ID and unique to the Data Client's system. The userpermit is created by taking the assigned HW\_ID and encrypting it with the manufacturer key (M\_KEY). The CRC32 algorithm is run on the encrypted HW\_ID and the result appended to it. Finally the manufacturer attaches their assigned manufacturer identifier (M\_ID) to the end of the resultant string. The M\_KEY and M\_ID values are supplied by the SA and are unique to each manufacturer providing S-63 compliant systems.

The Data Client gains access to S-63 encrypted ENCs by supplying this userpermit to the Data Server who can then issue Cell Permits specific to it. Since the userpermit contains the manufacturers unique M\_ID this can be used by Data Servers to identify which M\_KEY to use to decrypt it. The M\_ID is the last four characters of the Userpermit. A list of the manufacturer M\_KEY and M\_ID values is issued and updated by the SA to all Data Servers subscribing to the scheme. This list will be updated periodically as new OEMs join the scheme.

### 5.2.1 Definition of Userpermit

The userpermit is 28 characters long and shall be written as ASCII text with the following mandatory format and field lengths:

Encrypted HW_ID	Check Sum (CRC)	M_ID (Manufacturer ID)
16 hex characters	8 hex characters	4 characters
<hr/>		
Any alphabetic character will be written in upper case.		



### 5.2.2 HW\_ID Format

The HW\_ID is a 5 digit hexadecimal number defined by the OEM manufacturer. Such a HW\_ID can be implemented as a dongle or by other means ensuring a unique identification of each installation<sup>2</sup>. The HW\_ID must be stored within the system in a secure way.

The OEM manufacturer must assign a unique HW\_ID for each installation. It is recommended that the HW\_IDs are not sequential.

The HW\_ID will be stored in an encrypted form in the Userpermit. It is encrypted using the Blowfish algorithm with M\_KEY as the key resulting in a 16 digit (8 bytes) hexadecimal number. The encrypted HW\_ID is then represented in its ASCII form in the userpermit as 16 characters.

Example of HW\_ID is: **A79AB**

Example of encrypted HW\_ID is: **73871727080876A0**

<sup>2</sup> Manufacturers, with the consent of the Data Server, may use the same HW\_ID on more than one unit.

### 5.2.3 Check Sum (CRC) Format

The Check Sum is an 8 character hexadecimal number. It is generated by taking the encrypted HW\_ID and converting it to a 16 character hexadecimal string. It is then hashed using the algorithm CRC32 [ISO/IEC 13239:2002](#) and the 4 bytes converted to an 8 character hexadecimal string.

The Check Sum is not encrypted and allows the integrity of the Userpermit to be checked.

The Check Sum in the above example is: **7E450C04**

### 5.2.4 M\_ID Format

The M\_ID is a 2-character alphanumeric code expressed as ASCII representation provided by the SA. The SA will provide all licenced manufacturers with their own unique Manufacturer Key and Identifier (M\_KEY and M\_ID) combination. The manufacturer must safeguard this information.

The SA will provide all licenced Data Servers with a full listing of all manufacturer codes as and when new manufacturers subscribe to the scheme. This information is used by the Data Server to determine which key (M\_KEY) to use to decrypt the HW\_ID in the Userpermit during the creation of Data Client cell permits.

The M\_ID in the above example is: **01** or **3031** (ASCII<sup>3</sup>)

### 5.2.5 M\_KEY Format

The M\_KEY is a 5 digit hexadecimal number provided by the SA. The OEM uses this key to encrypt assigned HW\_ID when generating userpermits. The OEM must store it securely. This key is used by the Data Server to decrypt assigned HW\_IDs.

Example of M\_KEY is **123AB** or **3132334142** (ASCII)

## 5.3 The Cell Permit

To decrypt an ENC cell the Data Client must have access to the encryption key (see [Clause 4.2](#)) used to encrypt it. Since the encryption keys are only known to the Data Server there needs to be a means of delivering this information to Data Clients in a protected manner. This information is supplied by the Data Server (e.g. RENC or VAR) to the Data Client in an encrypted form known as a cell permit. A single file is provided to deliver the cell permit and is named PERMIT.TXT (see [Clause 5.3.1](#)). This file may contain several cell permits based on the ENC coverage required by the Data Client.

The PERMIT.TXT file will be delivered either on hard media or using online services in accordance with the Data Servers operating procedures. These procedures will be made available to Data Clients when purchasing a licence.

Each cell permit record also contains additional fields that are supplied to assist OEM systems to manage the Data Clients licence and permit files from multiple Data Servers, see [Clause 5.3.3](#).

Data Clients can obtain a licence to access ENCs by supplying the Data Server with their unique userpermit (see [Clause 5.2](#)). Data Servers can then extract the HW\_ID from userpermit, using the Data Client's M\_KEY, and create client specific cell permits based on this value. The format of a cell permit record is described below in [Clause 5.3.2](#) & [Clause 5.3.3](#).

Since Cell Permits are issued for a specific HW\_ID they are consequently not transferable between installations (Data Client Systems). This method of linking the permit to the installation supports the production of generically encrypted CDs which can be distributed to all Data Clients subscribing to a service.

The Data Clients system decrypts the Cell Permit using the assigned HW\_ID stored securely by hardware or software means. The decrypted cell keys can then be used by the system to decrypt the ENC cell.

---

<sup>3</sup> NOTE: The hex encoding may be unfamiliar to some readers. For historical reasons it has been preserved in this version of the standard. “1 2 3 4 5” is translated into “31 32 33 34 35” because the ASCII Base 16 representation of the character “1” is “31” etc. Though confusing at first this convention is used throughout the standard consistently as is standard hexadecimal and binary representations. To differentiate it is referred to as “(ASCII)”

Since several Data Servers can make permit files for ENCs in their service, it is the responsibility of the Data Client system to manage permit files from several Data Servers.

**NOTE** **Data Servers** should continue to provide both types of permit files (ENC.PMT & PERMIT.TXT) as described in S-63 Edition 1.0. This should continue until such time that it can be determined that the omission of the ENC.PMT file will not compromise the safe use of older legacy systems. The timescale for this must be agreed between all stakeholders. **OEMs** must ensure that new implementations of their ECDIS software are able to merge permits from multiple data servers without losing permit information using only the PERMIT.TXT file.

### 5.3.1 The Permit File (PERMIT.TXT)

The Cell Permit will always be provided in a file called PERMIT.TXT, the filename will always be provided in UPPERCASE as will any alphabetic characters contained in the file. The file is completely encoded in ASCII<sup>4</sup> and contains 3 sections as follows:

Section	Description
<b>Header</b>	This includes the file creation date and the format version.
<b>:ENC</b>	ENC permits (official) from the Data Server are listed under this section.
<b>:ECS</b>	ECS permits (non-official) from the Data server can be listed under this section.

The Data Server will make available information regarding how the permit files will be made available whether on hard media or online services. The following table defines the content and format of each section within the permit files separated by "new lines [NL]".

### 5.3.2 The Permit File—Header Formats

The following table defines the content and format of each section header within the permit file.

Section	Fieldname	Value
<b>Date and time</b>	<b>:DATE</b>	The field name, date and time is separated by a space character (SP < h20 > ). The date will be provided as <b>YYYYMMDD</b> and the time as <b>HH:MM</b> using the 24 hour clock. Example: <b>:DATE 20050809 11:11</b>
<b>Meta Permit version</b>	<b>:VERSION</b>	Integer in range 1 to 99. It will be incremented by 1 for each new version of the permit file format specification. S-63 Edition 1.1 defines the value as "2". i.e. <b>:VERSION 2</b>
<b>Cell Permit type</b>	<b>:ENC</b>	Field contains definition of permits available in an ENC distribution license from the Data Server. Field is identified with the following label in upper case <b>:ENC</b>
<b>Cell Permit type</b>	<b>:ECS</b>	Field contains definition of the meta permits available in an ECS distribution license from the Data Server. Field is identified with the following label in upper case <b>:ECS</b>

EXAMPLE: **:DATE 20080809 11:11**

```
:VERSION 2
:ENC
[List of licenced cell permits for official ENCs]
:ECS
[List of licence cell permits for other vector products]
```

---

<sup>4</sup> OEMs should be aware that all ASCII text files generated by the scheme may contain ambiguous end-of-line markers such as CR or CRLF and should be able to deal with these.

### 5.3.3 Permit Record Fields

The Cell Permit Record is comprised of the following comma separated fields:

Field	Value
<b>Cell Permit</b>	As defined in <a href="#">Clause 5.3.4</a> & <a href="#">Clause 5.3.5</a>
<b>Service Level Indicator</b>	0 for subscription permit 1 for single purchase permit
<b>Edition Number [Optional]</b>	DSID-EDTN issue number of the ENC cell (for Data Servers use only)
<b>Data Server ID</b>	This is a two character alphanumeric issued by the SA
<b>Comment</b>	Free text field for comments on the cell permit etc.

NOTE The “Edition Number [Optional]” field is no longer a mandatory requirement in S-63, Edition 1.1. **OEMs** implementing edition 1.1 should no longer build any dependency into their systems that checks the relationship between the edition number of the ENC and cell key used to encrypt it. **Data Clients** should only check to see if there is a valid cell key in the permit string. **Data Servers** will continue to support edition 1.0 PERMIT.TXT files until such time as it can be determined that it is no longer required.

### 5.3.4 Definition of the Cell Permit

The following table defines the fields contained in cell permit with a definition of the purpose of each.

Field	Purpose
<b>Cell Name:</b>	The cell name enables Data Client systems to link the correct encryption key to the corresponding encrypted ENC cell file.
<b>Expiry Date:</b>	This is the date when the Data Clients licence expires. Systems must prevent any new ENC cells, new editions or updates created after this date from being installed.
<b>Encrypted Cell Key 1 (ECK1)</b>	ECK1 contains the decryption key for the current version of the ENC Cell.
<b>Encrypted Cell Key 2 (ECK2)</b>	ECK2 contains the decryption key to be used when the cell key is next iterated. The future key is contained within the cell permit to allow Data Servers to periodically change the Cell Key without simultaneously issuing new cell permits to all Data Clients.
<b>Check Sum (CRC)</b>	This value is provided to protect against tampering or accidental corruption.

### 5.3.5 Cell Permit Format

The Cell Permit shall be written as ASCII text with the following mandatory format and field lengths:

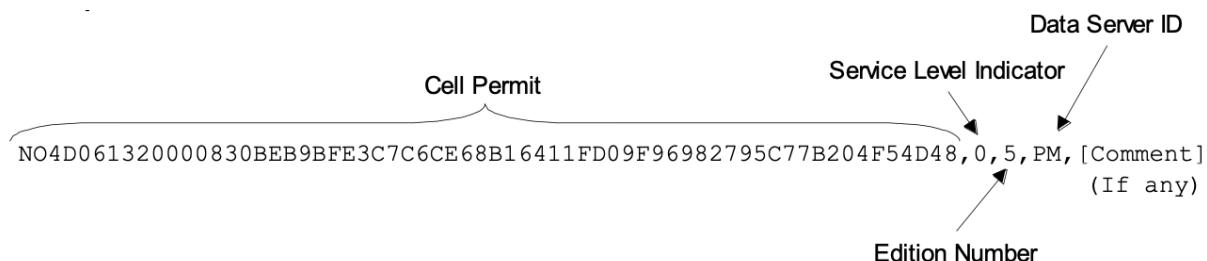
Field	Characters	Format
<b>Cell Name</b>	8	An alphanumeric string following the convention defined in S-57 Edition 3.1 Appendix B section 5.6 for cell names excluding the filename extension. Example is: NO4D0613
<b>Expiry Date</b>	8	A numeric string that contains the license expiry date for each ENC in the format YYYYMMDD. Example is: 20000830 (30 <sup>th</sup> August 2000)
<b>ECK1 &amp; ECK2<sup>a</sup></b>	16	The Cell Keys are 5 byte random numbers – their hex representations are encrypted using Blowfish and then expressed in hexadecimal in the permit. NOTE: The blowfish encryption algorithm will cause the encrypted data to be padded to a multiple of 8 bytes in length. This means that encrypted Cell Keys are actually 8 bytes long, even though unencrypted they are only 5 bytes long (10 hex characters) Example:

Field	Characters	Format
		ECK1: BEB9BFE3C7C6CE68 ECK2: B16411FD09F96982
<b>ENC Permit Checksum</b>	16	Contains the encrypted check sum for the Cell Permit. It is encrypted using the Blowfish algorithm with the Data Client's specific HW_ID and is an 8 byte number. This check sum is encrypted as opposed to the unencrypted check sum of the User Permit. e.g. The ENC Check Sum in the example below is: <b>795C77B204F54D48</b>
<sup>a</sup> The cell permit contains two fields for providing the data client system with the cell keys necessary to decrypt a specific ENC cell file. These fields may contain either two identical cell keys or two different cell keys and may differ between data servers. Some data servers may prefer to increment the cell keys only in the event of the security scheme is compromised others may prefer to periodically increment them according to their service procedures. The mechanism for data servers producing these keys is described in more detail in <a href="#">Clause 10.5.1</a> . OEMs should note that any dependency on the edition number should be removed from theirs systems in edition 1.1 of the scheme.		

NO4D061320000830BEB9BFE3C7C6CE68B16411FD09F96982795C77B204F54D48

Cell Name	Expiry Date	Encrypted Cell Key 1	Encrypted Cell Key 2	Check Sum (CRC)
-----------	-------------	----------------------	----------------------	-----------------

#### Cell Permit Field



#### Cell Permit Record

##### 5.3.6 Additional Licence File (Optional)

Data Servers may wish to include an additional file, along with the PERMIT.TXT file, to identify the licensee and provide information relating to system ID<sup>5</sup>. This file will be named \*\*.LIC, where \*\* represents the data server ID.

Data client systems can access this file (if present) to display user information and provide userpermit information.

The file contains a single record with the following fields:

Field ID	Characters	Notes
Licensee	40	Name of company or individual signing the licence.
Vessel Name	40	Optional. This field may be left as spaces.
Fixed Site #1	240	Company Name and Address. This field contains free format text arranged in 6 x 40 byte sub-fields. Text will not cross the boundaries of the sub-fields.

<sup>5</sup> It may be useful when processing data client queries to have instant access to customer information such as licencing information and manufacturer ID. Data clients could supply this file with the query to speed up response times.

Field ID	Characters	Notes
Host System Name	40	For instance, Main, Backup, etc.
User Permit	28	Hexadecimal user permit
Licence Type	40	Service Indicator, e.g. Primar Stavanger ENC Service
HO data	36	Data for HO / Agent / Distributor use.
Total number of bytes: 464		

## 6 Data Authentication

### 6.1 Introduction to Data Authentication and Integrity Checking

The digital signature technique used in the S-63 scheme uses a standard algorithm and key exchange mechanism widely used. S63 digital signatures use asymmetric public key algorithms within a PKI-like infrastructure scheme to unbreakably bind a data file with the identity of the issuer.

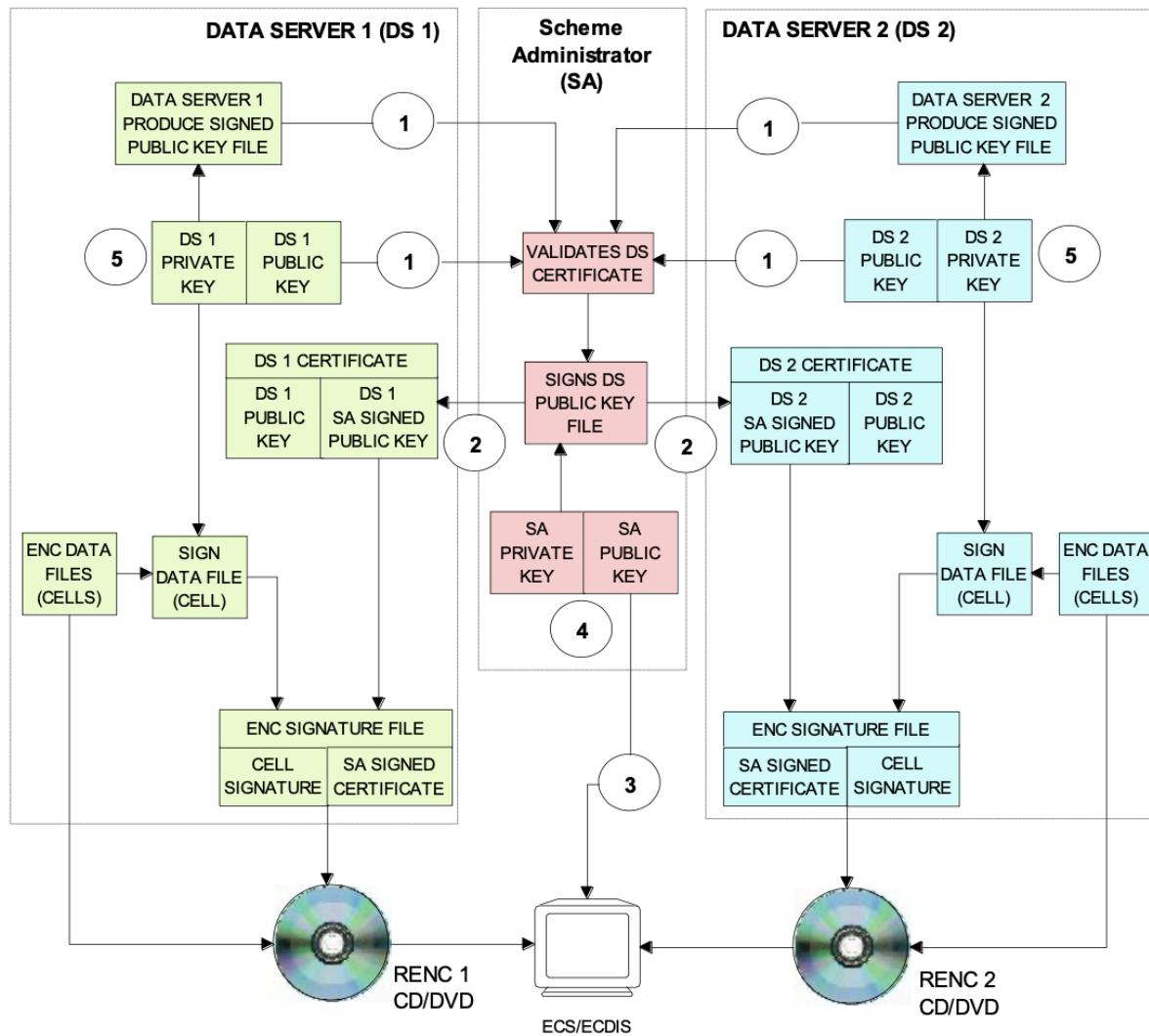
The scheme relies on asymmetric encryption<sup>6</sup> of a checksum of a data file. By verifying the signature against the issuer's public key, and also verifying the issuer's public key against a top level identity the user is assured of the signer's identity. A detailed explanation digital signatures is beyond the scope of this document and the reader is referred to the Digital Signature Standard (DSS), FIPS Pub 186 ([www.itl.nist.gov/div897/pubs/fip186.htm](http://www.itl.nist.gov/div897/pubs/fip186.htm)) for a more detailed and accessible explanation.

The scheme can be considered to have three distinct phases:

- 1) A Scheme Administrator (SA) verifies the identity of a supplier of ENC information and provides the supplier with data to allow them to sign ENC data.
- 2) A Data Server (e.g. RENC or VAR) issues ENC data signed with their identity (and its verification by the SA).
- 3) The subsequent verification by the Data Client of the Data Server's identity (by its association with the SA) and the integrity of the ENC data.

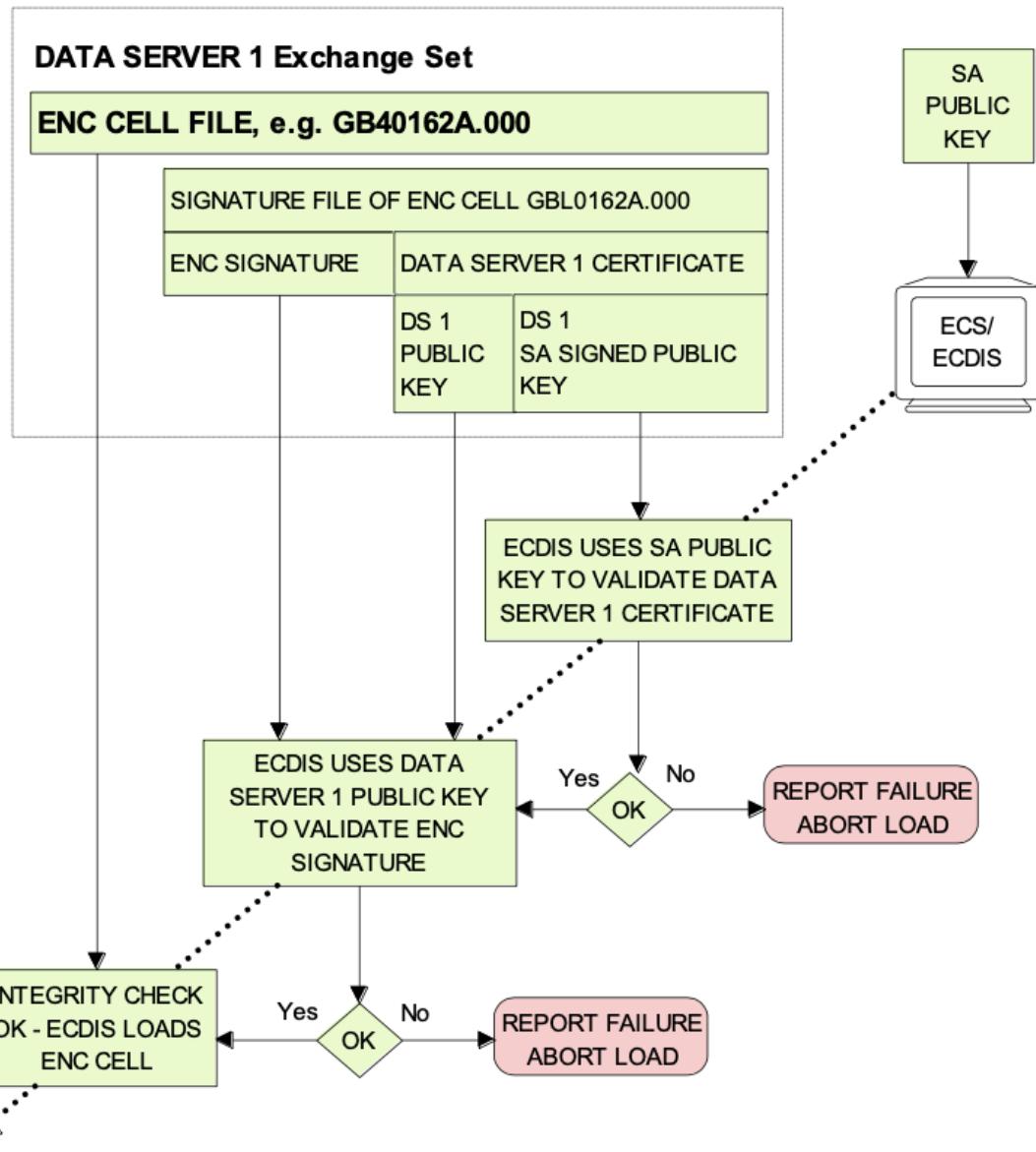
---

<sup>6</sup> Asymmetric cryptography relies on algorithms where encryption and decryption take place with different cryptographic keys. Therefore one person can encrypt data and make available a decryption key for others to decrypt it. These keys are referred to as the "private key" and the "public key", collectively known as a "key pair"

**NOTE**

- 1) The Data Server's Public Key and Self Signed Key (SSK) File are sent to the SA for validation when applying to join the IHO S-63 Data Protection Scheme.
- 2) If accepted the SA signs the Data Server's SSK with its own private key to produce a SA signed Data Server Certificate which is then returned to the Data Server.
- 3) The SA Public Key is widely distributed and installed independently in OEM systems.
- 4) SA Public and Private Key pairs must be different from all other Data Servers.
- 5) All Data Server Public and Private Keys must be unique to each other and the SA.

**Figure 6-1 — ENC AUTHENTICATION PROCESSES**



**NOTE** If an ECS/ECDIS is using the method depicted above, and if the SA Key Pair is different from the Data Server key pair, then it is able to authenticate and validate ENCs from Data Server 2 (or any other Data Server in the scheme) using the same SA public key.

- 1) **Authentication** : The ECS/ECDIS uses the SA public key, previously installed independently of the CD, to check the certificate part of the signature file to confirm that the supplier's public key in the certificate is valid. That is, the Data Server is a bona fide member of the scheme
- 2) **Integrity Check**: The ECS/ECDIS uses the public key from the certificate to check the signature of the ENC cell (data) file.

**Figure 6-2 — Data Authentication and Integrity Checking**

#### 6.1.1 SA Verification

The ECDIS needs to be able to verify that the ENCs are from a bona fide source. It does this by ensuring that the data server's public key provided within the ENC signature files can be validated against the SA's public key.

The SA provides certificates to each data server in the scheme; each certificate is unique, the SA only has to do this task once for each data server when they join the scheme. To obtain a certificate, data servers generate a key pair and provide the SA with their public key (as a self signed certificate); the SA (using their existing key pair) uses their private key to sign the data server's public key. The resulting

certificate contains a signature of the supplier's public key. This certificate is then included within all ENC cells' and updates' signature files.

The SA makes their own public key widely known to the ECDIS community and OEMs should provide a means for the user to load this independently of the data.

### 6.1.2 Data Integrity

After the source of the ENC exchange set has been authenticated the ECDIS then checks data integrity by validating the signature file provided for each ENC by the data server.

The data server creates a signature file for each cell which consists of the following two parts:

- The signature of the dataset [which is created using the data server's private key, half of the data server key pair (in essence this is an encrypted checksum of the data) and is different for each cell]
- Their Data Server certificate (which remains constant).

The ECDIS uses the data server's public key that is included in the certificate to validate the data file signature (it decodes this data file signature and compares the checksum against the ENC cell). If this validation check is successful then it proves that the ENC has not been corrupted in any way and that the identity of the Data Server within the cell signatures is validated by the SA.

## 6.2 Digital Certificates (SA Authentication)

Certificates are digital files issued by a certification authority. They bind a specific public key together with other information to an individual or organisation. Certificates help prevent someone from using a fake public key to impersonate someone else. The scheme uses a chain of certificates, each one certifying the previous one until all parties are confident as to the identities in question. The SA certificate used by the IHO will be a self signed certificate<sup>7</sup> and is the **root certificate** for the scheme.

The SA will issue a digital certificate to all approved Data Servers by signing the Data Server's verified public key file. The following list of high level operations is performed in the issuing of digital certificates.

### Scheme Creation

- SA creates a unique top level public and private key pair.

### Establishment of a Data Server

- Data Server creates a unique public and private key pair.
- Data Server creates a Self Signed Key (SSK) by signing own public key file with own private key.
- Data Server supplies the SSK to the SA by a trusted means.
- SA verifies the Data Server's SSK using the Data Server's public key.
- SA signs the verified Data Server public key file using the SA private key.
- SA supplies the Data Server with its own unique SA signed Data Server Certificate.

### Creation of Signed Data Sets

- Data Server verifies the resultant certificate with the SA public key (supplied separately).
- Data Server stores verified certificate and uses it in the creation of ENC signature files.

The format of the various files, certificates and signatures are described in more detail in [Clause 6.4](#).

**NOTE the SA public key is made widely available to all interested parties, e.g. Data Servers, Data Clients and OEMs, in a number of ways, e.g. web, e-mail, etc.**

---

<sup>7</sup> The SA public key signed using the SA private key.

### 6.2.1 The SA Public Key

The scheme requires that the SA public key is installed on the Data Client's systems independently of the ENC exchange set. This can be pre-installed by the OEM. However, the Data Client system must have a method of installing a new public key<sup>8</sup> on the system in the case where a new one is issued by the SA.

If the user installs a new SA certificate or public key the system must confirm that a new one has been installed. If installing a new SA certificate (IHO.CRT) the system must inform the user as follows:

***"A new SA certificate (public key) has been installed this is valid to [enter expiry date] or unless the SA issues a new one for security reasons."***

If installing a new SA public key (IHO.PUB) the system must inform the user as follows:

***"A new SA public key has been installed this is valid until the SA routinely issues a new one or unless one is issued for security reasons."***

Should the system report an authentication error during the loading process it should alert the user to the possibility that the SA may have changed the public key. Therefore a warning message must be displayed explaining the reason for this as follows:

***"SSE 06 – The SA Certificate/Public Key is invalid. The SA may have issued a new public key or the ENC may originate from another service. A new SA public key can be obtained from the IHO website or from your distributor."***

### 6.2.2 New Data Servers

The IHO, in conjunction with the DPSWG, will establish the identity of any organisation or commercial company wishing to join the protection scheme as a Data Server. If the SA revokes a Data Server Certificate, it will inform all Data Servers and Manufacturers about the change.

## 6.3 Digital Signatures (Verify Data Integrity)

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and to ensure that the original content of the sent message is unchanged. Digital signatures are portable, easily verified and cannot be forged.

It is also acceptable for Hydrographic offices or other Data Server organisations (e.g. RENC/VAR) to use digital signatures to maintain provenance and data integrity between them in the delivery of ENC information. Each ENC file (both base and update files) will always have a single unique signature file associated with it. No other files in an encrypted ENC exchange set have a digital signature.

NOTE An exchange set may contain signatures issued by different data servers and therefore each ENC file must be authenticated individually.

### 6.3.1 Technical Overview of Digital Signatures

Data authentication is provided using a digital signature compliant with the Digital Signature Standard (DSS) [NIST FIPS 186 fpd](#). The DSS uses the Secure Hash Algorithm (SHA-1) [NIST FIPS 180-1 fpd](#) to create a message digest (hash). The message digest is then input to the Digital Signature Algorithm (DSA) [NIST FIPS 186 fpd](#) to generate the digital signature for the message using an asymmetric encryption algorithm and the 'private key' of a key pair. Asymmetric algorithms have the property that data encrypted using the 'private key' of the key pair can only be decrypted using the 'public key' of the key pair.

A consequence of encrypting the message digest with the private key is that anyone who has the public key (which as its name suggests can be made public) can decrypt and verify the message digest. Further information on Digital Signatures and their use may be obtained from the IHO website ([www.ihonet.org](http://www.ihonet.org)).

---

<sup>8</sup> It is envisaged that data servers will supply this independently of the exchange set to coincide with data that authenticates against the new public key.

### 6.3.2 ENC Signature File Naming Convention

The digital signature file will match the cell file name except that the navigational purpose codes, digits 1–6, will be replaced by the characters I – N.

#### In general:

ENC file: CC [1–6] XXXXX.EEE (see S-57 Appendix B1)

Signature file: CC [I–N] XXXXX.EEE

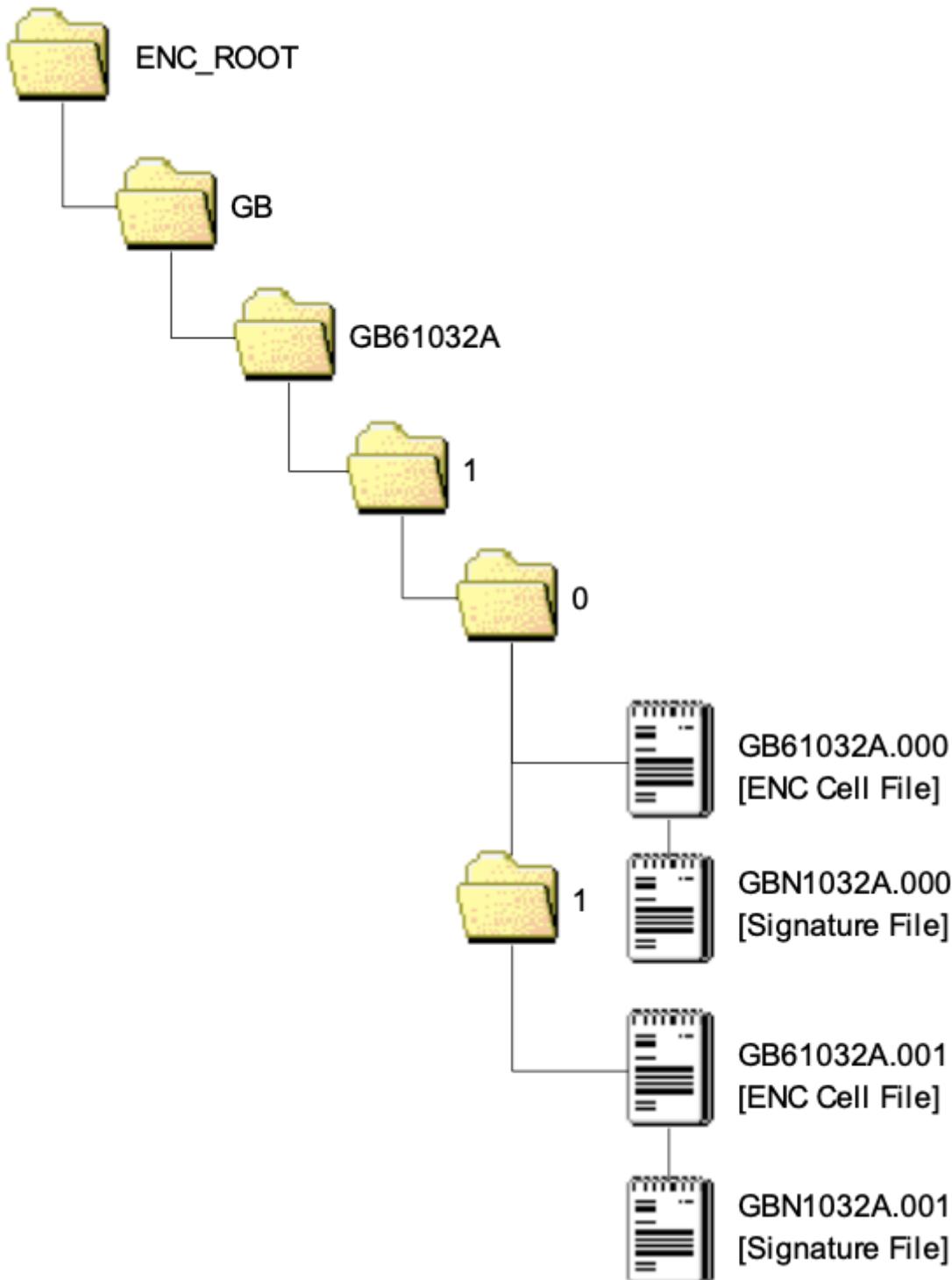
Navigational Purpose	Signature Character
1. Overview	I
2. General	J
3. Coastal	K
4. Approaches	L
5. Harbour	M
6. Berthing	N

EXAMPLE: Cell file GB100001.000 will have a signature file named GBI00001.000

Cell file GB61032A.002 will have a signature file named GBN1032A.002

### 6.3.3 Storage of the ENC Signature File

The ENC signature file must be uniquely identifiable as belonging to a particular ENC data file as outlined in [Clause 6.3.2](#) above. The digital signature file will always be located in the same directory as the ENC cell file that it relates to, as illustrated in [Figure 6-3](#).



**Figure 6-3 — ENC DIGITAL SIGNATURE FILES PLACEMENT**

#### 6.4 Data Authentication File Formats

There are a number of files associated with the authentication processes within the S-63 Data Protection Scheme. Among these are the certificate and signature files, as described in [Clause 6.2](#) & [Clause 6.3](#) and the private and public keys created to sign and authenticate them. Although these may be derived independently the various component parts contained within each file share common elements that are always formatted in the same way. The following table lists the files that are fundamental to the

authentication of S-63 encrypted ENCs. This table also identifies those participants of the scheme who create them.

File Types	Scheme Administrator	Data Server
PQG File	✓	✓
Private Key (X file)	✓	✓
Public Key (Y file)	✓	✓
X509 v3 Certificate	✓	✗
Self Signed Key (SSK)	✗	✓
Certificate	✓	✗
Signature	✗	✓

#### 6.4.1 File Elements

All elements comprise of two parts, a header and a data string. The following table lists all the possible elements that may go to make up a particular file, certificate or signature:

Element	Header	Data String
R	// Signature part R:	10 blocks of 4 characters.
S	// Signature part S:	10 blocks of 4 characters.
p	// BIG p	32 blocks of 4 characters.
q	// BIG q	10 blocks of 4 characters.
g	// BIG g	32 blocks of 4 characters.
x	// BIG x	10 blocks of 4 characters.
y	// BIG y	32 blocks of 4 characters.

##### 6.4.1.1 Element Header and Data String Formatting

Each data string:

- Is preceded by a single header line. Header lines are indicated by two forward slashes (// ASCII—0x2F2F) at the start followed by a space (SP ASCII 0x20) and the header characters in ASCII text as per the format descriptions below..
- Is expressed in ASCII text hexadecimal digits (0-9, A-F). Any alphabetic character will be in upper case.
- Is terminated by a full stop (. ASCII 0x2E).
- Has a space (ASCII SP 0x20) separating each group of 4 characters.
- Has a Carriage Return (ASCII CR 0x0D) and New Line (ASCII LF 0x0A) at the end of each data string.

#### 6.4.2 Examples of File, Certificate and Signature Formats

The following section includes a set of examples of all the various files associated with this aspect of the S-63 Data Protection Scheme. A detailed explanation of how these files are created is outlined later in this document.

##### 6.4.2.1 PQG Format

The PQG parameters are produced from a random string and are used in the creation of the X and Y private/public key pairs. After these have been made, the PQG parameters will be contained within the X and Y private/public key pairs.

P, Q and G are numerical parameters used in the Digital Signature Algorithm as input to the key creation process. Each data server can use a different set of P, Q and G or use an existing set to generate random key pairs. The Digital Signature Standard [NIST FIPS 186 fpd](#) describes their derivation and use.

**EXAMPLE — Example of PQG Format:** // BIG p

```
D0A0 2D76 D210 58DA 4D91 BBC7 30AC 9186 5CB4 036C CDA4 6B49 4650 16BB 6931 2F12
DF14 A0CC F38E B77C AD84 E6A1 2F2A A0D0 441A 734B 1D2B E944 5D10 BA87 609B 75E3.

// BIG q
8E00 82E3 C046 DFE6 C422 F44C C111 DBF6 ADEE 9467.

// BIG g
B08D 786D 0ED3 4E39 7C6B 3ACF 8843 C3BF BAB1 A44D 0846 BB2A C3EE D432 B270 E710
E083 B239 AF0E A5B8 693B F2FC A03B 6A73 E289 84FF 8623 1394 996F 6263 0845 AA94.
```

#### 6.4.2.2 The X (Private Key) Format

The X file can be written as ASCII text in the following format:

**EXAMPLE:** // BIG p

```
D0A0 2D76 D210 58DA 4D91 BBC7 30AC 9186 5CB4 036C CDA4 6B49 4650 16BB 6931 2F12
DF14 A0CC F38E B77C AD84 E6A1 2F2A A0D0 441A 734B 1D2B E944 5D10 BA87 609B 75E3.

// BIG q
8E00 82E3 C046 DFE6 C422 F44C C111 DBF6 ADEE 9467.

// BIG g
B08D 786D 0ED3 4E39 7C6B 3ACF 8843 C3BF BAB1 A44D 0846 BB2A C3EE D432 B270 E710
E083 B239 AF0E A5B8 693B F2FC A03B 6A73 E289 84FF 8623 1394 996F 6263 0845 AA94.

// BIG x
EBAF 2948 1485 7E7C 2F48 C7B2 9334 2F09 DA1A EB04.
```

#### 6.4.2.3 The Y (IHO or Data Server Public Key) Format

Both the SA and Data Server public key are provided in the following format, the scheme uses a DSA Public Key of length 512 bits.

**EXAMPLE:** // BIG p

```
D0A0 2D76 D210 58DA 4D91 BBC7 30AC 9186 5CB4 036C CDA4 6B49 4650 16BB 6931 2F12
DF14 A0CC F38E B77C AD84 E6A1 2F2A A0D0 441A 734B 1D2B E944 5D10 BA87 609B 75E3.

// BIG q
8E00 82E3 C046 DFE6 C422 F44C C111 DBF6 ADEE 9467.

// BIG g
B08D 786D 0ED3 4E39 7C6B 3ACF 8843 C3BF BAB1 A44D 0846 BB2A C3EE D432 B270 E710
E083 B239 AF0E A5B8 693B F2FC A03B 6A73 E289 84FF 8623 1394 996F 6263 0845 AA94.

// BIG y
444B BA17 1758 0DAF 71AB 52A5 6CCA 8EAB 4C51 E970 0E37 B17B BB46 C0B9 4A36 F73F
0244 7FBF AE5B 7CA9 3870 5AB9 E9EE 471C E7B0 1004 6DF1 3505 42B3 0332 AE67 69C6.
```

#### 6.4.2.4 The SA Digital Certificate (X509v3) Format

The SA Digital Certificate will be in X509v3 format [ITU-T X.509 \(11/1988\) / ISO 9594-8](#) and represents a DSA Public Key of length 512 bits. The SA Digital Certificate will always be available in a file called IHO.CRT. The IHO.CRT file is available from IHO at [www.ihoint](http://www.ihoint).

All Data Servers providing an ENC service may include the SA certificate, for reference in the root directory of the media (e.g. in D:\IHO.CRT on a CD-ROM) but, as stated in [Clause 6.2.1](#), the installation on a Data Client's system of the SA certificate should be done independently. The check of the validity of the SA signature against each ENC signature must be done from the independently installed version of the SA certificate.

The SA public key in ASCII format (as opposed to the binary X509v3 format) is also made available on the IHO website at [www.ihoint](http://www.ihoint) (the format is described in [Clause 6.4.2.3](#)).

#### 6.4.2.5 The Self Signed Key (SSK) Format

This is the file format that the Data Server uses to sign its own public key before sending to the SA for signing. The signature is the signature of the whole public key file (i.e. the PQG and Y parameters).

```

// Signature part R:
752A 8E5C 3AF5 6CCD 7395 B52E F672 E404 554F AAB6.
// Signature part S:
1756 E5C0 F4B6 BC90 4EC6 5F94 DF93 3ADF 68B8 86C4. } Single Signature Element
Data Server (DS) Signature of DS Public Key

// BIG p
D0A0 2D76 D210 58DA 4D91 BBC7 30AC 9186 5CB4 036C CDA4 6B49 4650 16BB 6931 2F12
DF14 A0CC F38E B77C AD84 E6A1 2F2A A0D0 441A 734B 1D2B E944 5D10 BA87 609B 75E3.

// BIG q
8E00 82E3 C046 DFE6 C422 F44C C111 DBF6 ADEE 9467.

// BIG g
B08D 786D 0ED3 4E39 7C6B 3ACF 8843 C3BF BAB1 A44D 0846 BB2A C3EE D432 B270 E710
E083 B239 AF0E A5B8 693B F2FC A03B 6A73 E289 84FF 8623 1394 996F 6263 0845 AA94.

// BIG y
444B BA17 1758 0DAF 71AB 52A5 6CCA 8EAB 4C51 E970 0E37 B17B BB46 C0B9 4A36 F73F
0244 7FBD AE5B 7CA9 3870 5AB9 E9EE 471C E7B0 1004 6DF1 3505 42B3 0332 AE67 69C6.

```

Data Server Public Key File

Data Server Public Key

The DS Signature is authenticated by the SA against the DS supplied Public Key

#### 6.4.2.6 The SA Signed DS Certificate File Format

This is the file format used by the SA when it issues a Data Server Certificate file. The SA also uses a DSA Public Key of length 512 bits. The R & S pair is what is transcribed into the Data Server's ENC signature files.

```

// Signature part R:
6FD6 2AC7 27D2 8D0B CD27 BDF2 5CC6 9656 10E3 751F. } Single Signature Element
// Signature part S:
3DE7 DA37 5A40 80FC 4203 5C6E 37DE A984 2A88 2BDC. } SA Signature of DS Public Key

// BIG p
D0A0 2D76 D210 58DA 4D91 BBC7 30AC 9186 5CB4 036C CDA4 6B49 4650 16BB 6931 2F12
DF14 A0CC F38E B77C AD84 E6A1 2F2A A0D0 441A 734B 1D2B E944 5D10 BA87 609B 75E3.

// BIG q
8E00 82E3 C046 DFE6 C422 F44C C111 DBF6 ADEE 9467.

// BIG g
B08D 786D 0ED3 4E39 7C6B 3ACF 8843 C3BF BAB1 A44D 0846 BB2A C3EE D432 B270 E710
E083 B239 AF0E A5B8 693B F2FC A03B 6A73 E289 84FF 8623 1394 996F 6263 0845 AA94.

// BIG y
444B BA17 1758 0DAF 71AB 52A5 6CCA 8EAB 4C51 E970 0E37 B17B BB46 C0B9 4A36 F73F
0244 7FBD AE5B 7CA9 3870 5AB9 E9EE 471C E7B0 1004 6DF1 3505 42B3 0332 AE67 69C6.

```

Data Server Public Key File

Data Server Public Key

SA Signed Data Server Certificate

The SA Signature is authenticated by the SA Public Key held in the ECS/ECDIS

#### 6.4.2.7 The ENC Signature File Format

The signature file must contain a signature and certificate pair. A file with just a signature is invalid as it does not certify the Data Server's identity. The ENC digital signature file has format, structure and order as in the following example:

```

// Signature part R:
77D3 4D86 DA6E 6E01 7058 7140 74FC 7E3D 21CD E80B.
// Signature part S:
04A1 7B52 081F B6CE 10FE 5AD9 1CCE 3F25 FEAC DA05.
// Signature part R:
8FD6 2AC7 27D2 8D0B CD27 BDF2 5CC6 9656 10E3 751F.
// Signature part S:
3DE7 DA37 5A40 80FC 4203 5C6E 37DE A984 2A88 2BDC.
// BIG p
D0A0 2D76 D210 58DA 4D91 BBC7 30AC 9186 5CB4 036C CDA4 6B49 4650 16BB 6931 2F12
DF14 A0CC F38E B77C AD84 E6A1 2F2A A0D0 441A 734B 1D2B E944 5D10 BA87 609B 75E3.
// BIG q
8E00 82E3 C046 DFE6 C422 F44C C111 DBF6 ADEE 9467.
// BIG g
B08D 786D 0ED3 4E39 7C6B 3ACF 8843 C3BF BAB1 A44D 0846 BB2A C3EE D432 B270 E710
E083 B239 AF0E A5B8 693B F2FC A03B 6A73 E289 84FF 8623 1394 996F 6263 0845 AA94.
// BIG y
444B BA17 1758 0DAF 71AB 52A5 6CCA 8EAB 4C51 E970 0E37 B17B BB46 C0B9 4A36 F73F
0244 7FBD AE5B 7CA9 3870 5AB9 E9EE 471C E7B0 1004 6DF1 3505 42B3 0332 AE67 69C6.

```

The diagram illustrates the structure of the IHO Data Protection Scheme. It shows two sets of signature pairs (R & S) and their corresponding public keys. The first set of signatures (R & S) is associated with the 'Data Server Public Key' and is used to verify the Data Server's digital certificate. The second set of signatures (R & S) is associated with the 'SA Public Key' and is used to verify the SA digital certificate. The 'Data Server Public Key' and 'SA Public Key' are both contained within the 'Data Server Public Key File'. The 'Data Server Public Key File' and the 'SA Signed Data Server Certificate' are grouped together under the heading 'SA Signed Data Server Certificate'.

The first Signature/R & S Pair is authenticated by the Data Server's Public Key

The second Signature/R & S Pair is authenticated by the SA Public Key stored in the ECS/ECDIS

The second R and S pair is used to authenticate the Data Server digital certificate (p, q, g and y strings). If verified successfully, the Data Server public key (y string) can be extracted and used to verify the digital signature (first R and S pair) of the encrypted ENC. This allows the Data Client to verify the SA digital certificate, to extract the Data Server public key, and to verify the digital signature of the ENC data.

## 7 Data Management

### 7.1 Introduction

The loading and import of ENCs to an ECS/ECDIS must be carefully managed; this is especially true in a multiple Data Server environment. Since the scheme encrypts the entire contents of an ENC cell file (base and update), this restricts access to certain subfields in an ENC cell file required by OEM systems to manage the import of ENCs to the ECS/ECDIS SENC. As a consequence additional S-63 files are necessary to supplement this inaccessible data as well as modification to an existing S-57 file, i.e. the CATALOG.031 file.

It has also been identified that the import of large numbers of ENCs has rendered some aspects of S-57 impractical to implement, e.g. a single exchange set split across multiple media volumes. For this reason it has been necessary to modify the loading strategy and utilise the additional S-63 files to better manage the installation and loading of ENCs across multiple exchange sets.

As mentioned previously S-63 is designed to operate in a multiple data supplier environment. S-57 does not have a mechanism to discriminate between ENC exchange sets supplied by different data servers and therefore it has been necessary to cater for this in version 1.1 of this standard.

ENC updates are compiled in accordance with IHO S-57. In order to assist end users in the management of their updates S-63 defines certain files which can assist an ECDIS in informing users of the revision status of their ECDIS. In addition to loading and installation functionality ECDIS manufacturers also are required to implement a report called the ENC update status report, fully defined at Annex C, which lists ENCs loaded into the SENC and their revision information as distributed by a data server.

The content delivered in the additional S-63 files contain important information that, make the S-57 import process more efficient and intuitive for the Data Client and which help meet standard functionality required by the IMO Performance Standard. These files and their use are defined in this section.

The loading/import method can be broken down into the following processes:

- Manage the import of Data Server specific ENC exchange sets using the Data Server ID.
- Manage a Data Server's service if extended across multiple exchange sets.

- Manage the import of licenced ENC cells in a contiguous manner, ensuring all ENC base cells and corresponding update files, if any, are imported correctly and sequentially.
- Manage the import of text and picture files by maintaining a relationship between them and the cell file they are associated with.

The following table lists the additional S-63 files and file modifications together with their main purpose within S-63. These files and their associated formats are described in more detail at [Clause 7.2](#), [Clause 7.3](#) & [Clause 7.4](#).

File/Field	Primary Management Function
<b>PRODUCTS.TXT</b>	Required to provide the following information: 1. The Issue Date of the Products File being installed. 2. A catalogue of all available cells in a Data Server's service. 3. The coverage of all available cells in a service. 4. The latest Issue Date of all available cells in a service (including cancelled cells). 5. The destination exchange set (base or update) where the ENC base cell file (EN Application Profile) resides. This may be a base cell, new edition or re-issue.
<b>SERIAL.ENC</b>	Required to provide the following information: 1. The Data Server ID. 2. The Exchange Set week number and date of issue. 3. Type of Exchange Set (base or update) 4. The Exchange Set number in a multiple series.
<b>CATALOG.031 [CATD-COMT]</b>	Required to provide information originally contained in the DSID field of the cell file to import the complete, sequential content of an exchange set.

## 7.2 ENC Product Listing (PRODUCTS.TXT)

The file named 'PRODUCTS.TXT' will be supplied with each encrypted exchange set and will be stored in a folder named 'INFO' held in root directory. It is the mechanism for managing data within an ENC Service and exchanging it with data already held in the Data Client's system SENC. The structure and format of this file is described in more detail in [Clause 7.2.1](#), [Clause 7.2.2](#), [Clause 7.2.3](#) & [Clause 7.2.4](#).

There are two types of PRODUCTS.TXT file, "PARTIAL" and "FULL". A partial products listing contains the current status of all ENCs contained in a single exchange set. A full product listing contains the current status of ALL cells in a Data Server's service, that is, all exchange sets. Although procedures may vary between Data Servers a full product listing will always be provided with the weekly update exchange set. In instances where a Data Server issues a complete set of new base media (no weekly update), each base media must contain a full product list of all ENCs in a service

NOTE OEMs should ensure that their systems are able to handle "FULL" and "PARTIAL" product listings ([Clause 7.2.2](#) refers). Base CDs may contain a partial listing with only the contents of the CD included. The Update will always carry a full product listing of all available ENCs in a Data Server's Service.

### **WARNING**

*If a PARTIAL exchange set is loaded it may adversely affect the behaviour of the ENC Status report described in Annex C for an ECDIS. Data Servers should be careful to ensure their data clients are aware of this behaviour.*

Licence and ENC information from different Data Server's must be stored independently on the manufacturer's system. The SERIAL.ENC file (see [Clause 7.3](#)) contains the Data Server ID and should be used in conjunction with the associated product listing to identify the source of the service. The latest product listing contains the current status of ENC cell data in a service. This file is used to compare available ENC cell data in the exchange set with information already stored in the OEMs SENC. The OEM system can then determine what new data is available for import.

It is recommended that OEMs maintain a copy of the latest product listing on their systems to reflect the current status of a particular service. To manage both "FULL" and "PARTIAL" product listings it is essential that new information is merged with existing stored data and not overwritten.

### 7.2.1 Product List File Structure

The content of the product list will be divided into sections. The Product List file is completely encoded in ASCII and contains 3 sections as follows:

Section	Description
<b>Header</b>	Contains general information about the nature of the Product List, e.g. the time of creation, version number.
<b>:ENC</b>	Contains the current status of all ENC cells/updates provided by the data server.
<b>:ECS</b>	Contains information about other digital chart information provided by the data server.

### 7.2.2 Product List Header

The Product List will always start with one Header Section. The Header Section will consist of several records. Each record will start at a new line and be terminated with ASCII CR/LF characters as within the signature files.

The Header will consist of the information fields defined in the example and table below. All the fields are mandatory and will always be defined in the same order.

Field	Fieldname	Value
Date and Time	:DATE	YYYYMMDD HH:MM The field name, date and time will be separated by a space> character. The date will be provided as 20060627 and the time as 09:00:00 using the 24 hour clock. Example: :DATE 20061019 09:00:00
Product List Version	:VERSION	Integer in range 1 to 99. It will be incremented by 1 for each new version of the PRODUCTS.TXT file specification. S-63 Edition 1.1 defines the value as "2". i.e. :VERSION 2
Content	:CONTENT	"FULL" Full copy of Product List "PARTIAL" Partial copy of Product List Code used to indicate if the Product List file contains a full or partial copy of the complete Product List. Example: :CONTENT FULL

EXAMPLE: :DATE 20061019 09:00:00

```
:VERSION 1
:CONTENT FULL
```

### 7.2.3 Product List 'ENC' Section

The Product List will always contain one ENC Section. It will contain information about the current navigational status of all official ENC cells and updates supported by the Data Server.

This section will start with one *ENC Section Identifier* record as defined below.

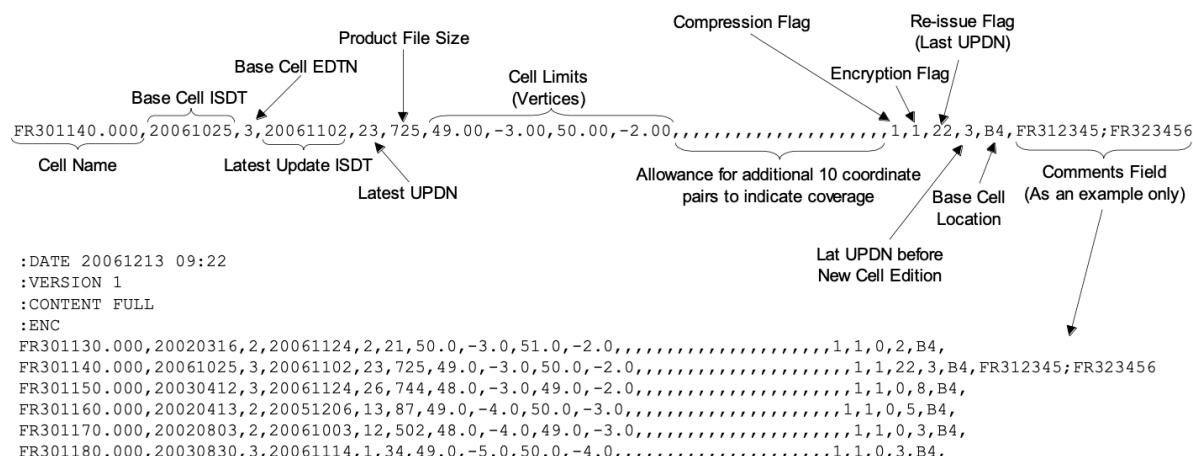
Field	Fieldname	Value
ENC Section Identifier	:ENC	Not applicable

The ENC Section will then consist of repeating records defining the status of each ENC supported by the data server. The definition of this record is defined in the table below:

Field	Value
<b>Product Name</b>	Name of product as defined in S57e3 DSID-DSNM subfield. The file extension will always be 000. Example: GB202400.000

Field	Value
<b>Base Cell Issue Date [EN Application Profile]</b>	YYYYMMDD This date is only used for the base cell files (i.e. new data sets, re-issue and new edition), not update cell files. All updates dated on or before this date must have been applied by the producer. Cancelled cells with the edition number '0' (zero) will carry the issue date of the update used to cancel it. Example: 20050222
<b>Base Cell Edition</b>	Edition number of base [EN] ENC cell. Integer in range 1 to 999 Identical to content of S57e3 DSID-EDTN. In the case where a cell is cancelled the Product Edition will be set to '0' (zero), see <a href="#">Clause 7.2.3.1</a> . This allows the ECDIS system to quickly identify cells that have been removed from a service.
<b>Issue Date Latest Update [ER Application Profile]</b>	YYYYMMDD Date on which the latest update for the current ENC cell edition was issued. This field is used whenever there is an update or a re-issue of the cell.
<b>Latest Update Number</b>	Integer in range 1 to 999 Update number of the latest update message issued for the ENC cell edition. Identical to content of DSID-UPDN. Left blank when no update is available for the current edition of the base cell. Used only for updates and re-issues.
<b>File Size</b>	Integer in range 1 to 999999 Total file size in Kilobytes for all files issued for the product. This will include the size for the base cell, updates and any applicable text and picture files.
<b>Cell limit Southernmost latitude</b>	Degrees of arc, south is negative. Southernmost latitude of data coverage in the ENC product. Example: 49.898773299986 (49°53'.93N)
<b>Cell limit Westernmost longitude</b>	Degrees of arc, west is negative. Westernmost longitude of data coverage in the ENC product. Example: -1.927277300003 (001°55'.64W)
<b>Cell limit Northernmost latitude</b>	Degrees of arc, south is negative. Northernmost latitude of data coverage in the ENC product. Example: 50.922828000014 (50°55'.37N)
<b>Cell limit Easternmost longitude</b>	Degrees of arc, west is negative. Easternmost longitude of data coverage in the ENC product. Example: -0.000166700008 (000°00'.01W)
<b>10 Data Coverage Coordinates</b>	Optional. Degrees of arc, south and west are negative. 10 coordinate pairs can be supplied to indicate the data coverage within the ENC cell. It will be provided as repeating Y-coordinate and X-coordinate pairs.
<b>Compression</b>	Integer in range 0 to 99 "0" No compression "1" Compression is used (see <a href="#">Section 3</a> )
<b>Encryption</b>	Integer in range 0 to 99 "0" No encryption "1" Encryption is used (see <a href="#">Section 4</a> )
<b>Base cell update number</b>	In the event of a cell being re-issued the update number current at the time of the re-issue should be inserted here. If a cell edition does not have a re-issue then this field is blank or zero filled.
<b>Last update number for previous edition</b>	Empty if no previous editions available in the data server database. If previous editions of the cell are available then this field will contain the last update number for the previous edition.
<b>Base Cell Location (See note below)</b>	<b>CD-ROMs</b> The location within the exchange set where the base cell can be found. Base cells may be located on either one or several base or update exchange sets. This is an integer in

Field	Value
	<p>range 1 to 99 proceeded either by a 'B' if on a base CD or 'U' if on the update, e.g. <b>B7</b>, <b>B11</b>, <b>U1</b>, etc.</p> <p><b>Large Media Support</b></p> <p>In the case where a service supports large media this field is divided into two subfields delimited by a ";" (semi colon). The first subfield contains the media number ID and the second the exchange set number. The Media ID is designated with a "M" followed by a number. The ExSet number is formatted in the same as for CD-ROMs, e.g. "<b>B1</b>". For example a base cell could be located in the following ways, "<b>M1;B1</b>", "<b>M1;B2</b>", "<b>M2;B10</b>",etc. Updates for example, "<b>M1;U1</b>" or <b>M1;U2</b> if more than one update ExSet on the same media. See <a href="#">Appendix 2</a> of this document for details.</p>
<b>Cancelled Cell Replacements (Old Comments Field))</b>	If a cell is cancelled and a replacement cell(s) is issued this field is used to identify the replacement(s). In cases where there are more than one replacement the cell names will be delimited by a ";" (semi-colon). See <a href="#">Clause 7.2.3.3</a> for further details.
NOTE The "Base Cell Location" is the location where the latest version of the base cell (EN Profile) resided this can be either the base media or in the case of new cells, new editions or re-issues the update media.	



### Example of Structure and Format

#### 7.2.3.1 Managing Cancelled Cells (Data Servers)

When a cell is cancelled by a HO an update cell file is created, containing only the Data Set General Information record with the 'Data Set Identifier' [DSID] field. The 'Edition Number' [EDTN] subfield of the DSID field must be set to 0 (zero). Cancellation messages are only used to cancel a base cell file.

In an encrypted service this information is unavailable to the Data Client unless the update is decrypted first. To avoid the need to decrypt first there are two methods of encoding this in an encrypted exchange set as follows:

- 1) The EDTN subfields of the CATD-COMT field in the CATALOG.031 file (see [Clause 7.4.1.1](#)).
- 2) The 'Base Cell Edition' field in the PRODUCTS.TXT file (see [Clause 7.2.3](#)).

The CATALOG.031 file can be used to identify any cancelled cells in an exchange set at import whilst the PRODUCTS.TXT file acts to highlight all cancelled cells in a Data Server's Service. ENCs that have been cancelled should remain on the base or update media, including references in the PRODUCTS.TXT file, for a minimum of 12 months.

#### 7.2.3.2 Managing Cancelled Cells (Data Clients)

Cancelled cells are those ENCs that have been removed from a data server's ENC service and as such are no longer supported or updated by the issuing authority. There are two options available to manufacturers when managing cancelled cells as follows:

- 1) Automatically remove the cell from the SENC when a cell is identified as cancelled.
- 2) Allow the user to decide whether to retain the cell in the SENC or remove it.

ECDIS/ECS manufacturers are free to decide which of these options to implement in their systems. However it is important that the system informs the user of the fact that a particular cell is cancelled and, in the case of option 2, the consequences of retaining it.

With option 1 the user must be informed that a particular cell is cancelled either during load time or, preferably, in a report at the end of the process.

With option 2 the user is offered the option to retain or remove the cell from the SENC. If the user chooses to retain the cell a permanent warning must be displayed, on screen, when the cancelled cell is viewed. The message should be similar to the example below:

***"Cell <name> has been cancelled and may not be up to date. Under no circumstances should it be used for primary navigation".***

#### 7.2.3.3 Cancelled ENC Cell Replacements

In instances where an ENC cell has been cancelled it is often replaced by one or more ENC cell(s). This may be due to re-scheming on the part of data servers. Provision has been made in this edition of S-63 to display this information in the data client. The comments field of the PRODUCTS.TXT has now been made available to display information relating to replaced cells. The formatting of the cell record in the products listing is given in [Clause 7.2.3](#).

When a cell is identified as cancelled the data client should read the "Cancelled Cell Replacement" field to check if there are replaced ENC cell(s) encoded. If there are then the data client is to make this information available to the user. A message similar to the one below should be displayed:

***"Cell <name> has been cancelled and has been replaced by cell(s), <name1>; <name2>. Please contact your data supplier to obtain the additional ENC permits".***

#### 7.2.4 Product List 'ECS' Section

The Data Server may also issue other types of digital chart products such as backdrop charts that can be used to display chart coverage. Information about these products can also be made available in the Product List if the data server wishes to.

The content of this section is identical to the ENC Section defined in [Clause 7.2.3](#). The only difference is the *Section Identifier* which will be "**:Ecs**".

EXAMPLE — Encoding example of a Product List which utilises all the features defined in [Clause 7.2.1](#):

```
:DATE 20061019 09:00:00 :VERSION 1 :CONTENT
FULL :ENC AR201130.000,20051118,1,20060703,1,-36.43335487,-57.41667361,-34.69998565,
-54.33335853,,,,,,,,,,1,1,0,0,B3, AR302120.000,20051219,1,20060427,2,-39.
44997766,-62.39166614,-38.74168723,-61.11683505,,,,,,,,,,1,1,0,0,B3,
AR402490.000,20051206,1,20060330,1,-39.11668811,-61.94017540,-38.95167627,-61.
76656919,,,,,,,,,,1,1,0,0,B3, AR402550.000,20051219,1,20060427,1,-39.
01664968,-62.16649373,-38.88332240,-61.94017540,,,,,,,,,,1,1,0,0,B3,
AR402560.000,20051122,1,20060427,1,-38.99166872,-62.39166614,-38.74168723,-62.
16649373,,,,,,,,,,1,1,0,0,B3, AR420010.000,20060912,2,-35.16832135,-56.
07497834,-35.03499407,-55.84166992,,,,,,,,,,1,1,0,3,B3, :ECS PM1WORLD.000,
19990101,1,,3000,-90,-180.0,90.0,180.0,-90.0,-180.0,90.0,180.0,,,,,,,,,,0,0,
,B5,
```

### 7.3 Serial File (SERIAL.ENC)

A file named SERIAL.ENC is supplied so that Data Clients can identify the following information prior to import:

- Data Server ID (registered with the SA)
- Week of Issue
- Date of Issue
- CD Type (Base or Update)
- Format Version

- Exchange Set Number (of a series of exchange sets)

### 7.3.1 SERIAL.ENC File Format

The SERIAL.ENC file is provided to assist Data Client's systems manage the import ENC CDs supplied by a specific Data Servers across multiple exchange sets. It should be the first file that is read from the exchange set as it contains important information about the IHO assigned Data Server's ID, the CD Publication Date, type of CD, number of CDs in that particular Data Server's service, etc.

The contents of this file can be cross referenced with the installed permits to check the status of the Data Client's subscription status.

Field ID	Domain	Bytes	Range	Notes (see below)
Data Server ID	character	2	Any two alphanumeric	1
Week of Issue	character	10	Any ASCII characters	2
Date of publication	date	8	YYYYMMDD	3
CD Type	character	10	BASE or UPDATE	4
Format version	decimal	5	01.00 – 99.99	5
Exchange Set Number	character	6	B01-99X01-99 or U01-99X01-99	6
End of record delimiter	hexadecimal	3	0xB0D0A	7

Notes	Explanation and Description
1	Data Server ID should be registered with the IHO; where the data server is also an HO the Agency code for the organisation is obtained from S-62 – IHO Codes for Producing Agencies.
2	The week of issue specifies the week and year that the CD is distributed, e.g., <b>WK12-99</b> , <b>WK45-99</b> , <b>WK23-00</b> , etc.
3	Date of publication is in the regular date format, <b>YYYYMMDD</b> , e.g., <b>19990414</b> , <b>20000102</b> , <b>20061102</b> , etc.
4	The CD can be issued in two different types: BASE: The format should be defined as BASE, the CD contains all ENs and any additional ERs. UPDATE: The format should be defined as UPDATE, contains any new ENs and all ERs issued since the issue of the last relevant Base CD.
5	Format version describes the version of the SERIAL.ENC file. The version that relates to edition 1.1 of S-63 is <b>02.00</b>
6	This field must be used to show the exchange set number of a series, e.g. <b>B02X03</b> , which equates to Base CD 2 of a total of 3 Base CDs, <b>U01X01</b> which equates to Update CD 1 of a total of 1.
7	The end of the record delimiter consists of binary characters, and therefore care should be taken when attempting to edit the file – it cannot be edited in Windows Notepad! This is the reason why the SERIAL.ENC file must always be edited in an ASCII/Hexadecimal editor. The delimiter does not normally need to be changed. The delimiter used is <b>0xB0D0A</b> .
The SERIAL.ENC file should be stored directly under the media root file, i.e. on the same level as the ENC_ROOT and INFO directories.	

**EXAMPLE — Example of SERIAL.ENC files:** PRWK15-99 19990414BASE 02.00B02X030x0B0D0A

PRWK20-99 19990601UPDATE 02.00U01X010x0B0D0A

(Where **0xB0D0A** is the end of record delimiter converted to hex)

## 7.4 The S-57 Catalogue File (CATALOG.031)

The “Data Set Identification” [DSID] field is used by ECS/ECDIS to ensure that base cells and update files are imported to the SENC in the correct sequence and without omission. Since the complete ENC Cell file is encrypted, information in the DSID field of each cell file is not available to OEM systems, unless it is decrypted first.

The “Comments” [CATD-COMT] field in each cell record of the CATALOG.031 file is used to store the required DSID information. Since the CATALOG.031 file acts as the table of contents for the exchange set and identifies where all files are stored it is ideally suited for this purpose.

The information stored in this field must be identical to that stored in the DSID field of the cell file which in turn must conform to section 5.7 of the IHO S-57, Appendix A, Product Specification. This is summarised in the table below. This table specifies the rules for encoding ENC EN & ER application profiles.

Event	File Extension	EDTN	UPDN	UADT	ISDT	Comments
New ENC Cell	.000	1	0	19950104	19950104	UADT < or = ISDT
Update 1	.001	1	1	Prohibited	19950121	ISDT only
Update 2	.002	1	2	Prohibited	19950225	ISDT only
...						
Update 31	.031	1	31	Prohibited	19950905	ISDT only
Re-issue of an ENC Cell	.000	1	31	19950905	19950910	UADT < or = ISDT
Update 32	.032	1	32	Prohibited	19951023	ISDT only
...						
Update 45	.045	1	45	Prohibited	19951112	ISDT only
New edition of ENC Cell	.000	2	0	19951201	19951201	UADT < or = ISDT
Update 1 to edition 2	.001	2	1	Prohibited	19960429	ISDT only

Data Servers must extract the necessary information from the DSID field prior to encryption and encode it in the CATD-COMT of the CATALOG.031 file. The structure and format of this field is described in more detail in [Clause 7.4.1](#). Data Client systems must then read the CATD-COMT field as though accessing the DSID field in an unencrypted exchange set.

### 7.4.1 The CATD-COMT Structure and Format

The DSID information stored in the CATD-COMT field is subdivided into four or five comma separated subfields. This is dependant on whether the ENC file has an EN or ER application profile. The final subfield is punctuated by a semi colon (;).

EXAMPLE: VERSION=1.0,EDTN=1,UPDN=0,UADT=20060703,ISDT=20060703;  
VERSION=1.0,EDTN=1,UPDN=1,ISDT=20060710;

#### 7.4.1.1 Encoding Cancelled Cells (see also [Clause 7.2.3](#), [Clause 7.2.3.1](#), [Clause 7.2.3.2](#) & [Clause 7.2.3.3](#))

Since an update is provided containing just the delete message it should be treated as an ER. Therefore for the purposes of the CATD-COMT field it should be encoded as follows:

VERSION=1.0,EDTN=0,UPDN=2,ISDT=20060814;

The following table illustrates the conditions that apply to all the different types of transactions.

Version Number	Edition Number	Update Number	Update Application Date [UADT]	Issue Date [ISDT]	Comment
VERSION=1.0	EDTN=1	UPDN=0	UADT=20060703	ISDT=20060703	New Cell (EN)
VERSION=1.0	EDTN=1	UPDN=1	Prohibited	ISDT=20060710	Update (ER)
VERSION=1.0	EDTN=1	UPDN=10	UADT=20060710	ISDT=20060717	Re-issue (EN)
VERSION=1.0	EDTN=1	UPDN=11	Prohibited	ISDT=20060724	Update (ER)
VERSION=1.0	EDTN=2	UPDN=0	UADT=20060731	ISDT=20060731	New Edition (EN)
VERSION=1.0	EDTN=2	UPDN=1	Prohibited	ISDT=20060807	Update (ER)
VERSION=1.0	EDTN=0	UPDN=2	Prohibited	ISDT=20060814	Cancelled Cell (ER)

## 7.5 ENC Update Management

A file is supplied that allows Data Clients to check the compatibility and suitability of a particular ENC update exchange set prior to import. The Data Client can use this file to check that the last Base Exchange sets imported to the SENC are compatible with the update currently being installed on the ECDIS. This file describes the current status of all base media associated with a data server's service. It is named STATUS.LST. The following section describes the format and content in more detail.

### 7.5.1 STATUS.LST File

This file will be stored in the INFO folder on the Update Exchange Media that relates to base media containing either a single media set or multiple ones (see [Appendix 2](#)). It is supplied so that Data Clients can check the current status of the SENC against available base media. This file can be used to check that an update exchange set is compatible with the latest base media installed on the Data Client. An update media MUST be made available at regular intervals<sup>9</sup> for services provided in accordance with this version of the standard.

NOTE When the data server issues a new update only one update media will be supplied. However there may be more than one update exchange set on a single update media in the case of services supplied on large media such as DVD.

#### 7.5.1.1 Status Header Format

The header is a fixed length record containing the following information:

Field ID	Domain	Bytes	Range
Data Server ID	character	2	Any two alphanumeric
Week of Issue	character	10	Any ASCII characters
Media Type	character	10	UPDATE
Issue Date	decimal	8	YYYYMMDD

<sup>9</sup> Even if all bases are re-issued in the same week, although this is considered unlikely.

Field ID	Domain	Bytes	Range
End of record delimiter	hexadecimal	2	CR/LF

EXAMPLE — Example of Status Header: GBWK15-08 UPDATE 20080403

### 7.5.1.2 Status Record Format

This is a comma separated record with an end of line CR/LF delimiter.

Field ID	Domain	Bytes	Range
Base Media Number	character	2-3	Alphanumeric [e.g. B1, B11, M2, etc.]
Data Server ID	character	2	Alphanumeric [e.g. GB]
Week of Issue	character	7	Any ASCII characters [WKWW-YY]
User Information	character	1-100	ASCII Text string contained within single quotation marks ('') [HEX 27] that can be used as a prompt to the user. (See note below)
Base Media Issue Date	decimal	8	YYYYMMDD
End of record delimiter	hexadecimal	2	CR/LF

NOTE This information is intended to be used by Data Clients as a prompt to users. It is the responsibility of the Data Servers to ensure that the "User Information" is consistent with the information contained on the media (CD, DVD, etc) label.

EXAMPLE — Examples of Status Record: B1,GB,WK52-07,'BASE CD 1 dated 27 December 2007',20071227

M1,GB,WK19-07,'BASE MEDIA 1 dated 10 May 2007',20070510

Systems must appropriately manage the import of base data from different Data Servers and store information of installed base data. When loading new update media (either CD, DVD, etc) Data Clients should check that latest base media listed in the STATUS.LST is concurrent with those installed on the system. If not the system should report a message similar to the following:

EXAMPLE: **"This 'Update Media' is not compatible with the actual installed 'Base Media'. Please install the following 'Base Media' first and then continue with the 'Update Media'."**

**<Field: User Information 1>**

**<Field: User Information 2>**

**<Field: User Information x> (where x is the base media number)**

**Example:**

**"This 'Update Media' is not compatible with the actual installed 'Base Media'. Please install the following 'Base Media' first and then continue with the 'Update Media'."**

**'BASE CD 2 dated 03 April 2008'**

NOTE The user should only be prompted to install compatible base media that contains licenced ENC cells.

**Complete Examples<sup>10</sup> :**

For updates that relate to base media containing a single exchange set, for example CD

---

<sup>10</sup> Most Data Servers currently re-issue all their base CDs concurrently it is recognised that this will probably change to an incremental method of issuing bases.

**EXAMPLE:** GBWK15-08 UPDATE 20080403  
 B1,GB,WK52-07,'BASE CD 1 dated 27 December 2007',20071227  
 B2,GB,WK14-08,'BASE CD 2 dated 03 April 2008',20080427  
 B3,GB,WK07-08,'BASE CD 3 dated 08 February 2008',20080227  
 B4,GB,WK07-08,'BASE CD 4 dated 08 February 2008',20080227

For updates that relate to base media containing multiple exchange sets, for example DVD

**EXAMPLE:** GBWK37-07 UPDATE 20070913  
 M1,GB,WK19-07,'BASE MEDIA 1 dated 10 May 2007',20070510  
 M2,GB,WK23-07,'BASE MEDIA 2 dated 07 June 2007',20070607

## 7.6 The S-57 Readme File (README.TXT)

Data Servers, RENCs and ENC producers currently use the README.TXT to encode important information that relates to their services. The structure and content of the file should be as follows:

**SECTION 1 – Important General Information:** Information relevant to all ENC users such as ECDIS; Temporary and Preliminary Information; Overlapping Policy Descriptions; and Disclaimers. Other information regarded as important may also be added.

**SECTION 2 – HOs information:** Information provided by individual Producing Agencies providing specific copyright statements and information about their ENCs.

**SECTION 3 – Withdrawn Cells:** Overview of ENC cells which have been removed from the service due to unforeseen events. ENCs being cancelled as part of producers' normal ENC management routines should not be included.

**SECTION 4 – Miscellaneous Information:** Placeholder for additional information not fitting in the other sections.

Although the inclusion of the README.TXT file is not mandated in the S-57 Product Specification it has become an important source of information in all commercial ENC services, especially given the increasing amount of ENCs available from many different producer nations.

With this in mind it is strongly recommended that Data Client systems are able to display this file on demand. Since this file is relatively unknown to users it would be useful for the Data Client system to display when installing ENC data to forcibly bring it to their attention.

## 8 Directory and File Structure

### 8.1 Introduction

The scheme does not mandate the use of a particular directory or file structure. However, because the entire ENC data file is encrypted it is difficult to maintain some vital file associations, e.g. text and picture files with the relevant ENC cell file (base or update). The directory structure that has been adopted by existing Data Servers is given in an example below in [Clause 8.5.1.1](#). This structure enables text and picture files to be safely managed by maintaining a direct relationship between them and the corresponding ENC data file.

### 8.2 S-57 File Management

The directory structure is not mandated and may vary between Data Servers. The location of all S-57 files in an encrypted exchange set is defined in the CATALOG.031 file. That is, the path to all files in the exchange set is specified in each file record.

### 8.3 File Structure

As well as the exchange set [ENC\_ROOT] the root directory contains a folder named 'INFO' that contains the PRODUCTS.TXT file (see [Clause 7.2](#)), STATUS.LST (see [Clause 7.5](#)) and any additional, or extra, yet to be defined, files as specified by individual Data Servers. The root directory also contains the SERIAL.ENC file (see [Clause 7.3](#)). Each ENC Cell file in the exchange set under ENC\_ROOT has a corresponding signature file (see [Clause 6.3](#)).

Data Servers currently supply the authentication certificate (.CRT) with an S-63 encrypted exchange set to support S-63 edition 1.0 implementations. This certificate file is contained in the root directory. Edition 1.1 does not support the supply of this file with S-63 exchange sets. Data Servers will continue to support this for a limited period after which it will be withdrawn from their services.

OEMs can program their systems to automatically detect an exchange set or a group of exchange sets however; this should not be hard coded into the system. If the media contains an unexpected format the system should default to a browse facility so that users can manually specify the location of the ENC\_ROOT directory of a required exchange set. An S-63 exchange set must always contain a folder named ENC\_ROOT which must contain a single CATALOG.031 file and at least one data set file.

### 8.4 Folder and File Naming

All folders and files must be named according to the conventions set out in the IHO S-57 Product Specification and this document. All folders and files in an S-63 encrypted exchange set must be in UPPER CASE.

### 8.5 Exchange Set Media

Data Servers may supply exchange sets to Data Client's using several different methods, for example:

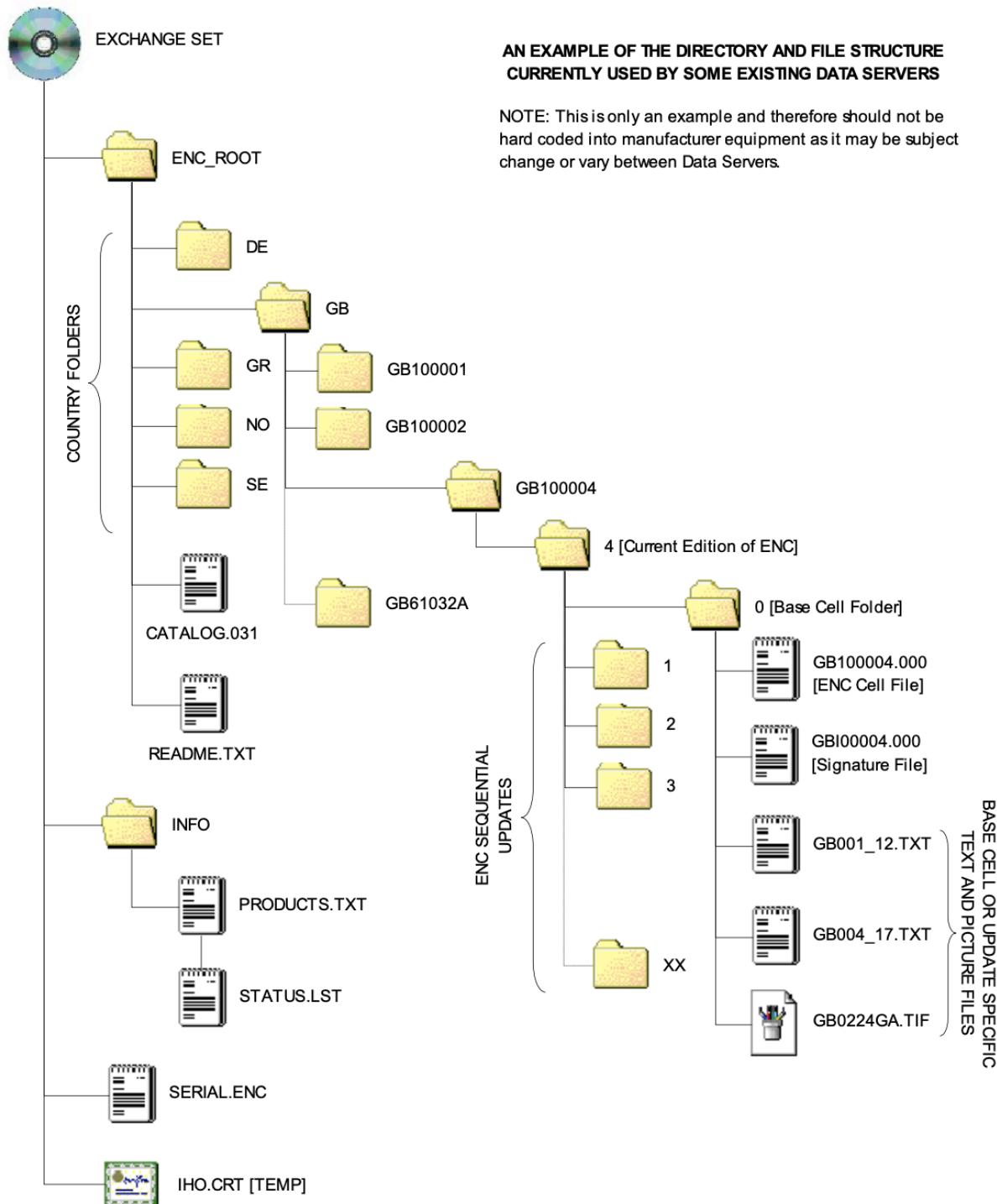
- 1) CD-ROM
- 2) Large Media Support
- 3) On-line Services

#### 8.5.1 CD-ROM

Encrypted exchange sets delivered by this method will be given the volume ID consistent with the IHO S-57 Data Protection Scheme, i.e. V01X03, V01X02, etc. S-63 can be delivered as a single exchange set across multiple CD-ROMs but experience gained by existing Data Servers has shown this to be inadvisable. The method currently operated by certain Data Servers is to issue single exchanges sets across multiple CDs.

##### 8.5.1.1 Folder Definitions

Although the example below is based on a Base CD the Update CD is very similar, the only difference being that the update does not necessarily hold all the base cell data. However the update must contain data that is consistent and sequential for the Base CD to which it applies.



### 8.5.2 Large Media Support

Large Media Support is defined as devices capable of storing much larger volumes of data than a standard CD-ROM. Details relating to the storage of S-63 encrypted ENCs on such devices is given at [Appendix 2](#).

### 8.5.3 On-Line Services

Data Clients can download exchange sets from RENC/VAR as defined by the service provider. The download is then copied to a hard media and depending on the media the RENC/VAR will advise on the volume ID to assign to the media. It must be re-iterated that any copied exchange sets [ENC\_ROOT] must at all time conform to section 5.4 of the IHO S-57 Appendix B, Product Specifications.

## 9 Scheme administrator processes

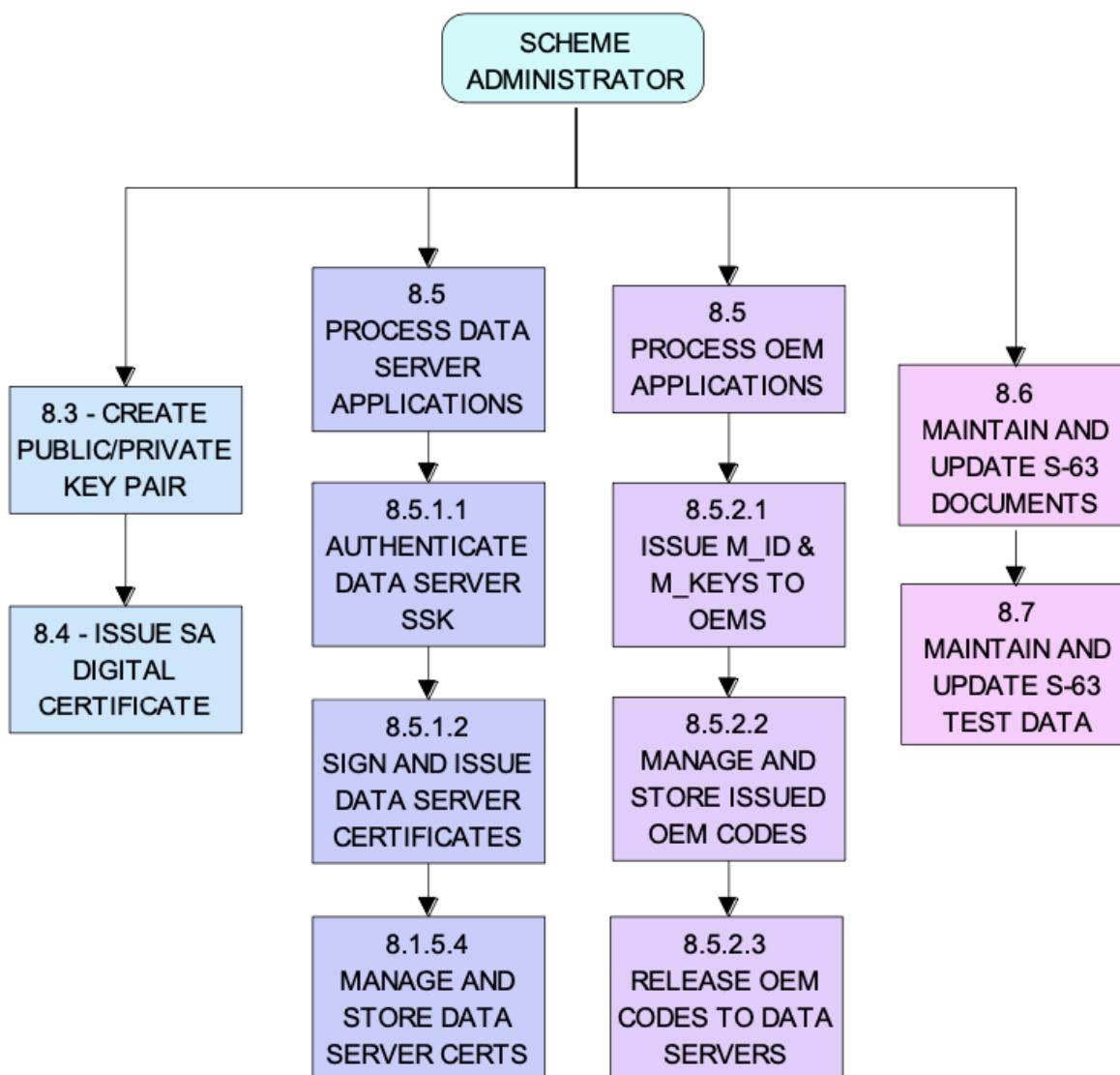
### 9.1 Data Protection Scheme Administrator

The Data Protection Scheme Administrator (SA) is solely responsible for maintaining and coordinating the S-63 Data Protection Scheme (DPS). The SA role is operated by the IHO Secretariat on behalf of the IHO member states.

The SA is responsible for controlling membership of the scheme and ensuring that all participants operate according to defined procedures. The SA maintains top level encryption keys used to operate the complete scheme and is the only body that can issue certificates to other participants. The SA is the custodian of all documentation relating to the scheme.

### 9.2 Scheme Administrator Processes

The main responsibilities of the IHO as the S-63 Scheme Administrator are depicted in the [Figure 9-1](#). Each “Process Box” cross references the particular section where these operations are outlined in more detail.



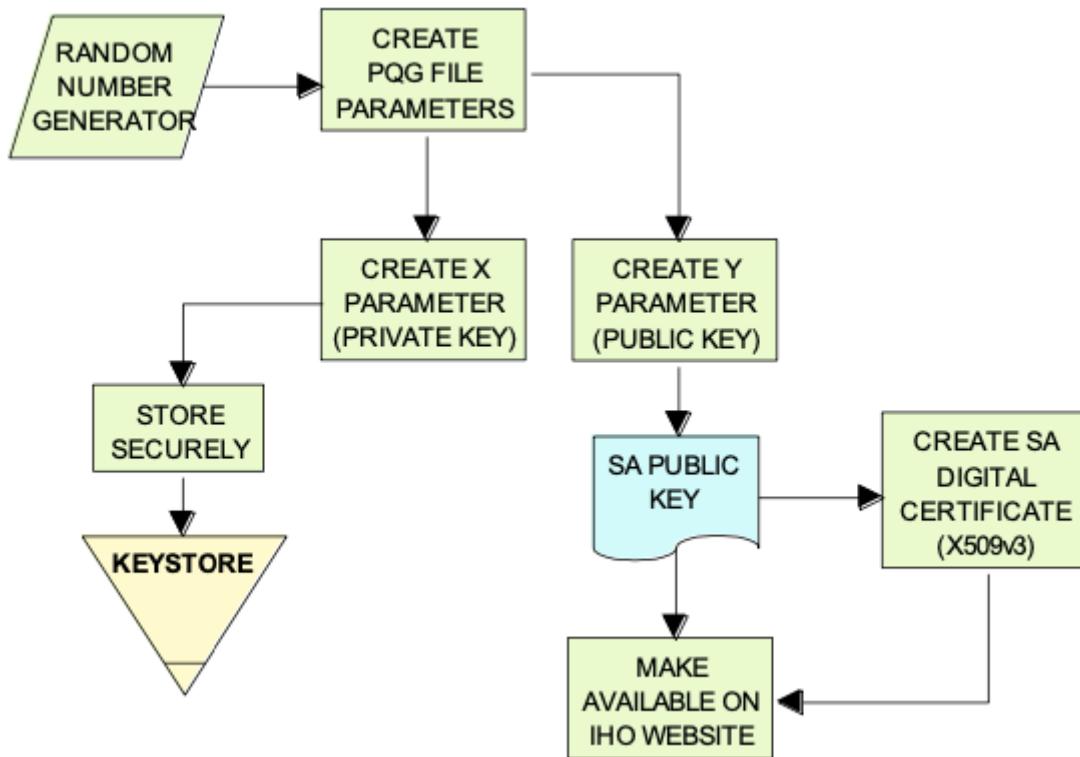
**Figure 9-1 — Main Scheme Administrator Processes**

### 9.3 Create Top Level Key Pair

The IHO as scheme administrator must create a top level public and private key pair. The private key will be used to sign Data Server certificates and the public key to authenticate the signature. The public key must be installed on the Data Clients system independently of the Encrypted ENC data.

#### 9.3.1 Create PQG Parameters

This procedure is normally performed by the SA and Data Servers during the creation of public/private key pairs. Although the PQG parameters generated by Data Servers do not need to be identical to those contained within the SA public key and the SA Digital Certificate, the key lengths used must be identical.



**Figure 9-2 — Make Top Level Key Pair**

The PQG file only exists by itself for a short period during the creation of the X and Y files. After these have been made, the PQG file will be contained within the X and Y files.

The creation of appropriate PQG parameters is covered in more detail in the Digital Signature Standard (DSS) [NIST FIPS 186 fpd](#). For information relating to the format of the PQG file see [Clause 6.4.2.1](#).

#### 9.3.2 Create Private Key

The private key is an output of the key generation process. The private key must be stored securely and access limited to only those persons that have a need to know. Unauthorized possession of the SA's private key can potentially undermine the security of the authentication part of the scheme. The SA will issue a new public key (and corresponding SA certificate) if the private key is compromised. Details of the X file (Private Key) format are contained in [Clause 6.4.2.2](#).

#### 9.3.3 Create Public Key

The public key is an output of the key generation process. The public key is sent to all participants of the scheme in both a digital and a printed form. The two forms are to be sent by different means. Details of the Y file (Public Key) format are contained in [Clause 6.4.2.3](#).

## 9.4 Create and Issue SA Digital Certificate (X509v3)

The SA Digital Certificate will be compliant with X509v3 [ITU-T X.509 \(11/1988\) / ISO 9594-8](#). The SA Digital Certificate will always be provided in a file called IHO.CRT. The IHO.CRT file is available from IHO at [www.oho.int](http://www.oho.int).

The SA uses a DSA Public Key of length 512 bits.

All Data Servers providing an ENC service may include the SA certificate, for reference in the root directory of the media (e.g. in D:\IHO.CRT on a CD-ROM) but, as stated in [Clause 7.1](#), the installation on a Data Client's system of the SA certificate should be done independently. The check of the validity of the SA signature within each ENC signature file must be done from the independently installed version of the SA certificate.

The SA public key (as opposed to the digital certificate) is also made available as an ASCII file on the IHO website at [www.oho.int](http://www.oho.int) (the format is described in Section 6.5).

### 9.4.1 Update SA X509v3 Digital Certificate (Public Key)

The SA will publish and make a new SA Digital Certificate available under the following circumstances:

- When the SA Digital Certificate expires. In this case the Certificate shall not contain a changed public key.
- When the SA private key has been compromised. In this case a new public key shall be contained within the SA Digital Certificate.

The SA will publish its new Digital Certificate and, if applicable, a new printable version (ref section 6.5) of the public key on the IHO website ([www.oho.int](http://www.oho.int)). All Data Servers and Manufacturers will immediately be informed and will receive copies of the new Digital Certificate and, if applicable, the new public key in printable format.

The Data Server and Manufacturers are collectively responsible for informing their Data Clients of any new SA Digital Certificate and, if applicable, any new SA public key.

This procedure is normally performed by all users of the protection scheme when a new SA Digital Certificate or public key is issued and is performed as follows:

- Obtain the new SA Digital Certificate and printable SA public key from the IHO website ([www.oho.int](http://www.oho.int))
- The application shall load the new SA Digital Certificate and check the public key and the printable public key are identical. Only when this has been done is the application to assume that the SA public key is correct. This same process is applied to the replacement of the original SA public key.
- Replace the existing SA Digital Certificate with the newly issued certificate.

## 9.5 Process Applications from Data Servers & OEMs

The Scheme Administrator is responsible for processing applications from Data Servers and OEMs who wish to subscribe to the IHO S-63 ENC Data Protection Scheme. This includes the management and issuing SA Signed certificates to Data Servers and the management and issuing of Manufacturer Codes (M\_ID & M\_KEY) to accepted OEMs and their distribution to authorised Data Servers. The application processes are outlined in more detail at **ANNEX A & ANNEX B** of this document.

### 9.5.1 Process Data Server Request for Data Server Certificate

A successful Data Server applicant will be required to supply a certificate signed with the Data Server private key, this is known as Self Signed Key (SSK). The certification process is then carried out by the SA and is detailed step by step below.

#### 9.5.1.1 Authenticate Self Signed Key (SSK) File

The SA authenticates the Data Server SSK file before creating and issuing a Data Server Certificate. Initially the SA should confirm that the SSK has been supplied in the correct format as described in [Clause 6.4.2.5](#), if incorrect the process should be terminated and a warning given. If correct the process to authenticate should proceed as follows:

- 1) Extract the signature elements 'R' and 'S' (i.e. the first two data strings and their attendant headers from the SSK file supplied by the Data Server). This leaves a public key file.

- 2) Hash the public key file using the algorithm SHA-1. All bytes within the file are to be hashed.
- 3) Verify the signature (the elements removed at 'a' above) by passing it, together with the public key file and the hash of the public key file (as obtained at 'b' above) to the DSA. This will return a status (correct or incorrect).

If the signature verifies correctly, the SA can produce the Data Server Certificate.

#### **9.5.1.2 Create Data Server Certificate**

The SA creates a Data Server Certificate after the SSK has been authenticated. The details of the digital signature algorithm DSA are covered in the publication FIPS 186 Digital Signature Standard (DSS). The procedure is as follows:

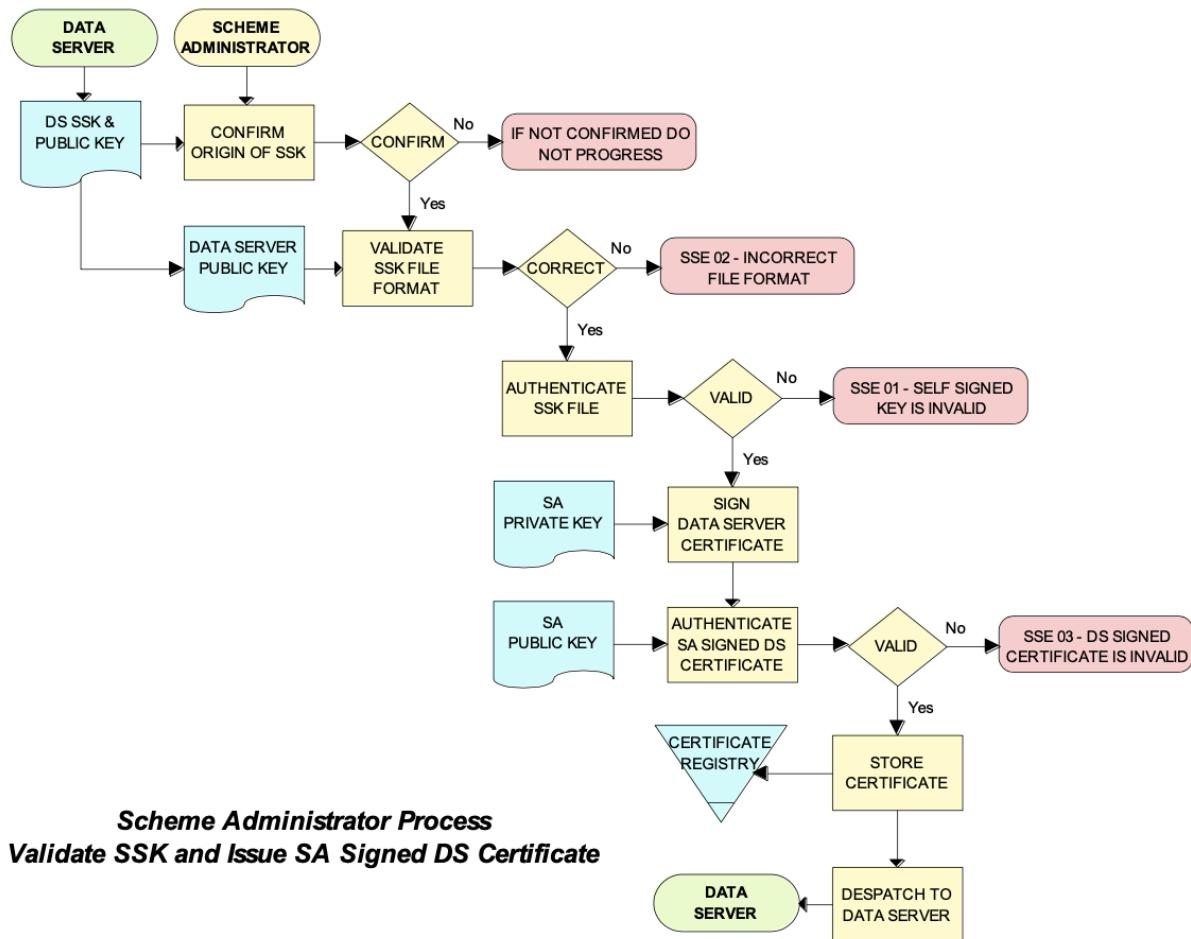
- 1) Discard the signature elements (i.e. the first two data strings and their attendant headers) from the self signed key file. This leaves a public key file.
- 2) Hash the public key file using the algorithm SHA-1. All bytes within the file are to be hashed.
- 3) Sign the public key file (as hashed at 'b' above) by passing the SA private key, the hash of the public key file (as obtained at 'b' above) and a random string to the DSA. This will return the two signature elements ('R' and 'S').
- 4) Write these to the certificate file and append the public key file (as left at 'a' above) to form the certificate.

#### **9.5.1.3 Authenticate SA signed Data Server Certificate**

The SA confirms the newly signed certificate is valid before despatching it to the Data Server. The procedure is as follows:

- 1) Extract the signature elements (i.e. the first two data strings and their attendant headers) from the newly created DS certificate file. This leaves the DS's public key file.
- 2) Hash the DS public key file (obtained from 'a') using the algorithm SHA-1. All bytes within the file are to be hashed.
- 3) Verify the signature elements (as removed at 'a' above) by passing it, together with the SA public key and the hash of the DS public key file (as obtained at 'b' above) to the DSA. This will return a status (correct or incorrect).

If the DS Certificate authenticates correctly, it can be sent to the DS and used in the construction of ENC digital signatures.



#### 9.5.1.4 Manage Data Server Certificates

When a new SA signed Data Server Certificate has been issued to a Data Server it should be stored securely in a certificate store. The certificate should be uniquely assigned to the Data Server and cross referenced to the private key used to sign it and the public key used to confirm authentication.

#### 9.5.2 Process OEM Application

Manufacturers must apply to the SA to become a member of the IHO S-63 Data Protection Scheme.

##### 9.5.2.1 Issue and Manage S-63 Manufacturer Codes

Successful OEM applicants will be supplied with their own unique Manufacturer ID (M\_ID) and Manufacturer Key (M\_KEY) see [Clause 5.2.4](#) and [Clause 5.2.5](#). These codes must be stored securely together with the manufacturers contact details and whether they are still an active participant in the scheme.

##### 9.5.2.2 Issue M\_ID and M\_KEY listings to Data Servers

Data Servers require the M\_ID and M\_KEY values so that they can identify a specific manufacturer and derive the correct M\_KEY for extracting the Data Clients HW\_ID from the userpermit. The SA will supply Data Servers with a complete list of codes for all approved manufacturers of S-63 compliant systems. This list will be supplied in a protected form every time a manufacturer is added to the list or if the status of a manufacturer changes, e.g. membership of the scheme revoked.

## 9.6 S-63 Test Data

The S-63 data protection scheme is supported by a comprehensive set of test data, see S-63 Appendix 1—Data Protection Scheme Test Data.

## 9.7 Scheme Administrator – Security QA Procedures

### 9.7.1 Documentation

The SA shall hold the documentation for the Data Protection Scheme. This shall be held under change control procedure and the SA shall inform all participants (Data Servers and developers of Data Client applications) of the Data Protection Scheme, of changes to the standard.

Test data for the Data Protection Scheme and a software kernel are also available for system manufacturers to test their implementation for full compliance. The test data and software kernel are described in Appendix A and B and obtainable from the IHO website ([www.ihonet.org](http://www.ihonet.org)).

### 9.7.2 Administration of Confidentiality Agreement

All details required to operate the security scheme and all proprietary information (e.g. M\_KEY) will be provided to interested parties under cover of a Confidentiality Agreement. The SA shall be responsible for administering this agreement. The Confidentiality Agreement will limit the possibilities for participants to breach the Data Protection Scheme.

### 9.7.3 Audit of Security Registers

The SA shall have the ability to audit all security registers maintained by the participants of the Data Protection Scheme. The content of these registers are defined in [Clause 10.3.2.3](#), [Clause 10.3.3.3](#), [Clause 10.7.3](#) and [Clause 11.10.3](#). The SA shall audit these registers to confirm that they are complete and up-to-date. Any problems must be corrected immediately or the participant shall become non-compliant and optionally may be withdrawn from the protection scheme.

### 9.7.4 Creation of M\_IDs and M\_KEYS

The SA shall be responsible for creating and issuing the M\_ID and M\_KEY values used within the Data Protection Scheme. The SA shall record, in a M\_ID / M\_KEY Register all M\_ID/M\_KEY values and which organisations have received which values. The SA will ensure that no duplicate values are created.

The SA will provide information to all Data Servers in the protection scheme on amendments to M\_ID and M\_KEY values.

### 9.7.5 Creation of Digital Signature Keys (Private and Public Keys)

The SA shall have the ability to create a private and public key pair. The private key is used in the certificate signing process and the public key in the signature authentication process.

The private key must be stored securely and access to it limited to only those persons that have a “need to know”. The SA will issue a new public key (and corresponding SA certificate) if the current private key is compromised.

The SA public key should be made available to all participants of the S-63 Data Protection Scheme in both digital and printed forms, e.g. fax and downloadable from a website. The two formats are to be sent or made available by different methods.

### 9.7.6 Acceptance of Self Signed Keys (SSK)

The SA shall confirm that any self signed key provided by a Data Server is bona-fide by contacting the originating organisation. This can be done either by phone, fax or mail but the origins must be confirmed to the Scheme Administrator’s satisfaction before the DS certificate is signed by the SA using the self signed key. The SA is to record all SSKs received in a SSK Register.

### 9.7.7 Creation of Data Server (DS) Certificates

The SA shall be able to create SA signed DS Certificates from the self signed keys provided by a DS and the SA private key. The signed certificate should be authenticated against the DS public key before being sent to the DS. The SA shall keep a record of all DS certificates in a DS Certificate Register.

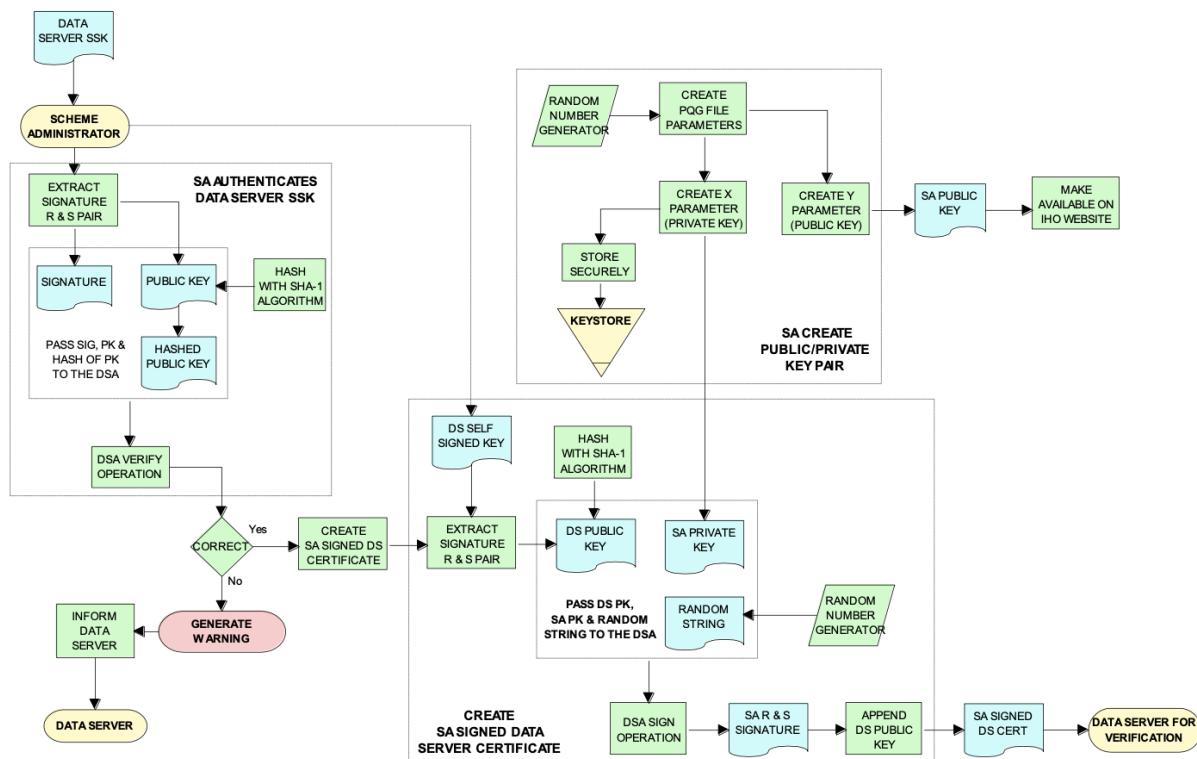
The DS will be required to sign a Confidentiality Agreement before the SA will issue the DS Certificate. The SA will provide information to all participants of the protection scheme on any revoked Data Server Certificates.

### 9.7.8 Creation of Random Strings

In order to sign data (required as part of the certificate creation), the SA will have to create random strings. The SA shall ensure that the same value is not used for any two separate signings. Although it is not possible to guarantee this if the strings are generated randomly. However, the chance of the same string being generated twice is extremely small.

### 9.7.9 Handover of M\_ID and M\_KEY

When a system manufacturer completes their internal compliance testing, they will be required to sign a Confidentiality Agreement before the SA will issue the M\_ID and M\_KEY.



**Figure 9-3 — Scheme Administrator (SA) - SSK Authentication & Certificate Signing Process**

## 10 Data server processes

### 10.1 Overview

Data Servers are responsible for encrypting and signing the ENC information in compliance with the procedures and methods defined by the IHO S-63 Data Protection Scheme.

Hydrographic Offices and RENC organisations are examples of Data Servers. Organisations wishing to become a Data Server must first sign and submit an [S-63 Data Server Agreement](#) together with a completed [Data Server Certificate Request Form](#). This process is outlined in more detail on the IHO website ([www.ihonet.int](http://www.ihonet.int)).

### 10.2 Data Server Processes

The main responsibilities of approved Data Servers operating under the IHO S-63 Data Protection Scheme are depicted in the [Figure 10-1](#). Each top level “Process Box” cross references the particular section where these operations are outlined in more detail.

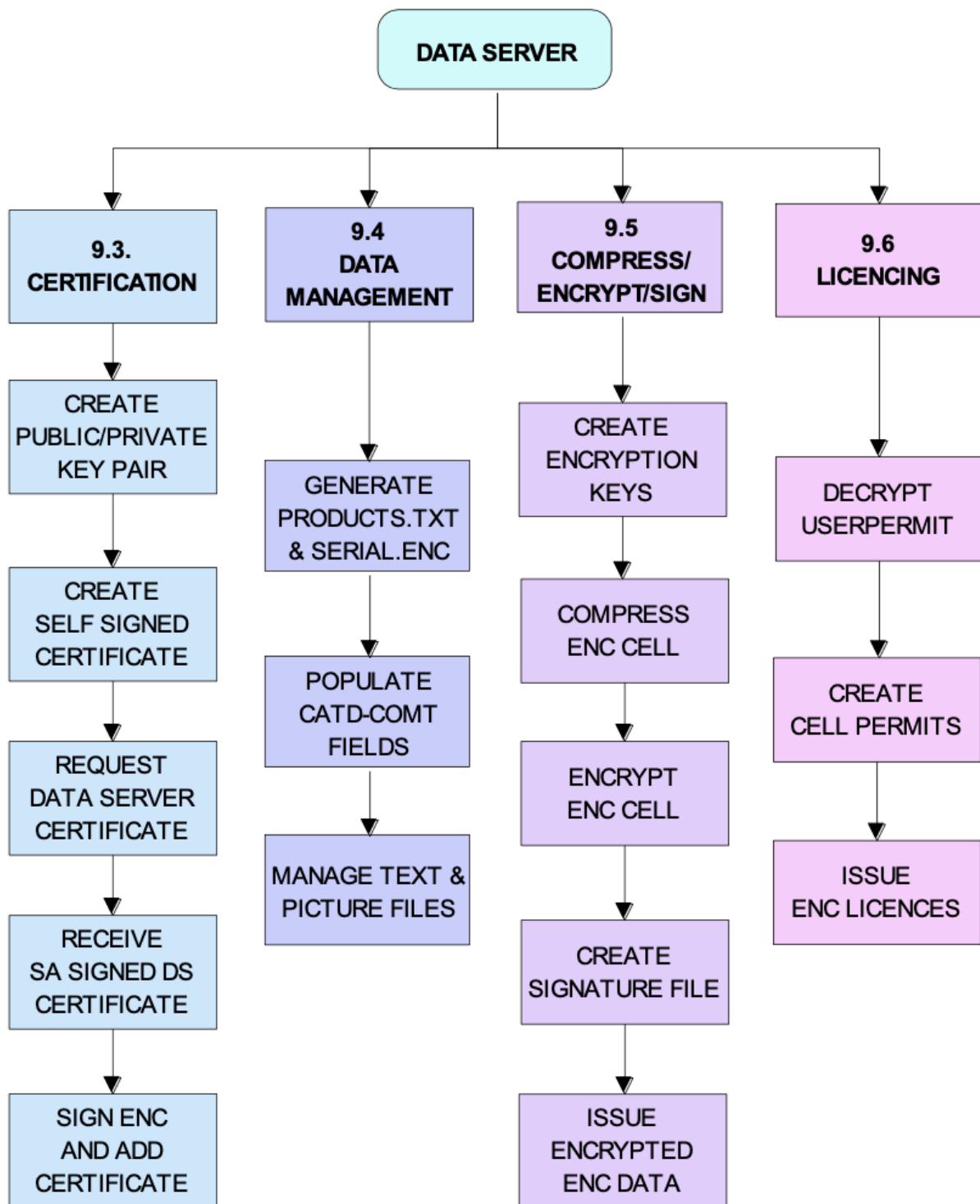


Figure 10-1 — Main Data Server Processes

### 10.3 Certification Processes

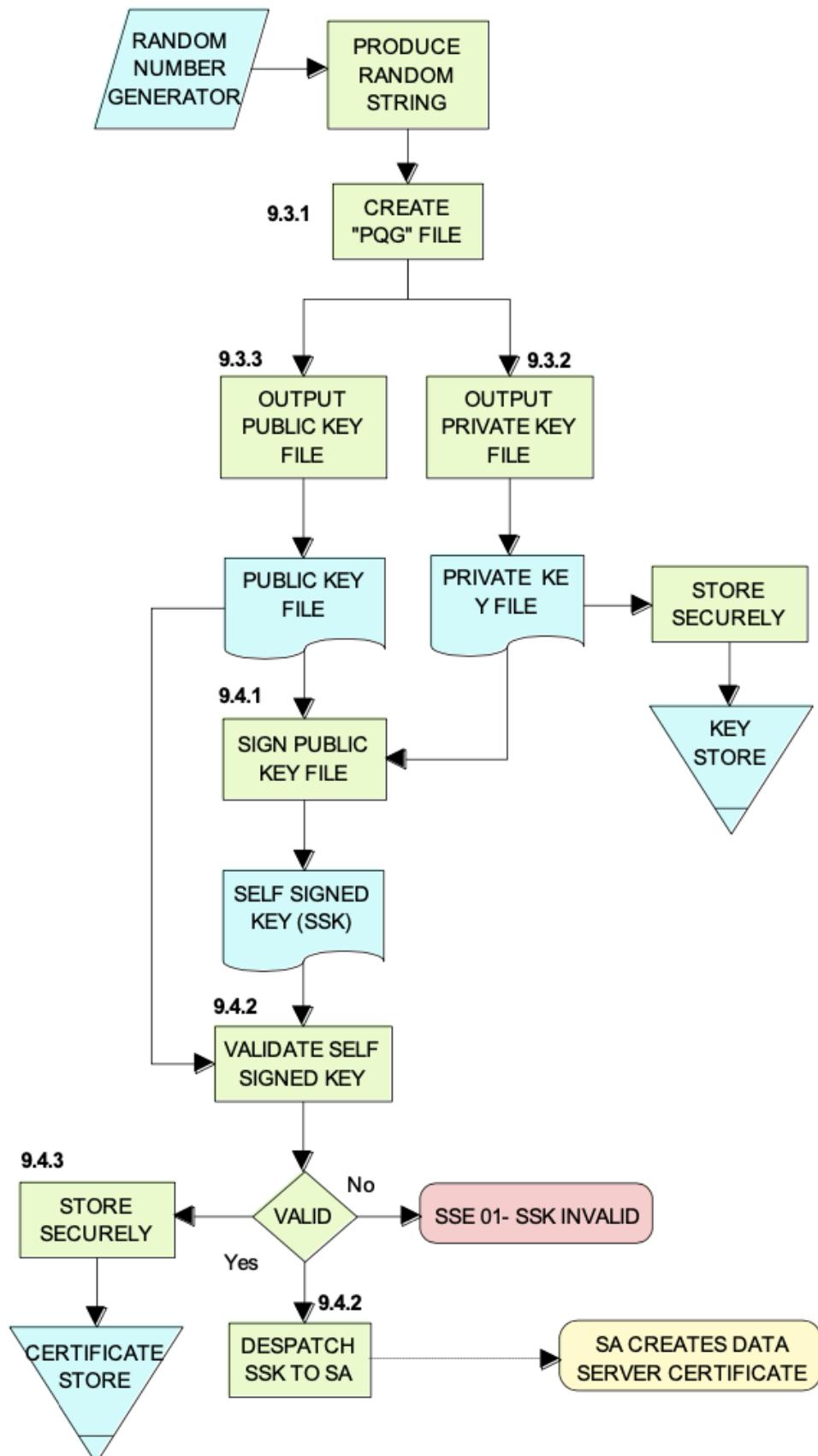
#### 10.3.1 Produce Public/Private Key Pair

Data Servers will need to create a Private and Public Key pair as part of the ‘asymmetric’ encryption methodology adopted by the IHO S-63 Data Protection Scheme. The Data Server’s Public and Private Keys are used in the following functions:

- The Private Key is used to sign the Data Server's Public Key to create a Self Signed Certificate (SSK).
- The Public Key is used to validate the SSK before it is supplied to the SA.
- The Private Key is used to sign all compressed and encrypted ENC data files produced by the Data Server.
- The Public Key is used to check the integrity of the ENC data files in the ECS/ECDIS.

#### **10.3.1.1 Create PQG Signature Parameters**

This procedure is normally performed by the SA and Data Servers during the creation of public/private key **pairs**. Although the PQG parameters generated by Data Servers do not need to be identical to those contained within the SA public key and the SA Digital Certificate, the key lengths used must be identical.



**Figure 10-2 — Data Server Processes - Create Public/Private Key Pair - Produce & Authenticate Self Signed Key (SSK)**

The PQG file only exists by itself for a short period during the creation of the X and Y files. After these have been made, the PQG file will be contained within the X and Y files

The creation of appropriate PQG parameters is covered in the publication Digital Signature Standard (DSS) [NIST FIPS 186 fpd](#).

#### **10.3.1.2 Create Private Key File**

The private key is an output of the PQG generating process. The private key must be stored securely and access limited to only those persons that have a need to know.

Unauthorized possession of the Data Server's private key can potentially undermine the security of the authentication part of the scheme. The Data Server will issue a new public key if the private key is compromised. Details of the X file (Private Key) format are contained in [Clause 6.4.2.2](#).

#### **10.3.1.3 Create Public Key File**

The public key is an output of the PQG generating process. The public key is contained in the SA signed Data Server Certificate that forms part of the ENC Signature File (see [Clause 6.4.2.7](#)). The Data Clients system extracts the public key element of this file to check the integrity of the ENC data file against the ENC signature. Details of the Y file (Public Key) format are contained in [Clause 6.4.2.3](#).

### **10.3.2 Create Data Server Self Signed Key (SSK)**

The SSK is created and submitted to the SA to obtain a Data Server Certificate. The SSK contains the Data Server public key with a signature created by the Data Server. Although the SSK format is identical to the Data Server Certificate defined in [Clause 9.5.1.2](#), the only difference is the SSK is created by the Data Server and the Data Server Certificate which is created and issued by the SA.

The SSK defines a signature of the Data Server's public key. The input to the signature should be the Data Server's public key, formatted according to the Public Key file format as described in [Clause 6.4.2.3](#). The SSK file shall be written as ASCII text with the format, structure and order described in [Clause 6.4.2.5](#).

#### **10.3.2.1 Sign Public Key and Generate SSK**

This procedure is normally performed once by a Data Server to create its self signed key (SSK) which is then sent to the SA who will use it to create a Data Server Certificate. The details of the digital signature algorithm DSA are covered in the publication FIPS 186 Digital Signature Standard (DSS) [NIST FIPS 186 fpd](#). The procedure is as follows:

- 1) Hash the public key file using the algorithm SHA-1 [NIST FIPS 180-1 fpd](#). All bytes within the file are to be hashed.
- 2) Sign the public key file (as hashed at 'b' above) by passing the private key file, the hash of the public key file (as obtained at 'b' above) and a random string through the DSA algorithm [NIST FIPS 186 fpd](#). This will return the two signature elements ('R' and 'S').
- 3) Write these to the self signed key file in the format defined in [Clause 6.4.2.5](#) and append the public key file to form the self signed key file.

#### **10.3.2.2 Authenticate/Validate Data Server SSK**

Data Servers must authenticate the SSK against the Data Server public key to confirm that a valid SSK has been produced.

- 1) Extract the signature elements 'R' and 'S' (i.e. the first two data strings and their attendant headers from the SSK file supplied by the Data Server). This leaves a public key file.
- 2) Hash the public key file using the algorithm SHA-1. All bytes within the file are to be hashed.
- 3) Verify the signature (the elements removed at 'a' above) by passing it, together with the public key file and the hash of the public key file (as obtained at 'b' above) to the DSA. This will return a status valid or invalid.

If the SSK is valid then it can be supplied to the SA with a copy of the Data Server's public key.

#### **10.3.2.3 Store Self Signed Key**

Any SSK produced by the Data Server must be stored securely in a **Certificate Register** and cross referenced with the associated Public/Private Key pair.

### 10.3.3 Validate Certificates

#### 10.3.3.1 Authenticate X509 SA Digital Certificate

This procedure is performed by:

- 1) Data Servers as part of verifying the SA public key required to authenticate the Data Server Certificate
- 2) Data Clients to verify the SA public key to be used to authenticate the digital signatures supplied with the ENC data

The Data Server procedure is as follows:

Manually compare the SA public key contained within the SA Digital Certificate with a copy of the printable public key available from the IHO website ([www.ihonet](http://www.ihonet)). If the above check fails, the Data Server shall not accept the SA Digital Certificate. Otherwise, the SA Digital Certificate is valid and the SA public key it contains can be used in the production of ENC signature files.

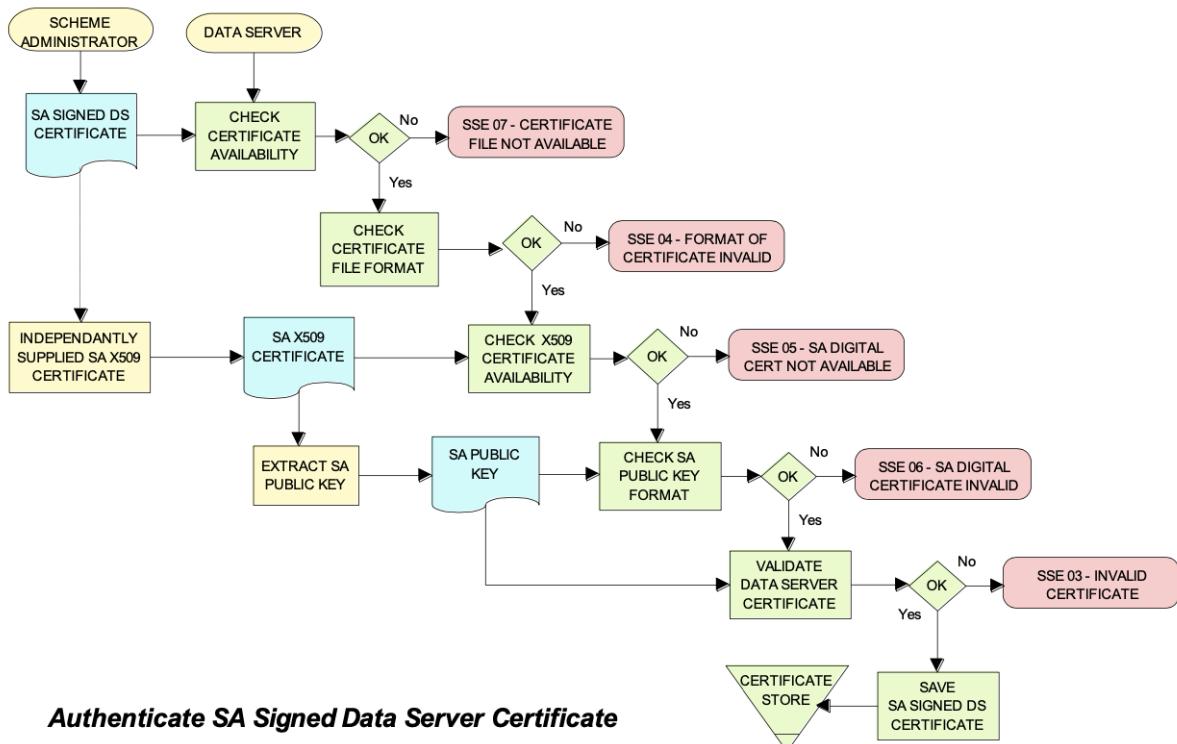
#### 10.3.3.2 Authenticate SA signed Data Server Certificate

This procedure is performed by Data Servers to authenticate the certificate obtained from the SA before it is used. If Data Servers use an automated means of authentication then the software employed should first check the following:

- 1) There is a certificate available to authenticate
- 2) If available, is it in the correct format as per [Clause 6.4.2.6](#)

If a failure is reported in either of these two options the process is to be terminated and an appropriate warning given. Otherwise the process to authenticate should proceed as follows:

- 1) Obtain the SA public key from the IHO website [www.ihonet](http://www.ihonet).
- 2) Extract the signature elements (i.e. the first two data strings and their attendant headers) from the certificate file. This leaves a public key file.
- 3) Hash the public key file (obtained from 'b') using the algorithm SHA-1 [NIST FIPS 180-1 fpd](#). All bytes within the file are to be hashed.
- 4) Verify the signature elements (as removed at 'a' above) by passing it, together with the SA Public Key (the key as obtained in 'a') and the hash of the public key file (as obtained at 'b' above) to the DSA [NIST FIPS 186 fpd](#). This will return a status (correct or incorrect).
- 5) If the Data Server Certificate authenticates correctly, its signature elements 'R' and 'S' may then be used in the construction of ENC digital signatures.



#### 10.3.3.3 Store SA Signed Data Server Certificate

All Certificates provided by the Scheme Administrator must be stored securely in a **Certificate Register** and cross referenced with the associated Public/Private Key pair and SSK.

### 10.4 Data Management Processes

The Data Management processes includes the creation and management of files for inclusion in an encrypted S-63 exchange set, this includes the following:

- 1) The PRODUCTS.TXT file (see [Clause 7.2](#))
- 2) The SERIAL.ENC file (see [Clause 7.3](#))
- 3) The CATD-COMT field of the CATALOG.031 file (see [Clause 7.4.1](#))
- 4) Text and Picture file records in the CATALOG.031 file (see [Clause 8.1](#))

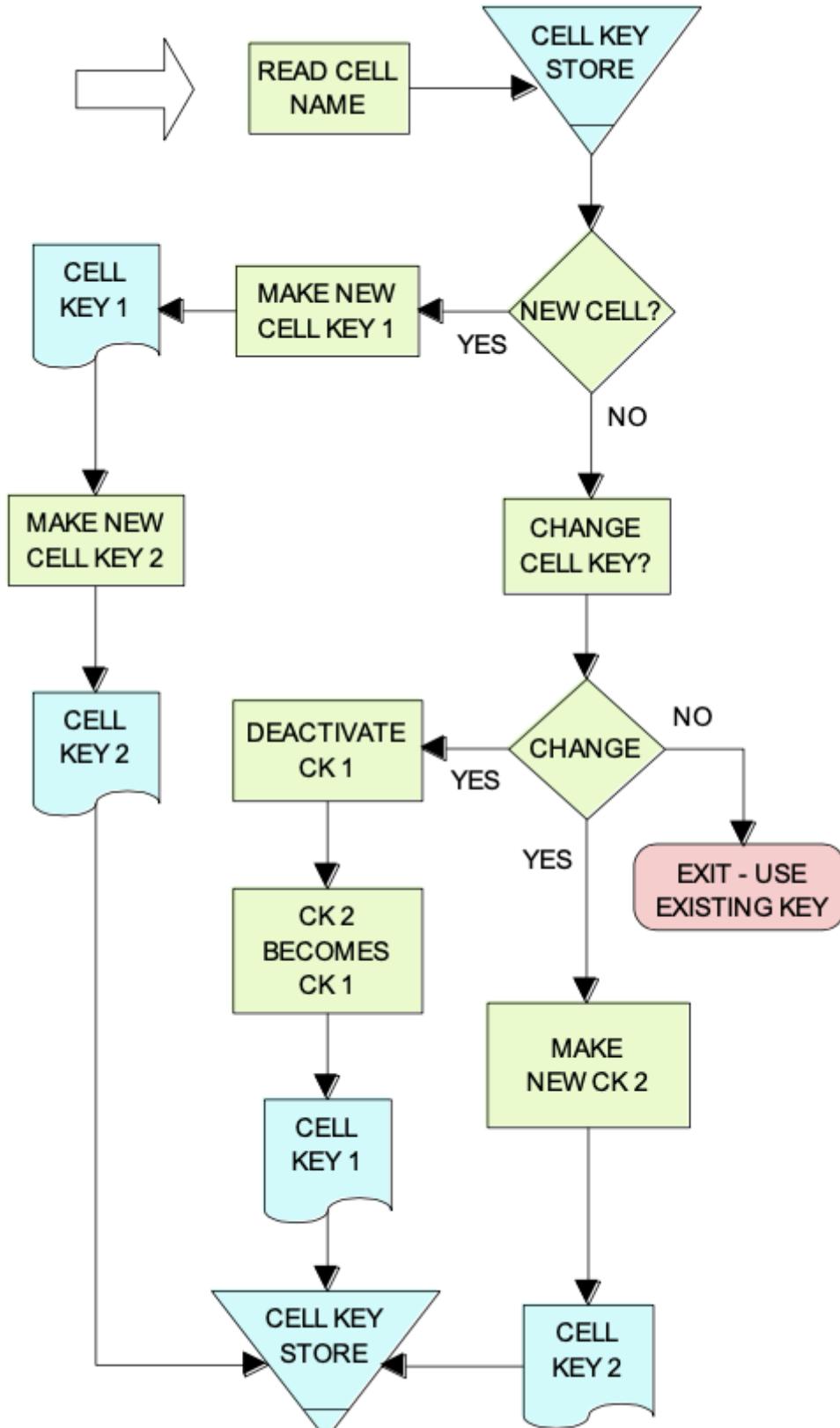
Each requires careful management within the Data Server's production software and should be generated in accordance with the formats and conventions described in [Section 7](#).

### 10.5 Encryption, Compression and ENC Signing Processes

#### 10.5.1 Management of Encryption Cell Keys (ECK)

Each ENC is encrypted using a unique cell key and each ENC permit has the capability to store two encrypted cell keys. These keys may be incremented from time to time at the discretion of the Data Server therefore it is important to manage them in an efficient and effective manner.

To create new cell keys and increment existing ones the Data Server will require an application to automatically manage the keys and store them securely. This application must have a method of generating random strings of the correct length and ideally a means of checking that duplicate cell keys are not produced within a set.



**Figure 10-3 — Data Server Process - Create and Manage Cell Keys**

The application must be able to create new cell keys as well as manage the incrementing of those cell keys already in service. The following steps show the logical processes associated with key management, the [Figure 10-3](#) is used to further illustrate this.

- 1) Get cell name and, if necessary, the edition number and determine whether it is a new cell.
- 2) If new cell make new cell key 1 & 2, if not go to 4?
- 3) Store new keys in the Key Store.
- 4) If not a new cell does the key require changing? If no go to 5, if yes go to 6.
- 5) Exit and keep using the existing cell keys.
- 6) Cell key 1 is now deactivated and cell key 2 now becomes cell key 1 and is flagged as such in the Key Store.
- 7) Create new cell key 2 and add to Key Store.

NOTE The incrementing of the cell keys is at the discretion of the Data Server and is based on the business rules associated with service delivery.

Examples of when keys could be incremented as follows:

- The current encryption keys have been compromised.
- Annually or at an interval defined by the Data Server.
- Synchronized with the issue of a cell new edition.

#### **10.5.1.1 Cell Key Format**

Unencrypted cell keys are 5 bytes long or 10 hexadecimal characters as shown in the example below:

<b>Cell Key 1</b>	C1CB518E9C	5 bytes
<b>Cell Key 2</b>	421571CC66	5 bytes

#### **10.5.2 Compress ENC file (base or update files)**

This procedure is normally performed by the Data Server on ENC files before they are encrypted. The procedure is as follows:

- Compress the ENC cell file using the ZIP standard [ZIP File Format Specification](#) documented at ([www.pkware.com](http://www.pkware.com)).

The resulting compressed ENC file is used as input to the Encryption stage of the scheme. Only the ENC cell files (base and update) are compressed. This process is always completed before the data is encrypted and signed.

#### **10.5.3 Encrypt ENC Files**

##### **10.5.3.1 Base Cell File**

This procedure is performed by the Data Server. The ENC file must be compressed before it is encrypted. The procedure is as follows:

- 1) Select the **Cell Key** to be used for encryption (see conditions at [Clause 10.5.1](#)).
- 2) Encrypt the ENC file using the **Blowfish** algorithm with the **Cell Key** (from 'a') to create an encrypted ENC file.

##### **10.5.3.2 ENC Update File**

This procedure is performed by the Data Server. The ENC update file must be compressed before it is encrypted. The procedure is as follows:

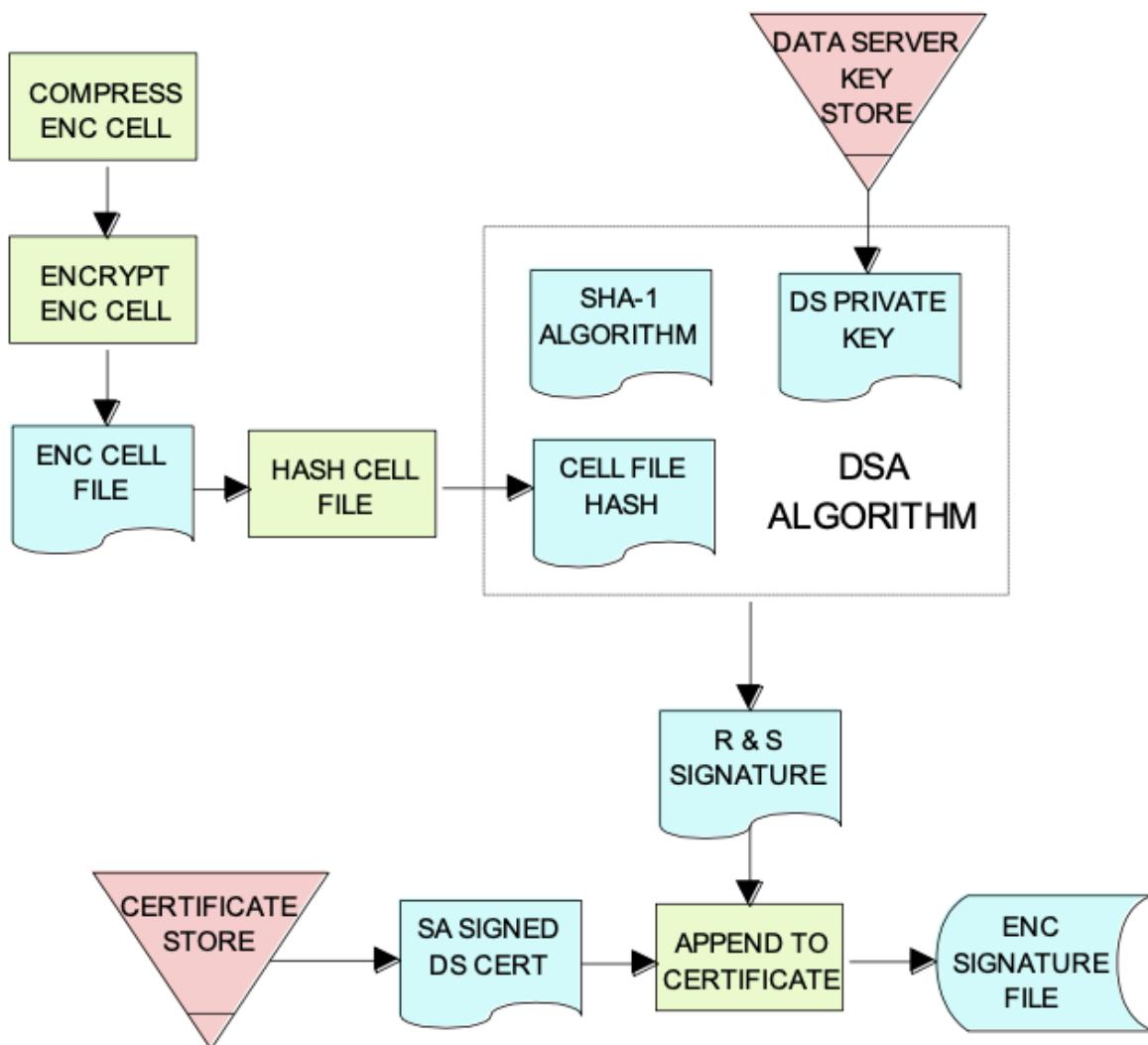
- 1) Select the **Key** used to encrypt the ENC base cell file to which the update applies.
- 2) Encrypt the ENC update file using the **Blowfish** algorithm with the **Key** (from 'a') to create an encrypted ENC update file.

#### **10.5.4 Sign ENC File (Base Cell or Update)**

This procedure is performed by Data Servers to digitally sign their ENC data files. The ENC files must be compressed ([Section 3](#) & [Clause 10.5.2](#)) and encrypted ([Section 4](#) & [Clause 10.5.3](#)) before they are signed. The procedure is as follows:

- 1) Pass the data server private key and the encrypted ENC file contents to the DSA algorithm [NIST FIPS 186 fpd](#). The DSA algorithm will hash the encrypted ENC file using the SHA-1 [NIST FIPS 180-1 fpd](#) algorithm.

- 2) The DSA algorithm will return two cell signature parameters (R & S).
- 3) Write these as the first two data strings within a signature file compliant with the format and naming convention defined in [Clause 6.4](#). The remainder of the file is to be composed of the Data Server Certificate that contains the public key associated with the private key used to create the signature.



**Figure 10-4 — Process to Create ENC Signature Files**

#### 10.5.5 Issue S-63 Encrypted ENC Data

Data Servers will issue S-63 encrypted exchange sets in accordance with the business rules aligned to their data provision services.

### 10.6 Licensing Processes

#### 10.6.1 Decrypt User Permit

This procedure is performed by the Data Server to extract the HW\_ID (unique system identifier) in order to produce cell permits for the Data Client system. The structure of the User Permit is defined in [Clause 5.2.1](#). The Procedure for decryption of the User Permit is as follows:

- 1) Extract M\_ID (4 hex characters) from the User Permit.
- 2) Extract the Check Sum (8 hex characters) from the User Permit.
- 3) Hash the Encrypted HW\_ID (the first 16 characters of the User Permit) using the algorithm CRC32.

- 4) Compare the outputs of 'b' and 'c'. If they are identical, the User Permit is valid. If the two results differ the User Permit is invalid and the HW\_ID cannot be obtained.
- 5) If the User Permit is valid, convert the Encrypted HW\_ID to 8 bytes.
- 6) Decrypt the Encrypted HW\_ID using the Blowfish algorithm with M\_KEY as the key. The output will be HW\_ID.

Data Servers should confirm that any derived HW\_IDS are of the correct length as defined in [Clause 5.2.2](#).

#### EXAMPLE

User Permit	73871727080876A07E450C043031
M_KEY	3938373635 (ASCII)

Output from 'a'	3031	Extracted M_ID
Output from 'b'	7E450C04	Extracted check sum in hexadecimal
Input to 'c'	73871727080876A0	The bytes are given to the hash function left hand byte first (i.e. 73, then 87, then 17 etc)
Output from 'c'	7E450C04	Check Sum of Extracted Encrypted HW_ID in hex.
Output from 'f'	3132333438	HW_ID in hexadecimal.

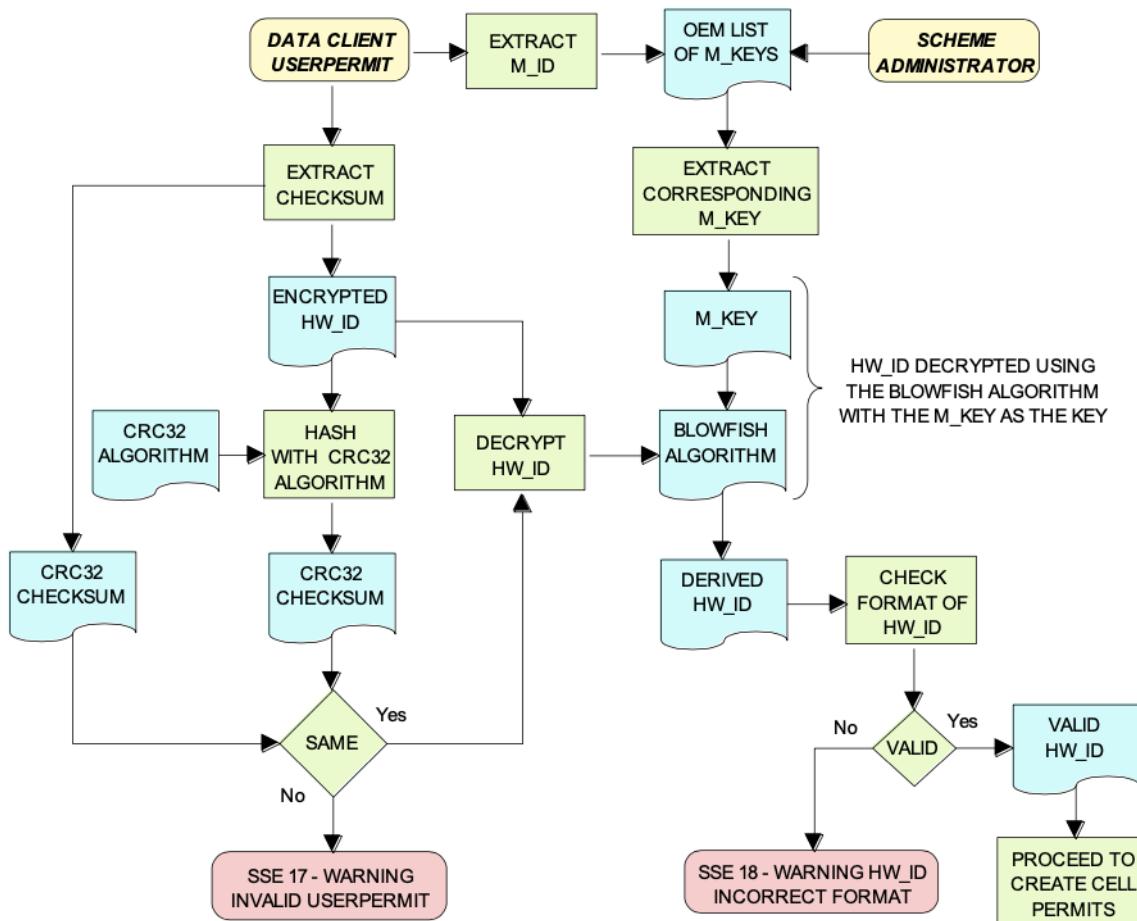


Figure 10-5 — Data Server Process - Extract HW\_ID from Userpermit

#### 10.6.2 Create Cell Permit

The process to create cell permits is performed by Data Servers based on a Data Client's request. The following process is used to generate Cell Permits in accordance with the structure defined in [Clause 5.3](#).

- 1) Remove the file extension from the name of the ENC file. This leaves 8 characters and is the Cell Name of the Cell Permit.
- 2) Append the licence Expiry Date, in the format YYYYMMDD, to the Cell Name from 'a'.
- 3) Append the first byte of HW\_ID to the end of HW\_ID to form a 6 byte HW\_ID (called HW\_ID6). This is to create a 48 bit key to encrypt the cell keys.
- 4) Encrypt Cell Key 1 using the Blowfish algorithm with HW\_ID6 from 'c' as the key to create ECK1.
- 5) Convert ECK1 to 16 hexadecimal characters. Any alphabetic character is to be in upper case.
- 6) Append to 'b' the output from 'e'.
- 7) Encrypt Cell Key 2 (CK2) using the algorithm Blowfish with HW\_ID6 as the key creating ECK2.
- 8) Convert ECK2 to 16 hexadecimal characters. Any alphabetic characters are to be in upper case.
- 9) Append to 'f' the output from 'h'
- 10) Hash the output from 'i' using the algorithm CRC32. Note the hash is computed after it has been converted to a hex string as opposed to the User Permit where the hash is computed on the raw binary data.
- 11) Encrypt the hash (output from 'j') using the Blowfish algorithm with HW\_ID6 as the key.
- 12) Convert output from 'k' to a 16 character hexadecimal string. Any alphabetic character is to be in upper case. This forms the ENC Check Sum.
- 13) Append to 'i' the output from 'l'. This is the Cell Permit.

EXAMPLE

<b>HW_ID</b>	<b>3132333438</b>	5 bytes in hexadecimal
<b>CK1</b>	<b>C1CB518E9C</b>	5 bytes in hexadecimal
<b>CK2</b>	<b>421571CC66</b>	5 bytes in hexadecimal
<b>Cell Name</b>	<b>NO4D0613.000</b>	Valid S-57 cell name including file extension
<b>Expiry Date</b>	<b>20000830</b>	Format YYYYMMDD

Output from 'a'	<b>NO4D0613</b>	This is the Cell Name
Output from 'b'	<b>NO4D061320000830</b>	Cell name + Expiry date
Output from 'c'	<b>313233343831</b>	This is the HW_ID6 in hexadecimal.
Output from 'd' or 'e'	<b>BEB9BFE3C7C6CE68</b>	This is ECK1 in hexadecimal
Output from 'f'	<b>NO4D061320000830BEB9-BFE3C7C6CE68</b>	Cell name + expiry date + ECK1
Output from 'g' or 'h'	<b>B16411FD09F96982</b>	This is ECK2 in hexadecimal
Output from 'i'	<b>NO4D061320000830BEB9-BFE3C7C6CE68B16411FD09F96982</b>	Cell name + expiry date + ECK1 + ECK2
Input to 'j'	<b>NO4D061320000830BEB9-BFE3C7C6CE68B16411FD09F96982</b>	The ASCII values of the output from 'i' (36 bytes in total). The bytes are given to the hash function left hand byte first (i.e. xx, then xx, then xx etc).
Output from 'j'	<b>780699093</b>	CRC32 of 'j' 4 byte number
Output from 'k'	<b>8 byte non-printable</b>	Encrypted CRC32
Output from 'l'	<b>795C77B204F54D48</b>	Encrypted CRC32 in hexadecimal
Cell Permit	<b>NO4D061320000830BEB9BFE3C7C6CE68B16411FD09F96982795C77B204F54D48</b>	

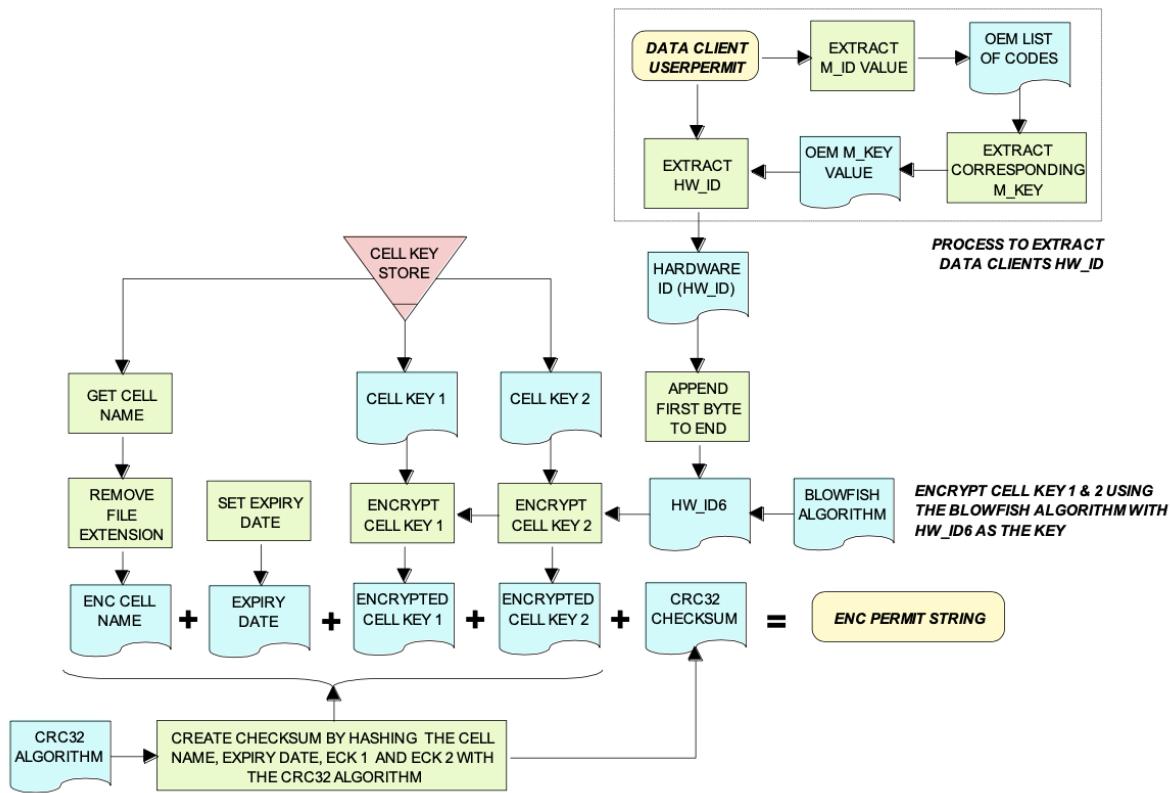


Figure 10-6 — Data Server Process - Create Cell Permit

### 10.6.3 Issue ENC Licences

Data Servers will issue ENC Licences to access S-63 encrypted ENC in accordance with business rules aligned to their data provision services. Data Servers will make the details of their services available to Data Clients before licences are issued.

## 10.7 Security QA Procedures – Data Server

### 10.7.1 Data Protection Scheme Information

The SA will provide copies of all information required to operate the Data Protection Scheme to a Data Server.

### 10.7.2 System Compliance Testing

The Data Server must perform internal compliance testing of their implementation of the protection scheme, based on the descriptions provided in this document and the supplied test data.

### 10.7.3 Storage of M\_IDs and M\_KEYs

When the Data Server joins the scheme, the SA shall provide the Data Server with the proprietary M\_ID and M\_KEY information for all participating manufacturers. The SA shall immediately inform all Data Servers about any amendments to the list of M\_ID and M\_KEYs as new manufacturers join the scheme.

The receipt of all M\_IDs and M\_KEYs by the Data Server are to be recorded securely in an **M\_ID / M\_KEY Register**.

### 10.7.4 Acceptance and Checking of the SA Digital Certificate (and Public Key)

A Data Server will receive the SA public key in two formats, as an X.509 Digital Certificate and as a printable public key. The Data Server shall have the capability to load the SA digital certificate and manually compare the public key against the printed public key. The Data Server shall only accept the SA public key when this has been done. This process applies to the original SA public key and to any subsequent keys issued by the SA.

The Data Server shall maintain records, in a **SA Public Key Register**; of what SA public keys have been used. This should contain a copy of each key as well as the date on which it was issued.

#### **10.7.5 Creation of Digital Signature Keys (Private and Public keys)**

The Data Server shall have the ability to create its own private and public key pair as detailed in [Clause 10.3](#).

The private key must be stored securely with access limited to only those persons who have a need to know. The Data Server will create a new public/private key pair and request a new Data Server Certificate from the SA if its private key is compromised.

The Data Server shall create a self signed key (SSK) and send it to the SA for conversion into a Data Server certificate. Upon receipt, the SA will contact the sending Data Server to confirm that the delivered SSK did originate from its stated source.

#### **10.7.6 Acceptance of the Data Server Certificate from the SA**

The Data Server shall verify and securely store the Certificate returned by the SA by following the process laid out in [Clause 10.3.3.3](#).

#### **10.7.7 Creation of Cell Keys**

The Data Server shall have the ability to create and manage Cell Keys as defined in the [Clause 10.5.1](#). The Data Server is responsible for ensuring that cell keys are securely stored once created.

#### **10.7.8 Compression, Encryption and Signing S-57 data**

The Data Server shall have the ability to compress, encrypt and sign ENC information as defined in [Clause 10.5.2](#), [Clause 10.5.3](#), and [Clause 10.5.4](#). Access to the signing program should be restricted to only those authorised to release data.

#### **10.7.9 Creation of Random Values**

In order to sign ENC information, the Data Server will create random values. The Data Server shall ensure that the same value is not be used for any two separate signatures.

#### **10.7.10 Creation of Cell Permits**

The Data Server must have the ability to create a Cell Permit for a Data Client. The Data Server must issue a new Cell Permit to its Data Clients when an ENC cell is encrypted with a different cell key (e.g. when it is issued as a new edition).

#### **10.7.11 Decryption of User Permits**

The Data Server must have the ability to decrypt User Permits to obtain the Data Client HW\_ID. The HW\_ID is required by the Data Server to create a Cell Permit.

### **11 OEM and Data Client Processes**

#### **11.1 Data Clients**

Data Clients are the users of ENC information and will receive protected information from Data Servers. The OEM is responsible for developing software applications capable of authenticating the ENC digital signatures and decrypting the ENC information in compliance with the procedures defined in the protection scheme. Navigators with ECDIS/ECS systems are examples of Data Clients.

#### **11.2 Original Equipment Manufacturers (OEMs)**

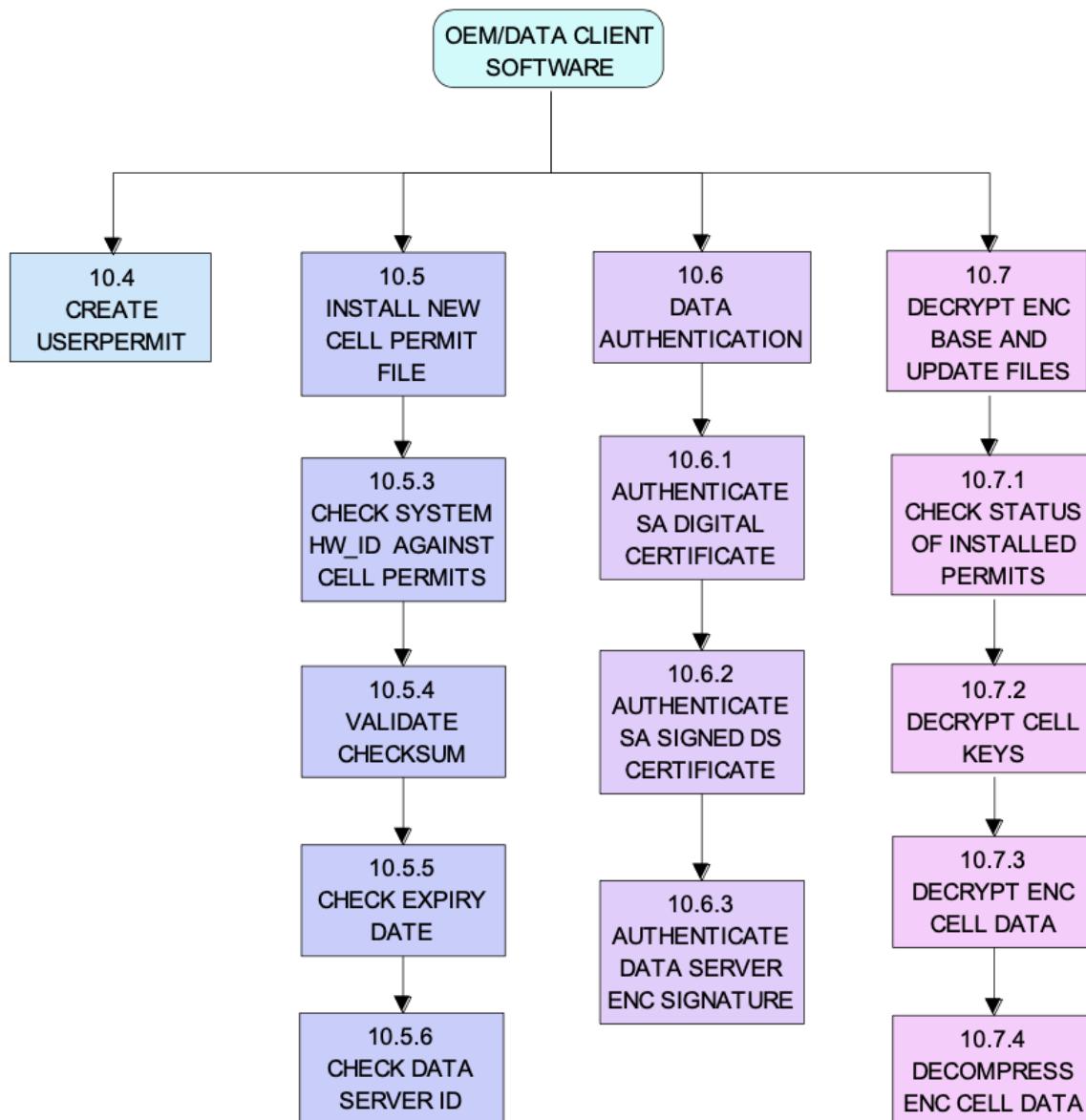
Manufacturers subscribing to the data protection scheme must build software routines in support of the scheme. The S-63 standard contains specifications and test data for validating the manufacturer's software application. The SA will provide the manufacturer with a unique set of manufacturer codes (M\_KEY & M\_ID). The manufacturer must also provide a secure mechanism within their software systems for uniquely identifying each end user installation. The data protection scheme requires each installation to have a unique hardware identifier (HW\_ID). The Data Servers will use the M\_KEY and HW\_ID

information to issue encrypted ENC cell keys to a Data Client specific installation. Each ENC is encrypted with a unique cell key however; by encrypting these using the Data Client's unique HW\_ID this ensures that they cannot be transferred between different ECDIS supplied by the same manufacturer.

The manufacturer is required to cooperate in the protection of the ENC information within end user systems. For example, if a hardware device such as a dongle is used to store the HW\_ID the Data Client must, periodically check for its continued presence. The Data Client must cease to operate if the device is removed after the application is started. On a networked system the security device must control the number of concurrent users of the application; this will depend on the terms and conditions of a Data Server's service.

### 11.3 OEM & Data Client Processes

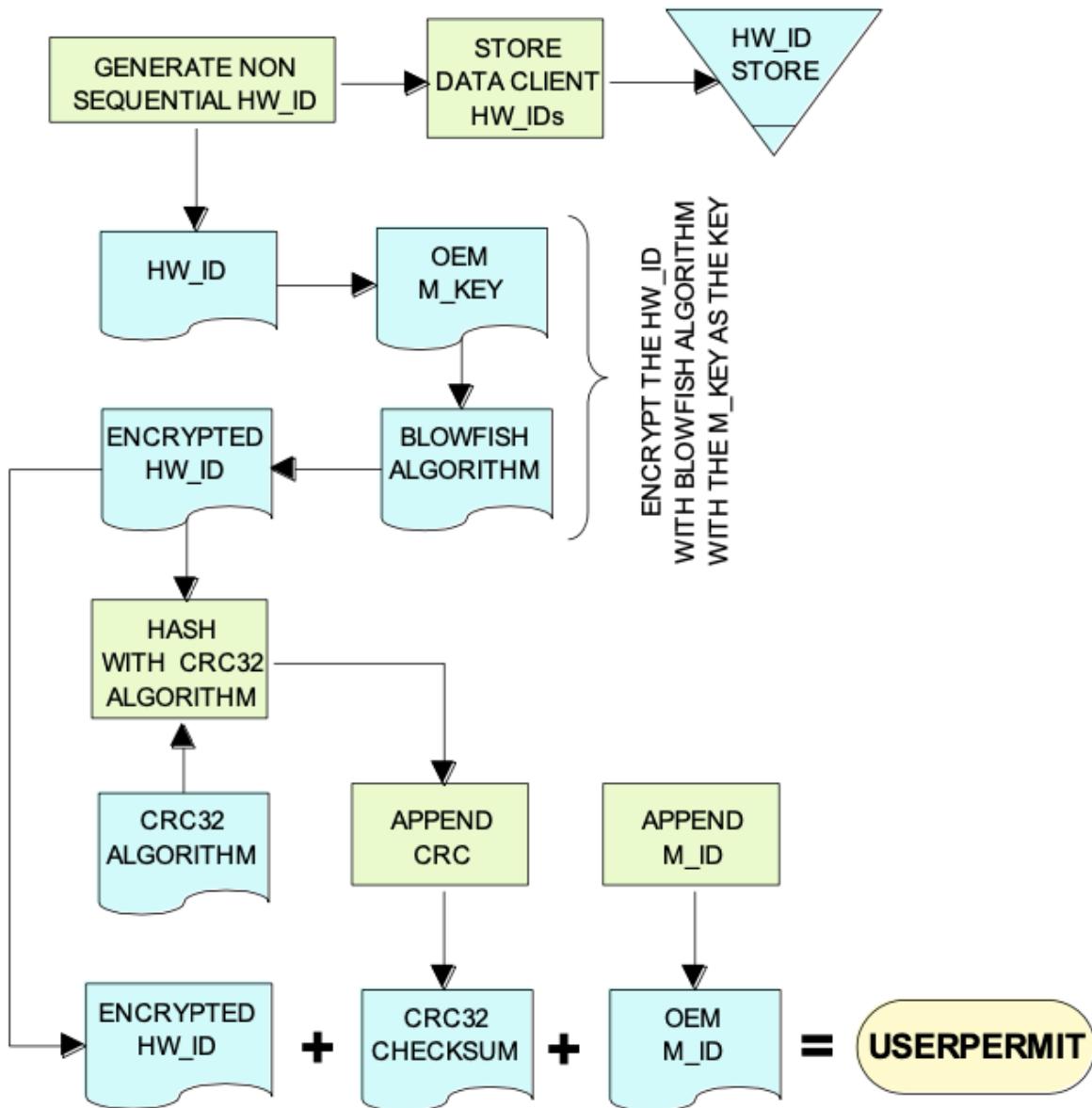
The main responsibilities of approved OEMs and their software applications are depicted in the [Figure 11-1](#). Each “Process Box” cross references the particular section where these operations are detailed.



**Figure 11-1 — Main OEM/Data Client Processes**

## 11.4 Create Data Client Userpermit

This procedure is performed by the system manufacturer (OEM) who creates a Data Client specific userpermit. This is provided to the Data Client usually when purchasing an ECS/ECDIS. This userpermit enables Data Clients to obtain cell permits from Data Servers. The cell permits are generated using the encrypted HW\_ID that is contained within the userpermit. The format and structure of the User Permit is defined in [Clause 5.2](#).



**Figure 11-2 — OEM - Create Userpermit**

The procedure for creating a User Permit is as follows:

- 1) Encrypt HW\_ID using the Blowfish algorithm with M\_KEY as the key.
- 2) Convert the resultant value to a 16 character hexadecimal string. Any alphabetic character should be in upper case.
- 3) Hash the 16 hexadecimal characters using the algorithm CRC32.
- 4) Convert output from 'c' to an 8 character hexadecimal string. Any alphabetic characters should be in upper case. This is the Check Sum.
- 5) Append to 'b' the output from 'd'.
- 6) Convert the M\_ID to a 4 character string. Any alphabetic characters should be in upper case.

7) Append to 'e' the output from 'f'. This is the User Permit.

#### EXAMPLE

<b>HW_ID</b>	3132333438 (ASCII)
<b>M_KEY</b>	3938373635 (ASCII)
<b>M_ID</b>	3031 (ASCII)

#### Expected Results:

<b>Input to 'a'</b>	3132333438 and 3938373635	<b>HW_ID and M_KEY in hexadecimal.</b>
Output from 'a'	8 bytes	Non-printable.
Input to 'c'	73871727080876A0	The hexadecimal values of the above string. The bytes are given to the hash function left hand byte first (i.e. 73, then 87, then 17 etc)
Output from 'c'	7E450C04	CRC32 result in hexadecimal
Output from 'e'	73871727080876A07E45-0C04	CRC32 result appended to the encrypted HW_ID
Output from 'f'	3031	Result appended to encrypted HW_ID & CRC32
User Permit	73871727080876A07E45-0C043031	

## 11.5 ENC Cell Permit Installation

New Cell permits are delivered to a Data Client's system in a file named PERMIT.TXT. The structure and format of this file are given in [Clause 5.3](#). The Data Clients system must be able to read in this file and perform a number of checks. Each cell permit record contains a Data Server ID that enables OEMs to manage permits and data in a multi supplier environment. The following sections outline how this file must be managed and the checks that must be carried out when installing a new permit file.

### 11.5.1 Check for a Cell Permit

The Data Client system must first check that a valid cell permit is available to install. A facility should be available for Data Clients to browse to a specific location on the system where the PERMIT.TXT file is available to install. If any text file other than one named PERMIT.TXT file is selected the system should return a warning as follows:

***"SSE 11 — Cell permit not found"***

### 11.5.2 Check Cell Permit Format

If a valid PERMIT.TXT is located the system must then check that the format of the file is correct as defined in [Clause 5.3](#). If not the data client must inform the user as follows:

***"SSE 12 — Cell permit format is incorrect"***

### 11.5.3 Check the HW\_ID

Data Client system must check that the HW\_ID encoded into the dongle/software security device is comparable with the HW\_ID encrypted in the cell permits. If the values are the same the system shall continue with the checks below, if not an error message must be returned as follows:

**~~"SSE 19 — Permits are not valid for this system. Contact your data supplier to obtain the correct permits".~~**

#### 11.5.4 Check Cell Permit Check Sum

This procedure is performed by the Data Client system and is comprised of the following steps.

- 1) Extract the last 16 hex characters (ENC Check Sum) from the Cell Permit.
- 2) Convert these 16 hex characters to 8 bytes.
- 3) Hash the remainder of the Cell Permit as left after 'a' using the algorithm CRC32.
- 4) Append the first byte of HW\_ID to the end of HW\_ID to form a 6 byte HW\_ID (called HW\_ID6).
- 5) Encrypt the hash (output from 'c') using the Blowfish algorithm with HW\_ID6 as the key.
- 6) Compare the output from 'e' with the output from 'b'. If they are the same, the Cell Permit is valid. If they differ, the Cell Permit is corrupt and Cell Permit is not to be used.

##### EXAMPLE

HW_ID	3132333438	in hexadecimal
Cell Permit	NO4D061320000830BEB9BFE3C7C6CE68B16411FD-09F96982795C77B204F54D48	Example cell permit

Output from 'a'	795C77B204F54D48	In hexadecimal
Output from 'b'	8 byte non-printable	Encrypted CRC32
Input to 'c'	NO4D061320000830BEB9-BFE3C7C6CE68B16411FD09F96982	Cell permit after removal of 16 hex encrypted CRC32The bytes are given to the hash function left hand byte first (i.e. xx, then xx, then xx etc).
Output from 'c'	780699093	4 byte CRC32 of cell permit after removal of 16 hex encrypted CRC32
Output from 'd'	313233343831	This is HW_ID6
Output from 'e'	8 byte non-printable	Encrypted CRC32

If the calculated CRC32 value is not the same as the value contained in the cell permit the system must inform the Data Client as follows:

***"SSE 13 Cell Permit is invalid (checksum is incorrect) or the Cell Permit is for a different system".***

The system must not install any invalid permits.

#### 11.5.5 Check Cell Permit Expiry Date

When installing a new PERMIT.TXT file the Data Client system must check that the permits being installed have not expired. The system must check that the expiry date of each permit against the system date (Computer Clock) and if available the time from the GPS receiver/signal. If the permits have expired the following message should be displayed as follows:

***"SSE 15 — Subscription service has expired. Please contact your data supplier to renew the subscription licence."***

NOTE The system may install expired/valid permits but any cells subsequently displayed in the viewer under these conditions **MUST** display a permanent warning to the user as follows:

***"SSE 25 — The ENC Permit for this cell has expired. This cell may be out of date and MUST NOT be used for NAVIGATION."***

See [Clause 11.7.1.1](#) for checking the expiry date at load time.

If the expiry date of the permit is in advance of the computer clock/GPS signal then a further check must be made to see how long the licenced subscription has to run. If this is 30 days or less then the system should give a warning informing the Data Client as follows:

***"SSE 20 — Subscription service will expire in less than 30 days. Please contact your data supplier to renew the subscription licence."***

The Data Client can then take steps to renew the licence before it expires. The system should then proceed to install the permits. If the permit has more than 30 days before expiring the permits should be installed without warning.

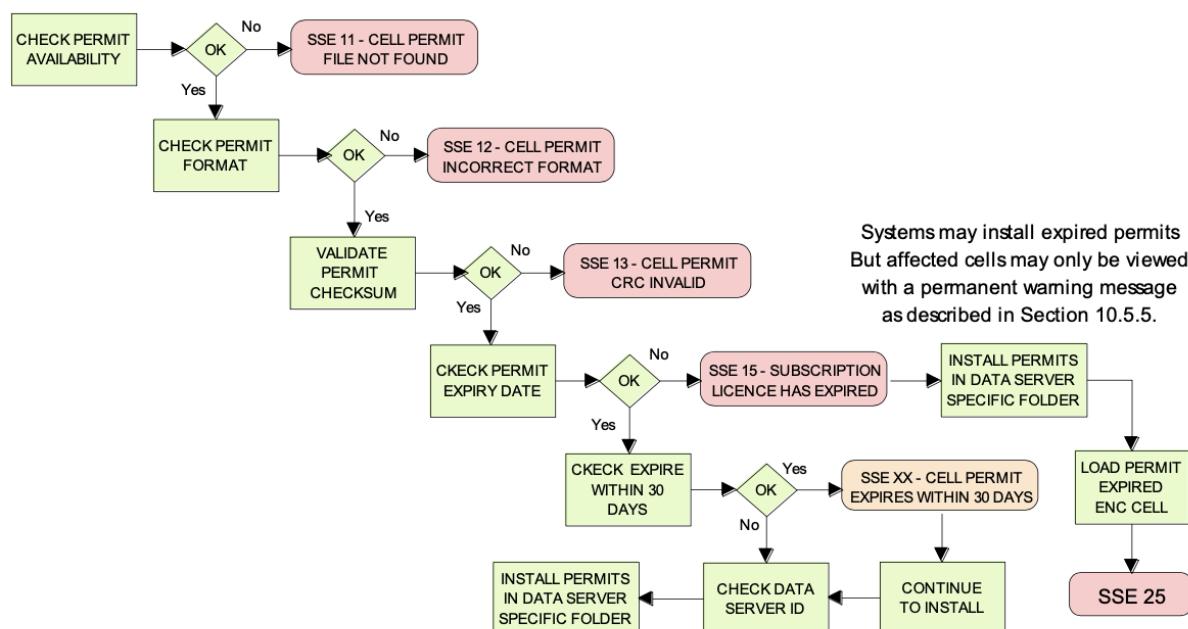
### 11.5.6 Check Data Server ID

The S-63 Data Protection Scheme makes takes account of a multiple supplier environment, that is to say Data Clients may obtain licences from more than one Data Server. There are several instances where Data Clients may have ENC data from multiple suppliers as follows:

- Duplicate cells licenced from different Data Servers
- Change from one Data Server to another

It is important that Data Client systems are able to manage these instances. Each permit record contains a Data Server ID field (see [Clause 5.3.3](#)). This field, if filled, contains a two character alphanumeric ID unique to each Data Server assigned by the SA. Since cell permits issued by one Data Server will not necessarily decrypt ENCs supplied by another it is important to maintain an association between the cell permits and encrypted ENCs. OEMs should ensure that their systems are capable of maintaining these associations, e.g. by creating Data Server specific folders where permits are stored.

The Data Server ID for encrypted ENC exchange sets is contained in the SERIAL.ENC file (see [Clause 7.3.1](#)) and is identical to that contained in the cell permit record.



**Figure 11-3 — OEM System - Install & Validate Cell Permit**

### 11.6 ENC Authentication and Integrity Checks

OEM systems must be capable of authenticating the source of the encrypted ENC data and validate its integrity. This is achieved in two ways as follows:

- By Authenticating the SA signature held as part of the Data Server Certificate that forms part of the ENC signature file.
- By validating the Data Server ENC signature (corresponding to the ENC Cell Data) in the ENC signature file.

OEMs and Data Clients must first of all confirm that the SA certificate (whether X509 or ASCII format) installed on the ECS/ECDIS is correct and current. This is dealt with in [Clause 11.6.1](#) below.

### 11.6.1 Authenticate/Verify SA Digital Certificate

This procedure is performed by OEMs or Data Clients to verify that the SA public key installed on the ECS/ECDIS is correct and current in respect of the IHO S-63 Data Protection Scheme. It is this SA public key that is used to authenticate the SA signed Data Server Certificate supplied by Data Servers as part of the ENC signature file. The procedure is as follows:

Manually compare the SA public key contained within the independently installed SA Digital Certificate with a copy of the printable public key available from the IHO website ([www.ihonet.org](http://www.ihonet.org)). If the above check fails, the system shall not accept the SA Digital Certificate. Otherwise, the SA Digital Certificate is valid and the Data Server public key it contains can be used to authenticate SA signed Data Server Certificate held as part of the ENC signature file.

**NOTE** The Data Client must have means by which users can access the installed certificate from the application.

#### 11.6.1.1 Manual Checking of the SA Public Key

The SA public key can be accessed from the IHO website as follows:

[www.ihonet.org](http://www.ihonet.org) → Home → Publications → Download List → S-63 → S-63 SA Certificate

The following webpage will be displayed:

#### S-63 DIGITAL CERTIFICATES

*Digital Certificates are files that bind a specific public key together with other information to an individual or organisation. The S-63 standard uses a 2-level chain of certificates to operate the data protection scheme.*

*The IHO Secretariat operates as the Scheme Administrator and has issued the root Digital Certificate for use within the protection scheme. The SA certificate used by IHO Secretariat will be a self-signed certificate. It is available both as a X-509 compliant file **IHO.CRT** and as a text file **Scheme Administrator Public Key.txt**. Both files are contained in an **SA Certificate** compressed file.*

*The SA will issue Data Server Certificates to all Data Servers participating in the protection scheme. The Data Server Certificate contains the Data Server Public Key and the SA signature of this Key. Since only the SA can issue Data Server Certificates, the chain of trust can be established by authenticating the SA signature on the Data Server Public Key.*

*The protection scheme requires the SA public key to be installed on end user systems by all users of the protection scheme. The Data Server Certificate is contained within each signature file and the Data Server Public Key can be trusted if the SA certificate is valid. The installation of the SA certificate (and the public key held within) should be carried out as a separate, independent operation and be subject to carefully controlled operating procedures.*

In the second paragraph above click on “**SA Certificate**” link and a “**File Download**” dialog will be displayed which gives the user the option to “**Open**” or “**Save**” the zipped file named “**S-63\_SA\_Certificate.zip**”. This file contains two files as follows:

##### 1) IHO.CRT (The X509 Certificate)

Opening this file reveals a “**Certificate**” dialog, selecting the “**Details**” tab and highlighting “**Public Key**” displays the IHO public key. The example below is the IHO public at the time this document was published. Note that the first 4 or 6 characters [024100] represent the certificate parameters and can be either positive [0240] or negative [024100].

**EXAMPLE:** 0241 0096 3F14 E32B A537 2928 F24F 15B0 730C 49D3 1B28 E5C7 6410 0256 4DB9  
5995 B15C F880 0ED5 4E35 4867 B82B B959 7B15 8269 E079 F0C4 F492 6B17 761C C89E  
B77C 9B7E F8

This character string (minus the certificate parameters) should be compared with the installed certificate to confirm that they are the same. If it is, then the certificate is authentic, if not, it should be rejected.

##### 2) Scheme Administrator Public Key.txt

Opening this file displays the following SA public key parameters.

```
EXAMPLE: // BIG p FCA6 82CE 8E12 CABA 26EF CCF7 110E 526D B078 B05E DECB CD1E B4A2
08F3 AE16 17AE 01F3 5B91 A47E 6DF6 3413 C5E1 2ED0 899B CD13 2ACD 50D9 9151 BDC4 3EE7
3759 2E17. 962E DDCC 369C BA8E BB26 0EE6 B6A1 26D9 346E 38C5. 6784 71B2 7A9C F44E E91A
49C5 147D B1A9 AAF2 44F0 5A43 4D64 8693 1D2D 1427 1B9E 3503 0B71 FD73 DA17 9069 B32E
2935 630E 1C20 6235 4D0D A20A 6C41 6E50 BE79 4CA4. 963F 14E3 2BA5 3729 28F2 4F15 B073
0C49 D31B 28E5 C764 1002 564D B959 95B1 5CF8 800E D54E 3548 67B8 2BB9 597B 1582 69E0
79F0 C4F4 926B 1776 1CC8 9EB7 7C9B 7EF8.
```

If this file is used for authentication it should be checked against the installed certificate or public key file. If checking against an installed certificate then only the “**BIG y**” string should be verified to see if it is the same. If checking against SA public key file then all parameters must be verified to see if it is the same. In either case if the file is correct then the public key is authenticated, if not, it must be rejected.

### 11.6.2 Authenticate SA signed Data Server Certificate

This procedure is performed by the Data Client's system to authenticate the SA signed Data Server Certificate stored as part of the ENC signature file against the installed SA public key. This process is carried out before the Data Server public key is extracted to authenticate the ENC signature. Refer to [Clause 6.3.2](#) for the structure of signature/certificate pairs in a signature file.

Prior to the authentication process the system must first check the availability, format and status of the certificate or public key installed on the system. If there are any problems this should be reported to the data client in a meaningful way as follows:

- 1) The SA certificate or public key is not present on the system (**SSE 05** and terminate process).
- 2) The format of the SA certificate or public key is incorrect (**SSE 08** and terminate process).
- 3) The SA certificate has expired (**SSE 22** and terminate process).

The authentication procedure is outlined below:

- 1) Extract the ENC signature file.
- 2) Discard the first signature part (i.e. the first two data strings and their attendant headers. This is the Data Server signature of the ENC data). This leaves the SA signed Data Server Certificate.
- 3) Extract the remaining signature part (i.e. the first two data strings and their attendant headers from the remaining file obtained from ‘b’). This leaves a public key file.
- 4) Hash the public key file (obtained from ‘c’) using the algorithm **SHA-1 NIST FIPS 180-1 fpd**. All bytes within the file are to be hashed.
- 5) Verify the signature part (as removed at ‘c’ above) by passing it (the signature), together with the SA Public Key file (the key) and the hash of the public key file (obtained at ‘d’) to the **DSA NIST FIPS 186 fpd**. This will return a status (correct or incorrect).

If incorrect the system must terminate the process and return the following warning message:

**“SSE 06 — “The SA Signed Data Server Certificate is invalid. The SA may have issued a new public key or the ENC may originate from another service. A new SA public key can be obtained from the IHO website or from your data supplier”**

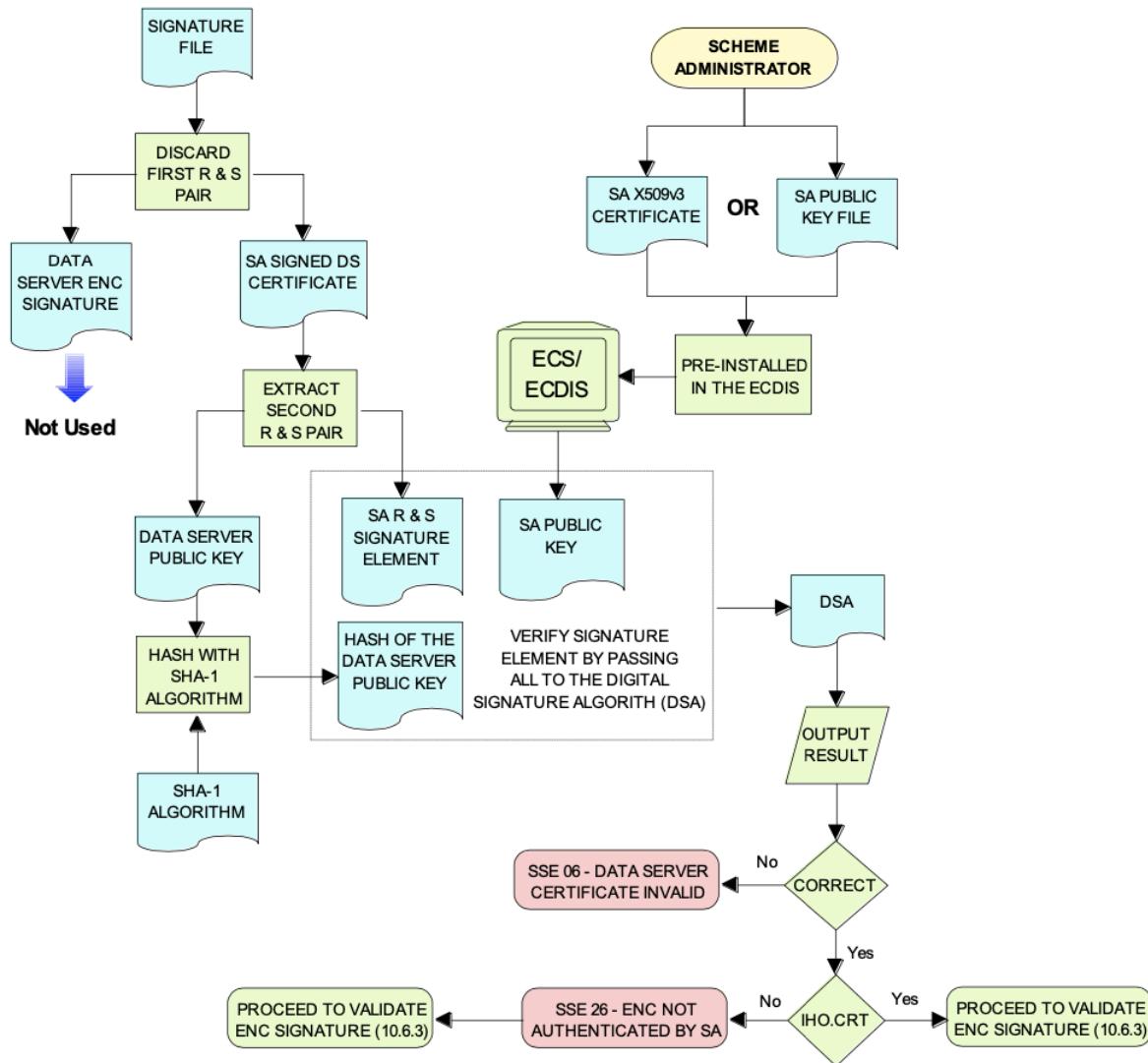
#### 11.6.2.1 Authentication against non-SA signed Data Server Certificate

There may be instances where there is more than one certificate or public key stored on the data client. This may be especially so during the transition to the correct use of the S-63 scheme. Therefore a check is necessary to ensure that the data server certificate authenticates correctly with the IHO.CRT or IHO.PUB installed on the data client.

If the data server certificate authenticates against anything other than the IHO.CRT or IHO.PUB stored on the data client then a warning message **MUST** be displayed as follows:

**“SSE 26 — “This ENC is not authenticated by the IHO acting as the Scheme Administrator”**

It is only necessary for data clients to display this warning once and not for every repeated occurrence of the same failure in an exchange set. If this message is displayed the data client should still continue to the next stage of authentication (ENC signature authentication) and decryption.



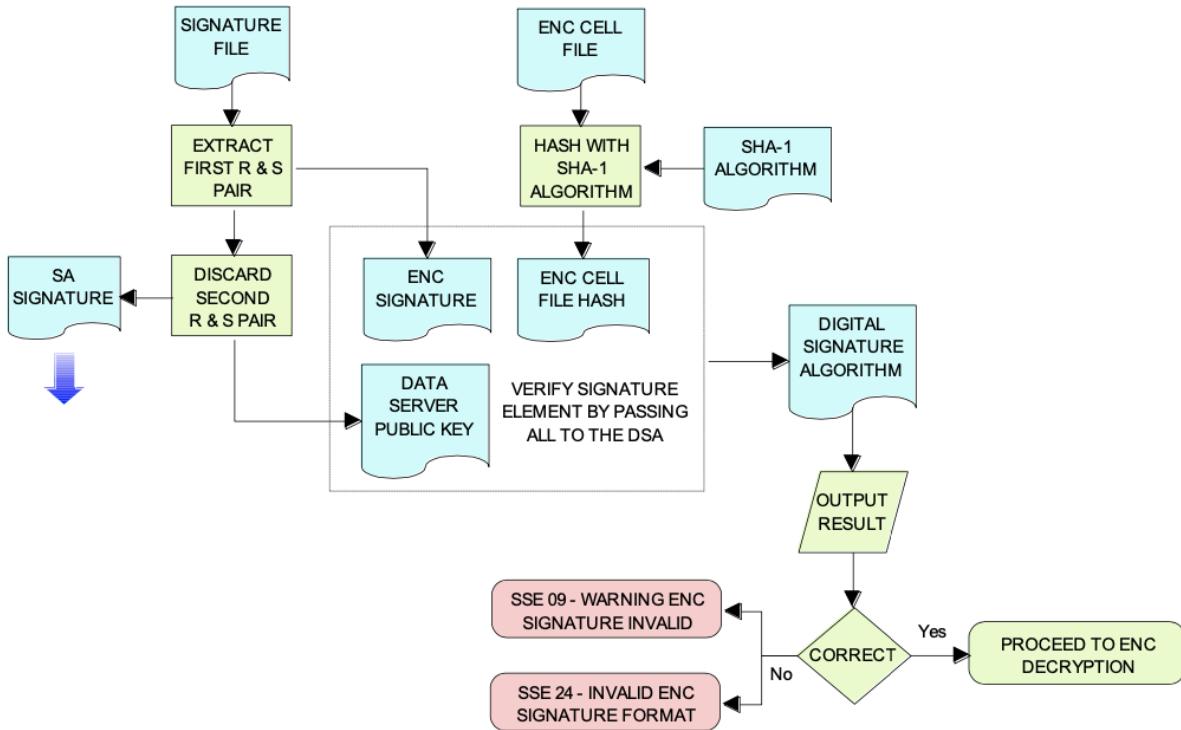
**Figure 11-4 — Authenticate SA Signed Data Server Certificate**

### 11.6.3 Authenticate ENC Cell File

This procedure is performed by Data Client's systems to validate the ENC signature (held in the ENC signature file) corresponding to a specific ENC cell file. It is expected that the Data Client has already performed the procedures to authenticate the SA digital certificate ([Clause 11.6.1](#)) and the Data Server Certificate within the signature file ([Clause 11.6.2](#)). The procedure to authenticate the ENC Cell File is as follows:

- 1) Extract the ENC signature file uniquely related to an ENC cell file.
- 2) Extract the first signature part (i.e. the first two data strings and their attendant headers). This leaves the certificate.
- 3) Discard the remaining signature part (i.e. the first two data strings and their attendant headers from the remaining file). This leaves a public key file.
- 4) Hash the associated ENC Cell File using the algorithm **SHA-1 NIST FIPS 180-1 fpd**. All bytes within the file are to be hashed.
- 5) Verify the signature part (as extracted at 'b' above) by passing it (the signature), the public key—as left at 'c' above (the key) and the hash of the ENC Cell File, as obtained at 'd' above, to the **DSA NIST FIPS 186 fpd**. This will return a status (correct or incorrect).

If the ENC signature is not authenticated correctly, the Data Client shall not decrypt the ENC because its origins cannot be verified. If the ENC is authenticated correctly, the ENC can safely be decrypted.



**Figure 11-5 — Authenticate ENC Cell File - Validate ENC Signature**

## 11.7 Decrypt ENC Base Cell and Update Files

Before decrypting new ENC base cells and update files the system should first check the subscription status of installed cell permits. This process is to determine whether the Data Client is licenced to receive and install new ENC data. It also seeks to give the Data Client adequate warning messages prior to the expiry of the licence.

### 11.7.1 Check Subscription Status of Installed Permits

[Clause 11.5](#) identified the processes and checks that are carried by the Data Client's system when installing cell permits. This section determines how cell permits are managed by a Data Client's system once installed. It is also designed to give Data Clients advanced warning of subscription permits that are about to expire, especially when ENC data is being used for navigation.

#### 11.7.1.1 Check if Subscription has expired in a Cell Permit – Required Warning

This check is performed on new ENC base cells and update files prior to decryption. This check is required to inform the Data Client that the subscription licence has expired but that additional ENC updates/base cells have become available. The warning is only applicable for subscription licenses and is not to be used for single purchase licenses, ref. [Clause 5.3.3](#). The procedure is outlined in the flowchart below and the subsequent step by step description:

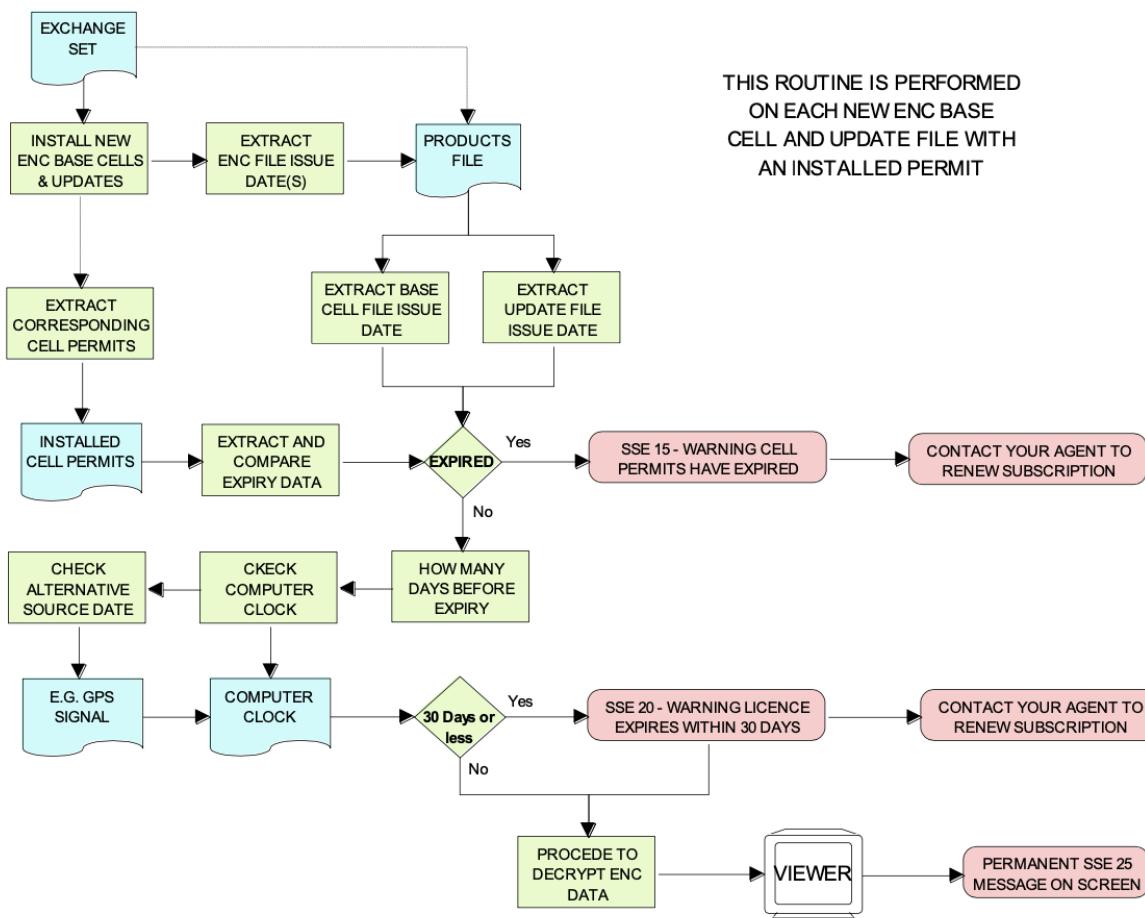
- 1) Extract expiry date of the loaded ENC Cell Permit corresponding to the ENC file to be decrypted.
- 2) Extract the issue dates of the ENC base cell and latest update file (if available<sup>11</sup>) to be decrypted from the PRODUCTS.TXT file. These are located in the second (Product Issue Date) and fourth (Issue Date of Latest Update) fields of the cell record corresponding to the cell being decrypted.

<sup>11</sup> If no updates have been issued for a cell there will be no information available.

- 3) If two dates (in fields two and four) are returned at b) then only the latest date<sup>12</sup> should be used when checking against the expiry date.
- 4) If the Issue Date of the base cell or the update obtained at b) and c) is newer (in advance of) the permit expiry date obtained at a) the permits are deemed to have expired. A warning message must be displayed as follows:

***"SSE 15 — Subscription service has expired. Please contact your data supplier to renew the subscription licence."***

The application may **install expired ENC permits** but must display the **"SSE 15"** warning above. It may also decrypt any ENC base cells and update files dated prior to the expiry date of the permits. This can be managed by using the issue date [ISDT] contained in the CATD-COMT field at import. No base cells or updates should be imported if the issue date [ISDT] is greater than the expiry date of the installed cell permits. The application must also display a permanent warning when cells with expired permits are viewed in the data client, see [Clause 11.8.1](#).



**Figure 11-6 — Process to Check Subscription Status before Decryption**

#### 11.7.1.2 Check Subscription Status – Required 30 day warning

This check must be performed every time new ENC base cell or update files are installed and is required to inform the Data Client on the status of the subscription licence ahead of expiry. The intention is to ensure that the Data Client has time to renew their subscription and obtain an updated Cell Permit from the Data Server. The warning is only applicable for subscription licenses and is not to be used for single purchase licenses, ref. [Clause 5.3.3](#). The procedure is as follows:

- 1) Obtain the system date and, if available, any alternative reliable time sources, e.g. GPS signal.

<sup>12</sup> The “Issue Date of Latest Update” field, if filled, will not always be in advance of the “Product Issue Date”, for instance in the case of re-issues.

- 2) Obtain the subscription expiration date from the Cell Permit file.
- 3) Compare the system date from 'a' and the subscription expiration date from 'b'.
- 4) If it is 30 days or more before the subscription expires, the system can operate without any further notices to the user.
- 5) If it is less than 30 days before the subscription expires, the system may be able to decrypt and uncompress new information issued during the subscription period. The system should issue a warning message to the user e.g.

*"SSE 20 — Subscription service will expire in less than 30 days. Please contact your data supplier to renew the subscription licence."*

### 11.7.2 Decrypt the Cell Keys in a Cell Permit

This procedure is performed by the Data Client system after the successful authentication of the ENC signature file. The decrypt process begins with the extraction of the cell keys required to decrypt the ENC and comprises of the following:

- 1) Append the first byte of the Data Client HW\_ID to the end of HW\_ID to form a 6 byte HW\_ID (called HW\_ID6).
- 2) Extract ECK1 from the Cell Permit and convert this from the 16 character hexadecimal string to 8 bytes.
- 3) Decrypt the converted ECK1 (output from 'b') using the Blowfish algorithm with HW\_ID6 as the key. This will yield CK1.
- 4) Extract ECK2 from the Cell Permit and convert this from the 16 character hexadecimal string to 8 bytes.
- 5) Decrypt the converted ECK2 (output from 'd') using the Blowfish algorithm with HW\_ID6 as the key. This will yield CK2.

#### EXAMPLE

HW_ID	3132333438	In hexadecimal
Cell Permit	NO4D061320000830BEB9BFE3C7C6CE68B16411FD-09F96982795C77B204F54D48	Example of cell permit

Output from 'a'	313233343831	HW_ID6
Output from 'b'	8 byte non-printable	Encrypted ECK1
Output from 'c'	C1CB518E9C	Cell key 1 (hex)
Output from 'd'	8 byte non-printable	Encrypted ECK2
Output from 'e'	421571CC66	Cell key 2 (hex)

Note that the unencrypted Cell Keys are 5 bytes in length even though the encrypted cell keys are 8 bytes in length. This is because blowfish pads the Cell Keys to 8 bytes in length when it encrypts them and it un-pads the Encrypted Cell Keys when it decrypts them.

### 11.7.3 Decrypt ENC Base Cell or Update File

This procedure is performed by the Data Client's system and is carried out as outlined in the flowchart (for [Clause 11.7.2](#) and [Clause 11.7.3](#)) and the step by step guide below<sup>13</sup>:

- 1) Decrypt the ENC file using the Blowfish algorithm with CK1 as the decryption key<sup>14</sup>.

<sup>13</sup> OEMs should note that there is no requirement to check the edition date against the permit or words to this effect.

<sup>14</sup> Rather than decrypting and decompressing the entire ENC file the data client can check that the decrypted header information is compliant with the ZIP standard [ZIP File Format Specification](#).

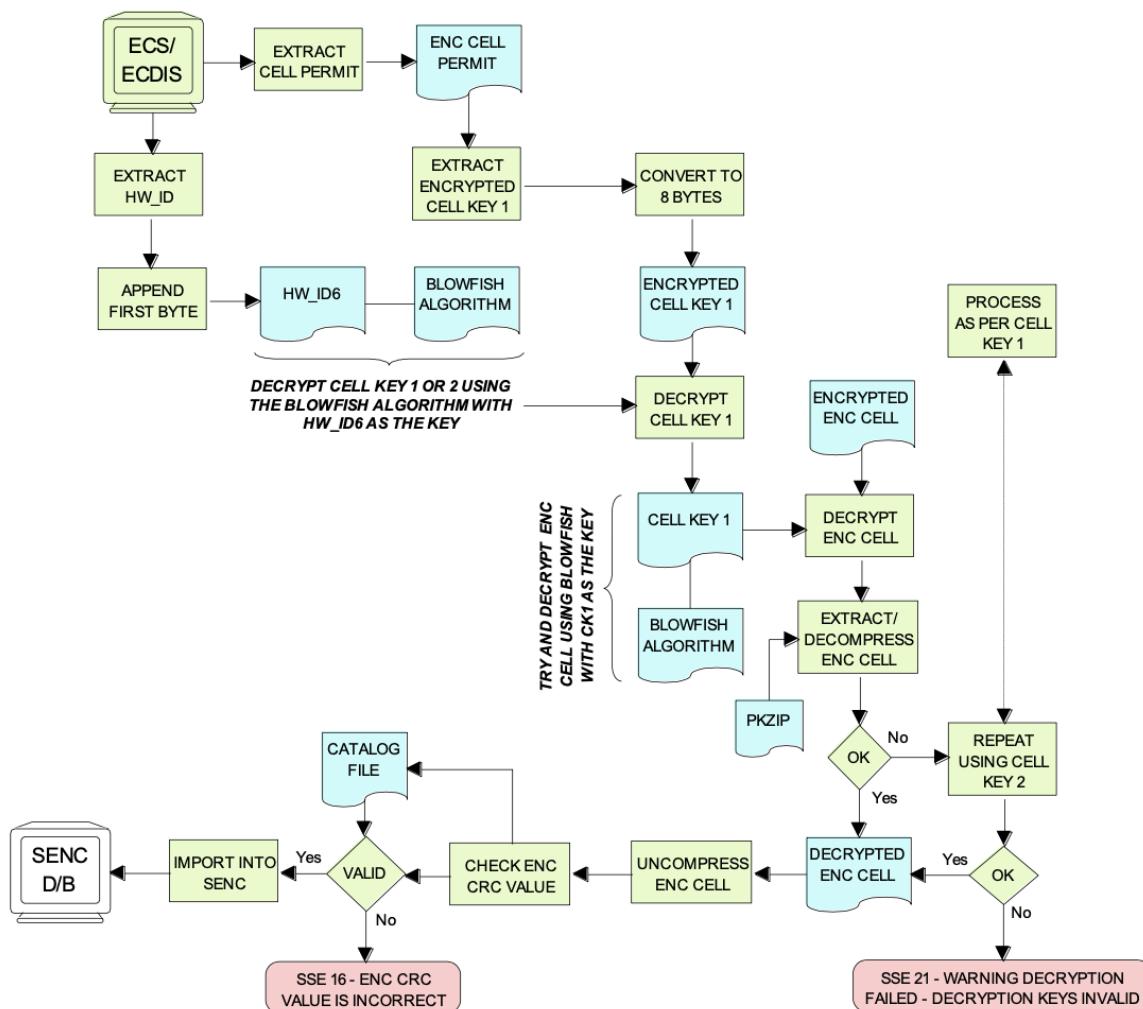
- 2) Decompress the ENC file. If decompression is successful, the ENC file is decrypted and ready for import.
- 3) If decompression is unsuccessful, decrypt the ENC file using the Blowfish algorithm with CK2 as the decryption key.
- 4) Decompress the ENC file. If decompression is successful, the ENC file is decrypted and ready for use.
- 5) If decompression is unsuccessful in 'b' and 'd', this means that the Cell Permit does not contain any valid cell keys. The system should return a relevant warning message and advise the Data Client that a new Cell Permit should be obtained from the Data Server.

***"SSE 21 – Decryption failed no valid cell permit found. Permits may be for another system or new permits may be required, please contact your supplier to obtain a new licence."***

#### 11.7.4 Decompress ENC file (base cell or update)

This procedure is performed by the Data Client on decrypted ENC files. The procedure is as follows:

Uncompress the ENC file using the ZIP standard [ZIP File Format Specification](#) to create a file fully compliant with the S-57 Edition 3.1 ENC Product Specification.



NOTE The CRC value of the ENC [S-57](#) is always computed on the unencrypted ENC information. The application must confirm successful decryption and decompression by conducting the CRC check on all ENC information.

**Figure 11-7 — Decrypt & Uncompress ENC Base Cell and Update Files**

## 11.8 Data Client Permanent Warnings

The data client already carries out checks when loading ENC permits and data files to validate conformance with this standard. However any resultant errors or warnings messages are not always translated through to the ECDIS when it is in use, e.g. route planning or navigation. It is possible, under the current data protection scheme, to use ENCs that are out-of-date without the user being aware of it. The purpose of this section is to identify any messages that should be permanently displayed by the data client when in use.

The data client must display permanent warning messages in the viewer when it can be determined that ENC information contained in the SENC is or may be out-of-date. The data client must carry out the following checks when displaying a cell in the ECDIS:

- Have the installed ENC permits expired?
- Is installed SENC data out-of-date in respect to the latest installed PRODUCTS.TXT file?

### 11.8.1 Expired ENC Permits

The data client must check the status of the installed ENC permit when displaying a particular ENC cell. If the permit has expired the ECDIS is to display a permanent warning informing the user that this ENC cell may be out of date as follows:

*"SSE 25 — The permit for ENC<cell name> has expired. This cell may be out of date and MUST NOT be used for Primary NAVIGATION".*

### 11.8.2 Out-of Date SENC Data

The data client must check the status of the ENC cell being displayed against the known status of that cell in a particular data server's service. This must be carried out by comparing the current Edition [EDTN] and Update [UPDN] contained in the SENC for any given cell against the corresponding cell record listed in the latest PRODUCTS.TXT file.

A permanent warning must be given when the ENC cell being displayed by the ECDIS is not updated to the latest new edition or update in service as follows:

*"SSE 27 — ENC<cell name> is not up to date. A New Edition, Re-issue or Update for this cell is missing and therefore MUST NOT be used for Primary NAVIGATION".*

## 11.9 QA Procedures – Data Client

### 11.9.1 Acceptance and Checking of the SA Digital Certificate (and Public Key)

A Data Client will receive the SA public key in two formats, as an X.509 Digital Certificate and as a printable public key. The Data Client shall have the capability to load the SA digital certificate and manually compare the public key against the printed public key (see [Clause 11.6.1.1](#)). The Data Client shall only accept the SA public key when this has been done. This process applies to the original SA public key and to any subsequent public keys issued by the SA.

### 11.9.2 Creation of User Permit

The system/application suppliers shall be able to create their own User Permit containing the encrypted HW\_ID. The User Permit will be provided to Data Servers who will then create Cell Permits for the requested ENC information. A User Permit shall only be created to request Cell Permits from a Data Server.

### 11.9.3 Verification of Data Server Certificate

The Manufacturer application shall allow the verification of a Data Server Certificate contained within an ENC signature file using the SA public key. If the Data Server Certificate is verified successfully, the application shall then extract the Data Server public key from the Data Server Certificate and use it to verify the ENC signature.

The SA will inform the Manufacturer about revoked Data Server Certificates.

#### 11.9.4 Validation of Cell Permits

The Data Client system must have the ability to validate the integrity of a Cell Permit by checking the encrypted check sum. This shall be done by following the procedure set out in [Clause 11.5.4](#) of the specification.

The Data Client must be able to manage Cell Permits provided by several Data Servers. The Data Client must also be able to manage Cell Permits for the same ENC provided by multiple Data Servers.

The Data Client must have the ability to manage stored Cell Permits so that old ones can be deleted and new ones added to, or merged with, those stored.

The Data Client application should not allow the Data Client to be able to view or copy the decrypted cell keys.

#### 11.9.5 Authentication and Decryption of ENC Information

The Data Client must be able to accept a signed and encrypted ENC data set by following the procedure defined in [Clause 11.6](#) and [Clause 11.7](#).

### 11.10 QA Procedures – Manufacturers (OEMs)

#### 11.10.1 Confidentiality Agreement

The SA will provide a manufacturer with copies of all information required to operate the Data Protection Scheme within a Confidentiality Agreement. The Manufacturer shall abide by the terms and conditions of the Confidentiality Agreement and ensure that all supplied information is kept up to date.

#### 11.10.2 System Compliance Testing

The Manufacturer shall perform internal compliance testing of their implementation of the protection scheme, based on the descriptions provided in this document and the supplied test data.

The SA will only issue M\_IDs and M\_KEYs on successful compliance as provided by a self certification document.

#### 11.10.3 Storage of M\_IDs and M\_KEYs

When the Manufacturer has joined the scheme, the SA shall provide the proprietary M\_ID and M\_KEY information for the creation of User Permits.

The users of the Manufacturer application must not be able to view or extract the M\_KEY information.

#### 11.10.4 Creation of HW\_IDs

The Manufacturer shall have the ability to create HW\_IDs of the format required within the standard. These are to be random so that they will not be sequential and cannot be duplicated.

The users of the Manufacturer application must not be able to view or extract the HW\_ID information from the application.

#### 11.10.5 Recording of HW\_IDs

The Manufacturer must record, in an **HW\_ID Register**, the values of each HW\_ID created. These details are to be made available to the SA upon request.

## 12 S-63 Error Codes and Explanations

The following error codes and messages are defined in the flowcharts in [Section 9](#), [Section 10](#), and [Section 11](#). It is expected that application developers support the error conditions with an appropriate error message. When an error occurs, this can in some instances, prevent further processing of the data.

Error Code	Error/Warning Message
SSE 01	" <i>Self Signed Key is invalid</i> "
SSE 02	" <i>Format of Self Signed Key file is incorrect</i> "
SSE 03	" <i>SA Signed Data Server Certificate is invalid</i> "
SSE 04	" <i>Format of SA Signed DS Certificate is incorrect</i> "
SSE 05	" <i>SA Digital Certificate (X509) file is not available. A valid certificate can be obtained from the IHO website or your data supplier</i> "
SSE 06	" <i>The SA Signed Data Server Certificate is invalid. The SA may have issued a new public key or the ENC may originate from another service. A new SA public key can be obtained from the IHO website or from your data supplier</i> "
SSE 07	" <i>SA signed DS Certificate file is not available. A valid certificate can be obtained from the IHO website or your data supplier</i> "
SSE 08	" <i>SA Digital Certificate (X509) file incorrect format. A valid certificate can be obtained from the IHO website or your data supplier</i> "
SSE 09	" <i>ENC Signature is invalid</i> "
SSE 10	" <i>Permits not available for this Data Server. Contact your data supplier to obtain the correct permits.</i> "
SSE 11	" <i>Cell Permit not found. Load the permit file provided by the data supplier.</i> "
SSE 12	" <i>Cell Permit format is incorrect. Contact your data supplier and obtain a new permit file.</i> "
SSE 13	" <i>Cell Permit is invalid (checksum is incorrect) or the Cell Permit is for a different system". Contact your data supplier and obtain a new or valid permit file.</i> "
SSE 14	" <i>Incorrect system date, check that the computer clock (if accessible) is set correctly or contact your system supplier.</i> "
SSE 15	" <i>Subscription service has expired. Please contact your data supplier to renew the subscription licence</i> "
SSE 16	" <i>ENC CRC value is incorrect. Contact your data supplier as ENC(s) may be corrupted or missing data.</i> "
SSE 17	" <i>Userpermit is invalid (checksum is incorrect). Check that the correct hardware device (dongle) is connected or contact your system supplier to obtain a valid userpermit.</i> "
SSE 18	" <i>HW_ID is incorrect format</i> "
SSE 19	" <i>Permits are not valid for this system. Contact your data supplier to obtain the correct permits</i> "
SSE 20	" <i>Subscription service will expire in less than 30 days. Please contact your data supplier to renew the subscription licence</i> "
SSE 21	" <i>Decryption failed no valid cell permit found. Permits may be for another system or new permits may be required, please contact your supplier to obtain a new licence</i> "

Error Code	Error/Warning Message
<b>SSE 22</b>	<i>SA Digital Certificate (X509) has expired. A new SA public key can be obtained from the IHO website or from your data supplier.</i>
<b>SSE 23</b>	<i>Non sequential update, previous update(s) missing try reloading from the base media. If the problem persists contact your data supplier.</i>
<b>SSE 24</b>	<i>ENC Signature format incorrect, contact your data supplier</i>
<b>SSE 25</b>	<i>Viewer – “The permit for ENC &lt;cell name&gt; has expired. This cell may be out of date and MUST NOT be used for Primary NAVIGATION”.</i>
<b>SSE 26</b>	<i>This ENC is not authenticated by the IHO acting as the Scheme Administrator</i>
<b>SSE 27</b>	<i>Viewer – “ENC &lt;cell name&gt; is not up to date. A New Edition, Re-issue or Update for this cell is missing and therefore MUST NOT be used for Primary NAVIGATION”.</i>

**SSE 01** must be returned when a self signed key (SSK) cannot be validated against the public stored as part of the SSK. The data server must check that its own SSK is valid before sending it to the SA. The SA will confirm that the date server SSK before returning the SA signed data server certificate.

**SSE 02** must be returned if the SSK is wrongly formatted. That is elements of the SSK or characters are missing. The SA and data servers must complete this check.

**SSE 03** must be returned if the SA signed data server certificate does not authenticate correctly against the SA public key. This validation process must be carried out by the SA before supplying it to the data server. The data server must validate the SA certificate received from the SA. The data client must validate the SA certificate contained in the ENC signature file prior to decryption.

**SSE 04** must be returned if the SA signed data server certificate is wrongly formatted. This must be carried out by the data server on receipt from the SA.

**SSE 05** must be returned if there is no certificate installed on the data client or the path to it cannot be found.

**SSE 06** must be returned if the SA digital certificate (public key) does not validate against the following:  
SA digital certificate will not validate against the SA public key. The SA public key contained in the digital certificate will not authenticate against the signature contained in the ENC signature file. This could be a case of the certificate being invalid or an invalid or badly formatted signature.

**SSE 07** must be returned if the SA signed data server certificate is not available to the data server for checking or is not present in the ENC signature file when the data client attempts to authenticate it.

**SSE 08** must be returned if the SA public key held in the SA digital certificate is wrongly formatted or the certificate file is unreadable.

**SSE 09** must be returned if the ENC signature element in the ENC signature file does not authenticate against the data server public key contained in the certificate element of the ENC signature file.

**SSE 10** must be returned if there are no cell permits available for a particular data server corresponding to the exchange set being loaded.

**SSE 11** must be returned if there are no permits installed on the system.

**SSE 12** must be returned if the cell permits are formatted incorrectly.

**SSE 13** must be returned if the calculated CRC of the cell permit does not validate against the CRC held in that cell permit. [Data Clients] This may be a HW\_ID problem, corruption during transmission or the permits are for a different system.

**SSE 14** must be returned if the system date does not agree with the date obtained from any alternative, reliable date source, e.g. GPS. [Data Clients]

**SSE 15** must be returned if the expiry date of the cell permit has an earlier date than that obtained from the validated system date. [Data Clients]

**SSE 16** must be returned if the calculated CRC value of the ENC (after decryption and uncompressing) does not validate against the corresponding CRC value in the CATALOG.031 file. This also applies to the unencrypted signature, text and picture files. [Data Clients]

**SSE 17** must be returned if the CRC contained in the userpermit does not validate against the calculated CRC of the extracted HW\_ID. [Data Servers]

**SSE 18** must be returned if the if the decrypted HW\_ID extracted from the userpermit is incorrectly formatted. [Data servers]

**SSE 19** must be returned if the HW\_ID stored within the hardware/software security device cannot decrypt the cell permits being loaded or already installed on the system.

**SSE 20** must be returned if the subscription licence is due to expire within 30 days or less.

**SSE 21** must be returned if a valid cell key (decryption key) cannot be obtained from the relevant cell permit to enable the system to decrypt the corresponding ENC cell.

**SSE 22** must be returned if the SA Digital Certificate (X509) has expired. That is if the “**Valid to**” date in the certificate is older than the validated system date.

**SSE 23** must be returned if the ENC update being imported is not sequential with the latest update already contained in the SENC for any given cell. Under these conditions the update process (for the cell) must be terminated and the ECDIS is to display a warning when the cell is displayed stating that the cell is not up to date and should not be used for navigation.

**SSE 24** must be returned if the ENC signature format (first R & S pair) is not compatible with the format outlined in this document. Under these conditions the import process for the cell should be terminated but the system should continue to authenticate the integrity of any remaining cells.

**SSE 25** must be returned if the stored ENC permit for any given cell has expired. It should be possible to view the cell but a permanent warning message must be displayed informing the user, e.g. “*The permit for ENC <cell name> has expired. This cell may be out of date and MUST NOT be used for Primary NAVIGATION*”.

**SSE 26** must be returned if the signed certificate (in the ENC signature file) authenticates against a certificate or public key file stored on the Data Client other than the one provided by the SA. This caters for instances where more than one certificate or public key is stored in the Data Client.

**SSE 27** must be returned if the status of the cell being viewed is not as up-to-date in respect of the latest PRODUCTS.TXT file loaded or maintained on the system. A permanent warning message must be displayed on screen informing the user, e.g. “*ENC <cell name> is not up to date. A New Edition, Re-issue or Update for this cell is missing and therefore MUST NOT be used for Primary NAVIGATION*”.

## Annex A

### Data Server Certificate Request Procedure

#### A.1 Purpose

The purpose of this procedure is to define the process for a Data Server to obtain a SA signed Data Server Certificate from the SA as defined by the IHO S-63 Data Protection Scheme Standard.

#### A.2 Responsibility

##### A.2.1 Need for Data Server Certificate

An organisation that encrypts and digitally sign ENC data as part of the IHO S-63 Data Protection Scheme will require a Data Server Certificate signed by the Scheme Administrator.

Users of encrypted and digitally signed ENC data (i.e. ECDIS systems to authenticate a signature and decrypt ENC information) do not need a Data Server Certificate. Agents or Distributors who will only provide ENC services supplied by a Data Server will not require a Data Server Certificate.

##### A.2.2 Hydrographic Offices and RENC Organisations

All Hydrographic Offices and RENC (Regional ENC Coordinating Centre) organisations only have to complete Part I of the attached form and include the required information to apply for a Data Server Certificate. A Data Server can only obtain one Data Server Certificate.

##### A.2.3 Non-Hydrographic Offices and Non-RENC Organisations

Other commercial organisations who wish to operate as Data Servers and encrypt and digitally sign ENC information compliant with the protection scheme can apply for a Data Server Certificate. Such organisations must get a Data Server, already a member of the protection scheme, to endorse the request and complete part II of the form. It is assumed that the Data Server providing the ENC data to the commercial organisation will endorse the request.

##### A.2.4 IHO Secretariat

The IHO Secretariat as Scheme Administrator has the sole responsibility to generate the Data Server Certificates compliant with internal procedures.

#### A.3 Definitions

Data Server	This is the term used to identify an organisation producing encrypted ENC data that is digitally signed and issuing Cell Permits to Data Clients (end-users).
Certificate	Certificates are digital documents attesting to the binding of a public key to an individual or organisation. They verify that a specific public key belongs to a specific organisation, in this case the IHO.

##### A.3.1 References

- [1] S-63 edition 1.2.1: IHO Data Protection Scheme, International Hydrographic Organization ([https://ihonet.int/uploads/user/pubs/standards/s-63/S-63\\_2020\\_Ed1.2.1\\_EN\\_Draft\\_Clean.pdf](https://ihonet.int/uploads/user/pubs/standards/s-63/S-63_2020_Ed1.2.1_EN_Draft_Clean.pdf)).
- [2] S-57 edition 3.1.0: IHO Transfer Standard for Digital Hydrographic Data, International Hydrographic Organization (<https://ihonet.int/uploads/user/pubs/standards/s-57/31Main.pdf>).

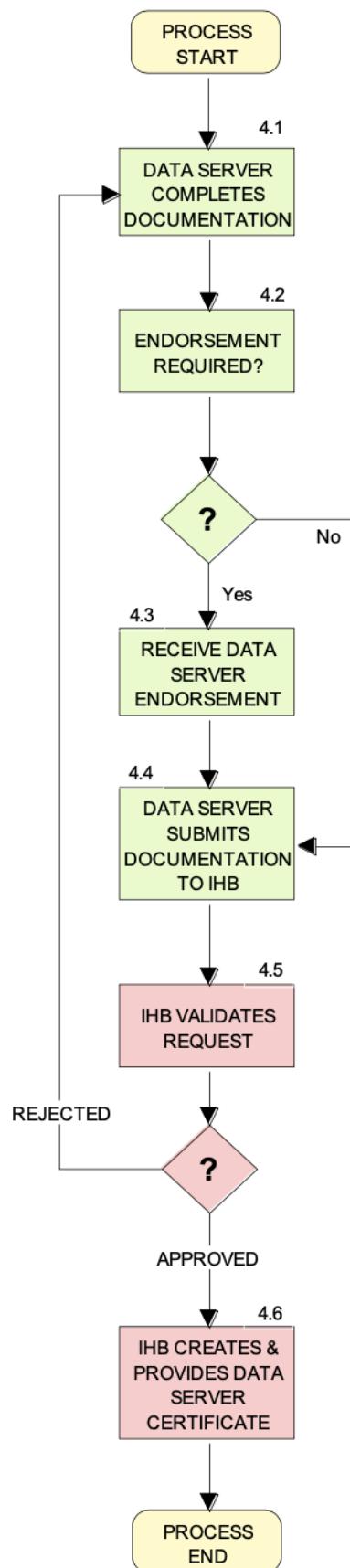
#### A.4 Procedure

This chapter defines the flow of information, responsibilities and detailed work instructions.

#### A.4.1 Completion of Forms and Attachments

A Data Server, who is already either a Hydrographic Office or a recognised RENC, who wishes to become a participant in the IHO S-63 Data Protection Scheme, is responsible for providing the following information to the IHO Secretariat:

- A signed IHO Data Server Agreement
- A signed Certificate Request Form with Part I filled out
- The Data Server's Public Key
- The Data Server's Self Signed Certificate (SSK)



#### A.4.2 Need for Endorsement

All non-hydrographic offices and non-RENC organisations wishing to become a Data Server must have the Certificate Request Form endorsed by an existing Data Server who is already a member of the scheme.

#### A.4.3 Endorsing Organisation

The endorsing Data Server must complete Part II of the Certificate Request Form and return it to the non-hydrographic offices or non-RENC organisation.

#### A.4.4 Submission of Request to IHO Secretariat

The Data Server is responsible for submitting the completed Request Form together with all other information listed in [Annex A.4.1](#) above to the IHO Secretariat.

#### A.4.5 Validation of Certificate Request

The IHO Secretariat will validate the origins of the Certificate Request and authenticate the public key by contacting the Data Server. It will also ensure the need for a Data Server Certificate is applicable by contacting the endorsing Data Server. The IHO Secretariat will report discrepancies back to the originator.

#### A.4.6 Creation of Data Server Certificate

The IHO Secretariat is responsible for the authentication of the SSK created by the Data Server. If authentic the IHO Secretariat then signs the Data Server public key to create the Data Server's Certificate, this is then supplied to the Data Server.

### A.5 Quality Metrics

The IHO Secretariat will archive the Data Server Request information and attachments compliant with internal procedures.

 <b>Figure A-1</b>	<b>IHO S-63 Data Protection Scheme Data Server Certificate Request Form</b> Ed.1-2003
Form to be returned to: <b>International Hydrographic Organization</b> 4, Quai Antoine 1 <sup>er</sup> , B.P 445 — MC 98011 MONACO Cedex Principality of Monaco Tel: +(377) 93 10 81 00, Telefax: +(377) 93 10 81 40	
<p><b>Part I: To be completed by Data Server organisation</b></p> <p>Organisation: .....</p> <p>Address: .....</p> <p>Address: .....</p> <p>Address: .....</p> <p>Postal number/place: ..... Country: .....</p> <p>Tel: ..... Fax: ..... Web: .....</p> <p><b>Administrative point of contact: Technical point of contact:</b></p> <p>Name: ..... Name: .....</p>	

<b>Tel:</b> ..... <b>Tel:</b> .....	<b>E-mail:</b> ..... <b>E-mail:</b> .....
<b>Please verify the following information is included:</b>	
<input type="checkbox"/> All fields in Part 1 2 of this form are completed	
<input type="checkbox"/> Data Server Public Key <input type="checkbox"/> Data Server Self Signed Key (SSK)	
<input type="checkbox"/> Signed IHO S-63 Data Server Agreement, or <input type="checkbox"/> already available with IHO Secretariat	
<b>Signed date:</b> ..... <b>Name:</b> .....	
<b>Part II: To be completed by endorsing HO or RENC organisation</b>	
<b>Organisation:</b> .....	
<b>Contact name:</b> .....	
<b>Tel:</b> .....	<b>Fax:</b> .....
<b>E-mail:</b> .....	
<b>Part III: To be completed by IHO Secretariat</b>	
<input type="checkbox"/> Form and attachments validated	
<input type="checkbox"/> Signed Data Server Agreement, ref. .....	
<input type="checkbox"/> Certificate created date: File ref: .....	
<input type="checkbox"/> Certificate returned to Data Server	
<b>Signed date:</b> ..... <b>Name:</b> .....	

## Annex B

### Manufacturer Information Request Procedure

#### **B.1 Purpose**

The purpose of this procedure is to define the processes that an OEM has to undertake to become a participant in the IHO S-63 Data Protection Scheme. To participate, OEMs will require their own unique M\_ID and M\_KEY values. These are supplied by the SA as defined by the IHO S-63 Data Protection Scheme so that OEMs can decrypt S-63 encrypted ENCs.

#### **B.2 Responsibility**

##### **B.2.1 OEMs**

Only OEMs that develop Data Client applications need a unique M\_ID and M\_KEY value. The IHO Secretariat as the Scheme Administrator will share this information with all the Data Servers participating in the scheme. An OEM will only be issued with one M\_ID and M\_KEY pair.

The M\_ID and M\_KEY values will be returned to the Scheme Administrator if the organisation ceases trading or no longer supports an application that accesses and displays S-63 encrypted ENCs. Data Servers will be informed of such instances so that no new licences are issued for that particular manufacturers system.

There is no need for Data Client to have access to the M\_KEY value because it is securely built into the end-user application (e.g. dongle) and supplied to Data Clients in an encrypted form known as a userpermit.

##### **B.2.2 IHO Secretariat**

The IHO Secretariat as SA has the sole responsibility for generating the M\_ID and M\_KEY values and supplying them to OEMs and distributing among Data Servers.

#### **B.3 Definitions**

M\_ID        Manufacturer Identification

M\_KEY        Manufacturer Key

OEM        Original Equipment Manufacturer

Userpermit    A 28 character alphanumeric string containing the Data Client's HW\_ID encrypted with the manufacturer's M\_KEY and containing the M\_ID.

Dongle        A hard lock device that contains the HW\_ID of the Data Clients system.

##### **B.3.1 References**

- [3]            S-63 edition 1.2.1: IHO Data Protection Scheme, International Hydrographic Organization ([https://ihonet/uploads/user/pubs/standards/s-63/S-63\\_2020\\_Ed1.2.1\\_EN\\_Draft\\_Clean.pdf](https://ihonet/uploads/user/pubs/standards/s-63/S-63_2020_Ed1.2.1_EN_Draft_Clean.pdf)).
- [4]            S-57 edition 3.1.0: IHO Transfer Standard for Digital Hydrographic Data, International Hydrographic Organization (<https://ihonet/uploads/user/pubs/standards/s-57/31Main.pdf>).

#### **B.4 Procedure**

This chapter defines the flow of information, responsibilities and detailed work instructions.

#### B.4.1 Completion of Request Form

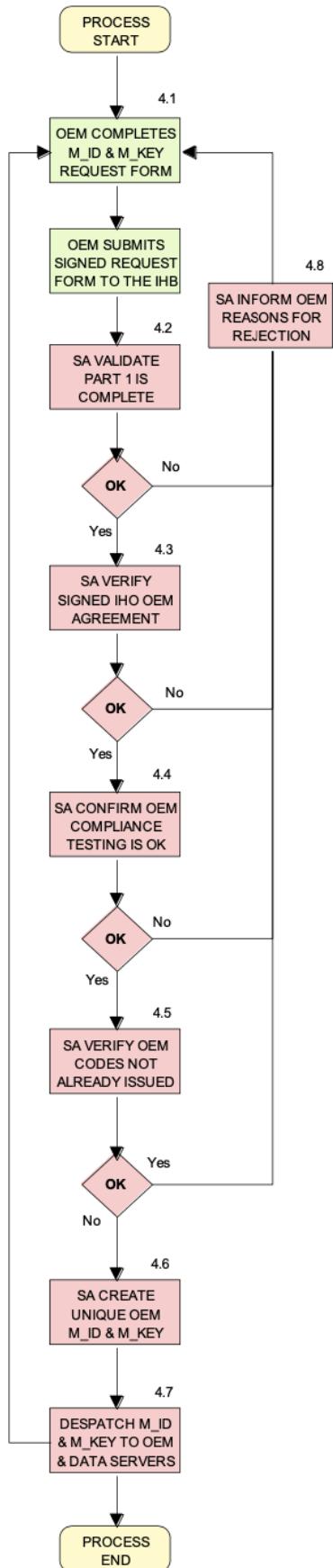
The OEM is responsible for completing all information in Part I of the attached M\_ID and M\_KEY request form. The IHO may wish to require further documentation such as Confidentiality Agreements – these are not detailed here.

Note that an OEM can:

- Only be assigned one M\_ID and M\_KEY pair
- Must return the information to the Scheme Administrator (SA) if it stops trading or does not deliver products authenticating signatures or no longer has a need to decrypt ENC information.

#### B.4.2 Verification of Request Form

The SA verifies that all information in Part I of the form is completed, or provide information to OEM about missing information.



#### B.4.3 Verification of Signed Confidentiality Agreement

The SA verifies that a signed Confidentiality Agreement is included with the request or already available in the IHO Secretariat archive. If an Agreement is not available, inform the OEM about the mandatory need for a signed Agreement.

#### B.4.4 Confirm Successful Testing with S-63 Test data

Verify that the OEM has completed successful testing of application with the available IHO S-63 test data. If not, request the OEM to complete the defined test procedure before M\_ID and M\_KEY are provided.

#### B.4.5 Check OEM has no Current M\_ID and M\_KEY

Verify the OEM has no previously assigned M\_ID and M\_KEY. If not, inform the OEM about the problem.

#### B.4.6 Creation of M\_ID and M\_KEY

The SA assigns the OEM an available and unique M\_ID and M\_KEY combination.

#### B.4.7 Inform About New M\_ID and M\_KEY

The SA informs the OEM about its M\_ID and M\_KEY. The SA informs all registered Data Servers about the new M\_ID and M\_KEY information.

#### B.4.8 Inform OEM about Problem with Request

The SA informs the OEM about specific problems with the request and requests updated information to be provided before a M\_ID and M\_KEY can be assigned. Further processing of the request is terminated.

### B.5 Quality Metrics

The IHO Secretariat will archive the Request form and all relevant information compliant with internal procedures.

 <b>Figure B-1</b>	<b>IHO S-63 Data Protection Scheme M_ID and M_KEY Request Form</b> Ed.1-2003
Form to be returned to: <b>International Hydrographic Organization</b> 4, Quai Antoine 1 <sup>er</sup> , B.P 445 — MC 98011 MONACO Cedex Principality of Monaco Tel: +(377) 93 10 81 00, Telefax: +(377) 93 10 81 40	
<p><b>Part I: To be completed by OEM organisation</b></p> <p>Organisation: .....</p> <p>Address: .....</p> <p>Address: .....</p> <p>Address: .....</p> <p>Postal number/place: ..... Country: .....</p> <p>Tel: ..... Fax: ..... Web: .....</p> <p><b>Administrative point of contact: Technical point of contact:</b></p> <p>Name: ..... Name: .....</p>	

<b>Tel:</b> ..... <b>Tel:</b> .....	
<b>E-mail:</b> ..... <b>E-mail:</b> .....	
<b>Please verify the following information is included:</b>	
<input type="checkbox"/> All fields in Part 1 of this form are completed	
<input type="checkbox"/> Signed IHO S-63 OEM Agreement, or <input type="checkbox"/> already available with IHO Secretariat	
<input type="checkbox"/> Completed successful testing of application with the M_ID and M_KEY provided with the S-63 test dataset	
<b>Signed date:</b> ..... <b>Name:</b> .....	
<b>Part II: To be completed by IHO Secretariat</b>	
<input type="checkbox"/> Verify Part 1 is completed <input type="checkbox"/> Signed OEM Agreement available, ref. ....	
<input type="checkbox"/> Verify OEM does not have a previously issued M_ID and M_KEY	
<input type="checkbox"/> Assigned M_ID: ..... M_KEY: .....	
<input type="checkbox"/> M_ID and M_KEY returned to OEM and all registered Data Servers	
<b>Signed date:</b> ..... <b>Name:</b> .....	

## Annex C ENC Update Status Report

### C.1 Purpose

This section of S-63 elaborates the definition of an “up to date” ENC. This is required by the IMO Performance Standard and all ECDIS users are required to be able to demonstrate to a vetting inspector that their ECDIS and its embedded ENCs are “up to date”.

This Annex of S-63 specifies the format and content of an “ENC update status report” which, if implemented, will demonstrate the revision status of ENCs within the ECDIS SENC.

### C.2 Use and Responsibility

The ENC update status report is designed as a concise and standardised format to assist end users in satisfying themselves that their ENC data is “up to date” and help satisfy inspection requirements in that respect.

The report is designed for two individual use cases:

- 1) To ensure that all ENC cells loaded into the SENC are up to date for the next leg of a particular route
- 2) To ensure that all ENCs loaded into the SENC are up to date.

S-57 ENC cells use edition and update numbers to denote their individual revision (see S-57 Appendix B1 – ENC product specification for details). These numbers uniquely identify how up to date a cell is. The difficulty with using edition/update numbers in isolation is that they do not document the date of revision of all cells relative to an installation date of a data server’s service giving the end user no indication of whether an ENC (or a collection of ENCs) is up to date with respect to the last S-63 dataset installed.

S-63 provides an issue date within its metadata for an entire ENC service as well as a snapshot of the edition and update information within an S-63 data service. The revision date embedded within the SERIAL.ENC file, is used in the ENC update status report to provide a reference date for every ENC either on the next leg of the vessel’s route or for the SENC as a whole.

The driving use case for the ENC update status report is that an inspector (for example flag state, port state or vetting inspector) or end user can check that an ECDIS is up to date with respect to the last dataset installed from each data server’s ENCs within the SENC. Note that this report specification is not a concrete definition of what an “up to date” ENC (or ECDIS) is, it only shows a status of each ENC with respect to the last data installed on the system. If a period of time has passed since the last update then ENC data may well be “out of date” relative to the time the report is run – the report only records the up to date status relative to the last data installed (the date being defined by the date contained in the SERIAL.ENC file as described in the specification). If this report is implemented then it should be clear to the user what exact definitions of the ENC status mean.

This report only reports the status of ENCs delivered as part of a data server service complying with the current version of S-63. Where other ENCs are installed on the system from other sources (in particular unencrypted ENCs) then they should be displayed with a status of “unknown” and the end user should be made aware of these definitions by reference to the Operator’s manual provided by the manufacturer.

This annex provides a specification for a report which can be run on a compliant ECDIS to determine the status of ENCs held within the SENC.

### C.3 Report Definitions

#### C.3.1 Report Types

The ENC update status report defined in this annex can take one of two forms:

- 1) A report detailing the status of all ENCs within the SENC of the ECDIS. This shows the status of the ENCs with respect to the date contained in the SERIAL.ENC of the last update for each data server’s service installed.

- 2) A report detailing the status of each ENC along a predefined section of a route contained within the ECDIS.

An example of the ENC update status report is shown in the [Figure C-1](#) (a complete version of the report is given in [Annex C.3.7](#)).

<b>Vessel Name:</b>	HMS Goteborg			
<b>Identifier:</b>	IMO 4653321			
<b>ENC Update Reference Date:</b>	16 May 2013: WK24/2013			
<b>Date of Report:</b>	1 Jun 2013			
<b>Content:</b>	Filtered for Route Plan "Goteborg – Kiel"			
<b>Start WP:</b>	Goteborg [57.7N,11.966667E]			
<b>End WP:</b>	Kiel [54.333742N,10.159607E]			
<b>Chart Status Summary:</b>				
<b>Chart Status:</b>	<b>Count</b>			
Total:	50			
Up to Date	38/50			
Not Up to Date	10/50			
Withdrawn	2/50			
Unknown	0/50			
<b>Data Server: GB</b>				
Cell Name	Edition	Update	Issue Date	Status
DE316001	5	1	13 Mar 2013	Not Up to Date
DE416010	1	1	12 Apr 2012	Not Up to Date
DE416020	6	2	11 May 2012	Not Up to Date
DE416021	8	3	10 May 2012	Not Up to Date

**Figure C-1 — Example ENC update status report.**

The ENC update status report is a formatted output from the ECDIS. It should be formatted to fit within the width of the ECDIS screen and, if printable, split into individual A4 pages.

Reports of both types (complete SENC contents and Filtered by route) are divided into two sections:

- 1) A header containing information on the vessel and report content selected (either filtered for a route (or part of a route) or for the entire SENC contents). This header contains vessel information and report reference dates followed by a summary totals for each report status.
- 2) A table containing information for each cell within the chosen content type. This provides detailed information on each cell within the chosen content category.

### C.3.2 Report Header

The data content of each of the header fields is defined in the table below:

Field Name	Type	Source
[start=1] . Vessel Name	Text	The name of the vessel as recorded within the ECDIS.
[start=2] . Identifier	Text	A unique identifier, the MMSI or vessel IMO number.
[start=3] . ENC Update reference date	Date	The data used as the reference for the status of each of the cells. This is the datestamp of the last data server's service media used to update the SENC. The date is taken from the S-63 SERIAL.ENC file as defined in section 6.3 and is expressed both in standard notation "NN MMM YYYY" and week number as defined in S-63 section 6.3. These fields are defined in S-63 section 6.3 as the "Date of Publication" and "Week of Issue" respectively.
[start=4] . Date of report	Date	The date the report was run.

Field Name	Type	Source
[start=5] . Content	Text	This field denotes the content type of the report. There are two possibilities:- “Filtered for Route Plan XXX to YYY” where XXX and YYY are the textual names of the point of origin and destination on the chosen route.- Full SENC contents.
[start=6] . Start WP	Text	This field is only present if the report is filtered for a route. It should comprise the textual name of the starting waypoint of the route (if one exists) and the lat/lon coordinates of the waypoint. There is no fixed form that the coordinates should take.
[start=7] . End WP	Text	This field is only present if the report is filtered for a route. It should comprise the textual name of the last waypoint of the route (if one exists) and its lat/lon coordinates. There is no fixed form that the coordinates should take.

### C.3.3 Filtering of ENC update status report for route section

Where the ENC update status report is filtered for a route plan then the cells in the SENC whose status are checked are defined by the intersection of the route corridor with the chart boundaries (as defined by the M\_COVR (CATCOV=1) features within the SENC for the installed ENCs).

The width of the filtering corridor is equal to the “user specified distance” implemented inside the ECDIS to fulfil IMO MSC.232(82) 11.3.5:

*“An indication should be given if the mariner plans a route closer than a user-specified distance from the boundary of a prohibited area or a geographic area for which special conditions exist (see appendix 4). An indication should also be given if the mariner plans a route closer than a user-specified distance from a point object, such as a fixed or floating aid to navigation or isolated danger.”*

This is not the same as the XTD distance.

### C.3.4 Summary Totals

The summary section of the report follows directly after the header. The summary contains the following information:

- 1) The title : **“Chart Status Summary”**
- 2) Totals of cells with the relevant status in the order defined below. The definitions for each status are defined in [Annex C.3.5](#).
  - a) Total – the total number of cells available in the SENC for the content type selected for the report (either full or filtered by route).
  - b) Up to date – the total number of cells (for the content selected) which have status “Up to date”.
  - c) Not up to date – the total number of cells (for the content selected) which have status “Not up to date”.
  - d) Withdrawn – the total number of cells (for the content selected) which have status “Withdrawn”.
  - e) Cancelled – the total number of cells (for the content selected) which have status “Cancelled”.
  - f) Unknown – the number of cells for which a status cannot be determined for any reason.

The possibilities for the ENC status are listed in the following table along with their definitions.

### C.3.5 Data Server content tables

The detailed tables in each report are arranged by data server – each separate data server or ENC data source within the SENC has its own separate table listing all ENCs by content type (as reported in the “Content” field in the report header). The detailed tables contain the following information:

- 1) Title: Data Server Name- this is the data server identified by the SERIAL.ENC file referred to in the header section as defined in section
- 2) For each cell installed in the SENC from the data server:
  - a) Cell Name – the name of the cell. The S-57 DSID DSNM subfield (S-57 Appendix B, 6.3.2.1)
  - b) Edition – the edition of the cell in the SENC. S-57 DSID EDTN.
  - c) Update – the update number of the cell in the SENC. S-57 DSID UPDN
  - d) Issue Date – the S-57 ISDT of the last applied update to the cell in the SENC

- e) Status – the status of the cell. The status may have one of four values determined according to the criteria in the following table:

Status Message	Specification
<b>Up to date</b>	This is where the SENC has all the latest update and/or new edition information for the cell installed as defined by the latest PRODUCTS.TXT data. The reference date for the most up to date information is defined by the “ENC Update reference date” defined in <a href="#">Annex C.3.2</a> (found within the latest SERIAL.ENC file installed on the system). The ENC Update reference date must be within the last four weeks from the time of the report execution or the cell shall be displayed as “Not up to date” regardless of its status as defined by the PRODUCTS.TXT data.
<b>Not Up to date</b>	This is where the SENC has NOT installed all the latest update and/or new edition for the cell. Again, the reference point for what should be installed is defined by the ENC Update reference date defined in <a href="#">Annex C.3.2</a> (found within the latest SERIAL.ENC file applied to the SENC from the data server). If the reference date is older than four weeks then cells shall be displayed as “not up to date” by definition.
<b>Withdrawn</b>	The number of cells which have been withdrawn by the data server or cancelled but which are still available within the SENC.
<b>Unknown</b>	Cells for which a status cannot be determined for any reason. If cells from a dataset with a “PARTIAL” PRODUCTS.TXT file are loaded then all cells in a data server’s service but not included in the partial PRODUCTS.TXT shall be deemed to be “Unknown” as no definitive information on them can be determined. A “FULL” PRODUCTS.TXT content is required to specify the status of all cells in a data server’s service.

### C.3.6 Optional columns in ENC update status report

If the OEM wishes to provide more information to end users in the ENC status report then two additional columns may be added to the report. These are defined below:

- 1) Expiry Date. This is the date of expiry of the ENC permit (as defined in S-63 part 3.4).
- 2) Action. An advisory-only action to be taken by the user based on the status of ENCs within the SENC, their expiry dates and availability of data within the data server’s service.

Action	Definition
Renew	If the expiry date of the ENC permit for the cell is less than 30 days from the time of the execution of the report then the entry in the table shall be “Renew”.
To be Ordered (Route Filtered report only)	If, when running the route filtered report, a cell is identified within the data server’s service which intersects the route (as defined in <a href="#">Annex C.3.3</a> ) but the cell is not currently installed, it shall be included in the table with the Action as “To be Ordered”.  Note that: <ol style="list-style-type: none"> <li>1) The cell limits defined in the PRODUCTS.TXT for the data server’s service shall be used to establish intersection with the route (as defined in <a href="#">Annex C.3.3</a>).</li> <li>2) The “advisory” nature of this column should be made very clear to the user as there may be many small scale charts which intersect a particular route, not all of which the mariner considers necessary.</li> </ol>
No action	If the cell expiry date is > 30 days from the time of the report execution it shall be marked as “No action”.
To be removed	If the cell is marked as cancelled or does not appear in the latest edition of the data server’s full PRODUCTS.TXT then it should be removed so that out of date information is not maintained within the SENC.
To be installed (Route filtered report only)	If a cell is identified as intersecting with the planned route (as defined in <a href="#">Annex C.3.3</a> ) and a permit is installed within the system but the cell itself is not installed then the entry shall be marked as “To be installed”.

### C.3.7 Examples of ENC update status report

EXAMPLE

***ENC Update Status Report.***

<b>Vessel Name</b>	HMS Goteborg
<b>Identifier</b>	IMO 4653321
<b>ENC Update Reference Date</b>	16 May 2013 : WK24/2013
<b>Date of Report</b>	1 Jun 2013
<b>Content</b>	Full

**Chart Status Summary:**

<b>Chart Status</b>	<b>Count</b>
Total	50
Up to Date	38/50
Not Up to Date	10/50
Withdrawn	2/50
Unknown	0/50

<b>Data Server: GB</b>				
<b>Cell Name</b>	<b>Edition</b>	<b>Update</b>	<b>Issue Date</b>	<b>Status</b>
DE316001	5	1	13 Mar 2013	Not Up to Date
DE416010	1	1	12 Apr 2012	Not Up to Date
DE416020	6	2	11 May 2012	Not Up to Date
DE416021	8	3	10 May 2012	Not Up to Date
DE416030	3	0	01 Jan 2013	Not Up to Date
DE516175	6	6	01 Jan 2013	Not Up to Date
DE516200	8	5	04 May 2013	Not Up to Date
DK2KATGS	4	4	22 Apr 2012	Not Up to Date
DK2LILBL	2	0	14 Nov 2012	Not Up to Date
DK2SKARK	6	7	25 Oct 2012	Not Up to Date
DK2STOBL	9	6	06 Aug 2011	Not Up to Date
DK4ABFNF	4	9	21 Jan 2011	Withdrawn
DK4FAVSF	2	1	19 Apr 2011	Withdrawn
DK4KATGN	1	2	28 Feb 2013	Up to Date
DK4KATGS	1	11	17 Jun 2012	Up to Date
DK4STOBN	1	2	14 Nov 2012	Up to Date
DK4STOBS	4	1	06 Jun 2013	Up to Date
DK5KALBG	5	8	03 Apr 2012	Up to Date
DK5KORSO	3	7	16 Aug 2012	Up to Date
SE2BHS0W	8	5	19 Nov 2012	Up to Date

SE2BI9SW	4	0	04 Jun 2012	Up to Date
SE3CI5D4	4	3	14 Nov 2012	Up to Date
SE3CI9T4	5	1	25 Oct 2012	Up to Date
SE3DI7L8	4	2	06 Aug 2011	Up to Date
SE3DI7LA	1	1	21 Jan 2011	Up to Date
SE3DI9T8	1	5	19 Apr 2011	Up to Date
SE4DI7L8	2	4	28 Feb 2013	Up to Date
SE4EI7LA	1	6	17 Jun 2012	Up to Date
SE4EI7LB	7	32	14 Nov 2012	Up to Date
SE4EI8PB	8	4	06 Jun 2013	Up to Date
SE4EI9T8	6	6	03 Apr 2012	Up to Date
SE4EI9T9	5	14	16 Aug 2012	Up to Date
SE4EIAX8	9	7	19 Nov 2012	Up to Date
SE4EIAX9	8	7	04 Jun 2012	Up to Date
SE4FI8PA	10	1	14 Nov 2012	Up to Date
SE4GI8PA	2	2	25 Oct 2012	Up to Date
SE4HI8PA	3	1	06 Aug 2011	Up to Date
SE4II8PA	1	11	21 Jan 2011	Up to Date
SE5DI7L8	13	2	14 Nov 2012	Up to Date
SE5EI7LA	3	9	25 Oct 2012	Up to Date
SE5EI9T8	14	8	06 Aug 2011	Up to Date
SE5EI9T9	2	7	21 Jan 2011	Up to Date
SE5EIAX8	6	5	19 Apr 2011	Up to Date
SE5EIAX9	8	3	28 Feb 2013	Up to Date
SE5FI7LB	8	4	17 Jun 2012	Up to Date
SE5FI8PA	1	1	14 Nov 2012	Up to Date
SE5GI7LB	7	2	06 Jun 2013	Up to Date

<b>Data Server: PM</b>				
<b>Cell Name</b>	<b>Edition</b>	<b>Update</b>	<b>Issue Date</b>	<b>Status</b>
SE5GI8PA	6	8	03 Apr 2012	Up to Date
SE5HI7LB	4	6	16 Aug 2012	Up to Date
SE5HI8PA	3	5	19 Nov 2012	Up to Date
SE5II7LB	5	4	04 Jun 2012	Up to Date
SE5II8PA	2	4	14 Nov 2012	Up to Date

SE6DI7LA	12	3	25 Oct 2012	Up to Date
----------	----	---	-------------	------------

**Route Filtered ENC Update Status Report.**

**Vessel Name** HMS Goteborg  
**Identifier** IMO 4653321  
**Report Date** 16<sup>th</sup> May 2013  
**Content** Filtered for Route Plan “Goteborg – Kiel”  
**Start WP** Goteborg [57.782324N,11.966667E]  
**End WP** Kiel [54.333742N,10.159607E]

**Chart Status Summary:**

Chart Status	Count
Total	50
Up to Date	38/50
Not Up to Date	10/50
Withdrawn	2/50
Unknown	0/50

Data Server: GB							
Cell Name	Edition	Update	Issue Date	Expiry Date	Status	Action	
DE316001	5	1	13032013		Not Up to Date	To be installed	
DE416010	1	1	12042012		Not Up to Date	To be installed	
DE416020	6	2	11052012		Not Up to Date	To be installed	
DE416021	8	3	10052012		Not Up to Date	To be installed	
DE416030	3	0	01012013		Not Up to Date	To be installed	
DE516175	6	6	01012013		Not Up to Date	To be ordered	
DE516200	8	5	04052013		Not Up to Date	To be ordered	
DK2KATGS	4	4	22042012		Not Up to Date	To be ordered	
DK2LILBL	2	0	14112012		Not Up to Date	To be ordered	
DK2SKARK	6	7	25102012		Not Up to Date	To be ordered	
DK2STOBL	9	6	06082011		Not Up to Date	To be ordered	
DK4ABFNF	4	9	21012011		Withdrawn	To be removed	
DK4FAVSF	2	1	19042011		Withdrawn	To be removed	
DK4KATGN	1	2	28022013		Up to Date	Renew	
DK4KATGS	1	11	17062012		Up to Date	Renew	
DK4STOBN	1	2	14112012		Up to Date	Renew	
DK4STOBS	4	1	06062013		Up to Date	No action	
DK5KALBG	5	8	03042012		Up to Date	No action	

DK5KORSO	3	7	16082012		Up to Date	No action
SE2BHS0W	8	5	19112012		Up to Date	No action
SE2BI9SW	4	0	04062012		Up to Date	No action
SE3CI5D4	4	3	14112012		Up to Date	No action

## **Appendix 1 Data Protection Scheme Test Data**

**Important Notice:** S-63 Appendix 1 includes test data which are provided separately as compressed (ZIP) files (see link:<https://ihonet/standards-and-specifications>). Embedded in the ZIP file is a document “Test Data Implementation Guide” providing instructions on how to use the test data. The text below provides a brief presentation of Appendix 1.

### **1.1 Introduction**

The S-63 Appendix 1 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. It includes a “Test Data Implementation Guide” which is provided along with the 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 provides a complete test sample for compliance testing.

The associated “Test Data Implementation Guide” will be maintained independent of the IHO S-63 main document and new versions will be published on the IHO website.

### **1.2 Organisation of the Test Definitions and Test data**

#### **1.2.1 Test Definitions**

The test definitions offers high level functional tests 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 3 of the “Test Data Implementation Guide”. Test definitions for the Scheme Administrator functionality has not been included in the document since only the IHO Secretariat will require these test scenarios.

Each test definition indicates if 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.

#### **1.2.2 Test data**

A range of test data has been developed to support the test definitions. The features of each test data set are defined in chapter 4 of the “Test Data Implementation Guide”.

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 developers for unit testing or other test situations for their application.

#### **1.2.3 Conditions of Use for the Test data**

The ENC information (the material) 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 be bound by these conditions then the material should not be used and it should be destroyed.

### **1.2.3.1 Conditions of Release**

The material supplied is protected by the copyright of the national Hydrographic Office. No part of the supplied material may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying or otherwise except as required to fulfil the purpose described above.

The material is NOT to be used for navigation.

When the material is no longer required to fulfil the purpose, it and any working copies, are to be destroyed.

### **1.2.3.2 Disclaimer**

Whilst the IHO Secretariat and the Hydrographic Offices have used its best endeavours to ensure that the material is suitable to fulfil the purposes, they offer no warranty guarantee or other assurances to the effect that it will meet the requirements. The IHO Secretariat and the Hydrographic Offices will accept no liability for any damage or loss of any nature rising from its use. The material supplied is used entirely at the recipient's own risk.

## Appendix 2

### Large Media Support

#### 2.1 Introduction

Until recently the majority of ECDIS/ECS only had the capability to load ENC Exchange Sets (ExSets) from CD-ROMs. However, it is becoming increasingly common for new OEM hardware to be delivered with DVD drives or other Large Media Support<sup>15</sup> (LMS). The inclusion of this media support now offers data servers the potential to include more ENC data on a single media.

Several issues have emerged during the operation of the existing S-63 encrypted ENC services using edition 1.0 of the standard. Not least of these is the fact that providing large exchange sets has resulted in unacceptable load times to the ECDIS/ECS. This is one of the principle reasons why data servers did not provide services that included single exchange sets spanning multiple CD-ROMs.

To store a single ENC exchange set on a mass storage device such as a DVD or USB that was similar in size to that stored on CD-ROM, would be an inefficient use of the media and the available memory. This being the case it would make sense to store multiple exchange sets on the same media, each about the same size as those currently stored on CD-ROM. Since this method of storage is not defined in the IHO S-57 Product Specifications or Edition 1.0 of S-63 a new configuration will have to be specified.

When designing the media structure the following considerations have been taken into account:

- ENC Services may be provided across multiple media sets
- ENC Services may contain data from more than one Data Server
- Suitable files must be provided so that manufacturer systems can manage and import S-63 encrypted ENCs in an efficient and expeditious manner and create intuitive systems which manage multiple pieces of media easily.

#### 2.2 Media Overview

The following section gives a high level view of how the data will be structured on the media. It also outlines how the S-63 exchange set structure has been modified for large media support; this is further supported by diagrams in Annexes A and B of this appendix. Detailed information relating to the content and format of these folders and files are provided later in this appendix.

##### 2.2.1 Media Types

There will be two types of media, “**BASE**”, containing one or more Base Exchange sets and, “**UPDATE**”, containing the weekly ENC updates, these may be contained in one or more exchanges sets on the update media. It was considered that because of the increased capacity which these types of media offer it could be possible to re-issue base ExSets on the update media and conversely weekly updates on the base media.

##### 2.2.2 Media Folder and File Structure

All exchange sets are located in the root directory of each media each within their own specific sub-directory. The configuration of all exchange sets are the same as outlined in 7.5.1 of the main document with the one notable exception. The “**INFO**” folder that includes the “**PRODUCTS.TXT**” file will no longer be stored in the root directory of the exchange set(s) but in the root directory of the media.

The “**INFO**” will continue to be used by data servers to include additional files unique and specific to their S-63 encrypted ENC services. Note that any data server specific files stored in this folder must be named in such a way that they **DO NOT** conflict with the S-63 file naming convention.

##### 2.2.2.1 Additional Media File

An additional file named “**MEDIA.TXT**” will be included on each piece of media to assist data clients in managing multiple exchange sets on the same media and across multiple media sets. It will also enable data clients systems to prompt users to insert the relevant media by including a machine readable

---

<sup>15</sup> Large Media Support can also be referred to as Mass Storage Devices.

string in each record referring to each piece of media. A more detailed explanation of the format of the **MEDIA.TXT** file is provided later in [Appendix 2.3](#).

### 2.2.3 Media Identification

There must be a method for differentiating between services provided on CD and those supplied using large media support. The first differentiator is the volume ID of the media (see [Appendix 2.2.3.1](#)). This will identify the use of large media format and notify the data client of the expected folder and file structure.

A further indication is the presence of the new MEDIA.TXT file in the root directory of the media is a further indication that an ENC service is being provided using large media support.

#### 2.2.3.1 Media Labelling

For large media support the media labelling convention will be similar to that used in the IHO S-57 product specification. Instead of “V01X01”, where “V” stands for “Volume”, the letter “M” for “Media” will be substituted.

The volume label for large media support will also indicate how many media sets there are in a service. Therefore if there are three media sets they will be labelled as follows:

M01X03 [Media set 1 of 3]

M02X03 [Media set 2 of 3]

M03X03 [Media set 3 of 3]

**NOTE** This only identifies the number of media sets in an ENC service and does not imply that this is a single exchange set covering multiple media sets. This purpose of this naming convention is to assist data clients to identify the media where licenced cells are located.

## 2.3 Media File Formats

### 2.3.1 Product Listing (PRODUCTS.TXT)

For “**Base Media**” the “**PRODUCTS.TXT**” file will contain records for all cells held on that particular media. The header as defined in section 6.2.2 of the main document will be labelled as “**FULL**” if there is only one media in a particular service. However if there is more than one media this will be labelled “**PARTIAL**”. A “**FULL**” products listing will always be provided on the “**Update Media**” with records of all cells in a data server’s service.

It is important that ECDIS/ECS manufacturers manage these records carefully; “**PARTIAL**” product listings must be merged with the “**FULL**” listing stored within the system. It must be noted that the system may contain product information from more than one data server. Therefore it is important not to overwrite “**FULL**” listings unless they are stored independently according to data server.

### 2.3.2 Media Listing (MEDIA.TXT)

This is a new file designed to manage services supplied using large media support. It is located in the root directory of the base and update media and contains information relating to all media in a data server’s service and the exchange sets contained on the media. The main purpose of this file is as follows:

- To provide data clients with a means to manage the import of a data server’s service that supports large media.
- To provide information to allow data clients to manage multiple media sets.
- To provide “User Information” so that data clients can make the import process more intuitive for the end user.

**NOTE** The latest update media **will always** contain the current status of the most recent base media (STATUS.LST) and base exchanges sets (MEDIA.TXT) in a data server’s service. This can be used to check the latest Base Media and Base Exchange sets have been installed. Further details on the structure and format of this file are outlined below.

#### 2.3.2.1 Header Format

The purpose of the MEDIA.TXT header is similar to that of the SERIAL.ENC file stored with the exchange set. It is used to manage the media installation by identifying the following:

- The media service provider

- The media date and week of issue
- The media number and media type
- Machine readable media name to display to users

The header is provided in two lines each containing a single record, the first is a fixed length, and the second is comma separated. The following table defines the format in more detail:

Field ID	Domain	Bytes	Range
Data Server ID	Character	2	Any pair of alphanumeric, e.g. PR
Week of Issue	Character	10	Any ASCII Characters, e.g. WKNN_YY
Date of Issue	Date	8	YYYYMMDD
Media Type	Character	10	BASE or UPDATE
Media Label ID	Character	6	M[01-99]X[01-99]
End of record delimiter	hexadecimal	2	CR/LF
Media ID	Character	2-3	For example, M1, M2 or M11.
Machine Readable Media Name	'Character'	0-100	Text string contained within quotation marks
Regional Information [Optional]	'Character'	0-100	Text string contained within quotation marks
End of record delimiter	hexadecimal	2	CR/LF

EXAMPLE: GBWK27\_07 20070621BASE M01X03 M1 , 'UKHO Week 27\_07 BASE MEDIA 1' , 'Europe, Africa, and Middle East'

### 2.3.2.2 Media Record Format

The “**MEDIA.TXT**” file also contains a list of records that identifies all current exchange sets in a data server’s service and the destination media where they can be located. Its purpose, together with the STATUS.LST, is to provide data clients with a means of managing the import of encrypted ENCs across multiple media sets and provide “User Information” so that the data client can prompt, using the STATUS.LST file, end users to load the appropriate media.

The “**MEDIA.TXT**” file stored on the **UPDATE** media will always contain a **FULL** list of media/ exchange sets contained in a data server’s service. It will also carry the date when the exchange sets were last issued, this way the ECDIS/ECS can always validate, together with the STATUS.LST, whether it holds the latest information.

The “**MEDIA.TXT**” file stored on the **BASE** media will contain a list of those exchange sets stored on the media. It will **NOT** contain information about the other volumes in the service.

Field ID	Domain	Bytes	Range	Notes (see below)
Media/Exchange Set Location	Character	5-7	<b>M1 to M99 ; B1 to B99</b> e.g. M2 ; B7 [Media 2, Base ExS 7] <b>M1 to M99 ; U1 to U99</b> e.g. M1 ; U2 [Media 1, Update ExS 2]	a
Exchange Set Issue Date	Date	8	YYYYMMDD, e.g. 20070621	b
Media Set Number [Long Name]	Character		‘Any ASCII Characters’	c
Regional Information [Optional]	Character		‘Any ASCII Characters’	d

Field ID	Domain	Bytes	Range	Notes (see below)
<b>Reserved Field</b>	Character			e
<b>Comments Field</b>	Character			f
<sup>a</sup> This field identifies on what media the base or update exchange set is located.				
<sup>b</sup> The ExSet Issue Date. This is the date when an ExSet is issued or re-issued2 on the base or update media. Although it may be more practical to re-issue all ExSets on a particular media simultaneously there may be occasions when the media is re-issued with just one ExSet re-issued. Data Clients may use this date to validate the status of the currently installed cells from the update media.				
<sup>c</sup> This is a machine readable text string that Data Clients can use to prompt end users to load the appropriate media.				
<sup>d</sup> This is an optional machine readable text string that can be used by data clients to display additional information relating to the regions/producer nations on a particular media..				
<sup>e</sup> Future Use				
<sup>f</sup> Additional comment information				

EXAMPLE: M1;B1,20070614,'Base Dataset 1','Europe',,

The update media “**MEDIA.TXT**” file will always contain the latest issue dates and information for all base media exchange sets in a media set. *Although provision has been made to have more than one update ExSet on the update media, it is not recommended for the reasons mentioned in Appendix 2.4. However, if there are more than one then this can be managed by the entries in the PRODUCTS.TXT and MEDIA.TXT file on the update media.*

EXAMPLE — Example of a complete **MEDIA.TXT [UPDATE]**:: GBWK28\_07 20070628UPDATE M01X02  
U1,'UKHO Week 28\_07 UPDATE MEDIA 1 of 2','Europe'  
M1;B1,20070614,'UKHO BASE MEDIA 1','Europe, Africa and Middle East',,  
M1;B2,20070614,'UKHO BASE MEDIA 1','Europe, Africa and Middle East',,  
M1;B3,20070621,'UKHO BASE MEDIA 1','Europe, Africa and Middle East',,  
M2;B4,20070517,'UKHO BASE MEDIA 2','North and South America',,  
M2;B5,20070517,'UKHO BASE MEDIA 2','North and South America',,  
M3;B6,20070405,'UKHO BASE MEDIA 3','Far East and Australasia',,  
M3;B7,20070405,'UKHO BASE MEDIA 3','Far East and Australasia',,  
M1;U1,20070628,'UKHO WK28\_07 ENC Update','Europe',,  
M1;U2,20070628,'UKHO WK28\_07 ENC Update','Rest of the World',,

EXAMPLE — Example of complete **MEDIA.TXT [BASE]** file on:: GBWK27\_07 20070621BASE M01X03  
M1,'UKHO Week 27\_07 BASE MEDIA 1','Europe, Africa, and Middle East'

M1;B1,20070614,'Base Dataset 1','Europe',,  
M1;B2,20070614,'Base Dataset 2','Africa',,  
M1;B3,20070621,'Base Dataset 3','Middle East',,

## 2.4 Media Management (Data Servers)

The issue and re-issue of base media is very much at the discretion of the data server. However, to prevent the continual renewal of base media it is recommended that individual exchange sets are not issued independently of one another on the same media. However, there may be occasions when this is necessary, e.g. the introduction of ENCs from a new country or essential management of the update exchange set.

It is probable that data servers will operate a two tier service, e.g. they will support both a CD-ROM and DVD services. To fulfil the recommendation in the paragraph above it may not be possible to maintain synchronicity between the two levels of service due to the greater flexibility that large media offers. DVDs for instance are capable of storing more data and therefore it may not be necessary to re-issue media as frequently as, for example, CDs.

**NOTE** It may be that a data server issue the base media using the large media option but, for reasons of cost, issues the update media on CD. In these instances it is important to note that the content and structure of the update MUST be consistent with that of the base media it relates to.

## 2.5 Media Management (Data Clients)

As the volume of ENCs continues to grow a more intelligent and “smarter” method of loading them into ECDIS/ECS is required. Since most customer only purchase a subset of all available ENCs it would seem prudent to base the import of S-63 encrypted ENCs directly against the customers permit holdings. The following bullet points are provided to illustrate the recommended steps for importing encrypted ENCs.

- Insert, read and validate the ‘**PERMIT.TXT**’ file
- Insert the ‘**Update Media**’
- Read the “**FULL**” products listing form the ‘**PRODUCTS.TXT**’ file
- Identify and flag all cells that are licenced (have valid permits)
- Identify the target ‘**Base Media**’ and ‘**BASE Exchange Set**’ location of each licenced ENC
- Prompts the user to install the appropriate ‘**Base Media**’
- Install all licenced ENCs from the relevant ‘**Base Media**’ and ‘**Base Exchange Sets**’
- Prompt the user to insert the latest ‘**Update Media**’ to bring all licenced ENCs up to date and complete the ENC loading cycle.

**NOTE** In the case of encrypted ENC data it is not necessary or desirable to read the complete CATALOG.031 file. This file should only be used to identify the target location of all licenced ENCs and any associated files in the exchange set.

### 2.5.1 Media Warnings

When the weekly update media is loaded data clients must check that the issue date of all installed base media are current and up to date. The “**STATUS.LST**” on the latest update media will always contain the latest issue date of each base media in the service.

If the ECDIS/ECS does not have the latest base media loaded a warning must be given informing the user similar to the following example:

**EXAMPLE: “This ‘Update Media’ is not compatible with the actual installed ‘Base Media’. Please install the following ‘Base Media’ first and then continue with the ‘Update Media’.”**

**<Field: User Information 1>**

**<Field: User Information 2>**

**<Field: User Information x> (where x is the base media number)**

**Example:**

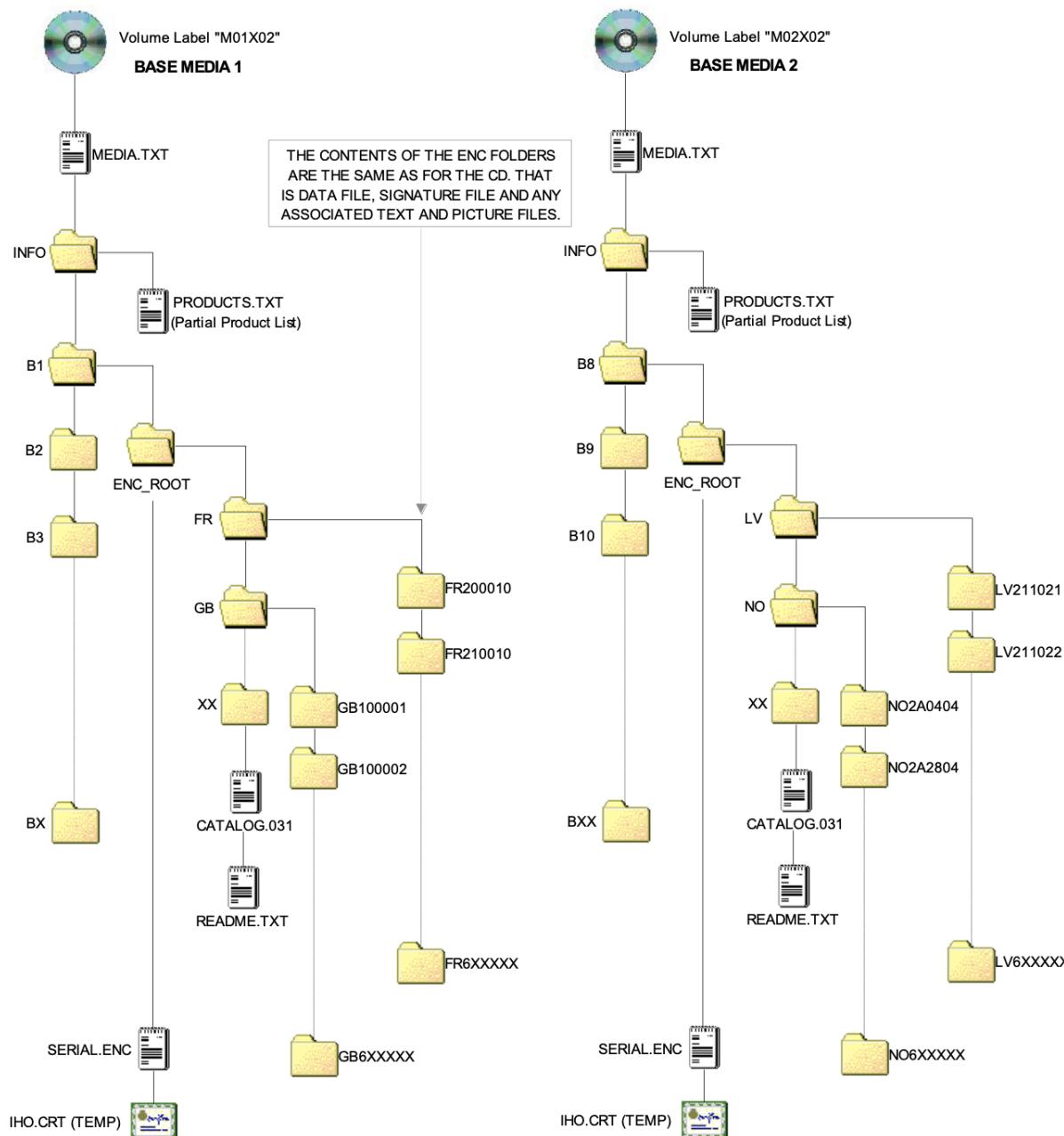
**“This ‘Update Media’ is not compatible with the actual installed ‘Base Media’. Please install the following ‘Base Media’ first and then continue with the ‘Update Media’.”**

**‘Base Media 2 dated 07 June 2007’**

**NOTE** The user should only be prompted to install compatible base media that contains licenced ENC cells.

## BASE MEDIA FOLDER AND FILE STRUCTURE

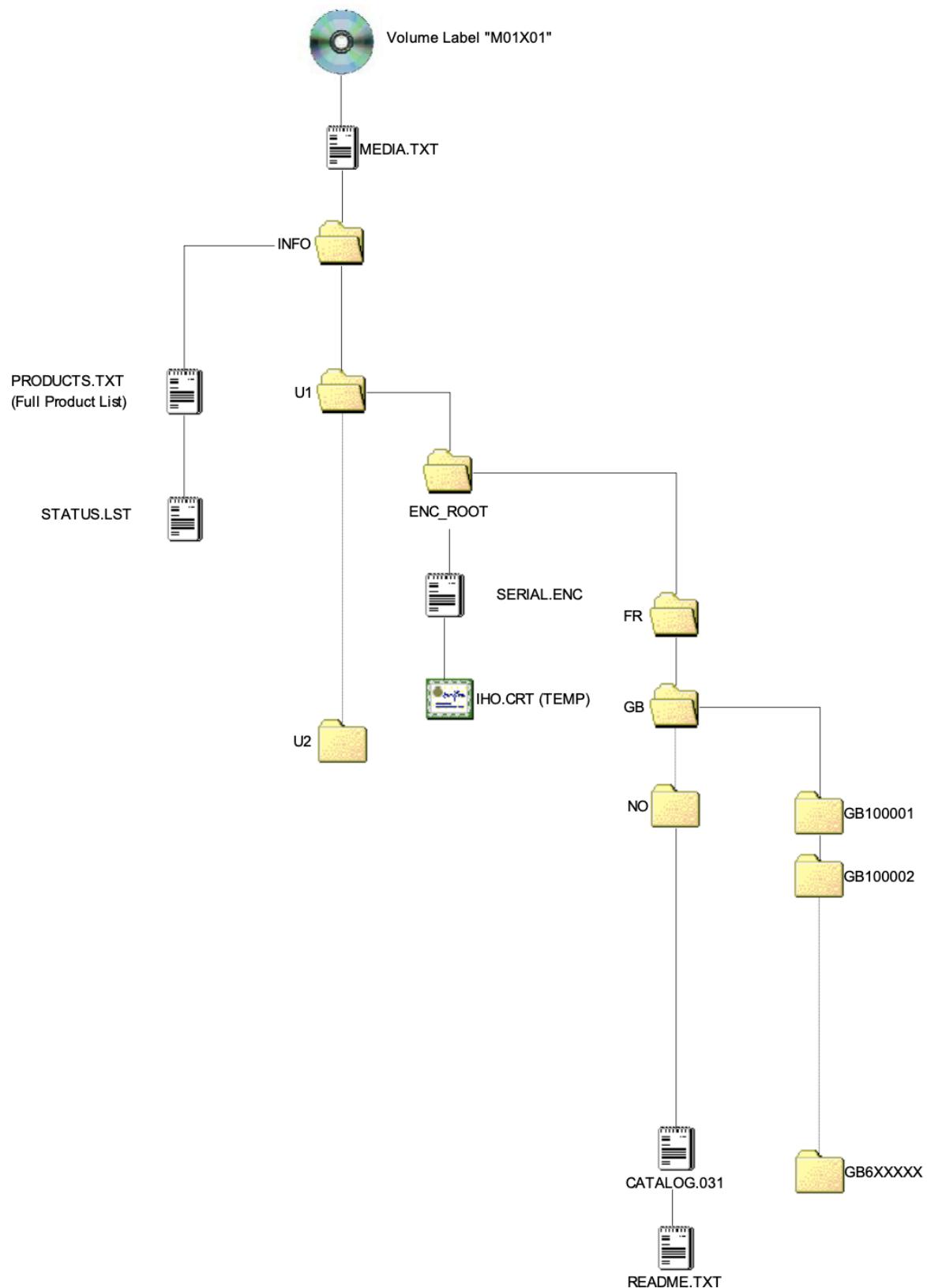
The [Figure Appendix 2-1](#) is for illustrative purposes only and outlines the top level folder and file structure that must be used by data servers when supplying S-63 encrypted ENC services utilising large media support. However, it is possible that the structure under each ENC\_ROOT folder of each exchanges set may vary between data servers.



**Figure Appendix 2-1 — LARGE MEDIA SUPPORT FOR S-63 ENCRYPTED ENC SERVICESBASE MEDIA FOLDER AND FILE STRUCTURE**

#### UPDATE MEDIA FOLDER AND FILE STRUCTURE

The [Figure Appendix 2-2](#) is for illustrative purposes only and outlines the top level folder and file structure that must be used by data servers when supplying S-63 encrypted ENC services utilising large media support. However, it is possible that the structure under each ENC\_ROOT folder of each exchanges set may vary between data servers.



**Figure Appendix 2-2 — UPDATE MEDIA STRUCTURE (Only top level folders & files)**