**D****RAFT**

**S-63e2.0.0**

**TABLE OF CONTENTS**

1 INTRODUCTION 8

1.1 General Description 8

1.2 Participants in the Protection Scheme 9

1.2.1 Scheme Administrator 9

1.2.2 Data Servers 9

1.2.3 Data Clients 10

1.2.4 Original Equipment Manufacturers (OEM) 10

1.2.5 S-63 Participant Relationships 10

1.3 References 11

1.4 Compatibility with Previous Versions 12

1.5 Main Document: 12

1.6 Maintenance 12

1.7 Support 13

2 DATA COMPRESSION 14

2.1 Overview 14

2.2 Compression Algorithm 14

2.3 Encoding 14

3 DATA ENCRYPTION 15

3.1 What Data is encrypted? 15

3.2 How is it encrypted? 15

3.2.1 Encryption of ENC Information 15

3.2.2 Encryption of Other Protection Scheme Information 15

3.2.3 Encryption Algorithm 15

4 DATA LICENSING 16

4.1 Introduction 16

4.2 The Userpermit 17

4.2.1 Definition of Userpermit 17

4.2.2 HW\_ID Format 17

4.2.3 Check Sum (CRC) Format 18

4.2.4 M\_ID Format 18

4.2.5 M\_KEY Format 18

4.3 The Cell Permit 18

4.3.1 The Permit File (PERMIT.TXT) 19

4.3.2 The Permit File - Header Formats 20

4.3.3 Permit Record Fields 20

4.3.4 Definition of the Cell Permit 21

4.3.5 Cell Permit Format 21

5 DATA AUTHENTICATION 23

5.1 Introduction to Data Authentication and Integrity Checking 23

5.1.1 SA Verification 25

5.1.2 Data Integrity 26

5.2 Digital Certificates (SA Authentication) 26

5.2.1 The SA Public Key 27

5.2.2 New Data Servers 27

5.3 Digital Signatures (Verify Data Integrity) 27

5.3.1 Technical Overview of Digital Signatures 28

5.3.2 The SA Digital Certificate (X509v3) Format 28

5.3.3 Digital Signature Encoding 28

**PREFACE**

Copyright infringement and data piracy are pervasive problems of the digital era. Electronic Navigational Charts (ENC) or other digital spatial products 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: IHB 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: IHB 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 13th meeting (Athens, Greece, September 2001), revisited the issue of an RSS and agreed that a small advisory expert group investigate the implications of IHB 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 IHB in January 2002 that there were no technical implications to the IHB becoming the security scheme administrator and that the level of effort to administer the security scheme would be limited and within the IHB 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 14th 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 IHB. These proposals (see: IHB CL 44/2002) were approved by a majority of Member States (see: IHB 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 18th 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 IHB 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 19th 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.

The development of S-100 and the IMO resolution MSC.428(98) has required a revision of the Data Protection Scheme. The operational principles for using the protection scheme have been maintained, but changes have been introduced for the individual security constructs to reflect operational experience with the current version of the protection scheme and better harmonisation with international security constructs. In addition will edition 2.0.0 also support more product specifications based on the S-100 data model and where other organisations than IHO can operate as domain owners. Edition 2.0.0 has selected to use international or industry standards for encryption and digital signatures, and this together with S-100 have required a change in how the information is encoded and distributed.

Changes to this Standard, as well as any further developments, will continue to be coordinated by projects team within the S-100 Working Group under HSSC Guidance.

**GLOSSARY**

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 manufacture. 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 [3] |
| SSK | Self Signed Key (Self Signed Certificate File) |
| User Permit | Encrypted form of HW-ID uniquely identifying the ECDIS system |

Chart Related Terms

|  |  |
| --- | --- |
| Cell | Common unit used to represent a single product of a product specification. It can be a single S-101 ENC cell or a single S-102 bathymetric file. |
| ECDIS | Electronic Chart Display and Information System as defined by IMO |
| ENC | Electronic Navigational Chart as defined by the ENC Product Specification [1]. |
| S-57 | Transfer standard for ENC defined by IHO |
| S-100 | Universal Hydrographic Data Model defined by IHO |
| SENC | System-ENC (This is the internal format that OEMs convert to when importing data) |

Organisations

|  |  |
| --- | --- |
| ECC | Electronic Chart Centre AS (www.ecc.no) |
| HO | Hydrographic Office (e.g. Data Server) |
| IALA | International Association of Lighthouse Authorities |
| IHB | International Hydrographic Bureau |
| IHO | International Hydrographic Organisation |
| IMO | International Maritime Organisation |
| PRIMAR | Regional ENC coordinating Centre operated by the Norwegian Hydrographic Service ([www.primar.no](http://www.primar.no)) |
| 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)) |

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 security within |
| XOR | Exclusive OR |

# INTRODUCTION

This appendix, later referred to as ‘the protection scheme’, describes the recommended standard for the protection of hydrographic or spatial information which are based on the IHO S-100 Universal Hydrographic Data Model. It defines security constructs and operating procedures that must be followed to ensure that the protection scheme is operated correctly and to provide specifications that allow participants to build 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) and published by IHO as the S-63 Data Protection Scheme. The S-63 standard is based on the protection scheme developed and operated by PRIMAR as part of their protected ENC service. The Electronic Chart Centre AS and United Kingdom Hydrographic Office were the original contributing organisations.

S-63 edition 2.0.0 is published as an appendix to the IHO S-100 publication. It uses the same security principles as earlier editions of S-63, but the algorithms, encoding and distribution of information has been revised based on the need to support more S-100 based product specifications, use of international security standards and operational experience. The use of digital signatures will also meet IMO resolution MSC.428(98) to reduce cyber security risks. The individual S-100 based Product Specifications will define in more detail which security constructs are being used and on product which files.

The first edition of S-63 standard was adopted as the official IHO standard, by the IHO member states in December 2002 (IHO CL 66, 2002). It defined the roles and responsibilities for protecting ENC data produced by National Hydrographic Offices and distributed to customers with ECS/ECDIS systems.

## General Description

This document specifies a method of securing digital nautical, hydrographic and spatial related products and information. The purpose of data protection is threefold:

1. Piracy Protection: To prevent unauthorised use of data by encrypting the product information.
2. Selective Access: To restrict access to only the products that a customer has acquired a license for.
3. Authentication: To provide assurance that the products has come from approved sources.

Piracy protection and selective access are achieved by encrypting the products and providing cell permits to decrypt them. Cell permits have an expiration date to enable access to the products for a licensed period. Data Servers will encrypt the digital products before supplying it to the Data Client. The encrypted products are then decrypted by the end-user system (e.g. ECS/ECDIS) prior to being reformatted and imported into the system internal format (SENC.) Authentication is provided by means of digital signatures applied to the product files.

The security scheme does not specifically address how the product 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 protected products on hard media (e.g. DVD) and can be accessed and used by all customers with a valid license containing a set of permits. Selective access to individual products is supported by providing users with a licensed set of permits containing the encrypted cell keys. This license is created using a unique hardware identifier of the target system and is unique to each Data Client. Consequently licenses cannot be exchanged between individual Data Clients.

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

## Participants in the Protection 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.

### Scheme Administrator

The Scheme Administrator (SA) is solely responsible for maintaining and coordinating the protection scheme. The SA role is operated by The International Hydrographic Organization on behalf of the IHO member states and other organisations participating in the protection scheme. These organisations can have a cocordinating role for a maritime product domain, e.g. IMO and IALA. IHO as SA will establish procedures with product domain operators using the protection scheme to protect their products. These procedures will enable these domain coordinators to digitally sign the digital certificates used by their member organisations to participate in the protection scheme.

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 root certificate used to operate the 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.

*[Discussion: Nothing in the scheme prevents a Data server, not SA, do digitally sign the certificate of another organization to establish a chain of trust which can be traced back to IHO. No possibilities to revoke]*

### Data Servers

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

Data Servers will use the M\_KEY and HW\_ID information, as supplied by the SA, to issue encrypted product 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 system installations from the same manufacturer.

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.

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

### 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 digital signatures applied to the product files and decrypting the ENC information in compliance with the procedures defined in the scheme.

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

### Original Equipment Manufacturers (OEM)

OEMs subscribing to the IHO Data Protection Scheme 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 will establish test data for the verification and validation of OEM applications for various S-100 based product specifications when products become available. 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 product files. Product integrity can be verified by authenticating the digital signature provided with the product files, and the underlying product file consistency controls available in the underlying S-100 based product files.

### 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.

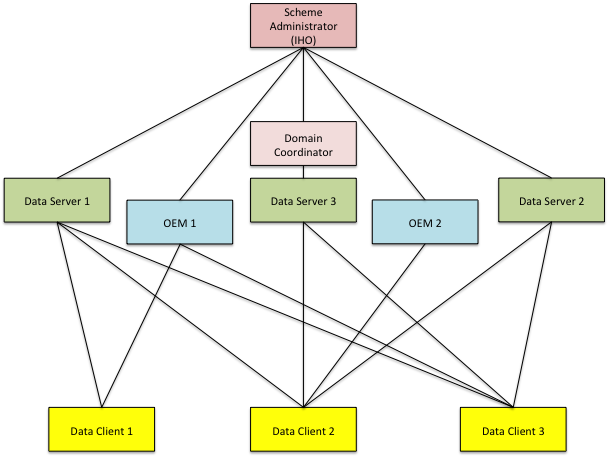


Figure 1: Relationship between protection scheme participants

## References

[1] S57 edition 3.1: IHO Transfer Standard for Digital Hydrographic Data, International Hydrographic Bureau (www.iho.int)

[2] Digital Signature Standard (DSS), FIPS Pub 186 (www.itl.nist.gov/div897/pubs/fip186.htm)

[3] Secure Hash Standard (SHA), FIPS Pub 180-1 (www.itl.nist.gov/div897/pubs/fip180-1.htm)

[4] Information Technology – Open Systems Interconnection – The Directory: Authentication Framework. X.509 version 3 - International Telecommunication Union

[6] ZIP File Format Specification, ISO/IEC 21320-1 "Document Container File — Part 1: Core"

[7] DES Modes of Operation, FIPS Pub 81 (www.itl.nist.gov/fipspubs/fip81.htm)

[8] RFC 1423: Privacy Enhancements for Internet Electronic Mail: Part III: Algorithms, Modes and Identifiers (ftp://ftp.isi.edu/in-notes/rfc1423.txt)

[9] Blowfish encryption algorithm, B. Schneier, Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204. (www.counterpane.com)

[10] CRC32 checksum algorithm. Information technology -- Telecommunications and information exchange between systems -- High-level data link control (HDLC) procedures. ISO/IEC 13239:2002.

[11] Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers, ISO/IEC 18033-3:

[12] The ESP CBC-Mode Cipher Algorithms, RFC 2451, <https://tools.ietf.org/html/rfc2451>

[13] Cryptographic Message Syntax (CMS), RFC 5652, <https://tools.ietf.org/html/rfc5652#section-6.3>

[14] Internet X.509 Public-key infrastructure and attribute certificate frameworks version 3, RFC 2459, ITU International Telecommunication Union, <https://tools.ietf.org/html/rfc2459>

[14] Secure Hash Standard (SHS), FIPS-PUB 180-4, National Institute of Standards and Technology, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>

## Compatibility with Previous Versions

The first 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 was published as 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 for this version 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.

Edition 2.0.0 of the protection scheme uses the same operational principles as earlier editions, but changes have been introduced for a majority of all security constructs to reflect the operational experience with the current version of the protection scheme and better harmonisation with international security constructs. This edition will also support more product specifications based on the S-100 data model and where other organisations than IHO can operate as domain owners. This edition of the standard can only be used to protect digital products based on the S-100 Data Model and is not compatible with the S-57 standard.

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

## Main Document:

To be completed

## Maintenance

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

## Support

Support in using and implementing this standard is provided to users by members of S-100 project team responsible for preparing and maintaining the S-100 protection scheme, via the IHO (info@iho.int). In addition an inventory of frequently asked questions (FAQ) is maintained by the IHO on the ECDIS section of the IHO website (www.iho.int).

# DATA COMPRESSION

## Overview

The content of producs based on the S-100 Data Model will, because of its structure, contain repeating patterns of information. Examples of this are small variations in the co-ordinate information within the product file.

If compression is applied, the files are always compressed before they are encrypted as the effectiveness of any compression algorithm relies on the existence of structured data contents. The individual S-100 based product specifications will specify if compression is being used.

## Compression Algorithm

The security scheme uses the ZIP algorithm1 [6] to compress and uncompress product files. It is identical to the algorithm used in previous versions of the IHO S-63 standard and available in many commercial applications e.g. WinZip, PKZIP.

The following restrictions are applied on the ZIP format in accordance with ISO/IEC 21320-1:2015:

* Files in ZIP archives may only be stored uncompressed, or using the "deflate" compression (i.e. compression method may contain the value "0" - stored or "8" - deflated).
* The encryption features are not used.
* The digital signature features are not used.
* The "patched data" features are prohibited.
* Archives may not span multiple volumes or be segmented.

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 product file leading to failing integrity checks. Data Servers and OEMs are advised to carefully implement compression/un-compression within their systems.

## Encoding

The individual S-100 based product specifications will provide more details if compression is being used, and which files will be compressed. If compression is applied, it is recommended that all product files within the exchange set will be compressed.

The use of compression will be encoded:

* S-100\_ExchangeCatalogue-compressionFlag with value **1**
* S-100\_ExchangeCatalogue-algorithmMethod with value **S63e2.0.0**

*[Discussion: Since the compression flag is located in the S-100\_ExchangeCatalogue-compressionFlag and algorithmMethod, either all or none of the files are compressed. Can not have some S-102 HDF5 files compressed and not others from multiple providers. Same situation for S-101 files, either all or none ENC files. Alternatively can the individual S-100 based product specification identify which files in the exchange set will be compressed]*

# DATA ENCRYPTION

## What Data is encrypted?

The product specifications based on the S-100 Data Model will define if encryption will be used and which files will be encrypted.

Only one encryption algorithm is used within the Scheme. Starting with S-63e2.0.0 to support S-100 based products, the encryption algorithm has been changed from Blowfish to Advanced Encryption Standard (AES) [11] in Cipher Block Chaining (CBC) [12] mode of operation.

It is always assumed that the complete product file will be encrypted. All information to be encrypted will use tAES-CBC algorithm.

In addition will the OEM System HW\_ID (hardware ID) be encrypted and provided to the Data Client in the form of a userpermit. The cell keys used to encrypt the product files are themselves encrypted by the Data Server and supplied to Data Clients as cell permits. Information about the encryption algorithm is available in section 3.2.3.

## How is it encrypted?

Each single product is encrypted using a unique Cell Key. The same Cell Key is used to encrypt all files associated with the product and all updates issued for the product edition. The scheme however, allows for the cell keys to be changed at the discretion of the Data Server when a new edition of the product is released. The Cell Keys are delivered to Data Clients in the form of cell permits.

### Encryption of ENC Information

The product files are encrypted using a 128 bit key.

### Encryption of Other Protection Scheme Information

The HardwareID, Userpermit and the Cell permit contents are encrypted using a 128 bit key.

### Encryption Algorithm

The scheme encrypts all relevant information using Advanced Encryption Standard (AES) [11] in Cipher Block Chaining (CBC) [12] mode of operation. The AES-CBC block size is 128 bits. The encryption key length is 128 bits. Block size padding will be in accordance with PKCS7 [13].

The AES-CBC initialization vector will always be 128 bits (16 bytes). It will be the name of the product file and padded in accordance with PCKS7 [13] if the file name is shorter than 16 bytes.

Refer to the S-100 based product specification for information on how encryption is applied to the product files.

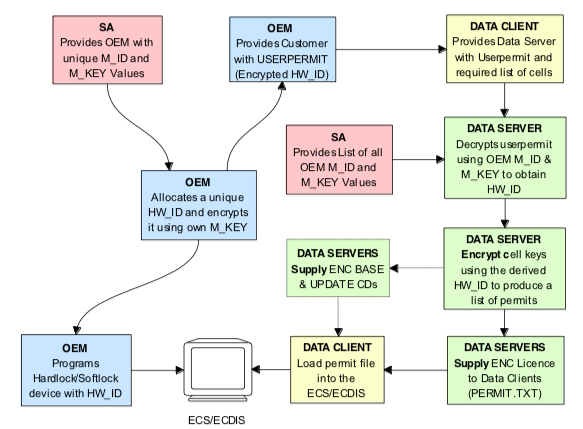
# DATA LICENSING

## Introduction

Data Clients do not buy the S-100 based products but are licensed to use it. Licensing is the method that Data Servers use to give Data Clients selective access to up-to-date products 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 licensed product files. 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. IHO as the Scheme Administrator provide the Data Servers 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.

Figur 2 High level licensing diagram based on S-101 ENC products

## 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 products 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 and tamperproof 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 S-100 based productss 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 six 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.

### 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** |
| 128 bits (32 hex characters) | 8 hex characters | 6 characters |

Any alphabetic character will be written in upper case.

Example: Userpermit Structure (to be completed)

111122223333444455556666AAAABBBB1234567830313233343536

### HW\_ID Format

The HW\_ID is a 32 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 and tamperproof identification of each installation. Manufactures, with the consent of the Data Server, may use the same HW\_ID on more than one system unit at an installation site; e.g. multiple ECDIS systems on a vessel bridge.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 AES-CBC algorithm with M\_KEY as the key resulting in a 128 bits digit encoded as a 32 digit (16 bytes) hexadecimal number. The encrypted HW\_ID is then represented in its ASCII form in the userpermit as 32 characters. Note that the size of the HW\_ID is identical to the AES-CBC block size and does not require any padding when used as the encryption key.

Example of HW\_ID is: 111122223333444455556666AAAABBBB

Example of encrypted HW\_ID is: (to be completed)

### 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 32 character hexadecimal string. It is then hashed using the algorithm CRC32 [10] 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: (to be completed)

### M\_ID Format

The M\_ID is a 6-character alphanumeric code expressed as ASCII representation provided by the SA. The SA will provide all licensed 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: 123456 or 30313233343536 (ASCII3)

### M\_KEY Format

The M\_KEY is a 32 digit hexadecimal (128 bits) 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. Note that the size of the M\_KEY is identical to the AES-CBC block size and does not require any padding when used as the encryption key.

Example of M\_KEY is 1234567890ABCDEF1234567890ABCDEF

## The Cell Permit

To decrypt a product file the Data Client must have access to the encryption key (see section 4.1) 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 it is named PERMIT.TXT (see section 4.3.1). This file may contain several product permits based on the product 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 license.

Each cell permit record also contains additional fields that are supplied to assist OEM systems to manage the Data Clients license and permit files from multiple Data Servers, see section 4.3.3.

Data Clients can obtain a licence to access products by supplying the Data Server with their unique userpermit (see section 4.2). 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 sections 4.3.2 & 4.3.3.

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 licensed products. Since several Data Servers can make permit files for a specific type of product, it is the responsibility of the Data Client system to manage permit files from multiple Data Servers.

### 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 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.

The PRODUXT.TXT file can contain multiple sections as follows:

|  |  |
| --- | --- |
| **Section** | **Description** |
| Header | This includes the file creation date and the format version. |
| Products | Cell permits from the Data Server for the specified product. |
| Signature | The Data Server digital signature appended to the PERMIT.TXT file |

Note that the PERMIT.TXT file can contain cell permits for multiple products provided by the Data Server. OEMs must ensure that their end-user software is able to merge permits from multiple data servers.

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]”.

### The Permit File - Header Formats

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

|  |  |  |
| --- | --- | --- |
| **Section** | **Fieldname** | **Value** |
| Date and time | :DATE | The field name, date and time is separated by a space character (SP <h20>). The date will be provided as YYYYMMDD and the time as HH:MM using the 24 hour clock.  Example: :DATE 20180320 17:11 |
| Provider | :DATASERVER | Name of Data Server who has generated the permit file. The Data Server should be consistent and use the same organizational name.  Example: :DATASERVER PRIMAR |
| Meta Permit version | :VERSION | Edition number of the S-63 standard. It will be compatible with the IHO version numbering scheme X.Y.Z.  Example: :VERSION 2.0.0 |
| Product type | :PRODUCT | All cell permits associated for the defined product type. Multiple product types can be included in PRODUCTS.TXT. All cell permits for a product type shall be grouped together  Example: :PRODUCT S101 |

Shall we include the User Permit of the destination system in the Header? End-user system can quickly check if permit is for this system on a multi system bridge?

Example: :DATE 20180320 17:11

:DATASERVER PRIMAR

:VERSION 2.0.0

|  |  |
| --- | --- |
| **Field** | **Value** |
| Cell Permit | As defined in section 4.3.4 & 4.3.5 |
| Service Level Indicator | 0 for subscription permit  1 for single purchase permit |
| Edition Number | Product edition number |
| Data Server ID | This is a six character alphanumeric issued by the SA |
| Comment | Free text field for comments on the cell permit etc. |

:PRODUCT S101

[List of licenced cell permits for ENC products]

:PRODUCT S102

[List of licence cell permits for bathymetric products]

### Permit Record Fields

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

The supplied cell permit is only guaranteed for the specified edition of the product.

### 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** |
| Product Name: | The product name enables Data Client systems to link the correct encryption key to the corresponding encrypted product name. |
| Expiry Date: | 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. |
| Encrypted Cell Key (ECK) | ECK contains the decryption key for the specified edition of the product. |

The Product Name and Expiry Date fields are separated by a comma (,) since the S-100 based product specifications will have different product naming conventions.

Note that the CRC Check Sum field defined in S-63e1.x has been removed since the PERMIT.TXT file will be digitally signed by the Data Server and provide the same level of integrity check as a CRC check sum.

### Cell Permit Format

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

|  |  |  |
| --- | --- | --- |
| **Field** | **Characters** | **Format** |
| Cell Name | Variable length | 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, |
| Expiry Date | 8 | A numeric string that contains the license expiry date for the product in the format YYYYMMDD. Single purchase permits will often have the permit issue as expiration date, while subscription licenses will have a future expiration date.  Example is: 20181224 (24th December 2018) |
| ECK |  | The Cell Key is 128 bit represented as 32 hexadecimal characters.  Example:  ECK: 1234567890ABCDEF1234567890ABCDEF |

Example Cell Permit field:

NO4D0613,20181221234567890ABCDEF1234567890ABCDEF

Example Cell Permit record:

NO4D0613,20181221234567890ABCDEF1234567890ABCDEF,0,2,PRIMAR,Comments

# DATA AUTHENTICATION

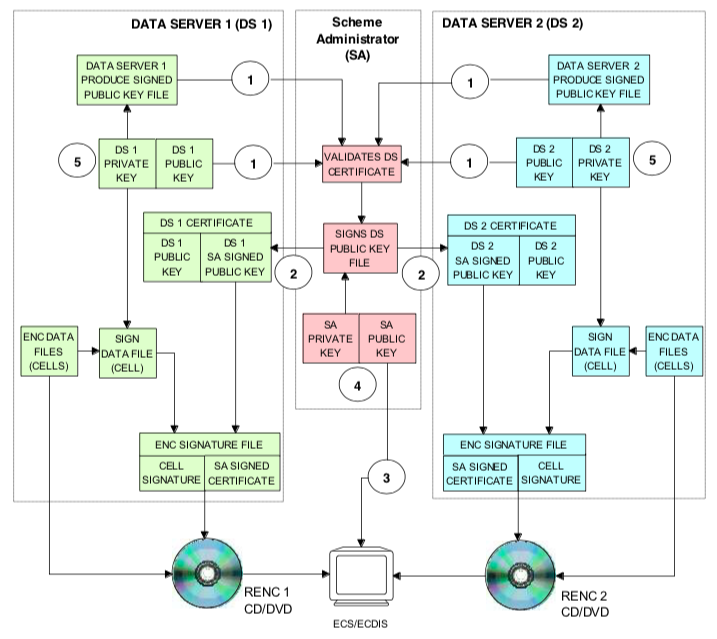
## Introduction to Data Authentication and Integrity Checking

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[[1]](#footnote-1) 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) for a more detailed and accessible explanation.

The scheme can be considered to have three distinct phases:

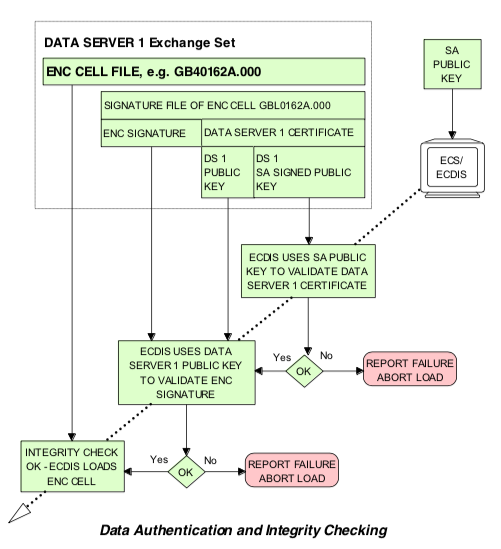
1. A Scheme Administrator (SA) verifies the identity of a supplier of products and provides the supplier with information to allow them to digitally sign their products.
2. A Data Server (e.g. RENC or VAR) issues products signed with their identity (and its verification by the SA).
3. The subsequent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



Figur 3 Example of authentication process using ENC products

**NOTES – ENC AUTHENTICATION PROCESSES**

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 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 independantly 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.



**NOTES – DATA AUTHENTICATION AND INTEGRITY CHECKING**

If an OEM system 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 OEM system uses the SA public key, previously installed independently of the supply media, 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 OEM system uses the public key from the certificate to check the signature of the product file.

### SA Verification

The OEM system needs to be able to verify that the products are from a bona fide source. It does this by ensuring that the Data Server’s public key provided within the signature of the product 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 Data Supplier’s public key. This certificate is then included with all the product´s signature files.

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

### Data Integrity

After the source of the product exchange set has been authenticated the OEM system then checks data integrity by validating the signature provided for each product by the Data Server.

The data server creates a digital signature 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 product file]
* Their Data Server certificate (which remains constant).

The OEM system 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 product 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.

## 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 signed by an international certificate authority, and is the root certificate for the protection 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 and and gets it signed by an international certificate authority.

**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 pubic 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 the product´s signature files.

The format of the various files, certificates and signatures are described in more detail in section 5.4.

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.

### The SA Public Key

The scheme requires that the SA public key is installed on the Data Client’s systems independently of the exchange or delivery of the products. This can be pre-installed by the OEM. However, the Data Client system must have a method of installing a new public key 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 and provide appropriate information to the end-user.

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. The end-user should try to obtain and install the updated version of the SA certificate.

Is it realistic to assume that other domain coordinators like IALA will sign their member organisations public key?

### New Data Servers

The IHO 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.

## 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 data producers (HOs) 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 products. All product files will always have a single unique digital signature associated with it.

An exchange set may contain product file signatures issued by different Data Servers and therefore each product file must be authenticated individually.

It is recommended that all files comprising the product exchange and service access should have an associated digital signature. For all product files included in an exchange set, fields have been defined in S-100 to specify that signatures are being used and to store the digital signature. Some files will however not be defined in the catalogue directory, and the method to provide a digital signature is to create a file with the same name as the source file but with the extension .SIGN.

Example: PERMIT.TXT Original source file

PERMIT.SIGN File containing the digital signature

### Technical Overview of Digital Signatures

Data authentication is provided using a digital signature compliant with the Digital Signature Standard (DSS) [2]. The DSS uses the Secure Hash Algorithm (SHA256) [14] to create a message digest (hash) that are 256 bits. The message digest is then input to the Digital Signature Algorithm (DSA) [2] to generate the digital signature for the message using an asymmetric encryption algorithm and the ‘private key’ of a key pair. The DSA keylength is 1024 bits. 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.

### The SA Digital Certificate (X509v3) Format

The SA Digital Certificate will be in X509v3 format [4] and represents a DSA Public Key of length 1024 bits and provided as PEM encoded text (base 64). The SA Digital Certificate will always be available in a file called IHO.CRT. The IHO.CRT file is available from IHO at http://www.iho.int.

(example to be completed)

### Digital Signature Encoding

All files included in the exchange set will have their signatures encoded in either the S100\_DatasetDiscoveryMetaData-digitalSignatureValue or S100\_SupportFileDiscoveryMetadata-digitalSignatureValue.

The digitalSignatureReference field shall be encoded **S63e2.0.0**.

The digitalSignature field shal be encoded **1** (true).

There will be additional files associated with an exchange set which will not have its digital signature value encoded; e.g. S102ed2.CAT containing the exchange catalogue. Its digital signature will be encoded in a separate file S102ed2.SIGN located in the same folder as the source file.

Other files included as part of service delivery will have its digital signature encoded in a .SIGN file. Example: PERMITS.TXT file will have its signature in PERMITS.SIGN

Shall we establish a possibility to support resigning of signatures?

Is it still a need to support:

* PRODUCTS.TXT as part of S63e2?
* SERIAL.ENC as part of S63e2?
* STATUS.LST as part of S63e2?
* README.TXT as part of S63e2?
* Specify a media structure as part of S63e2?

1. 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” [↑](#footnote-ref-1)