Implementation of S-63 - IHO Data Protection Scheme

Guidance Notes for OEMs and Data Servers

These notes are intended to assist both Equipment /Software manufacturers (OEMs) wishing to provide products compatible with S-63 protected ENCs and ENC data servers.

1. History

A little background to S-63 is helpful in understanding the current situation and in making decisions on your implementation of S-63 either as an ENC data server or as an OEM.

S-63 is based very largely on the Primar Security Scheme (PSS) initially used by Primar and later by both Primar Stavanger and UKHO to protect their ENC services. The original Primar service started in 1999 and a good number of ECS/ECDIS OEMs implemented the PSS within their systems between 1999-2002. During this period Primar was the sole supplier of ENCs protected by the PSS and this influenced some OEM implementations even though it was the intention that the scheme should be usable by multiple suppliers.

When a second service using the PSS was started in 2002 it was discovered that a number of OEMs had also closely tied their systems to specific attributes of the Primar ENC service. This meant that in order for other ENC services using the PSS to be compatible with existing ECDIS systems they had to use the same service attributes (e.g. CD directory structure). In addition it was found that some OEMs had implemented the scheme in a way that meant their ECS/ECDIS systems could not easily handle ENC services from more than a single ENC supplier.

It is important for OEMs and potential ENC service suppliers alike to understand this background and the potential constraints on their systems or services in the transition period before the S-63 scheme, which is administered by the IHB, is fully adopted by all parties. Information on the factors that should be taken into consideration are provided below.

2. General considerations for OEMs and Data Servers

Currently (December 2003) there are two ENC data servers using the PSS to protect their ENC services and approximately 25 OEM/s/w providers that have systems compatible with the scheme. Since the adoption of the PSS as S-63 there has been considerable interest from both potential data servers and OEMs in participating in the scheme and it is very likely that within one year there will be 5 or 6 service suppliers and 40 OEM participants. In order for S-63 to run smoothly for all participants (including end users and distributors) it is very important that new implementations of the scheme take account of lessons learnt to date

ENC service suppliers wish to ensure their services are compatible with the maximum number of OEM systems; including those already at sea. In the same way OEM providers will wish as far as possible to ensure their systems are compatible with all service suppliers and that their customers can manage ENCs from several ENC data servers concurrently.

For these reasons the following recommendations are made to all scheme participants:

3. Authentication and Verification of ENCs

3.1 Correct Sequence of authentication and verification of digital signatures.

The correct sequence of authentication is not implemented in all ECDIS/ECS systems; this has been demonstrated in the last year since a second ENC service has been available. In order for multiple data servers to be able to co-exist it is essential that scheme implementations follow the correct method of authentication (see diagram at Annex C). The next section of this document contains more information on the management of SA and Data Server keys within ECDIS systems.

There are several entities within an S-63 dataset to consider:

- The primar.crt file (see section 4.2 for further details) included in the CD.
- The SA public key installed on the ECDIS system
- The Data Server/SA certificate included as the 2nd R,S pair in every cell's digital signature.
- The Cell signature included as the 1st R,S pair in every cell digital signature.
- The Data Server public key included in every cell digital signature as p,q,g,y parameters.

The correct sequence of S-63 authentication and verification of a cell signature is as follows:

1. Authenticate the Data Server certificate from the cell signature using the SA key installed (by independent means) on the system (NOT against the primar or iho.crt file on the CD).

2. Validate Cell signature against Data Server public key and cell contents. To date, there are some ECDIS implementations that use the primar.crt file or the Data Server/SA certificate to validate the ENC signature. This situation has led to the distribution of self-signed data (i.e where the primar.crt file contains the Data Server public key and the Data Server certificate (the 2nd R,S pair in every signature) is produced by the Data Server themselves, rather than an independent SA.

Additionally it should be noted that the sequence of authentication and the tying in of the SA key on the system means all ECDIS should at least contain the following functionality:

- The ability to change the SA public key. It should be possible for all ECDIS systems to import a new SA key in the event of its change or revocation.
- The ability to understand and process digital signatures from more than one VAR data providers.

Recommended actions:

OEMs: See guidance notes on management of authentication keys and the following roadmap (3.2 below) for full S-63 compliance within this document.

Data servers: Support SA signed data when enough implementations are available as per recommendations in the roadmap.

During the transition period between using the PSS to S-63 it is suggested that you use the following procedure:

1. Insert a self-signed primar.crt X509 certificate containing your own public key[1] on each product CD
2. Use self-signed cell signatures within the signature files for each cell and update

3.2 Roadmap for correct S-63 Data authentication.

Currently, S-63 data servers are producing self-signed data (where the primar.crt file, the cell signature and the cell signature certificate entries are all produced with a single data server key). This is the best way of getting good coverage with the current implementations on the market.

OEMs should evaluate how their system deals with data authentication with particular reference to the following areas:

- How the system uses the primar.crt file contained within current data server offerings.
- How they authenticate cell signatures against the SA public key held independently on the system.
- Whether it is possible to update and hold SA public keys on their system.
- How their implementation deals with data offerings from multiple data servers.

Given that the current S-63 data servers will be producing self signed data; there are several options for OEMs to deal with this:

- Store multiple SA keys on the systems. Store different SA keys under the names of the relevant Data Server (e.g. there will be an SA key for UKHO, Primar-Stavanger, 7Cs and potentially others). Note there is no need for an ECDIS to import keys in X.509 format. The IHO key and data server keys are all available in plain text form either from the IHO website (www.iho.shom.fr > ENC > Data Protection) or on request from the data servers.
- Allow conversion to SENC if authentication fails provided a prominent warning is displayed and is accepted by the user.
- Swap public keys around when encountering keys from different data server

OEMs should refer to the S-63 standard and the DPSWG working group to make sure the authentication sequence within their ECDIS implementation is correct (See diagram in Annex C).

When all systems allow the change of SA key and follow the correct authentication/verification path then the Data Servers will move to producing signature files that contain only the cell signature (created with the data server private key) and their data server certificate (the Data server public key along with a version signed by the IHB, as Scheme Administrator). This will mean the end user systems will gradually move to only having a single SA public key (the IHO key). Data servers will move to eliminating the inclusion of SA public keys on the data CD (the S-63 iho.crt file). Data Servers will continue to provide a .crt file on the CDs in the short term to cater for systems in the field pending system upgrades.

Further questions on current implementation should be addressed in the first instance to the Open ECDIS forum (www.openecdis.org) which can provide advice, guidance and assistance with the IHO S-63 data encryption standard and the roadmap to full compliance.

[1] Contact DPSWG working group (www.iho.shom.fr > Committees > CHRIS/DPSWG) for information on how to produce an X509 self-signed public key using publicly available tools.

4. ENC Media Content and Format

4.1 Content of the serial.enc file

Serial.enc – is a file that is included in the top level directory of the product CD. The format is included in Annex A. This is included to allow OEMs to identify the source of media being loaded into the ECS/ECDIS and it is recommended that a supplier identifier is included in this file. The two character ID should be registered with the Scheme Administrator to avoid any duplication of IDs.

Recommended actions:

OEMs: Read the identifier and use this to identify media and associated files supplied. This can be used to link to cell permits – see 5.1 below

Data servers: Register identifiers with IHO and include on CDs

4.2 Content of primar.crt file

Currently data servers include another file "primar.crt" on their CDs in the root directory. This is because some ECDIS implementations use this file as the source of the SA public key against which the cell signatures are authenticated (this file led to the specification of the optional iho.crt in the S-63 specification.). Currently the content of the file is the self-signed data server public key encoded as an X509 certificate.

Recommended Actions:

OEMs: Refer to section 3.2 in this document for a more detailed set of recommendations for dealing with the primar.crt file and ensuring the authentication sequence on the ECDIS implementation is correct.

Data Servers: Data Servers should include a primar.crt file on their CDs containing the data server public key as a self-signed X509 root certificate. This will allow compatibility with those ECDIS systems relying on the existence of this file. Data Servers should also make themselves aware of the roadmap for the primar.crt/iho.crt files and the planned phasing out of the inclusion of these files and their content.

4.3 Catalogue file comment fields *(also defined in S-63 Section 5.1):*

Data servers need to include this additional information to satisfy some OEM requirements. The COMT field in the CATALOG.031 file needs to include the following text:
"VERSION=1.0,EDTN=XX,UPDN=YY,UADT=<upd date>,ISDT=<iss date>"

where EDTN=Cell edition number, UPDN=Cell update number and UADT/ISDT represent the last Update and Issue dates of the cell respectively.

Recommended actions:

OEMs: Only use these fields if you have to make this knowledge available to data servers.

Data servers: Be aware that some OEMs need this information to be present in the catalogue file comment entries.

4.4 Catalog entries for signature files.

It is stated explicitly within the S-63 documentation that the signature files are located in the same directory as the ENC cells. It is the case that some ECDIS rely on the existence of the signature catalogue entries in order to locate the correct files.

Recommended actions:

OEMs: The CATAOLG 031 file should be used to locate all ENC files including the signature files on the CD.

Data servers: Include catalogue entries for all signature files.

4.5 CD directory structure Content / Format

S57 does not define a fixed directory structure to be used with ENC data on hard media. Instead it requires that all pathnames for files in the exchange set are included within a CATOLOG 031 file located in the root directory of the media.

The original Primar service used a detailed directory structure (described below) and at the time of writing some OEMs look for this specific structure rather than read the catalogue file. Although not mandated by either S57 or S-63 it is known that some ECDIS implementations can not deal with arbitrary cell pathnames and for compatibility with these implementations, ENC cells should, for a transitional period stick to the convention of

```
Cell pathname =
  ENC_ROOT\<country code>\<cell basename>\<edition number>\<update
number>\<cell file>
```

e.g for the cell GB54004B.001 (edition 2) the path on the CD (and reflected within the catalogue file) should be:

ENC_ROOT\GB\GB54004B\2\1\GB54004B.001

note that cell signatures are always included in the same directory as the cell as per the S-63 standard.

Recommended actions:

OEMs: Use the CATOLOG.031 file to locate files rather than hardwiring structures into software.

Data servers: You should be aware that if you use a different structure your service might not be usable by a proportion of ECS/ECDIS users.

4.6 Product listings

The original Primar service included a product listing provided on the Primar service CD. This listing is named products.txt (and is included in a subdirectory of the CD root directory called INFO) and contains information (such as edition number) about every cell in the service along with a timestamp of the file creation date. Many OEMs use this listing to decide which cells within the exchange set the ECDIS needs to decrypt (the file contains valuable metadata for the cells within the exchange set and hence is a useful source of edition/update information on the system).

Because initially there was a single service many OEM implementations simply overwrite product.txt files that have a later date. This leads to a problem when a user subscribes to more than one service as there is no time-ordering of different services' offerings. Details of the products.txt format are included at Annex A.

Recommended actions:

OEMs: For new implementations of the scheme it is recommended to not use the products.txt file and that cell data should be extracted from the exchange set CATALOG.031 file (and its COMT field as described previously). Where the products.txt files are used, implementations should ensure that data is not lost when updated versions of the file are loaded onto the system. In conjunction with the serial.enc file it would be possible to keep and manage these service specific listings separately. Do not rely on time ordering to determine data consistency between different data servers' services.

Data servers: Include a product listing as formatted in Annex A. Data Servers should consider whether it is necessary for their service to concatenate products.txt files between themselves. This is in order to support those OEMs still implementing an overwrite policy. Data Servers should also ensure they are implementing the CATALOG.031 COMT field as described in S-63 section 5.1 and referred to in section 4.3 of this document to make sure ENC cell information is available to ECDIS without the need to decrypt every cell first.

5. Cell keys and Permits

5.1 Cell Permits

Certain ECDIS implementations overwrite permits from multiple Data Servers.
Data servers currently issue two files, permit.pmt and permit.txt ; these contain duplicate information, the latter containing the cell edition number.

Recommended actions:

OEMs: Don't overwrite permits from different data servers on systems. Ensure that ECDIS systems are able to merge permits from multiple data servers without losing permit information. New implementations use only permit.txt files.

Data servers: Provide both permit files (permit.pmt and permit.txt) to customers.

5.2 Cell keys

Although the standard makes provision for dual encryption keys within permits and this feature has been implemented by most manufacturers, it should be noted that the association of the change of encryption key with cell new editions has not been implemented by all data servers and some data servers choose not to update the cell encryption keys every time a new edition is issued.

Whilst there is no intention to withdraw the dual encryption key feature from the standard, all parties should be aware that data server implemented dual encryption keys may, in fact, just be repeated single keys within the permits.

Recommended actions:

OEMs: Section 8.2.6 of the S-63 standard refers to an environment where new editions are infrequent. Because of the high frequency of new editions it is recommended that the procedure in section 8.2.6 is not implemented. Instead of this OEMs should use the simpler method defined in section 5.2.3 of the S-63 standard.

Data Servers: Data Servers should be aware of the common practice of not changing the encryption keys every time a new edition is released.
.

Annex A

ENC Service Provider Product Listing

This annex defines the format of the Product Listing provided by many data servers as a file called “products.txt” to give an overview of the ENCs available in their services.

The information contained in the Product List can be used to e.g.:

- determine if the users ENC chart portfolio is up to date
- determine the ENC coverage required is included in that service

The product list will be provided in simple text format that that can be imported and used within ECDIS systems. The product list will normally be updated on a regular basis in line with the service providers updating regime. The product list will normally be included on the service media (eg weekly update CD). The Product List will always include information about <u>all</u> the ENC cells and updates available in the service.

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 shown in

Figure 1:

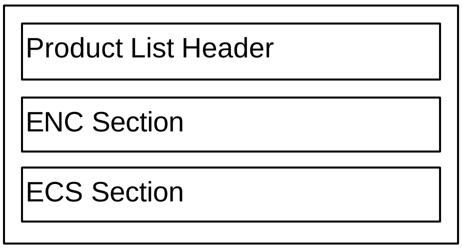


Figure 1: Product List structure

The various sections contain information about:

- Product List Header: Contains general information about the nature of the Product List, e.g. the time of creation, version number.
- ENC Section: Contains the current status of all ENC cells/updates provided by the data server.
- ECS Section: Contains information about other digital chart information provided by the data server. NB – This element is not currently used by data servers and may not be fully supported by OEMs.

Product List Header

The Product List will always start with <u>one</u> Header Section. The Header Section will consist of several records. Each record will start at a new line and be terminated with a CR/LF (carriage return and line feed).

The Header will consist of the information fields defined in Table 1. 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 date and time will be separated by the <space> character. The date will be provided as 19990319 and the time as 20:31 using the 24 hour clock.

Product List version	:VERSION	Integer in range 1 to 99. Will always start at 1 and be incremented by 1 for each new version of the Product List specification. Default is “1”.
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.

Table 1: Header Section

Example Product List Header
Below is an encoding example for the Product List Header:

```
:DATE 19990319 20:31
:VERSION 1
:CONTENT FULL
```

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/updates supported by the Data Server.

This section will start with one *ENC Section Identifier* record as defined in Table 2.

Field	Fieldname	Value
ENC Section Identifier	:ENC	Not applicable

Table 2: ENC Section Identifier

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 Table 3.

Field	Value
Product Name	Name of product as defined in S57e3 DSID-DSNM subfield. The file extension will always be 000. Example: PM211111.000
Product Issue Date	YYYYMMDD Date on which the base ENC cell was issued. Example: 19990319
Product Edition	Integer Edition number of base ENC cell. Identical to content of S57e3 DSID-EDTN. In the case where there is issued a cancellation of the cell, the Product Edition will be set to 0. This allows the ECDIS system to quickly identify cells that have been cancelled.
Issue Date Latest Update	YYYYMMDD Date on which the latest update for the ENC cell edition was issued. This field is used, when there is an update or a re-issue of the cell.
Latest Update Number	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.

File Size	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.
Cell limit Southernmost latitude	Degrees of arc, south is negative. Southernmost latitude of data coverage in the ENC product. Example: 59.5
Cell limit Westernmost longitude	Degrees of arc, west is negative. Westernmost longitude of data coverage in the ENC product.
Cell limit Northernmost latitude	Degrees of arc, south is negative. Northernmost latitude of data coverage in the ENC product.
Cell limit Easternmost longitude	Degrees of arc, west is negative. Easternmost longitude of data coverage in the ENC product.
10 Data Coverage Coordinates	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.
Compression	Integer in range 0 to 99 “0” No compression An integer number > 0 denotes compression is used and also denotes the version number of the compression specification used for the ENC product.
Encryption	Integer in range 0 to 99 “0” No encryption An integer number > 0 denotes encryption is used and also denotes the version number of the security scheme specification used for the ENC product.
Base cell update number	Update number for last re-issue. If an edition without any re-issues then this field is blank.
Last update number for previous edition	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.
Reserve	Future use
Comments	Future use

Table 3: ENC Record Definition

Note that if the field does not contain a value, e.g. no updates have been issued for the ENC cell, the field value will be empty.

Support for New Cell Editions

The data server will issue new editions of cells at regular intervals due to e.g. new survey information or extensive changes of the ENC. The Data Server will continue to provide support for the previous edition of an ENC cell for a limited time until all the users have received the new edition.

The Product List can, whenever a new ENC cell edition is issued contain 2 records defining the cell status, e.g. a record for the current and previous edition of the cell. The records will always be grouped together in the Product List with the latest edition of the ENC cell defined first.

Example ENC Section

Below is an encoding example for the Product List ENC Section:

```
:ENC
PM210000.000,19990101,1,19990131,2,1234,59.0,5.0,60.0,6.0,,,,,,,,,,,,,,,,,,,1,1,,
PM220000.000,19990101,1,,,950,59.0,7.0,61.0,8.0,59.0,7.0,61.0,8.0,,,,,,,,,,,,,,,,,,,1,1,,
PM222222.000,19990301,2,19990310,1,950,55.0,-1.0,57.0,1.0,55.0,-1.0,57.0,1.0,,,,,,,,,,,,,,,,,,,1,1,,
PM222222.000,19990101,1,19990228,3,955,55.0,-1.0,57.0,1.0,55.0,-1.0,57.0,1.0,,,,,,,,,,,,,,,,,,,1,1,,
```

Product List ECS Section

The Data Server will also issue other types of digital chart products. This will include backdrop charts that can be used to e.g. display chart coverage. Information about these products will also be made available in the Product List. Note however that all the products defined in this section will not be authorised for navigation.

This content of this section is identical to the ENC Section defined in 0. The only difference is the *ECS Section Identifier* which will be "`:ECS`."

Note that there will be no duplication of entries in this section. It is not expected that there will be issued any update messages for these type products. A backdrop chart can however be issued in a new edition including more features.

Example ECS Section

Below is an encoding example for the Product List ECS Section:

```
:ECS
PM1WORLD.000,19990101,1,,,3000,-90,-180.0,90.0,180.0,-90.0,-180.0,90.0,180.0,,,,,,,,,,,,,,,,,,,0,0,,
```

Product List Example

Below is a complete example of a Product List which utilises all the features defined in chapter 0.

```
:DATE 19990319 20:31
:VERSION 1
:CONTENT FULL
:ENC
PM210000.000,19990101,1,19990131,2,1234,59.0,5.0,60.0,6.0,59.0,5.0,60.0,6.0,,,,,,,,,,,,,,,,,,,1,1,,
PM220000.000,19990101,1,,,950,59.0,7.0,61.0,8.0,59.0,7.0,61.0,8.0,,,,,,,,,,,,,,,,,,,1,1,,
PM222222.000,19990301,2,19990310,1,950,55.0,-1.0,57.0,1.0,55.0,-1.0,57.0,1.0,,,,,,,,,,,,,,,,,,,1,1,,
PM222222.000,19990101,1,19990228,3,955,55.0,-1.0,57.0,1.0,55.0,-1.0,57.0,1.0,,,,,,,,,,,,,,,,,,,1,1,,
:ECS
PM1WORLD.000,19990101,1,,,3000,-90,-180.0,90.0,180.0,-90.0,-180.0,90.0,180.0,,,,,,,,,,,,,,,,,,,0,0,,
```

Annex B

Detailed specification of serial.enc file:

File Format

Field ID	Domain	Bytes	Range	Note
Organisation of origin	char	2	AA – ZZ	1
CD Number	char	10	Any ASCII characters	2
Date of publication	date	8		3
Format	char	10		4
Format version	dec		01.00 – 99.99	5
Copyright statement	char	0 – 500		6
End of record delimiter	hex	3	0x0B0D0A	7

General

- The SERIAL.ENC file should be stored directly under V01X01, i.e. on the same level as the ENC_ROOT and INFO directories.
- It should only be edited using an ASCII editor.

Note 1

- Organisation of origin 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.

Note 2

- The CD Number specifies the week and year that the CD is distributed, e.g., WK12-99, WK45-99, WK23-00, etc.

Note 3

- Date of publication is a regular date format, YYYYMMDD, e.g., 19990414, 19991224, 20000102, etc.

Note 4

- The CD can be issued in three different formats:

  BASE. The format should be defined as BASE, if the CD contain all EN and ER's.

  UPDATE. The format should be defined as UPDATE, if the CD contains new (compared with previous CD) ENs and ERs

Note 5

- Format version describes the version of the SERIAL.ENC file. The present version is 01.00

Note 6

- This field may be used for a Copyright Statement issued by the Data Server

Note 7

- The end of the record delimiter consists of hexadecimal characters, and cannot be edited in 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.

Example of SERIAL.ENC file

```
PRWK15-99   19990414UPDATE    01.000x0B0D0A
```

Must be converted to
hexadecimal

Annex C

Data Authentication and Integrity Checking within the S-63 Scheme

The digital signature technique used in the Primar and S-63 schemes uses an ‘asymmetric’ encryption methodology. This methodology relies on the fact that it is possible for an organisation to ‘sign’ a datafile with one key (a secret ‘private key’) and for another organisation to be able to ‘authenticate’ the signature with a different key (a widely known ‘public key’). The public and private keys are linked and are called a ‘key pair’.

The scheme breaks down into two elements:

1) Scheme Administrator (SA) provides the means for the ECDIS to check that the ENCs are from a bone fide supplier (eg RENC or authorised VAR).
2) Data Server (eg RENC or VAR) provides means for ECDIS to check the integrity of the ENCs.

These processes are shown in the diagrams below; they are detailed below:

1) SA Verification: The ECDIS needs to be able to verify that the ENCs are from a bone fide source (RENC or VAR). It does this by ensuring that the data server’s public key provided in the certificate file is valid.

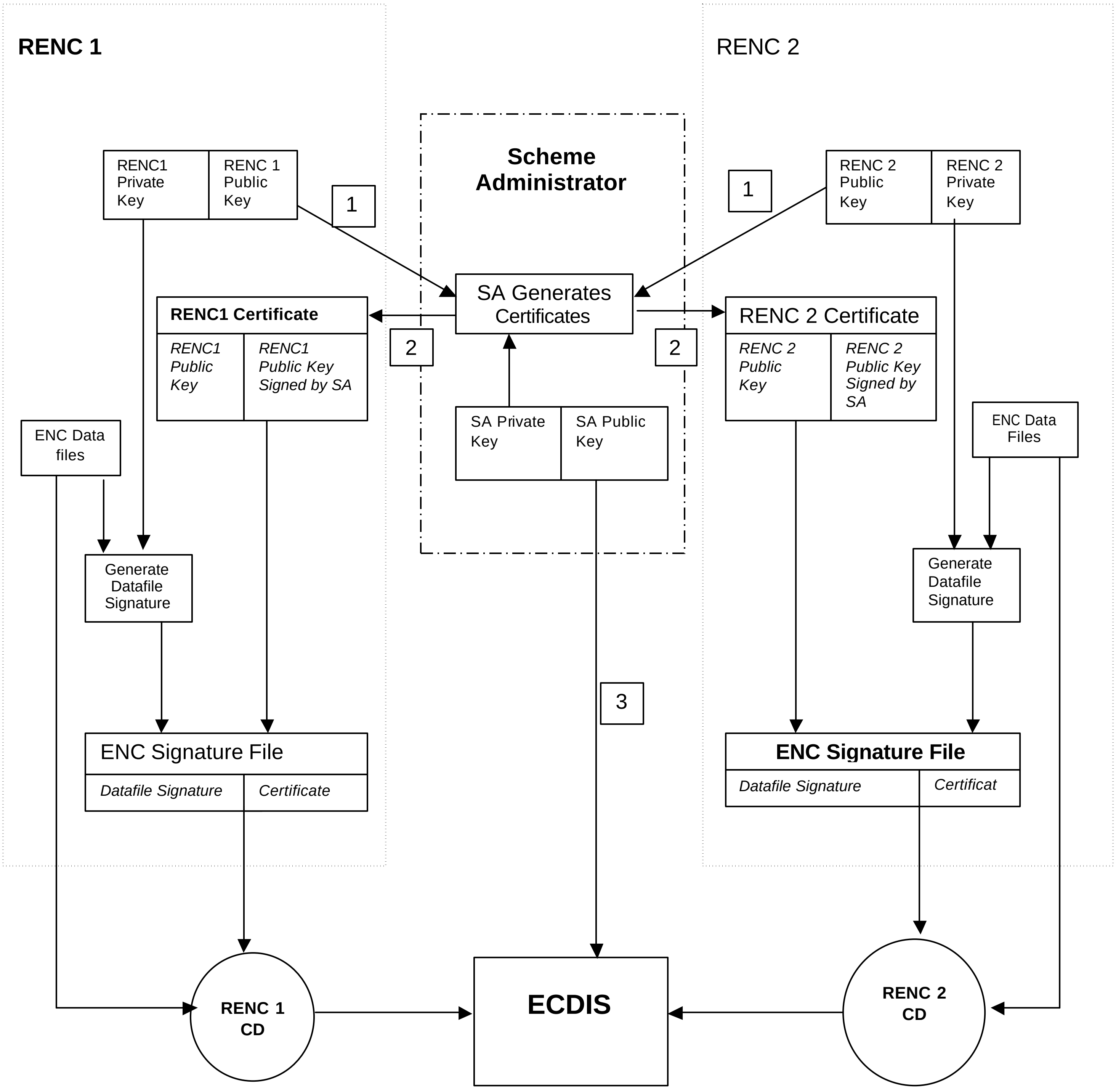
The SA provides certificates for each data server in the scheme; each certificate is unique, the SA only has to do this task once for each data server. To obtain a certificate, data servers must provide the SA with their own public key (as a self signed certificate); the SA (having also generated a key pair) uses his private key to sign the data server public key. The certificate produced contains the supplier’s public key and the signed version (created using the SA private key) of that public key. As stated above, the certificate is included within the signature file associated with all ENC cells and updates.

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

2) Data Integrity: Having authenticated the source of the CD the ECDIS then checks data integrity by inspecting the signature file provided for each ENC by the data server.

The data server creates a signature file for each cell which consists of two parts, the signature of the dataset [which is created using the private key, half of the data server key pair (in essence this is similar to a CRC checksum) and is different for each cell] and the certificate (which remains constant). The ECDIS uses the supplier’s public key that is included in the certificate to validate the datafile signature (it decodes this datafile signature and compares the result with the ENC cell). If this validation check is successful then it proves that the ENC has not been corrupted in any way.

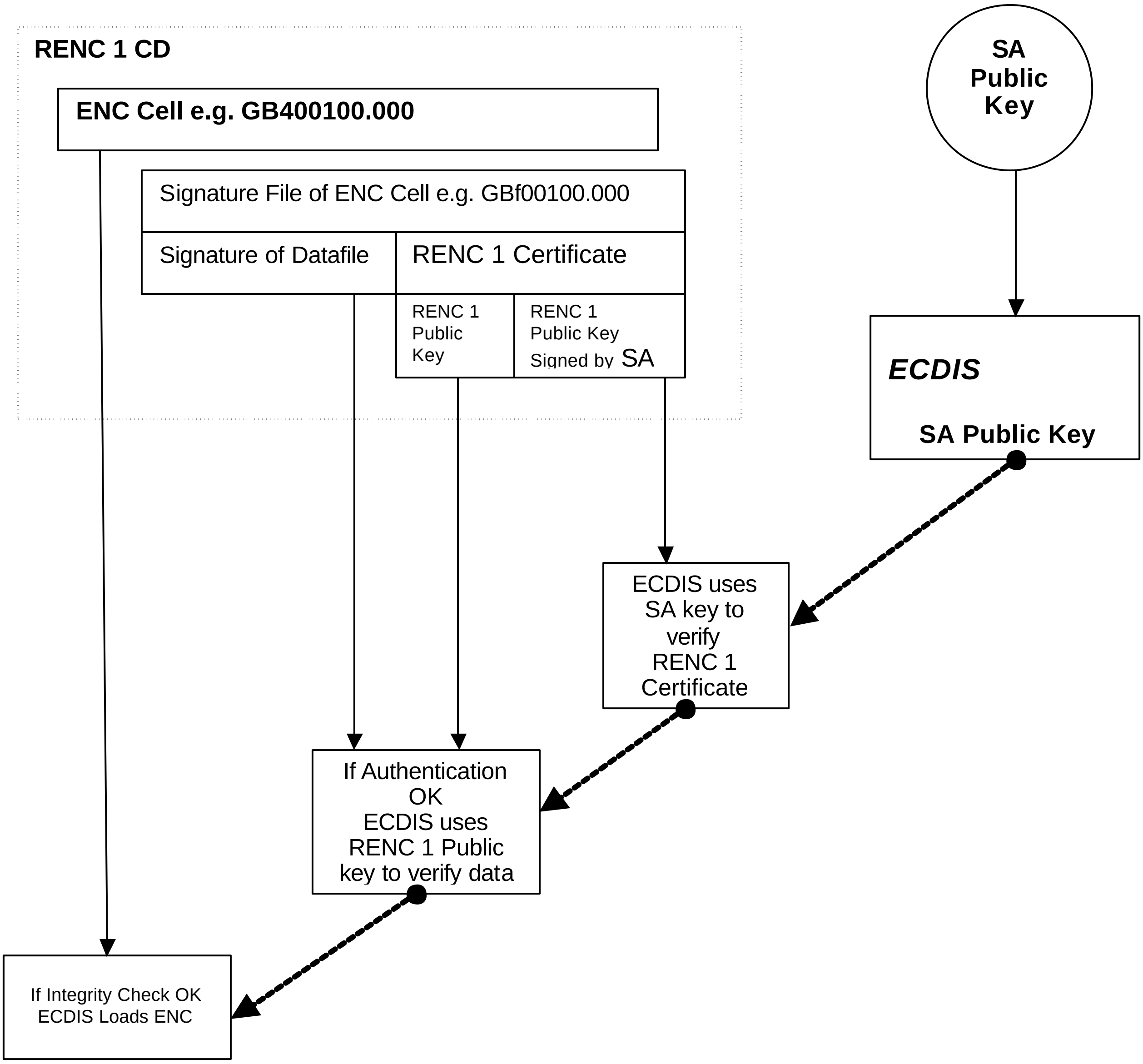
AnnexC (Contd)



Notes

1 Sent once when joining the scheme.
2 Returned once only when RENC joins the scheme.
3 Widely distributed and built into ECDIS.
4 SA keys must be different from RENC keys to provide intended security.

Annex C (Contd)


RENC 1 CD
ENC Cell e.g. GB400100.000
Signature File of ENC Cell e.g. GBf00100.000
Signature of Datafile
RENC 1 Certificate
RENC 1 Public Key
RENC 1 Public Key Signed by SA
SA Public Key
ECDIS
SA Public Key
ECDIS uses SA key to verify RENC 1 Certificate
If Authentication OK ECDIS uses RENC 1 Public key to verify data
If Integrity Check OK ECDIS Loads ENC

If an ECDIS is using the above method, and if the SA key is different from the RENC keys, then it is able to authenticate and verify the ENCs from RENC 2 (or any other RENC in the scheme) using the same SA public key.

1. Authentication:
ECDIS uses the SA public key (as has been stored within it) to check the certificate part of the signature file to confirm that the supplier's public key in the certificate is valid (ie the supplier is a bone fide member of the scheme).

2. Integrity Check:
ECDIS uses data server's public key from the certificate to check the signature of the datafile.

Annex D

S-63 Questionnaire:

For each of the areas raised within this document the IHB, as Scheme Administrator (SA), would like specific feedback from both OEMs and Data Servers regarding any issues within their implementation of the S-63 standard. To this end a questionnaire has been devised.

Please answer the questions set out below; feel free to add any comments you may have on the S-63 in general or aspects of your implementation. The SA is keen to learn of all OEM and Data Server approaches to the issues raised within this document and will treat all information supplied in confidence.

The questions should be answered having used the S-63 test data which is available as part of the S-63 specification on the IHO website (www.iho.shom.fr > ENC > Data Protection).

Questions:

Sections 3.1 and 3.2
a) Does your system store an SA public key?

b) If so just one or more than one?

c) Does it require the SA key in .PUB (ASCII text) or x509 format?

d) Is the end user able to swap SA public key(s)?

e) If yes – how does the user do this – from hard coded source (eg A drive) or is the user able to locate the file?

f) Does your system follow the authentication/verification route shown in Annex C?

g) If not, does it work if a .CRT file is present on the media. Does this .CRT file have to be named "primar.crt"?

h) Do you consider the options presented in the "Roadmap" (section 3.2) are reasonable, for correct authentication of digital signatures.

Section 4.1
a) Do you use the serial.enc file? – do you think it is a good idea to use this field to identify the service supplier?

Section 4.2
a) Does your system use the primar.crt file as the source of the SA public key used for authentication?

Section 4.3
a) Do you use the comments field in the catalog 031 file for determining what to decrypt?

Section 4.4
a) Does your system require entries for the signature files within the CATALOG.031 file?

Section 4.5
a) Does your system determine CD structure from Catalog 031 file or is this hard coded?

Section 4.6
a) Do you use the products.txt listing?

b) If so do you overwrite newer versions or merge?

Section 5.1
a) Do you use both the permit.pmt and permit.txt files? – do you use the NE number in the .txt file?

b) Does your system overwrite or merge permits?

c) Do you think that we should tag the permits with a server supplier identifier (as used in the serial.enc)?

Section 5.2
a) Does your system use both of the cell keys in a permit?

b) What means do you use to determine which cell key is to be used?

General
a) Is 'PRIMAR' hard coded into the user interface (can cause confusion for users loading ENCs from other suppliers)?

b) Very approximately how many systems are deployed that you consider would not currently be compatible with S-63?; or with multiple ENC data servers?

c) How long would it take to upgrade these to compatible systems? – what % would be left as non compatible long term?